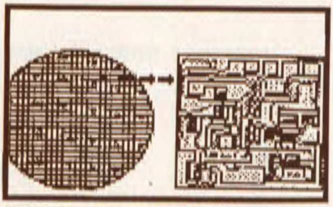
2600



The Hacker Quarterly

VOLUME ELEVEN, NUMBER THREE

$4 ($5.50 in Canada)

AUTUMN 1994

STAFF

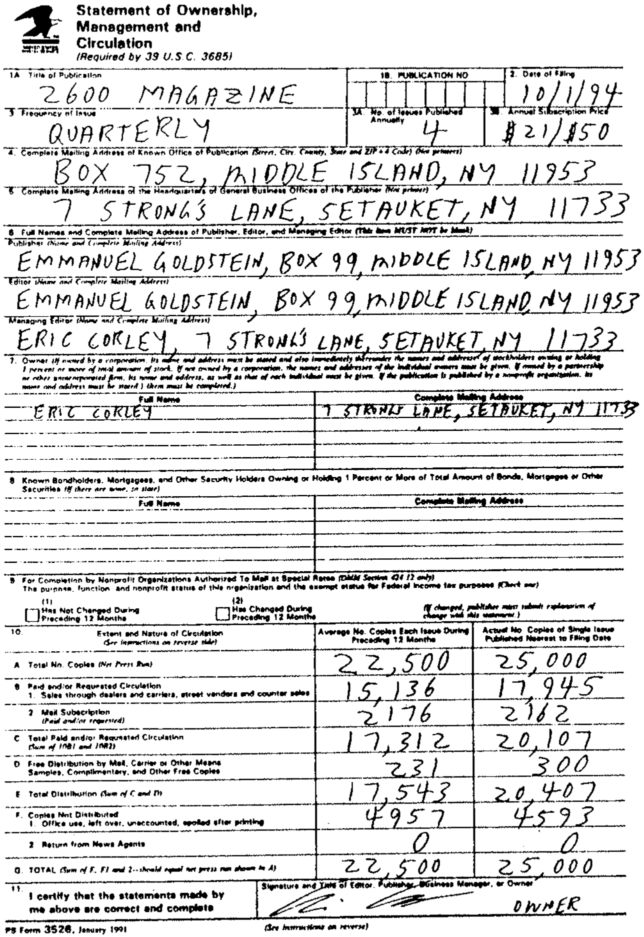
Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Holly Kaufman Spruch

"A pretty face can hide an evil mind.
Be careful what you say -
you'll give yourself away."
Johnny Rivers, "Secret Agent Man"

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the victims of TV.
Technical Expertise: Rop Gonggrijp, Joe630, Phiber Optik.
Shout Outs: New York 1994.



Statement of Ownership, Management and Circulation
(Required by 39 U.S.C. 3685)

1A. Title of Publication: 2600 MAGAZINE
1B. PUBLICATION NO: □□□□□□□□
2. Date of Filing: 10/1/94
3. Frequency of Issue: QUARTERLY
3A. No. of Issues Published Annually: 4
3B. Annual Subscription Price: $21/$50
4. Complete Mailing Address of Known Office of Publication *(Street, City, County, State and ZIP+4 Code) (Not printers)*
BOX 752, MIDDLE ISLAND, NY 11953
5. Complete Mailing Address of the Headquarters of General Business Offices of the Publisher *(Not printer)*
7 STRONG'S LANE, SETAUKET, NY 11733
6. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor *(This item MUST NOT be blank)*
Publisher *(Name and Complete Mailing Address)*
EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Editor *(Name and Complete Mailing Address)*
EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Managing Editor *(Name and Complete Mailing Address)*
ERIC CORLEY, 7 STRONG'S LANE, SETAUKET, NY 11733
7. Owner *(If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Item must be completed.)*

Full Name	Complete Mailing Address
ERIC CORLEY	7 STRONG'S LANE, SETAUKET, NY 11733

8. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities *(If there are none, so state)*

Full Name	Complete Mailing Address

9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates *(DMM Section 424.12 only)*
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes *(Check one)*
(1) □ Has Not Changed During Preceding 12 Months
(2) □ Has Changed During Preceding 12 Months
(If changed, publisher must submit explanation of change with this statement.)

10. Extent and Nature of Circulation *(See instructions on reverse side)*	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
A. Total No. Copies *(Net Press Run)*	22,500	25,000
B. Paid and/or Requested Circulation 1. Sales through dealers and carriers, street vendors and counter sales	15,136	17,945
2. Mail Subscription *(Paid and/or requested)*	2176	2162
C. Total Paid and/or Requested Circulation *(Sum of 10B1 and 10B2)*	17,312	20,107
D. Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies	231	300
E. Total Distribution *(Sum of C and D)*	17,543	20,407
F. Copies Not Distributed 1. Office use, left over, unaccounted, spoiled after printing	4957	4593
2. Return from News Agents	0	0
G. TOTAL *(Sum of E, F1 and 2—should equal net press run shown in A)*	22,500	25,000

11. I certify that the statements made by me above are correct and complete
Signature and Title of Editor, Publisher, Business Manager, or Owner
OWNER

PS Form 3526, January 1991 *(See instructions on reverse)*

internal contents

SOME THINGS WILL NEVER CHANGE

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.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1993 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.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

Opening Doors

You've probably noticed that this issue is coming to you a bit later than it should. We have one thing to say: blame HOPE.

Never before in this country has such an event occurred. And never again will we be able to say that. Things are different now and it's up to all of us to hold onto the ground that we've gained.

By all estimates, somewhere between 1,000 and 1,500 people descended upon the Hotel Pennsylvania in New York City on August 13th and 14th. At some point on the second day we just lost count.

In stark contrast to the commercialized "Son of Woodstock" taking place simultaneously to the north, Hackers On Planet Earth was a grass roots, down to earth labor of love and obsession. People came from all around the world with their computers, radios, music, toys, and expertise. For the first time, hackers in America were able to meet with the Chaos Computer Club of Germany. Other groups from Holland, England, Italy, Canada, Australia, Russia, Israel, and Argentina were also on hand, not to mention the diversity of all the attendees from the United States. Whether they journeyed cross country in a van, crosstown in a subway, or over the ocean in a plane, HOPE attendees came to learn and to share information about hacking and about technology.

It was really everything we could have hoped for. When people from the United States attended Holland's Galactic Hacker Party in 1989 and Hacking at the End of the Universe in 1993, they saw a spirit and an energy that had been largely quelled in this country. By organizing something as large as HOPE, we wanted to try and bring that spirit over here, or rather, nurture the spirit that has always been present. At long last, through the help of those present, we succeeded in doing this.

And for once, the press had something to say about hackers when we weren't being raided, charged, or sentenced to prison. Here we were holding seminars, reviewing our history, playing with new technology, and showing the public how to hook into the Internet. Of course, media stupidity is hard to defeat - one New York Times piece made it appear that our only purpose in gathering was to make free phone calls. But such blindness seemed to be the exception rather than the rule.

All of the worries about hackers roaming loose in such an environment proved unfounded. The massive crowd was extremely well behaved by any standard. We found this especially true in the face of our botched registration system, which forced people to wait on line for long periods of time in order to get a photo ID. It was a little taste of Eastern Europe and the patience of the participants was unbelievable. (Eventually we scrapped the system and just gave everyone handwritten numbers.) Our thinking was that having a picture that matched an existing face would be less intrusive than having a name printed on a badge. While that still may be so, the technology just wasn't with us. Maybe next time. (By the way, we had always planned on wiping the pictures out of the computer after HOPE. Through another misfortune, we managed to wipe them before the conference ended.) Attendees will also be pleased to know that all of the registration forms were intentionally destroyed - if this conference ever becomes the focus of some absurd investigation of "hacker conspiracy" in the future, gathering evidence on those present will be tricky at best.

Despite a flaky net connection, mostly because of an uncooperative hotel phone system, the internal network managed to keep going. And, no matter what the topic (social engineering, cellular phones, boxing, lockpicking, hackers from overseas), the auditorium always seemed to be filled with an enthusiastic audience. We even managed to get Phiber Optik on the phone live from prison to speak to the crowd. That in itself added a great deal of magic to the event.

We couldn't have come close to making this work without the dedicated help of many dozens of people. We toyed with the idea of trying to list them all by name. Then we realized that inevitably someone would be left out which might cause bad feelings. Or perhaps somebody who carried a small box from one room to another would be listed right next to someone who got no sleep for three days trying to keep the net up. This might cause resentment. Or maybe a person would be listed who wanted more than anything to remain anonymous. This could result in fear and paranoia. Rather than risk all of that negativity, we decided to keep it on a personal level. Suffice to say, we know who helped change the future of hacking this summer. And we won't forget.

For those of you who weren't able to make it, we will have video transcripts available in the future. We'll announce the details in a future issue.

We have been deluged with requests from people asking if they can help with HOPE 2 next summer. We need to set the record straight. There isn't going to be another one of these next summer. HOPE was a special event and such events don't take place on a regular schedule. This is not to say that there won't be other special events taking place in other parts of the world. But the next HOPE isn't going to happen for a while. One of the main reasons for this is the fact that such an endeavor is very draining. We have bill collectors, subscribers, and close personal friends who are very angry with us for having neglected them. If you're one of those, we apologize for our lapses. For now, our priority will be to continue the work of *2600*. And when it's time for another HOPE-like event, we know we can count on our readers to make it happen again.

monitoring u.s. mail

by Paranoia

For readers, including this one, reluctant to subscribe because they fear being added to some sort of spook hit list, here is some more fuel for the fire.

I'm sure readers have noticed the barcodes sprayed on the lower right front corner of all letters delivered by the United States Postal Service. These 5, 9, or 11 digit (plus check digit) codes are derived from the destination ZIP or ZIP+4, and the two digit Delivery Point. The goal of the system is to imprint each mail piece with a number uniquely identifying the destination mailbox. Ideally, the mail can be machine processed up to the point where a bundle is given to the letter carrier in the exact order that he or she walks the route. These codes are pre-printed by bulk mailers (to earn discounts by saving the Postal Service some work) and by Postal Service OCR's (Optical Character Readers). The OCR's are very high tech. They are constantly being improved and at this point can read virtually anything that is machine printed and most hand printed addresses at about ten pieces per second.

Nearly all possible destination addresses have been put in "standard form" and entered in a master database. The OCR must reformat each address into this standard form and look up the barcode. Naturally, variations in address preparation are a nag. The whole process is daunting. Math majors may want to figure out how many combinations and permutations of "201-C South Second Street" might exist (hints: "S", "S.", "s", "2nd", "2 nd", "ST", "ST.", "St.", etc., plus misspellings and "-C" may also be written as "APT. C").

With a system of discounts, large mailers are encouraged to use the automated CASS (Coding Accuracy Support System) to improve the accuracy of mail preparation and facilitate automated handling. Discounts are earned if 85 percent or more of the mail pieces have been checked and approved by a certified program working from a certified master file of addresses. Everything must be recertified regularly. Also available is NCOA processing (National Change of Address), which tracks all moves registered with the Postal Service. When the system works, it's dynamite (in spite of its bad rap, the Postal Service tries very hard and, in my opinion, succeeds most of the time). In a recent mailing, we submitted our list for NCOA processing at the end of a month and received data on moves occurring during that month (posting of moves can take up to six weeks). The completed First Class mail pieces were submitted to a bulk mail center half a state away at 5:00 pm on a Friday and most were delivered in the next morning's mail. We saved time, money, and trees by not mailing to the addresses we knew were bad - in advance.

But what happens when the automated system fails and the OCR can't decipher the address? Obviously, a person must get involved with these strays. In a new, still experimental, program an image of these stray addresses is sent electronically to an off-site processing center, coded, returned to the Bar Code Printer and reunited with the letter. You can tell when a letter went through the new process because it will bear an iridescent orange barcode on the back of the piece.

Now the spooky part. Let's assume that the spooks are gathering data on you. It doesn't take much imagination to assume that they would be interested in your mail. Even if they didn't actually read the contents of each piece (this would require a court order if they wanted to play by the rules), they could make a quiet deal with your letter carrier or show up at your local Post Office each morning and photograph each piece. Given the processing power now available at each OCR, it would not burden the system to include a list of thousands (or tens or hundreds of thousands) of destination addresses to watch. Think of the power! A terminal near the spook on a case (mobile terminals are not out of the question) beeps and displays an image of the letter that entered the mailstream at OCR #12-3-A just two minutes ago addressed to Dangerous John Hacker.

Now, with all that time and energy saved, the spooks can expand their watch. Technology to the rescue - I'm feeling safer already!

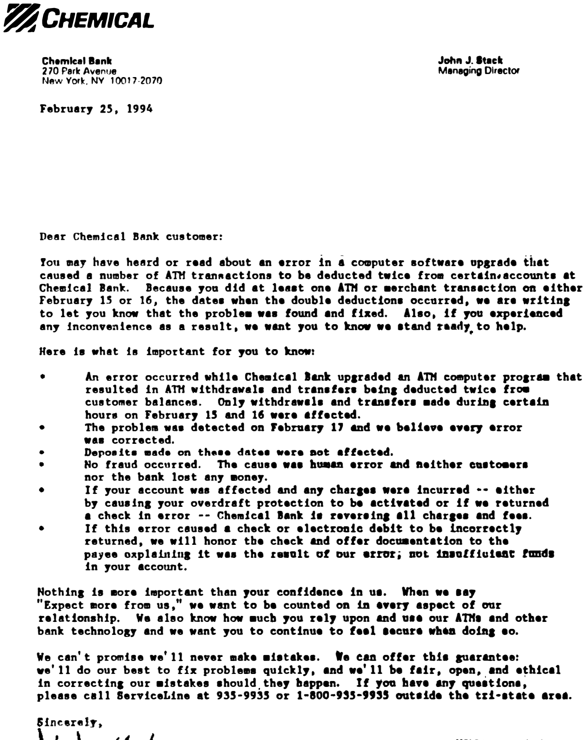
For The Curious

The POSTNET barcodes are made up of long and short bars at 22 per inch. Long bars (nominally 0.125") are about twice as long as short (0.050") bars. Nominal bar width is 0.020 inches. Each complete barcode is framed with one long bar at each end. Individual digits are made up from five bars, two long and three short. Digit values are:

```
1=00011
2=00101
3=00110
4=01001
5=01010
6=01100
7=10001
8=10010
9=10100
0=11000
```

"1" represents a long bar. Another way to view the codes is to assign weights 7, 4, 2, 1, 0 from left to right and define eleven as digit "0". The rightmost code is the check digit, assigned such that the sum of all digits, including the check digit, is a multiple of ten. Valid codes will have a total of 6, 10, or 13 digits. A 9-digit ZIP+4 plus the two digit Delivery Point will total 62 bars.

CORPORATE FOULUPS



CHEMICAL

Chemical Bank
270 Park Avenue
New York, NY 10017-2070

John J. Stack
Managing Director

February 25, 1994

Dear Chemical Bank customer:

You may have heard or read about an error in a computer software upgrade that caused a number of ATM transactions to be deducted twice from certain accounts at Chemical Bank. Because you did at least one ATM or merchant transaction on either February 15 or 16, the dates when the double deductions occurred, we are writing to let you know that the problem was found and fixed. Also, if you experienced any inconvenience as a result, we want you to know we stand ready to help.

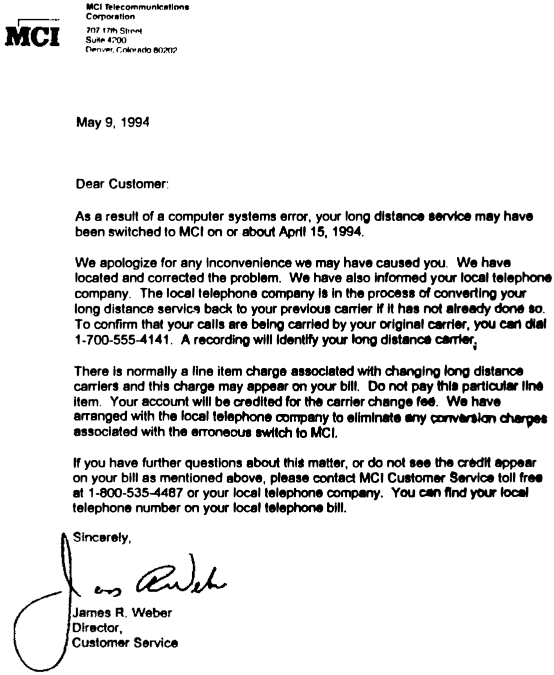
Here is what is important for you to know:

- An error occurred while Chemical Bank upgraded an ATM computer program that resulted in ATM withdrawals and transfers being deducted twice from customer balances. Only withdrawals and transfers made during certain hours on February 15 and 16 were affected.
- The problem was detected on February 17 and we believe every error was corrected.
- Deposits made on these dates were not affected.
- No fraud occurred. The cause was human error and neither customers nor the bank lost any money.
- If your account was affected and any charges were incurred -- either by causing your overdraft protection to be activated or if we returned a check in error -- Chemical Bank is reversing all charges and fees.
- If this error caused a check or electronic debit to be incorrectly returned, we will honor the check and offer documentation to the payee explaining it was the result of our error; not insufficient funds in your account.

Nothing is more important than your confidence in us. When we say "Expect more from us," we want to be counted on in every aspect of our relationship. We also know how much you rely upon and use our ATMs and other bank technology and we want you to continue to feel secure when doing so.

We can't promise we'll never make mistakes. We can offer this guarantee: we'll do our best to fix problems quickly, and we'll be fair, open, and ethical in correcting our mistakes should they happen. If you have any questions, please call ServiceLine at 935-9935 or 1-800-935-9935 outside the tri-state area.

Sincerely,



MCI

MCI Telecommunications Corporation
707 17th Street
Suite 4200
Denver, Colorado 80202

May 9, 1994

Dear Customer:

As a result of a computer systems error, your long distance service may have been switched to MCI on or about April 15, 1994.

We apologize for any inconvenience we may have caused you. We have located and corrected the problem. We have also informed your local telephone company. The local telephone company is in the process of converting your long distance service back to your previous carrier if it has not already done so. To confirm that your calls are being carried by your original carrier, you can dial 1-700-555-4141. A recording will identify your long distance carrier.

There is normally a line item charge associated with changing long distance carriers and this charge may appear on your bill. Do not pay this particular line item. Your account will be credited for the carrier change fee. We have arranged with the local telephone company to eliminate any conversion charges associated with the erroneous switch to MCI.

If you have further questions about this matter, or do not see the credit appear on your bill as mentioned above, please contact MCI Customer Service toll free at 1-800-535-4487 or your local telephone company. You can find your local telephone number on your local telephone bill.

Sincerely,

James R. Weber
Director,
Customer Service

IRISH TELEPHONES

The Irish Telephone System

by Wonko the Inane

The current state of the phone network in Ireland is debatable at this moment in time. Indeed the current state of Telecom Eireann - the company with a full monopoly that governs the network - is also debatable as one of the political parties (Fine Gael) is attempting to abolish their monopoly status.

Terrestrial access to Europe is provided on the TE-BT1 fibre optic system and the eastbound leg of the PTAT-1 cable. Satellite services to Europe are provided via the EutelSat system, while Earth stations in the Netherlands enable Telecom Eireann to access the Far East. A PTAT-1 cable spur landing in Cork and Telecom Eireann's holdings in the TAT cable systems provide diverse independent fibre optic routes to North America. Dedicated satellite links with North America are provided via Intelsat Business Services (I.B.S.) earth stations in Galway and Limerick.

There are now very few analogue lines in use, as these have been upgraded through digital lines to fibre optic cables. Which medium is used during a phone call is dependent on the root or S.T.D. code of the receiver.

"A.T.& T. Ireland is promoting its new Global Software Defined Network (G.S.D.N.) which provides a virtual private phone network for international calls, fax, and dial-up data traffic. It gives customers 7 digit international dialing, detailed call management reports, and very significant discounts on international calls. The system is to be interconnected with Telecom Eireann's International Virtual Private Network (I.V.P.N.). Switched Data and Image (S.D.I.) networking facilitates video-conferencing with the U.S.A., data files and C.A.D. or C.A.M. applications transmission, and interconnecting LANs. Customers of this joint AT&T/Telecom Eireann service are now able to dial up high speed digital links on demand."

"Eircell G.S.M. will offer you the same freedom, all over Europe. Eircell G.S.M. is part of a new, integrated, panEuropean digital mobile telephone system. One number will find you, right across Europe. Digital transmission means a new quality of sound, the ability to transmit and receive data as well as speech and a new level of privacy and security. The new Europe means we've now got a home market of 360 million. If you want to talk business with them, talk to us first.... Freephone 1800-225588"

The Network

Of the sample taken in Waterford it may be extrapolated that the most used type of exchange in Ireland is the Ericsson E10.

E10
Exchanges: 41
Capacity: 41,974
AXE
Exchanges: 22
Capacity: 25,472
ARF
Exchanges: 7
Capacity: 14,600
ARK
Exchanges: 55
Capacity: 22,000
Other
Exchanges: 6
Capacity: 3,015

The E10 and AXE exchanges are the only digital ones in use, the others are analogue "crossbars" in nature.

Gimmicks

There are many gimmicks available to those on digital exchanges. Examples being:

Call diversion
Call waiting
Hotline
24 Hour Alarm System

to mention but a few of those available.

The 24 hour alarm system is activated on digital exchanges by typing in: *55*hhmm# and then listening for a return tone and finally replacing the handset.

Payphones

The old rotary style payphone is identified by its very robust design and (very often) its black enamel flaking off of it. These are very hard to find nowadays and really are a collector's item. It can now only accept 10p and 50p coins (as most other coins have been replaced by smaller versions).

With these old rotary machines it is possible by depressing the switcharm rapidly to phone any destination without costing any money (except of course where Telecom

Eireann's concerned).

The remaining types of payphones are essentially the same, as far as the type of dialing goes anyway. These are keypad payphones but are not the R-type keypad which many of the gimmicks described above necessitate. In other words, not all of the gimmicks described above are available for use from a payphone.

Of these types the units are paid for via coinage (i.e., Payphone 50/400), smartcards or credit cards. The smartcard and credit type payphones are relatively new as they were introduced to the system only two years ago.

The smartcard payphones are, like the coinage ones, available for use on the streets and in pubs. The cards themselves are available in units of ten ($2), twenty ($3.50), fifty ($8), and a hundred ($16) on them.

The credit card payphones are, like the old rotary payphone, a collector's item and are available for use only in upmarket areas such as hotels, restaurants and even museums. (e.g. The Modern Art Museum at the Royal Kilmainham Hospital in Dublin.) As mentioned in the article on the Australian Phone System (Spring 1992), a P.I.N. is required to use this type of payphone.

Special numbers, Operator assistance, etc.

010

Advice of duration and charge.
Reverse charge request.
Personal calls.
Alarm calls.
Telecard service.

017

Ringback no. (characterised by a continuous ringing.)

088

Mobile Telephone service (Eircell) prefix.

114

International calls assistance excluding Britain.
Audio conference calls.
International reverse charge request.
International personal calls.
International advice of duration and charge.
Connection to Satellite Radio Maritime service, "Inmarsat" call.
Connection to Coastal Radio Station service.

191

Repair service.
Operator assistance.

196

Telemessage and International telegrams.

999

Emergency number. (Police, Ambulance, Fire Brigade, Boat & Coastal, Mountain & Cave) This is roughly equivalent to the U. S. 911 phone number.

1190

Direct inquiries within the whole of Ireland.

1191

The Speaking clock (24 hour format, at 10 second intervals).

1197

Direct inquiries within all of Britain.
Codes for British exchanges.

1800

The code prefix for Freephone numbers.

1850

The code prefix for Eirpage relays (pagers).

Long Distance Operators To Ireland

0014-881-353 from Australia.
078-110-353 from Belgium.
1800-463-2050 from Canada.
800-10-353 from Denmark.
9800-10-353 from Finland.
1900-353 from France.
0130-800-353 from Germany.
8000-353 from Hong Kong.
177-353-2727 from Israel.
1720-353 from Italy.
0039-353 from Japan.
0800-0-353 from Luxembourg.
06-0220-353 from Netherlands.
000-953 from New Zealand.
900-990-353 from Spain.

I think you get the idea!

Long Distance Operators From Ireland

00-61 to Australia.
00-61-2 to Sydney, Australia.
00-32 to Belgium.
00-34 to Spain.
00-44 to the U.K.
00-31 to the Netherlands.

Electronic Directory Service (E.D.S.)

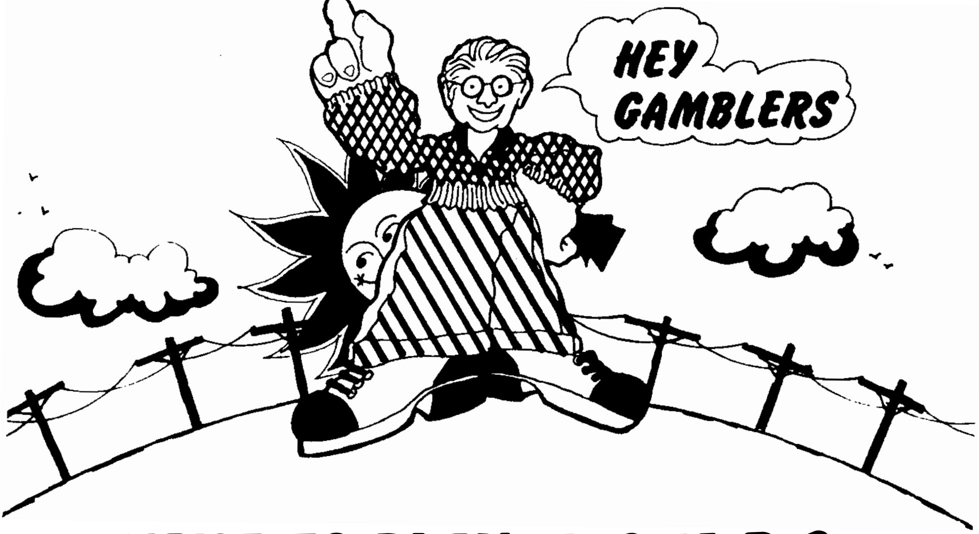
This service offers to the paying public a Minitel package where any telephone number (excluding ex-directory numbers) may be looked up via the software.

There are three options:

Surname plus STD code giving a range of possible numbers
Surname, first name plus STD code
Surname, first name, address + STD code

By being more precise the range is narrowed down until finally only one number is listed on the screen.

MINITEL operates at a baud rate of 9600.



WANT TO PLAY *R.O.M.B.?*

(RIP-OFF MA BELL)

HERE'S HOW YOU PLAY –

JUST GO TO THE NEAREST PHONE, AND PLACE AS MANY FRAUDULENT LONG DISTANCE CALLS AS YOU CAN. USE A FAKE CREDIT CARD; SOMEONE ELSE'S PHONE NUMBER; OR IF YOU'RE AN ELECTRONICS NUT, BUILD A BLUE, BLACK OR RED BOX. SOUND LIKE A GOOD RIP-OFF? RIGHT ON!

NOW, HERE'S THE HITCH . . . MA BELL DOESN'T GROOVE ON THIS ACTION, SO SHE USES HER COMPUTERS, CENTRALIZED TOLL INVESTIGATORS, AND SECURITY AGENTS (NOT TO MENTION LAW ENFORCEMENT AGENCIES) TO CATCH YOU. AND WHEN SHE DOES CATCH YOU, THE GAME IS OVER . . . AND YOU WIN!

NOW, DIG THE PRIZES –

1ST PRIZE: **YOU GET UP TO 5 YEARS IN PRISON.**
2ND PRIZE: **YOU GET TO PAY A FINE UP TO $1000.00.**
3RD PRIZE: **YOU GET TO PAY FOR ALL THOSE CALLS.**
GRAND PRIZE: **YOU GET ALL THE ABOVE PRIZES.**
BONUS: **YOU MAY GET TO PAY THE COURT COST.**

HEAVY, MAN!!

GUESS WHO THIS LITTLE WALL POSTER WAS AIMED AT?
Hint: It was hung at colleges in the early seventies! Far out.

The Ghost Board

by Autolycus

The Evergreen State College in Olympia, Washington is an "alternative" (aka hippie) college which grew out of the academic counterculture of the late 1960's. During the 70's and 80's, Evergreen was the home for a variety of innovative phreaks and proto-hackers (testimony of this can be found in the campus computer center occupying Room 2600 of the Evans Library building - but how we pulled that off is another story).

Some activities of this community are public knowledge due to individuals' entanglements with telco cops and other powers that be. The busts by the FCC over the campus radio station's (KAOS) bootleg phone switchboard system during the era of Ma Bell's monopoly over such systems was, fortunately, the worst bust we were ever involved in. A number of text files are circulating which document Saladin's conversion of an elevator emergency phone to an active WATS line, as well as his overdubbing the screech used in the Emergency Broadcast System radio tests with 2600 Hz. But nothing has been written about the locally infamous "Ghost Board". In the Pacific Northwest, the Ghost Board is legendary, though much that has been written about it is more mythical than factual (no, the Ghost Board never posted classified dialups for the nearby Bangor Missile Base).

The Ghost Board was a parasitic bulletin board - mostly a message system - which sporadically and temporarily operated covertly in a number of computer dial-up systems *without* the knowledge of the sysop (though more than once the assistance of a co-sysop was used). In the early days this was accomplished very simply (usually through shared accounts and simple encryption methods), but with time more intricate operational procedures were used. Regardless of the system used, the basic Ghost Board procedure was as follows:

1) Members would call the system in the wee hours of the morning and access non "advertised" message areas. (This was done in a variety of ways ranging from simply typing an unlisted character at the main menu of a Wildcat system, hitting ALT E, S, C on a LAN system, or using an ANSI bomb to drop to DOS.)

2) A message/database system was available where Ghost Board members could communicate, and a rough date for the next Ghost Board was listed.

3) The system would (ideally) self-delete at a predetermined time and no trace of the system would be left.

The Ghost Board only operated between midnight and 5 am. It was little more than a floating database system collecting: compiled addresses and phone numbers of every payphone in the area, test loop numbers, information on local computer systems and security flaws, flaws in local PBX system, pilfered system passwords and account names, etc.

The original Ghost Board never lasted for more than two or three evenings at a time and only operated every sixty days or so. In the late 1980's one ghost board member operated an elite local text and phreak-utility based BBS called the Ghost Board, but this was actually a separate entity.

With time, the method of notifying members where and when the Ghost Board was up and operating was changed. The most common method was to use the free lost and found classified ad section of the local newspaper where periodic messages conveyed the needed information (i.e., LOST - Dalmatian puppy with tag reading ATDT, call 555-7734 before 7/22, ask for Keith - where "Keith" was the name needed to gain access to the system).

As BBS systems proliferated in the early and mid eighties the Ghost Board began using simple ANSI bombs to gain superuser access to poorly tended systems. From this vantage unused menu keys were assigned to access the hidden sub-board system. At different times, work-study positions and academic "internships" at State agencies were used to burrow out hosts for the Ghost Board. For half a year I periodically set up a message system on a state agency's computer system and hooked up my own external modem. At a later date the local dialup card catalog for the library was hacked and bogus book entries were used to pass on information.

For a short period of time in the early 90's, one Ghost Board pioneer abandoned an AT (he'd purchased it for $40 at the Goodwill) on the roof of a rural supermarket. The AT was water-protected and hardwired into the store's power grid and the 2400 modem was spliced into the store's phone lines. This system operated for almost five months before it was (apparently) detected and shut down.

At present the Ghost Board is still sporadically operating with the assistance of various UNIX systems and child-operated BBS systems. With any luck, this is the last you will hear of us!

HACKING NETCASH

by Palindrome

Recently in the July issue of *Boardwatch* I stumbled across a pretty interesting article about Netcash. What Netcash is is online 'money' represented in an alphanumeric string, each standing for a certain amount of money, ranging from 25 cents to 100 dollars. A sample string of Netcash would look like this:

NetCash $1.00 E1234H5678Z

As you can probably see, Netcash is *begging* to be hacked. I have not seen many places accepting Netcash at the moment, however it is there, and how could we live with ourselves if we didn't take a crack at it?

Uses of Netcash

Let's say you were selling some program online, and you accepted Netcash as a form of payment. The buyer would get his Netcash by dialing 1-900-933-CASH with his modem. Then he will be issued a $10 Netcash string. After getting the string, he would leave you a message telling you the string and requesting the program.

Now to get your Netcash you must send a request message, asking for the validity of the string, to netbank@agents.com. In the body of the message, you have to ask them to validate it, in this format:

From: jo@blow.com
To: netbank@agents.com
NetCash $1.00 E1234H5678Z/Accept

Then the system will reply like this (for a valid string):

From: netbank@agents.com
To: jo@blow.com
Subject: NetBank Receipt, Accepted: 1, Rejected: 0
Input Transaction(s):
Accepted: NetCash $1.00 E1234H5678Z/Accept
Total Accepted: $1.00
NetCash $1.00 E54466122A

What has just happened is the system has validated the old string, which someone might have given to you to pay for something, and given you that amount in Netcash, as well as revoking the old string for use anymore.

If the string was not validated, the return message would look like this:

From: netbank@agents.com
To: jo@blow.com
Subject: NetBank Receipt, Accepted: 0, Rejected: 1
Input Transaction(s):
REJECTED: NetCash $10.00 K52286154A/Accept
Total Accepted: $ 0.00

This is just a basic rejection message sent to you.

There is also an option of 'Making Change' in Netcash. Let's say you want to buy multiple pieces of software, but you only have one $20.00 string in Netcash. What you do is send another message looking like this:

From: jo@blow.com
To: netbank@agents.com
NetCash $20.00 E54466122A/Change 1 Ten 2 Fives

That's all, they will send you a return receipt not differing in format from the others. They will then issue you one $10.00 Netcash string and two fives:

NetCash $10.00 L73522979A
NetCash $ 5.00 J83662917A
NetCash $ 5.00 M32299134A

If you bought a software program for $7.00 you would get Netcash change if you gave them a $10.00 string.

Doing all of this electronic money stuff is entertaining at first, but you're soon gonna want some real cash from this, so, you must fill out an e-mail form requesting an account on NetCash. Then, once issued to you, you deposit your Netcash as so:

NetCash $100.00 E4321J8765W/Deposit 123456

Where 123456 is your account number.

The company takes a twenty percent surcharge due to "costs of keeping up the 900 number".

Conclusion

Well, by now I hope you've gotten a pretty good idea of Netcash and maybe in the near future we'll get our hands on the algorithm for it. Here is a list of the important info for netcash:

1-900-933-CASH: Modem 900 number to get your $10.00 Netcash string.

netbank@agents.com: The e-mail address for all your transactions.

Netcash string: an alphanumeric string containing eleven ASCII characters.

Welcome to MEL

by EighT BaLL

Southwestern Bell has installed a new system, the Mechanized Employee Locator. This system provides access by telephone to the official company directory. Mechanized Employee Locator, MEL for short, provides name, phone number, address, department, and title information for *all* Southwestern Bell Telephone employees. MEL offers a call-completion function that will automatically dial the number of the person whose number you search for. Although this feature is not really important for us, it could be used for certain purposes like dialing an employee long distance for you for free.

MEL also offers a reverse-search capability, meaning you can search for a person's name by using his or her phone number. This system is similar to a computerized "yellow pages" for Bell employees. MEL is available 24 hours a day, seven days a week, and can be called from any touch-tone telephone.

How to Use MEL

First you must have a MEL access number, which I have included at the end of this article. MEL has access numbers for 16 area codes. If yours is not listed, then you can use the 800 access number. Then follow the steps below and voila, you have access to all of Southwestern Bell's employees.

1. When MEL answers it will ask you to press the * button if you have a touch-tone phone or if you are on a rotary-dial phone it will then transfer you to the SWB switchboard. This is not good... so call on a touch tone phone.

2. After you let MEL know you are on a touch-tone phone it will give you four commands you can use to access employee benefits, or go through the employee directory, etc.

Commands and Description

0: employee benefits
9: quick call options
#: company functions
**: employee locator (this is what we want)*

3. Now choose the command you want. I will describe each of them, although the employee locator is the most useful one.

0 - Telephone Company Benefits

If you choose the '0' command it will give you access to employee benefits for retired employees and current employees. If you choose retired employee benefits it will give you information about pension, medical, and other insurance matters. You can also report deaths. You can also change an employee's address.

This is not very useful, but if you had a good imagination you could really fuck with some SWB employees.

9 - Quick Call Options

1. Company line
2. EAP Counselor
3. Award Redemption Line
4. Affirmative Action Hotline
5. Tuition Plan Numbers
6. Open Network Architecture Hotline
7. Payroll

# - Company Functions

Enter a Keyword or abbreviation then pound.

I have no idea what this is and really don't feel like messing with it. Besides, it doesn't look very useful....

* - Employee Locator

Enter a last name then pound.

Let's say you enter 'Jone' in, which would stand for 'jones' but you only need to enter in four digits, which are 5663, then pound. It will then ask you for a first name. Say you put 'Sam' in, which is 726, then press pound. It will ask you if you want to narrow the search by entering the state abbreviation. You could do this but you would probably want to find all of the matches. It will find matches for this particular entry.

Call up MEL: 1-800-660-7635
*Press * to let it know you are on touch-tone.*
Press # to do an employee search.
Enter at least 4 characters of the last name then #.
Enter at least 1 character of the first name then #.
Enter a state (MO,AR,KS,OK,TX) to narrow the search.
Press # to skip listing or to reverse search by number.
*Press * to cancel and re-enter.*

Key functions:
0 Operator
1 Help
2 Complete Call (C)
3 Department (D)
4 Hear Again (H)
5 Location (L)
6 Number (N)
7 Spelling (S)
8 Title (T)
9 Work Cross Reference (W)
# Enter/Skip or Search
**** Cancel/Restart***

MEL Directory

Little Rock, AR (501) 373-1411, 1+990-5479
Fort Smith, AR (501) 785-1411, 1+990-5479
Pine Bluff, AR (501) 534-1411, 1+990-5479
Kansas City, KS (913) 676-1411
Topeka, KS (913) 276-1411
Wichita, KS (316) 261-1411
St. Louis, MS (314) 331-1411, 1+572-9040
Kansas City, MS (816) 275-1411, 1+572-9040
Springfield, MS (417) 836-7411, 1+572-9040
Oklahoma City, OK (405) 291-1411, 291-1775
Tulsa, OK (918) 586-1411, (918) 586-1775
Dallas, TX (214) 464-1411
Houston, TX (713) 871-1411
San Antonio, TX (512) 222-0411

1-800-660-7MEL is for toll-free access. The 1+ numbers are also toll-free. 1-800-GO-TO-SWB is toll-free access for areas outside Southwestern Bell and areas with no working local or intralata toll-free numbers.

GENERATING AN ESN

By Maldoror

This article explains how the ESN is generated based on the serial number stamped on the phone by the manufacturer. This will not aid you in cloning, but this will aid you in cross referencing phones, as well as deciphering ESN's to identify the type of phone making the call.

Serial Number to ESN Conversion

E.F. Johnson: 131 + 0's + 4, 5, or 6 digits of serial number.

G.E.: Serial number is the ESN.

Harris: Serial Number is the ESN in HEX.

Technophone: Serial Number is ESN in decimal.

Oki: Remove first 3 digits and letter, add 129. Serial # 603E00109249, ESN 12900109249.

NEC: Remove first 2 digits, add 135 plus 0's to equal 11 digits. Serial # 70-207470, ESN 13500207470.

Novatel: Serial number is ESN. Serial # 14200007306, ESN 14200007306.

Walker: Serial number is ESN. Serial # 15200010842, ESN 15200010842.

Audiovox BC-20: Remove first 4 digits, add 174 plus 0's to equal 11 digits. Serial # 7104007592, ESN 17400007592.

Mitsubishi: The ESN is written on a sticker on the transceiver labeled "Sec. Code".

Panasonic: Remove first 2 digits, add 136 plus 0's to equal 11 digits. Serial # 117591, ESN 13600117591.

Mobira: Add 156 plus 0's to equal 11 digits. Serial # 154056, ESN 15600154056.

Hitachi: Put 13200 in front of serial number. Serial # 157921, ESN 13200157921.

Manufacturer Decimal Codes
(Use As In Above)

Alpine: 150
AT&T: 132 or 134
Astrotel: (see Oki)
Blaupunkt: 148
Clarion: 140
Diamondtel: 134
EF Johnson: 131
Ericsson: 143
Fujitsu: 133
G.E.: (except mini) 146
Harris: 137
Hitachi: 132
Hyundai: 160
Kokusai: 139
Mitsubishi: 134
Mobira: 156
Motorola: 130
NEC: 135
Nokia: 165
Novatel: 142
Oki: 129
Panasonic: 136
Phillips: 170
Satellite: 161
Shintom: 174
Sun Moon: 178
Technophon: 162
Toshiba: 138
Uniden: 172
Walker: 152

Several phone companies share manufacturers, and the ESN code will be that of the manufacturer:

Alpine 9510 use Fujitsu 362A - ARA.

AT&T 1300, 1800 use Mitsubishi.

AT&T 1100, 1200, 1400, 1440, 1700, 1710 use Hitachi.

Audiotel 1000, 3000, 500, BC-40, 400, 450, 550, 600 use Toshiba.

PC 100, 200 use Technophone.

BC-20, CMT-125 use Shintom.

Tactel use Toshiba.

Blaupunkt, most are Panasonic, but some are Blaupunkt.

GE Mini use Mitsubishi.

Glenayre-301 use Mitsubishi.

Mitsubishi 460 use Toshiba.

USA A&B use Mitsubishi.

Walker Pocketphone use Technophone.

Western Electric use Hitachi.

Western Union use E.F. Johnson.

GTE Bronze uses Sun Moon Star.

Tandy/Radio Shack uses Nokia.

For serial numbers over 999,999 you will need to subtract 737,856.

For Example: 01,123,456 - 737,856 == 385,600. Then convert this to the ESN as: (If it were Bronze, 17800385600 = ESN.

If you have any questions, try to find some of Tesla's books, and you'll have a lot more.

the ten dollar red box

by Toxic Avenger

I bought the guts to a Hallmark card at 3 pm yesterday. Before 5 I had a working box. Here are the instructions for the complete idiot (or those just having trouble).

Materials

1 Hallmark digital recording card (~$8, card store)

1 1/8 inch mono phono plug (~$1 or in a junk bin)

1 SPST switch, or momentary contact NORMALLY CLOSED (~$1 or junk bin)

The sound of magical quarter tones (you can get these from payphones, computer sound files (QUARTER.VOC is one), other red boxes, tape recorders, etc.)

A case of some sort (I used a case from a DAT, but anything you can put the stuff in will work. Perhaps the case from a data tape or an 8mm videotape, or just a cassette.)

A Tube of silicone sealant (epoxy will probably do, I just happened to have silicone on hand)

What To Do

1. Remove all components from the plastic thing inside the card. This includes sliding the battery pack out of its drawer.

2. Cut the following wires:

Both wires going to microphone (both are green, mark which one goes to the center of the mike)

Both wires to the battery pack (red and white)

Both wires to the switch mechanism (green and black)

2a. **(optional)** It is a wise idea (if you are fairly experienced at soldering/desoldering on small PC boards) to desolder all the wires and replace them with ones of a thicker gauge. The ones that Hallmark supplies are just too damn thin and have a real tendency to break at connections. *Remember,* the wires in this card are supposed to be protected in the little plastic grooves that you removed them from.

3. Discard the switch mechanism.

4. Wrap the battery pack in electrical tape (I used red tape just to be cheesy, since the box is clear).

5. Solder the SPST switch to the black and green wires that used to go to the original switch (polarity is *not* important).

6. Solder the phono plug to the two green wires. Polarity shouldn't really be important, but to be on the safe side, the wire that ran to the center of the mike (I told you to mark it) should go to the TIP of the plug.

7. Connect the battery. (This battery pack puts out 6.25 VDC. I suppose you could replace it with another battery, but why bother?) *Polarity is extremely important!* The red wire goes to the positive terminal, and the white goes to the negative. On my box, if the pack is laying flat, with the exposed part of the batteries pointing up, the positive terminal is the one on the left (if you are facing the terminals). I'd use a multimeter just to be sure.

8. Glue the PC board to the top of the battery (this saves space and hassle later, but is not necessary for operation).

9. Program the thing....

I used the QUARTER.VOC file and I looped it 10 times, with a random delay of between .5 and 1 seconds between each quarter (who puts them in at regular intervals anyway?) If you have this file, plug the phono plug into your soundcard, turn the volume *way* down (trial and error will give you the proper volume) and play the VOC file (after setting the switch on the PC board to the record position, and flipping the SPST at the beginning of the VOC file).

10. Test it....

Best way to test is to call long distance Directory Assistance (I'm partial to 808-555-1212 which is Hawaii).

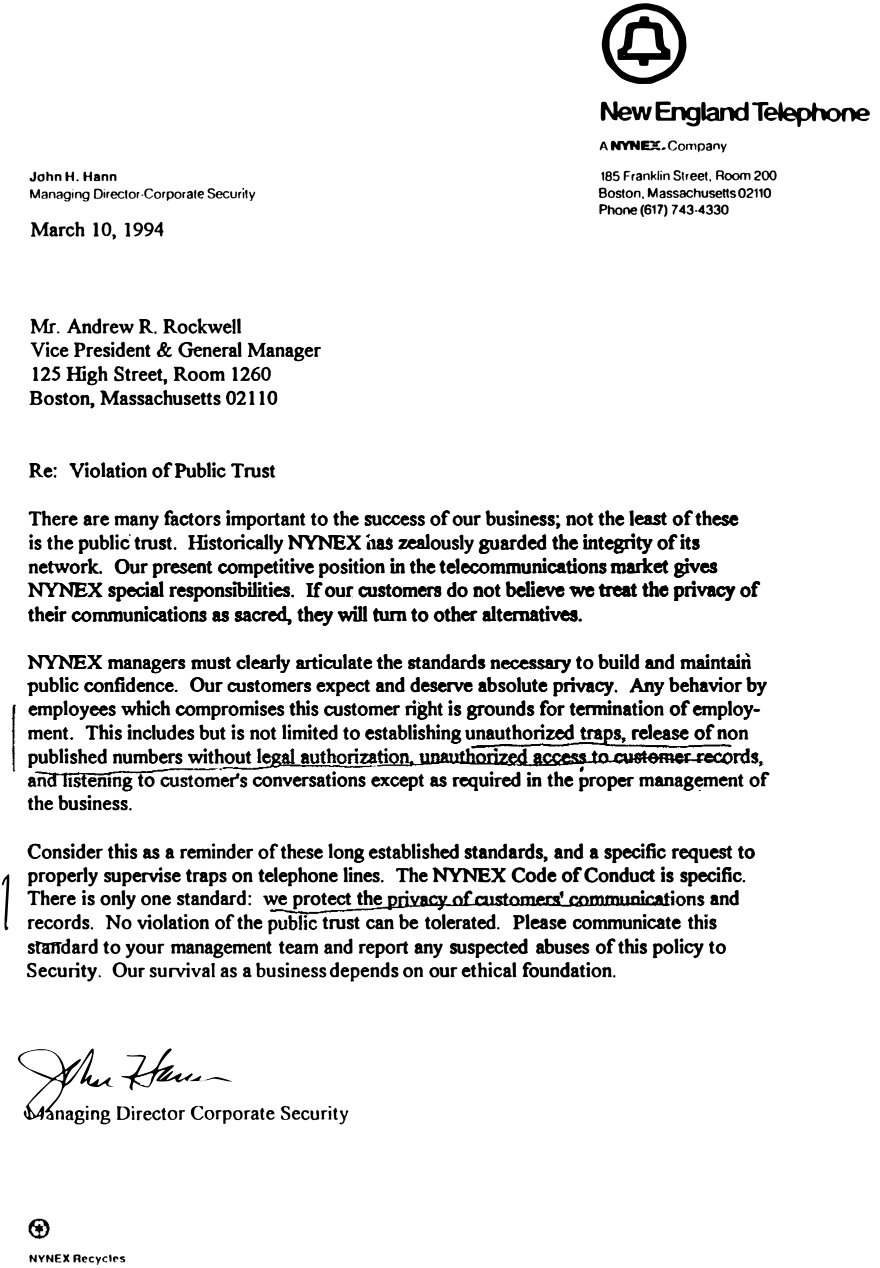
If it doesn't work, go back to step 9. The ideal volume is one that can be heard clearly, but does not cause the speaker to break up.

11. Once you have the thing programmed, there is no need to keep the phono plug attached. If you want to save room, cut it off.

12. Put the thing in the case. Drill several holes in the case where the speaker will mount. I mounted the speaker with silicon very carefully applied to the edges of the speaker. Same was true of the battery pack. The switch obviously mounts in a hole on the side of the case.

Why the SPST Switch?

First off, I thought the switch that came with the thing looked really cheaply made, and would probably break. Secondly, by putting in a switch instead of a momentary switch, it allows me to record $2.50 on the box, and play the whole thing back just by flipping the switch, rather than having to hold it down.



New England Telephone

A NYNEX Company

John H. Hann
Managing Director-Corporate Security

185 Franklin Street, Room 200
Boston, Massachusetts 02110
Phone (617) 743-4330

March 10, 1994

Mr. Andrew R. Rockwell
Vice President & General Manager
125 High Street, Room 1260
Boston, Massachusetts 02110

Re: Violation of Public Trust

There are many factors important to the success of our business; not the least of these is the public trust. Historically NYNEX has zealously guarded the integrity of its network. Our present competitive position in the telecommunications market gives NYNEX special responsibilities. If our customers do not believe we treat the privacy of their communications as sacred, they will turn to other alternatives.

NYNEX managers must clearly articulate the standards necessary to build and maintain public confidence. Our customers expect and deserve absolute privacy. Any behavior by employees which compromises this customer right is grounds for termination of employment. This includes but is not limited to establishing unauthorized traps, release of non published numbers without legal authorization, unauthorized access to customer records, and listening to customer's conversations except as required in the proper management of the business.

Consider this as a reminder of these long established standards, and a specific request to properly supervise traps on telephone lines. The NYNEX Code of Conduct is specific. There is only one standard: we protect the privacy of customers' communications and records. No violation of the public trust can be tolerated. Please communicate this standard to your management team and report any suspected abuses of this policy to Security. Our survival as a business depends on our ethical foundation.

John Hann
Managing Director Corporate Security

NYNEX Recycles

We sure hope NYNEX guards our communications better than they guard their own. We also have to wonder if this little memo means they're having a bit of trouble with integrity.

how to listen in

by Q

This article relates to the field of surveillance. I will not digress into an explanation as to the great importance of surveillance to the serious hacker or phreaker, nor will I attempt to delve into the many legalities regarding this field, as a whole book could be written on this fascinating and important topic. While reading this article, the question might arise as to what surveillance has to do with the field of hacking, phreaking, and computer security. Without getting technical, the answer is simply "everything". As a professional in the surveillance and countermeasures field as well as being an avid telephone phreak and "network traveler", I have found that my professional line of work in surveillance greatly complements my explorations in hacking and phreaking.

The following information is only a partial listing of the many devices that are available to the general public. There are many more advanced methods developed and utilized by federal agencies with one sole purpose, and that is to spy upon innocent Americans.

Long Range Listening Devices

Shotgun Microphones: A shotgun microphone consists of a long tube either of metal or plastic with a length of 12 to 36 inches. One end of the tube is open while the other end consists of a super-sensitive microphone. The microphone is surrounded by a damper to eliminate vibrations of the tube being picked up. The microphone is connected to a powerful handheld amplifier that usually contains a low pass audio filter to cut out low frequency sounds such as wind and vibrations. The shotgun microphone is extremely directional. A top of the line model can pick up ordinary voices from 3/4 of a mile away.

Parabolic Microphones: A parabolic microphone consists of a "dish" composed of metal or plastic with a diameter of 12 to 32 inches. The dish focuses sound waves onto a center focal point an inch above the reflector dish. This sound is picked up by an extremely sensitive microphone and is sent to an amplifier with a low pass audio filter to eliminate wind noise. A top of the line parabolic dish can pick up ordinary voices from over one mile away. As a note, the pattern of pickup is much wider with a parabolic dish so it picks up more background noise than a shotgun microphone would, however the range is considerably greater.

Laser Listeners: This is a truly remarkable and complex device that picks audio by demodulating the interference patterns in a laser or microwave beam. A simple system consists of a 15 milliwatt laser. The laser beam is aimed at a piece of glass such as a window. Whenever someone talks, the audio waves vibrate the window a minute amount. As the glass vibrates, it modulates the laser beam much in the same manner that a transmitter modulates voices onto a radio wave. A collector on the receiving unit captures the reflection from the light bounced off the window and an electronic circuit demodulates the collected light and amplifies the audio producing the voices of the subjects under surveillance. Low end units have a range of 60 feet while top of the line units can pick up audio from over 500 feet away. High end systems utilize multiple laser and/or microwave beams to cancel out noise caused by wind. In addition, mylar reflectors are utilized. These reflectors are an inch wide and allow an increased reception range.

Through-Wall Listening Devices

Contact Microphones: A contact mike is a sensitive microphone utilizing a unique principal that listens for vibrations rather than sound waves. It usually consists of a piece of piezoelectric material that produces an electric current that is modulated by vibrations caused by audio. The contact microphone is coupled to a powerful handheld amplifier either as an integral or separate unit. Contact microphones can clearly pick up a voice through up to 12 inches of concrete or 3 inches of solid wood.

Spike Microphones: A spike microphone consists of a supersensitive crystal or electret microphone, and is coupled to a 2 to 12 inch metal spike. This metal spike is driven into the wall and picks up resonations from the wall very clearly. The audio signal from the microphone is then fed into a powerful handheld amplifier.

Tube Microphones: A tube microphone consists of a small 2 to 12 inch hollow metal tube approximately 1/8th of an inch in diameter. The tube microphone is placed into a hole in the wall or through an air duct, etc. and picks up sounds coming from directly in front of it. The sound resonates inside the small diameter tube and is amplified by resonation. The audio then reaches a sensitive microphone on one end of the tube. The electric signal from the microphone is then amplified by a powerful handheld amplifier.

Hardwired Room Microphones

Occasionally the placement of a transmitter aka "bug" is impossible, impractical, or unnecessary. In certain situations it may only be necessary to use a wired remote microphone. Police often use this technique in hotels when engaged in sting operations. Typically, one hotel room is used as the set-up room, and an adjacent room contains the surveillance listening post.

Microphone with In-line Amplifier: This technique simply consists of a miniature microphone hidden about the target's room. This microphone is then wired into the adjacent surveillance room via an air duct or a hole in the wall. When the microphone is to be placed over 50 feet from the listening post, a miniature in-line amplifier is used to boost the audio signal, and increase the microphone's sensitivity.

Hidden Wire-Line Microphone: This is a clever technique similar to the above method, only a pre-existing wire is utilized so as to avoid detection. Usually an electret microphone is hidden inside a splice block, modular phone jack, coaxial cable, intercom wire, or an alarm sensor element, and is connected to a pair of alarm or telephone wires. The listening post simply taps into the wire pair and can monitor all sound within the target room.

Fine Wire Laying Kits: This is an old but very advanced technique of hardwiring a microphone that was extensively used by government agencies. It utilizes ultra-thin coated wires, similar to magnetic winding wire. This wire can be layed and run throughout a room or house and remain undetected indefinitely. A fine wire laying tool is used to spool the wire, as it is layed. This wire can be placed into cracks in the floorboard and under carpet, as well as behind moldings. After laying, a small amount of silicone or beeswax is used to hold the fine wires in place. Advanced fine wire kits utilize a three wire system, where two of the wires are intertwined and the third is run alongside. This eliminates any RF emission from the wire, making it extremely difficult to detect.

Hookswitch Bypass: This is an old but very effective technique to monitor room audio by bypassing or shorting out the hang-up switch on a telephone receiver making the phone "hot-on-hook". The room audio can then be monitored by **simply tapping into the subject's telephone wire pair.**

Telephone Line Microphone: This method is similar to the hidden wire-line technique. Only the telephone equipment is used to hide and transmit the room audio. A simple electret microphone could be placed inside a modular phone jack, or perhaps connected somewhere along the line in the target's room, picking up all of the room sounds, when the telephone is not in use. The listening post then taps into the subject's wire pair. A specialized audio filter is then used to strip off the dial tone.

Coaxial Cable Microphone: This device consists of a microphone placed onto a television coaxial cable. This method is subject to interference, and there are much better methods discussed later in this article.

Transmitters aka "Bugs"

Transmitters, often referred to as "bugs" or, when worn on the body, as "wires", are perhaps the most commonly known form of surveillance. This equipment is also the subject of the most misinformation and exaggeration created by the media and Hollywood. Bugs come in a variety of sizes ranging from the size of a beeper to slightly smaller than your pinky fingernail. The greatest falsity created by Hollywood is that bugs can transmit at a range of miles. This is entirely false - bugs transmit on the order of feet, not miles. Typically, bugs can transmit between 75 and 2000 feet. Another misconception is that the greater the range, the better. While a greater range is certainly more convenient, it leaves the bugged conversations open to accidental interception. "Bugs" are often pre-packaged in various innocuous household items such as RJ-11 telephone jacks and electrical outlets, and can also be carried on your person concealed in fountain pens, calculators, watches, beepers, lighters, etc.

> *"Contact microphones can clearly pick up a voice through up to 12 inches of concrete or 3 inches of solid wood."*

FM Transmitters: These are the most commonly available bugs that amateurs can obtain and lawfully use. They operate at a frequency range of 88-130MHz, and have a power output of between 10-100mW. High level amateurs will usually want to transmit on the 109-130MHz air band because that frequency can only be picked up on a wide band scanner. **FM bugs use a circuit called a free-running oscillator for convenience.** This allows the bugs to be tuned on a variety of chosen frequencies. The main problem with operating within the FM radio band is the strong background emissions from commercial radio stations. If the signal from the bug is too weak, it will be ignored by the receiver in favor of the stronger commercial signal. FM bugs are also subject to interference from aircraft.

VHF Transmitters: VHF transmitters are occasionally used by law-enforcement personnel and amateurs. They operate at anywhere between 130MHz-450MHz. They either have free running oscillators or are crystal controlled.

UHF transmitters: Almost all professionals or law enforcement personnel use UHF transmitters. These operate at much higher frequencies, between 400MHz and 3GHz. UHF units are always crystal controlled and operate on a very narrow bandwidth. As a result of the higher transmission frequencies coupled with a narrow bandwidth, these UHF units are free from interference caused by commercial RF background signals and natural anomalies. The transmission range is typically 3-5 times further than their free-oscillating counterparts.

Wafer Transmitters: Wafer transmitters are the most exotic devices ever designed. They are extremely small in size and do not even require an internal power source. They are specially designed transmitters that are powered by strong highly-directional RF signals, usually in the microwave range. These powerful signals charge up the circuits of the wafer transmitter. The range of these devices is not very far, but they are extremely small, being no larger than the size of your pinky fingernail. There is another unique type of listening device often categorized as a wafer transmitter that operates on a principal similar to a laser listener. A strong highly directional microwave RF signal is aimed at a target's area. This type of bug simply consists of a very small special piece of material that is flexible and will be modulated by voice waves, and is highly reflective to microwave signals. When room audio is present the wafer transmitter will vibrate. This in turn will modulate the microwave signals that are being beamed into the area. The receiver simply demodulates the reflected microwave signals, producing the audio which was present in the target's room. This technique is extremely high-level and was believed to have been invented by the Russians, who developed this type of device and used it to spy on the American Embassy in the USSR.

Crystal Controlled vs. Free Oscillating: Free running oscillators are always used on lower grade bugs. FRO's can be tuned through a great range of frequencies for convenience. This type of circuit suffers from three main problems. The first being that the signals are untuned and can produce spurious outputs and harmonics, which allow the frequency to drift, making reception somewhat difficult if the signal is weak. In addition, harmonics allow the signal to be picked up on alternate frequencies by "ghost" images of the signal. The second problem is the weak power output of the circuit. The signal of an FRO is not maximized for any one frequency. As a result, the power output is not as high. And third, an untuned circuit is not as efficient and uses more power, resulting in a shorter operating lifetime and a higher operating current. Crystal controlled units, however, are locked on one particular frequency and, as a result, apply all of their energy to a very narrow bandwidth, making the crystal controlled circuit very efficient. This higher efficiency allows a greater power output per size ratio compared to an FRO. In addition, the highly tuned circuit produces no harmonics, spurious emissions, and no frequency drift, allowing a much greater receiving distance. The power supplies of crystal controlled units typically last 5-10 times longer than FRO's.

Mains vs. Battery Powered: All transmitters are of two types, the first being battery powered. Typically, a battery powered device will last between one day and three weeks, depending upon the efficiency, the power output, and whether the device is free oscillating or crystal controlled. Mains powered devices are powered by anything but batteries. Mains powered transmitters usually come pre-packaged into wall outlets or plug adapters. But a clever surveillance expert can wire a transmitter up to anything that runs on house power producing either AC or DC electricity, such as thermostats, intercom wires, alarm wires, and anything else you can think of.

Remote Activation and VOX: In order to extend the lifetime of battery powered bugs, the transmitter must have the ability to turn itself off when not in use. This is done in one of two ways: by remote activation or by VOX (a voice actuation circuit). Remote activation utilizes a special receiver on the transmitter. When the signal is given by the listening post, a particular bug will either turn on or off. A better method is to utilize a voice actuation circuit referred to as a VOX. When a voice of sufficient amplitude is present around the bug, the transmitter will automatically turn on. Both of the aforementioned techniques use a very small amount of current to operate the activation circuits. VOX activated transmitters can have a lifetime of up to one month. Aside from conserving power, an actuation circuit serves another purpose and is useful on both mains devices as well as battery powered devices.That purpose is to prevent detection of the device. If a transmitter is left running constantly it has a much greater chance of being discovered by various means, including accidental interception on a scanner. A remotely or

VOX activated bug is extremely hard to detect except by using advanced countermeasures equipment. If a bug is not activated, then it cannot be detected by conventional transmitter detectors. Specialized devices such as Non-Linear Junction Detectors, or a simpler device that feeds an audio source into the room to activate the device, can be used in conjunction with a standard bug detector.

Advanced Modulation Techniques: Very advanced bugs are utilized only by government intelligence agencies. Very high-level bugs operate using odd modulation techniques that cannot be demodulated by an ordinary scanner. These odd modulation transmissions also allow for a greater transmission range due to their very nature.

Frequency Hopping Transmitters: One method developed to prevent accidental interception or discovery of a bug by a countermeasures expert is to rapidly alter the frequency at a preset rate. This makes it nearly impossible to receive the transmission by accident or on purpose. Even if one knew the various frequencies that this bug operated on, it would be impossible to hear any audio. The reason is that the frequency hopper alters the frequency at such a rapid rate that a modern digital wideband receiver would be too slow to lock onto the signal. All that would be heard is a popping sound for a brief fraction of a second. It takes a specialized multi-crystal, multifrequency receiver to receive this type of signal.

Scrambled Transmitters: Scrambled transmitters encrypt the audio signal before it is transmitted, using various methods including the very simple frequency inversion technique, as well as utilizing much more sophisticated methods. If anyone were to intercept a coded signal the speech would be unintelligible. A special receiver is needed to decrypt the signal.

Spread Spectrum Transmitters: Spread spectrum transmission is a fairly sophisticated method of preventing interception of the signal. The RF signal is transmitted on an extremely wide bandwidth. If anyone were to intercept the bugs signal with a wideband receiver, they would hear only an extremely small portion of the transmitted audio. In order to hear the bug's signal one would need several receivers operating simultaneously, each picking up a separate band of audio. A special ultra-wideband receiver is needed to pick up transmissions from this type of bug.

Wideband Transmitters: Similar in operation to the spread spectrum transmitter, this type of device operates on a slightly smaller bandwidth. The signals from this type of bug can be picked up on high-end scanners which have a wide band FM (WFM) mode.

Narrow Band Transmitters: Narrow band transmitters have a smaller bandwidth than ordinary RF transmissions. The signal from this type of bug can be picked up on high-end receivers with a narrow band FM (NFM) mode.

Sliver Band Transmitters: This is an advanced form of bug that transmits the signal over an extremely small bandwidth. A special ultra-narrow band receiver is needed to demodulate the audio signal.

Subcarrier Transmitters: Subcarrier transmitters use an advanced transmission technique to prevent accidental reception and detection of the RF signal. A subcarrier is a type of hidden signal that is modulated piggy-back style on a regular radio signal, both operating on the same frequency. One cannot receive a subcarrier signal with a standard receiver. It takes a special receiver or device connected to a receiver to "strip away" the hidden subcarrier signal. This makes the transmission secure from being received by ordinary persons. One of the problems with sub-carriers is that of inefficiency. The subcarrier is only about 10 percent as strong as the main parent signal. Meaning that it requires a great deal of electric power to transmit a signal of sufficient strength. As a result, the batteries on this type of device usually do not last very long. Most subcarrier bugs are "mains" operated, meaning they operate using household A.C. power. Using utility power, the device has an infinite lifetime and can transmit a much stronger signal. An example of a subcarrier signal is elevator music. This music is transmitted by a regular radio station, on their subcarrier signal. Another example is the closed caption for the hearing impaired on television transmissions. You cannot see the closed caption words because it takes a special subcarrier decoder to demodulate them.

Carrier Current Devices

Carrier current devices are a combination of technologies. They are a cross between wired microphones and subcarrier transmitters. The only difference is that the signal is not transmitted via radio waves, but rather through a wire pair. A person cannot accidentally intercept or detect a carrier current signal by simply tapping into a wire like with wired microphones. A carrier current device works by picking up room audio through a microphone. The signal from the microphone is then modulated by a low frequency circuit which produces a carrier current signal at approximately 100-200kHz. A common example of carrier current devices are the newer wireless telephones, intercoms, or baby monitor type devices that plug into the electric socket and use the pre-existing wiring rather than having wiring run all over the house. A special circuit which can demodulate the low frequency signal is used as the receiver. Carrier current devices require no batteries, as they are powered by the mains. Only a sophisticated receiver with a low frequency probe can detect this sort of device.

Powerline Carrier Current Device: Powerline carrier current devices are usually placed inside of wall outlets and are clipped to the powerline. These types of devices are often pre-packaged inside of wall outlets. All that is necessary is to replace the old wall socket for the "modified" wall socket. The receiver can occasionally be placed at any point along the powerline, but usually it has to be on the same side of the utility company power transformer. This is by far the most common form of carrier current device.

Telephone Line Carrier Current Device: This type of carrier current device is usually pre-packaged inside of modular phone jacks, and then you simply swap the old jack for the new one during the installation process. Telco carrier current devices also can be purchased as separate units that are approximately 1/2 inch in diameter and are clipped onto the phone line with alligator clips.

Piezoelectric Coaxial Microphone: This is perhaps the most ingenious method ever invented for intercepting room audio. Unlike the hidden wired-line method which utilizes a microphone to pick up sounds and then transmits the audio down a set of wires. This device consists of a length of coaxial wire 2-6 feet in length which contains a thin layer of piezoelectric shielding which is sensitive to vibrations produced by sounds. When audio vibrations are detected by the piezoelectric material, an electric audio signal is sent down the cable wire. All one has to do is tap into the coax at any point and the target's room audio can be heard. An agent simply replaces the pre-existing wire for the "special" wire. Even though the audio is quite easily intercepted, this method will escape detection by even the greatest TSCM experts, because very few people know of this method (until now!).

"Bugs come in a variety of sizes ranging from the size of a beeper to slightly smaller than your pinky fingernail."

Infinity Transmitters

This is one of the most diverse and useful pieces of surveillance equipment. It is a room audio monitoring device designed to operate on your telephone line. Unlike a bug that can only receive the signal at a finite distance, the infinity transmitter can work at an infinite distance. The design of this device has varied greatly over the years with the advancement of telephones. The device is placed inside of a telephone jack or a telephone itself, and is connected in series to the line. To operate the device, you call the target's house and before the phone rings once, the infinity device answers the phone. You temporarily activate the device using a touch tone code. This puts the device in a stand-by mode. You then have a brief amount of time to enter an access code consisting of two or three touch tone digits. If the code is correct the device will be activated and an audio path is established. You will hear all of the sounds within a particular room. *Note:* If a person does not enter the correct access code then the device will not activate and calls will go through as normal. Infinity transmitters lost a bit of popularity after telephone companies switched to electronic switching systems. Under crossbar switching systems, telephone lines possessed an audio path between the calling and destination points even if the destination line had not answered the phone.

Hook-Switch Bypass: This is one of the most popular surveillance devices of the past. They are not as useful today, because of the switchover to ESS. The "hot-on-hook" technique involved placing a microphone on the target's telephone line, or shorting out the hangup switch of a phone so that it picked up room audio even when the phone was hung up, and that room audio would be sent down the line. To activate a hot-on-hook device one would call the target's house and enter a touch tone code before the first or second ring. That code would activate a circuit, which would stop the ringing, and activate the microphone, which would send the target's room audio down the line. The surveillance technician could listen to the line without ever being charged for the call, because the phone was never actually answered. However this type is defunct, because nowadays, under ESS, a device cannot be activated on the target's line until the target answers. This is because ESS never actually connects the two line pairs together until the destination line is answered. Modern infinity devices have found ways around this limit, mainly by having a circuit that answers the phone by itself. You can create a simple hot-on-hook device by placing a microphone on the phone line and listening at some point down the line with a high impedance telephone tap.

Dial-Up DTMF Activated: This is similar to the device described above. You can have multiple infinity devices in one house connected to each phone, each using a different activation code. Each device can be switched on at any time during the monitoring process.

Slaves and Loop Extenders

Modular telephone taps, often referred to as a slave unit and loop extenders (LE's) are more advanced models of the infinity transmitters. They utilize various multiple line and dial-out techniques. A slave is generally any device that bridges two lines together by a capacitively coupled circuit.

Dual Line Bridge Slave: A dual line bridge is a simple connection between two wire pairs. The target's line is bridged at some point along the telephone line, such as an entrance bridge, 99 block, junction or splice box, or a cross-connect-cabinet to a pre-existing or leased line specifically ordered for surveillance purposes.

Multi Line Dial-Out Slave Infinity Device: This unit is a slightly more advanced type of device that utilizes two phone lines that are bridged across the line pairs at some point. There are two versions of this type of device. The first is a room monitor that is placed within the target's premises and is either built into the telephone or is hidden in a phone jack. The device is actuated by voices through a VOX circuit, which dials out to the listening post on a second line not used or owned by the target. The second is a telephone monitoring device which can be placed at any point along the telephone line, such as at 99 blocks, entrance bridges, splice boxes, junction boxes, and cross-connect-cabinets. The target's line pair is bridged onto another line usually owned or leased by the surveillance expert. When the target attempts to use his telephone or a call is received, this slave unit automatically dials out on another line to the listening post, which enables the surveillance expert to monitor and record the target's phone calls.

Advanced Dial-Out Slave Infinity Device: A third more advanced type of unit is simply a combination of the above two that incorporates voice infinity and telephone infinity transmission. Units may be a combination of dial out or dial in. Typically the dial out function is for telephone, and the dial in function is for room monitoring.

Remote Listening Post Infinity Device: This is the most advanced and diverse type of slave infinity device that utilizes multiple telephone lines as well as radio receivers, and a built in tape recording unit, which is all microprocessor controlled. This unit is an all-in-one surveillance infinity monitoring system.

Loop Extenders: These devices are too complex to discuss in detail in this brief article.

Telephone Taps and Transmitters

Hardwired Tap: A hardwire tap, which is commonly referred to as wiretapping, is the easiest and oldest form of monitoring telephone conversations. All that is needed is a pair of mono headphones with the jack cut off and replaced with alligator clips, or a lineman's handset (often referred to as a butt set). A phreak might refer to a lineman's handset as a beige box. An individual can tap into a phone line at virtually any place along the line including entrance bridges, 99 blocks, junction boxes, and cross-connect-cabinets. This type of tap is extremely simple and can be performed by even an amateur. If a permanent tap is left in place by running a wire to the listening post, and is too close to the target's residence or office, it could be detected by physical search or with advanced equipment such as TDR's or phone analyzers, if countermeasures sweeps were performed.

Inductive Coupled Line Pick Up: This is virtually the same type of hardwire tap as above, however no direct connection is actually made to the line. An inductive probe is simply clipped around the telephone wire and the emanations from the wire are picked up by the probe. Since no actual electrical contact is made during the tap, not even the most advanced equipment could detect such devices. As with the hardwire tap, if a permanent induction tap is left in place too close to the target's residence or office, a thorough physical search could find the tap.

Series Transmitter: A series transmitter is a bugging type of device that monitors phone conversations instead of room audio. This type of device is connected in series to the phone line and never requires batteries because it draws its power from the phone line itself. The range is not as great with series transmitters as it is with parallels, however its virtually infinite lifetime is an advantage. The frequency and power output of telephone transmitters is virtually the same as for standard room bugs. Series transmitters occasionally incorporate an automatic activation switch which turns the device on only when a telephone conversation is taking place.

Parallel Transmitter: A parallel transmitter hooks to the phone lines in parallel, which enables the transmitter to be simply clipped on without breaking any connections. The power output of parallel telephone transmitters is a bit higher than with series devices usually by 20-50 milliwatts.

However, parallel devices must use their own power source, usually a 1.5-12 volt battery. The frequencies are identical to that of series telephone taps and room bugs. The lifetime of these devices is finite and can only operate constantly for 2-5 days. Higher quality models almost always incorporate an automatic activation circuit which will turn the device on only when the telephone being monitored is in use. This additional circuit extends the lifetime of the tap from three weeks to a month.

Advanced Transmitters: This advanced type of tap is a combination of series and parallel circuits and bridging. When the phone is not in use the parallel circuit "trickle charges" a rechargeable battery. The device contains an automatic activation circuit and when the phone is being monitored by lifting the handset from the base, the series circuit activates and transmits using the self contained battery. This device yields the higher RF output of a series device while having a virtually unlimited battery lifetime similar to a parallel device.

Super Miniature Tape Recorders

Super miniature tape recorders are extremely useful devices for surveillance purposes. They have many uses - primarily recording conversations pertaining to illegal or civil matters, which can be either used as evidence in a court of law or simply to alert law enforcement personnel. Recording devices vary greatly in size, recording quality, as well as other important features. Top of the line models designed and manufactured specifically for surveillance purposes can cost several thousand dollars.

Size Specifications: Super-miniature recorders designed specifically for surveillance are generally much smaller than tape recorders available for consumer purposes. Many of the features available on consumer recorders are not necessary on covert surveillance recorders. Only the most important features are designed into these super small recorders in order to save space. High-level recorders never have built in speakers, since speakers take up a considerable amount of space and serve no purpose on a recorder. In order to play back the recorded media, a separate speaker and amplifier playback unit is used.

Electronic Shut Off: Surveillance recorders almost always incorporate electronic shut off. The mechanical shut off buttons are too bulky, and more importantly make too much noise when the tape automatically is shut off. Should a surveillance recorder ever shut off automatically, the loud click of the mechanical button could make the subject being recorded very suspicious.

Silenced Motors: In typical consumer micro-miniature recorders, the tape drive motors can produce a sufficient amount of unwanted noise. Surveillance recorders contain extremely quiet motors that cannot be heard even in the quietest atmosphere.

Altered Bias Oscillator Frequency: This is perhaps the most advanced feature of surveillance recorders. When recording a subject, every precaution must be made to avoid detection and suspicion. If the person under surveillance is an expert in surveillance or if he is particularly suspicious, then the subject could use a countersurveillance device that detects tape recorders. This anti-bugging device detects the emanations from the bias-oscillator of a tape recorder within a certain range. These devices can detect a tape recorder from up to several feet away. A true surveillance recorder will alter its bias oscillator frequency so that it cannot be detected by the aforementioned countermeasures device, rendering it undetectable. Tape recorders that alter the bias-oscillator frequency must contain special audio compression circuits to compensate for the effects of the altered circuit.

Multitrack Recording: High-end recorders will usually have several tracks for recording. Two tracks are usually for the stereo signal and the third is for time coding or reference signals.

Extended Play: Surveillance recorders often are required to record for extended periods of time. Rather than using longer tapes, the recording speed is slowed down. This results in a bit of distortion, so extended play recorders incorporate compensation circuitry.

Nagra Magnetic Recorders Inc. is the leader in manufacturing surveillance recorders. Their top of the line model is the Nagra JBR, which contains all of the advanced features described. Its dimensions are 110x62x20mm and it weighs 143 grams.

The National RNZ 36 is one of the smallest units ever produced, however it does not contain several advanced features necessary in high security situations. This unit has a 3 hour extended recording time. Its dimensions are 85x54x14mm making it nearly as small as a credit card.

vocals

Worrisome Questions

Dear *2600:*

I need to know a few things about red boxes.

If someone calls their home to check their answering machine using a box and the operator figures it out, calls them at the payphone and tells them that the call is being billed to that number and security is being told and "you know what I'm talking about" (from the operator) does this mean that this person whose home phone was called is going to: 1) have his phone records meticulously checked over from way far back to see where he goes and who he calls, 2) have his travel records checked by tracing credit card purchases, 3) have his email monitored, 4) have a case constructed to charge him with a crime, 5) have the police at his door.

I am also wondering: if a red box is used at a payphone, can all the outgoing numbers that the payphone called be accessed? So if there was a payphone in California that this person used to call his home, would that call appear on a log somewhere and would the phone cops be able to call up on a computer all the times your home phone was called and check the number that was calling?

Susan

Your scenario is a few years ahead of its time. To be honest, nobody really knows how far the phone company and the authorities can and will go in such cases. In the case you mention, the operator would have had to be listening in on the call to know that it was the person's home phone. And that is a far greater offense than red boxing. Can outgoing numbers at a payphone be accessed? Any phone has that capability. But there would be no way to distinguish between calls made with red boxes and calls made with real coins. Unless you stay on the phone for twelve hours long distance and there's only thirty cents in the phone when the telco comes calling. Even the phone company is capable of piecing a puzzle like that together.

Defeating Call Return

Dear *2600:*

I have some advice for the many would-be war dialers out there. In the San Francisco and greater Bay Area they've installed that annoying Call Return function onto the system. Whenever I'm scanning I always get people calling back in the middle of the night screwing up my scan. I've found an easy way to get rid of that problem - use call forwarding. It's easy, rather cheap, and legal. People call and get the number you've forwarded them to, even if the number you are calling from is busy. Usually I go and find a nice payphone in a mall or something, write down the number, and then set that up as the number to be forwarded to. In San Francisco it's simple to program in the number. Using your DTMF phone, type in 72#, then wait for the second dial tone and punch in whatever number you want. This may seem like a piddly thing to do as far as tricks go, but most people don't think about it.

Another easy thing to do is scan at 300 baud with a fax modem. You catch the faxes and the normal carriers and sometimes test tones.

Emperor

*Some parts of the country activate call forwarding with *72. We've found different results from forwarding lines that get *69 (Call Return) sent back to them. Sometimes it doesn't forward at all. Other times, the caller simply gets a reorder. Your scenario is the best, though - it's very easy to convince someone that another person has been calling them.*

Info

Dear *2600:*

In reply to DY from Weston, ONT in the Winter 93-94 issue: The Motorola guide (item #68-093-00a60) can be obtained by calling (800) 331-6456. If that number cannot be reached from your calling area, write to them at Motorola, 600 North U.S. Highway #45, Room DC266, Libertyville, IL 60048. They will happily send you the guide. If you want, just send them a personal check and tell them what you want. They never asked me any questions when I ordered mine.

Quinton McHale
Seneca, IL

Dear *2600:*

The Fax on demand number for Southwestern bell internal news is 314-444-7575 with an info number at 314-331-0160.

WW
Austin

Make sure and read about MEL on page 13.

Dear *2600:*

I trust you have this phone number in your vast files: 212-395-2200. It's NYNEX's employee newswire. It's updated daily, with a mix of interesting and boring telephone related news stories. I believe it's toll-free from within the LATA.

Norm D'Plume
No Fixed Address

More Questions

Dear *2600:*

I just finished reading my first copy of your magazine. I have been hacking around a bit since I got my first 300 baud modem for my TI99 4/A back in 1984. Unfortunately I did not know of your magazine at the time.

I have two questions. Firstly, when I went to college in upstate New York in 1990 we used a very simple method to get free long distance calls. At a payphone in the 518 area code we simply dialed 10000 before the call and they were all free. This worked for a few months and then I guess they caught on. Why did it work and might it work again?

Secondly in your current issue you have an article on software/hardware to decode Cellular Phone traffic. Is there any comparable box/software for a pocket pager/beeper? I know that the system is similar in fact even simpler since it is only one way. I would appreciate any info you may have and I compliment you on a great magazine.

10000 is a carrier access code. Last we checked, it was owned by AT&T. By dialing this code before a call, you were routed through AT&T as if you had dialed normally. Many phone programmers missed blocking this code for some reason, possibly because it doesn't look like a code. But alas, 10000 no longer works at all from our area. There is indeed software to decode pager traffic. We suggest checking out the Universal M-400 Reader or the Universal M-1200 Decoder Card. Each is capable of decoding both POCSAG and GOLAY formats, plus all kinds of other things. Each costs about $400. You can contact Universal Radio at 800-431-3939 or (614) 866-4267.

Privacy Violation

Dear *2600:*

I got a piece of direct mail from AT&T today which has a check you can cash if you switch your long distance carrier to them. The letter goes on to explain how much better they are and tells about TrueVoice and some other lame features.

The short of it: I was *amazed* that my name, address, and *unpublished* phone number (along with the internal 3 digit PIN) appear on this check. I talked to my long distance carrier (Working Assets). They certainly aren't giving out this info. My local phone company claims they won't give it out unless there was some 3rd party bill that could not be collected. I have lived at the said address for only about a year now. I have two phone lines, both with Working Assets and both unpublished. I probably shouldn't be making so much of this but they printed, not my main number but my second number on the check, which has no phone attached to it, just an answering machine from which I run a sort of phone game/art project - all callers are anonymous. My concern, if they can find my name and address with the phone number, then perhaps any number of the sicko callers who play the phone game and threaten to kill me in various explicit ways can also?! Besides, there is a principle involved here... something isn't right. How is AT&T coming up with this info? I called the 800 number in the letter several times and got lots of different answers depending on who I was talking with. Variations included: well, you must have had some dealings with AT&T in the past. Perhaps you accepted a collect call from someone using AT&T, etc. My checkbook shows I have never written a check to AT&T and I'm certain I have never done any business with them at all. Other phone companies suggested that they bought my name and number from a mailing list of a department store or such where I used my credit card... at first I thought this might be possible, but AT&T claims they do not purchase outside lists. Besides the phone number also had the PIN attached. My favorite answer from an AT&T representative was that they own all the phone numbers prior to divestiture and they lease the numbers to other phone companies. My local company is New England Telephone (part of the NYNEX family), so that theory sounds like a pile of #$*& to me (we are not allowed to swear here, the system monitors us).

Anyway, after tying up AT&T's personnel and 800 number for over an hour, I finally got to speak to "Marsha" the executive complaint person.... She took down as much info as we could salvage from the direct mail piece and said she would look into it.

I just want to know whose list I'm on, how I got there, and how I can get off. I can understand AT&T's reluctance to spend a lot of time looking into the matter since they aren't making any money in the process... but since they were nice enough to add me to their mailing list I think they should be nice enough to explain how I got there.

(Trying To Be) Anonymous

Based on what you told us, it appears the culprit is NYNEX. You mentioned a three-digit number that also appeared. This number is used by NYNEX to verify your identity so you can change or disconnect your service by computer. No other company would have this number. Unless, of course, they'd been in touch with NYNEX.

Meetings

Dear *2600:*

I love your stuff guys! The little article about the Digital locks really helped me alot! See, my dad owns a building that uses those, and I finally convinced him that they aren't as safe as he thought! By the way, is there a phone number or e-mail address where I could contact someone who attends the Kansas City *2600* meetings? I'd really like to start attending....

Frank

We don't give out phone numbers but we suggest you simply show up at the right place and time.

Reader Reunion

Dear *2600:*

Recently, I was visiting an alternative clothing, book, magazine and "other" store located in the near north region of Chicago, and happened upon the Spring edition of *2600*.

Many, many, many years ago a friend of mine who is a computer wiz would share issues of *2600* with me that appeared to be hand-typed and xeroxed. I enjoyed reading *2600* a great deal back then - I always would find something of interest and things that would make me pause to think (like *Creative Computing* and *Dr. Dobb's Journal* did before they sold out).

Well, I'm here to tell you that although *2600* has brushed its teeth and combed its hair somewhat, it is the same enjoyable and thought provoking magazine that I remember.

Congratulations for surviving all these years, and thank you for keeping your high standards and focus!

All the best.

Mike

A Strange Number

Dear *2600:*

I was on my phone and was pressing the hang up/flash button on my phone repeatedly while looking up a number in the Yellow Pages and then I let go of the button for about 30 seconds and heard a recording that said "You have reached code 211 NXX in 215 [area code, I think]." and then repeated it. I tried to dial numbers and things like that but to no avail. I'm able to get that recording by the same process but I have not found any information on what this means. Any help you can offer?

John Q Public

You've reached the verification number for that area. You can figure out what you dialed by simply counting the number of times you flashed your switchhook. Three flashes equals the number three, etc. Let us know what the number is - we've been looking for those.

Dear *2600:*

When I was younger, a common phone trick was to dial the number 666-6666 in our area code, 404. When the line answered, it gave a strange series of DTMF tones that kind of played a song. Then, I thought nothing of it. A few weeks ago, I remembered about the number and dialed it again only to find that it has been doing the same thing for all these years. I got curious, so I programmed a war-games type dialer, and called all 404 numbers with the prefix 666, and every one gave me the same thing. I can't seem to figure this out, so could you please help? Is it a BellSouth utility for line-testing, or is it nothing?

Zappy
Atlanta, GA

Sounds like a whole lot of touch tones to us. Readers?

Dear *2600:*

I recently acquired your magazine, and I would like to say I enjoyed it. (Volume 11, Number 2) However, there was a lack of information for the area in which I live, being the San Francisco Bay area. I was wondering if there were any past issues that maybe had some information for my area. For example, "Life under GTD5" doesn't apply to Pac Bell's system. The second question I have is this - I don't know if this would be such a good idea to publish this in your book: I recently found a telephone number - (510) 210-7100. When you dialed up this number you got a connection. It clicked, then gave you a dial tone. From there you could call anywhere you wanted including 976 and 1-900 telephone numbers! Although it would ask for a security code when you tried to call long distance, you could call numbers which normally cost money through Pacific Bell but aren't far enough to go through a long distance carrier. This completely baffled me. Why would this number exist - is it a cheap long distance service?

It was amazing that someone, or some company, would be so stupid as to have this number be completely open with no security and such an easy number to remember. Someone, if they wanted to, could call all kinds of 1-900 services for free, some, by the way, cost over $50 per call! Not that I would do this of course. Well, some time went by, and last time I tried to call it, it only rings and rings. No answer. So my question is what was it, why was it, and where did it go? Are there more numbers like this?

My second issue is law - what are our rights as hackers? A friend of mine brought up the issue that every phone call you make from home is recorded by the phone company. If they see a pattern of calls this could raise certain "red flags" with them. Is this true? Do they have the right to do this? I thought I was allowed to make unlimited phone calls from my home. That is the service I pay for. Is there a law against randomly dialing numbers just for the hell of it? How do they now I'm not a telemarketer or a salesman? Businesses make lots of calls in a day. I would just like a little light shed on this subject - I feel that we have certain constitutional rights that may become jeopardized by the big evil phone companies.

Mr. Asshole

First, we should point out that you insisted on signing your letter that way. As for the number you found, it probably was something a company was using so its employees could make local calls to an extended region as well as long distance calls if they had the proper code. The failure to block 976 and 900 numbers was obviously a big oversight. Concerning randomly dialing numbers, there are many states that forbid such activities, particularly when done by telemarketers. It's not likely they'd make an exception for hackers. Sequential dialing is very easy for the phone companies to detect. Random dialing, however, is not. If nobody complains (and there's little reason anyone should - you're only calling each number once), it's likely you'll have no problems.

Inside Info

Dear *2600:*

Well, I just began the hacking and phreaking stuff last summer when I bought the issue with the red box. It was a real treat because I lived in a very small town on the west coast where the phone system was ancient. The mall phones were a pushover. I also would like to thank you for helping me seek revenge against a local BBS with the help of your ANSI bomb!

Getting to the point here, I recently started work in the office of a very high-ranking official in Washington DC. I won't say who, because as you stated in the spring issue, nothing is secret.

Two things: First, to stand up for the big guys, the e-mail IS read. Not by the actual people, except in special cases. The mail is received and filed just like regular mail and it is given with other letters of the similar subject to one of the L.A.'s (Legislative Assistants). The L.A. then carefully reads the mail, usually responds to it, deals with the issue if it is a request, and/or sums up the general opinion over the issue and presents it to the official.

Second, the computers I am working on have a section of the drive allocated for the network. When I type "cd\" or anything like that, it won't acknowledge. It won't recognize any DOS commands on the allocated drive, but it will on the A: drive (5 1/4). How did they do this? Oh, last thing - I am eager to learn more about this stuff because it really is a thrill when you log in on something you've never been able to before, or find a telephone number that does interesting things - you're right!

Where can I learn about this? I'm not in it to rip off someone's credit account or log in 2500 minutes of free long distance. I'd just like to know *how* these things are done and why they work. Just stuff like that, so I can sit down at my keyboard on a charming night like tonight and hack and phreak away.

Regarding Randy815@Dallas' letter in your spring issue, sending your mag to congressmen is useless. The most annoying thing they get in the mail is magazines because no one has time to read them. Honestly. The best way to get your point across to a congressman is to write a letter and attach a photocopy of the specific article in the issue you want to address. Then send it only to your congressman. If you send it to all of them, they usually don't care because you aren't a constituent of their district and they throw it out. They usually only make the decisions in the best interest of their own districts because bad decisions could hurt them when it comes time for re-election.

King of Spam

It sounds as if the computer you're on is partitioned into different sections. We'd need to know more about the non-DOS part in order to tell you what you can do. Regarding learning, apart from reading, the best way to learn is to make contact with others and share information. This can be a lot harder than it sounds but if you persevere, it will be worth the effort. Good luck.

Strange Situation

Dear *2600:*

Here's the deal: We have two phone lines in our apartment. We had one active for a while and then my roommate got the second line turned on. After she moved out we turned it off. There's a jack in my room which I had checked before and it was my roommate's so I left it alone. Really. But the apartment was wired with standard 2 pair with one line on one pair and the other on the other. I never got around to switching the jack because I didn't care whether I had a phone in my room. Now here's the weird part.

I got my new PC and wanted to hook up my modem. I had forgotten if the phone jack in my room was our line or the turned off line. So I plugged in the phone line and tried dialing. It worked fine. So whenever I dialed out I would warn my roommate not to use the phone. One night I was in my room and was logged onto my Internet account. I spaced out and picked up the cordless and turned it on. I heard my roommate talking on the phone and started freaking out. I went over to my PC, did an ls, a more and some other commands to confirm that I was indeed logged on. I couldn't figure it out. Being a little baked added to my confusion.

It turns out, I have this line I can dial out on and we never get a bill. This has been going on for about three months. I have called BBS's in Europe, Mexico, and all over the U.S. I have been careful to never dial 900 lines because I figure that the billing would draw attention. I only use the line for data because I am too lazy to wire up a phone, although I should.

Another thing I noticed is that I can't disable call waiting. This is probably because the line does not have it. It was something I wondered about back when I thought I was using our regular line. It worked from the kitchen, but when I tried it in my room I got an error message from the phone company.

Can you tell me anything about this? Can I get a huge bill one day from the phone company and be forced to pay it? Are there any other possibilities? I have no idea what phone number I am using either.

Sometimes I sit at my PC logged onto a long distance BBS, look over at my TV, where the cable company didn't shut off the cable in a room where I think I get power for free from a neighboring apartment and I shake my head and wonder how long this can last.

Feasting on technology droppings
Marcus

You called boards all over the planet but not 900 numbers because you didn't want to draw attention to yourself? Odds are the people you've been ripping off (most likely your friendly neighbors powering your PC and modem) got a phone bill that sent them through the roof. In fact, it wouldn't surprise us if you've met them by now. Luckily, you can blame the phone company since they did wire it that way - this kind of thing happens far more often than people realize. But you will get stuck with the bill if and when they figure it out. To find out what your phone number is, dial 10732-1-404-988-9664.

Replies to Readers

Dear *2600:*

Today I read the Summer 1994 issue of your great magazine and saw a few things that interested me. I wanted to reply to some of the letters.

In response to The Roadkill in his letter "Tyranny in Church", I have the perfect utility for you. Forget the others that were posted in "Monitoring Keystrokes" on page 38! I have a TSR that will not only record all the keystrokes in memory, but it also has other features (that some lazy people like me would find useful) like file encryption, a text editor, cut and paste, and some DOS functions. I found it in one of my Government teacher's old computers. Its called Keyworks and the filename is K.EXE. If you have access to internet mail, I am at 15660@ef.gc.maricopa.edu - mail me and I will send you a uuencoded copy of K.EXE. I don't have FTP right now but if someone wants to get it from me and put it on a site, that would be cool.

I also saw the letter "Secrets of a Super Hacker". I have found a store in my area called "Spy Headquarters" and they carried a large selection of "Hacker" and "Anarchy" books. Most were published by Loompanics. I have heard from people on IRC that they have Spy Headquarters stores in their areas as well so other stores might carry these books also. As for JB, I don't think they have Spy Headquarters stores in Belgium.

I was at the store where I usually buy *2600* today and

I started looking for a nice clean non-folded up and non-crumbled up copy of *2600*. To my surprise, *all* of them had been mangled up in some way! And it looked like the printer wrote *over* the creases since there were many crooked columns. Can you guys send me a nicer copy? The one I have is barely readable and I can't find *2600* anywhere else!

By the way, your new FAX number spells 516-ISHCORS (516-474-2677). It could even spell 516-IRIBOPS (whichever makes you laugh more). When I saw the thing on page 45, I *had* to reply.

Da Phigzter

We can't replace copies that were mangled at the newsstand. But we do replace defective copies that our subscribers get. If there's a problem with an issue that you bought in a store, return it to them and get a replacement or a refund. And let us know if issues in that location continue to be mangled.

Dear *2600:*

I got my Summer edition pretty late but loved every page! I had a couple of comments about two of your letters.

In "A Busy Connection" by Reuben (Page 24), he brings up the usage of the XXX-9970 numbers on NYNEX. Well, you said to let you know about any other parts of the country with this. From the 913 AC, I got something. I tried three local prefixes 539, 537, and 776. 539 and 537 both gave me the described busy tone and the clicks - *but* the 776 prefix rang three times, gave the "thank you" bitch that comes on when you call from a pay phone (which I didn't) and then beeped four DTMF tones at me (which I was unable to decipher since I haven't had time to build the one on page 32).

Second, I'd like to make a comment in reply to sciri's article (page 29) about there being too many lamers in his area. Lighten up, man, we were all lame at one time or another. Hell, I *still* do lame things from time to time. I think it's just a stage that everybody has to go through.

I admit it's sometimes hard to deal with all the newbies from AOL on alt.2600 (my kill file is huge), but I think what you *2600* guys said hits the nail on the head. Teach a lame hacker not to be lame once in a while - don't be cockey about it - just help, even if it's only giving him a pointer to a FAQ. It takes a little extra time, but it'll be worth it. Just think, there are going to be *millions* of newbies flooding the Internet in the next year - and they're not going to go away. So try to show them how to do it right. Otherwise, 75 percent of future bandwidth is going to be newbie flame. Sheez, what a waste.

.gKo.

We cannot get through to your 537 and 539 exchanges at all. We suspect they're non-working exchanges and every number in them probably gives you the same thing if you're within the area code. Regarding the "thank you" lady, you have reached a COCOT, which is why it sounded familiar to you. We have yet to hear exactly what she's waiting for you to do or why she's thanking you.

Cordless Clarification

Dear *2600:*

In your Summer 94 issue an article, "Cordless Fun" by NYMPHO said that it was legal to "drive around in your car and tape people's cordless conversations." Both you and I know this is not so. Federal Law is quite vague in this matter: "It is a crime under federal law for any person... to wiretap or otherwise intercept a telephone call...". Please inform the readership before someone goes off and tapes a phone call and plays it in public. If there is a loophole to this law that I'm not aware oflet me know, but I'm fairly certain there is not. I would hate to hear of a naive individual charged with wiretapping after reading in *2600* magazine that it was legal.

Gladshiem

The article stated correctly that there is no law against monitoring or taping a cordless phone call - such calls are considered to be radio transmissions, therefore, "wiretapping" doesn't apply. They are not protected in any way. Cellular calls, while just as easy to listen in on, are protected by a law that merely says they're protected by law. Get the picture?

Mac Hacks

Dear *2600:*

The letter by Deus, The Black Night, etc. talks about a long way around "AtEase". If the school has Think Pascal or Think C (any Think class software) just go to the "Transfer" option in the file menu, and open "Finder" in the system folder. A little faster, and you can jump back into AtEase if a teacher shows up. Also "DisEase" by Josh Horan is another easy way to get past AtEase.

Second, FileGuard cannot be turned off by turning off the extensions with the shift key down! The only hack I know for FileGuard is called "An INIT's Best Friend" and "Airplane" (they work together). They work well and fast.

Lastly, "DisEase", "An INIT's Best Friend", and "Airplane" can be found any where, even on AOL!

Xausii

Dear *2600:*

I need to respond to "The Bard" who wrote "High School Mac Hack" that appeared on page 15 of the Winter 93-94 issue. The article is filled with too many inaccuracies to allow me to let it slide by.

Mr. Bard claims that AppleShare is hard to hack. Considering that AppleShare is a control panel in the System Folder and is only hackable from a hex editor then yes, I would agree. AppleShare is hard to hack. However if what he meant to say, and by his article I think he meant to say, AppleTalk is hard to hack then I must disagree.

Mr. Bard suggests that you could write a program to simulate a Mac interface to get user passwords - that is a helluva long way to go about it. A simple control panel placed in the System Folder to capture keystrokes would work fine. I know of two that have already been written.

Mr. Bard says that you should "make an Alias of his Appleshare, and copy to disk. Then... go back to the computer he used and open the Alias AppleShare." This is pointless, not to mention that it will not work. If you are going back to the same computer, why not just open the original as opposed to the Alias? The Bard says the disk might be locked, in which case you couldn't make an alias anyway. Even if you could, the alias on the floppy can't point to a locked disk. (Oh, you can unlock a disk by selecting it and hitting Command-I.)

If you have access to the target machine as Mr. Bard's previous example required, then just create your own damn account. Go to the Users and Groups Control Panel and create away. Using Norton Utilities to find hidden password files as Mr. Bard suggests is also useless as the passwords are written in hex inside one of the AppleTalk Control Panels. He would have better luck with ResEdit.

If your machine has Empower, DiskLock, FileGuard, or even wimpy ole AtEase, good luck. These are all passable - they just require a little more work and poking around with and each deserve their own article.

Just remember that AppleTalk is a very insecure protocol. It is peer to peer and not really meant for large networks. Most of the stuff in this letter can be found in any Apple Manual that comes with every Macintosh. May I suggest that Mr. Bard find one and read it.

Space Rogue (617)
RDT Syndicate

Sick ATM's

Dear *2600:*

I was in Soho, London one night where I seem to spend most of my nights guzzling coffee, etc. I went to my usual cashpoint (ATM) at a branch of Barclays Bank. There are two machines side by side. The first was as usual, I stuck my card in, got my cash. I noticed the machine next to me was not all it should be. I assumed at first it was in "Sorry can't give out your cash!" mode, but on closer inspection I noticed something odd.

The machine had apparently crashed. It was in "Diagnostic" Mode. The screen displayed the letters A thru F aligned to the top 6 of the 8 buttons to the side of the screen, used for "Fast Cash", receipt request, whatever. There was a message at the bottom of the screen along the lines of, "Enter engineer clearance code" and a prompt ">". After a bit of pissing about I deduced that it was expecting a 4 digit Hex code, followed by "Enter" to allow you to get to the nitty gritty of testing the note dispensing mechanism over and over again. Given that I only had a few minutes before I was due elsewhere, I had little time to have a stab at the possible 65,536 combinations, but here's to dreaming. Presumably each machine's code is different, maybe it is written on the inside? Keep your eyes pealed next time you're in a bank and the machine is being filled!

Lowdown on LoJack

Dear *2600:*

Reference the letter titled "Car Tracking" on page 25 of your Summer issue, the author, "Tommy B." doesn't know what he's talking about.

His letter was full of paranoia which - while technically feasible by some tracking systems - will *not* work with LoJack. Contrary to what he said, LoJack uses a VHF (173 MHz) frequency, *not* 900MHz. Once activated, the LoJack units send out a signal giving a serial number of the unit (which shows up on the special LoJack receivers/RDF gear some police cars are equipped with). This serial number is then entered into the law enforcement computer network (statewide or perhaps NCIC) which will then return with a description of the vehicle, so the police will know what to look for while homing in on the signal. The range of this transponder is just a few miles at best (depending on terrain, etc.).

Now some of the other tracking systems, such as Teletrac, do use a 900 MHz, spread-spectrum radio link, and can be interfaced into things like the vehicle's ignition system (when the police close in, they can request that Teletrac send a signal to the car, having the ignition disabled, in order to prevent a car chase). There is also the capability for two-way voice communications between the vehicle and Teletrac's regional operations center - you can manually activate your Teletrac transponder, for example, selecting the "Tow truck" depiction will alert the Teletrac Ops center that you're having a non-emergency problem, and they can then initiate two-way voice contact with you to get info on the specific problem, which they can then pass to the wrecker service.

These high-tech systems only provide coverage in certain areas, and should prove beneficial to many people. There's a simple way to alleviate Tommy B.'s paranoid fears - don't sign up for the service! If Tommy B. is driving around in a Porsche or Lamborghini and his insurance agent "forces" him to get a vehicle tracking system installed, either just go with the relatively primitive LoJack system, or use a secondary vehicle when you'd rather keep your whereabouts unknown (but be sure to keep your cellular phone off, too!).

Like with most pieces of technology, there can be some vulnerabilities or disadvantages as well as advantages. But Tommy B. should try to have some factual knowledge before he decides to fear something, if for no other reason than to be able to alert people, instead of misinforming them.

Just because Tommy B. is paranoid, it doesn't mean that people *aren't* out to get him! Just the other day, I was watching Tommy's car using a Keyhole satellite I hacked into, and I clearly saw him blow through a red light at 60 mph!

CARTWHEEL

Still More Questions

Dear *2600:*

I have been a subscriber to your magazine for a few years. Overall, I have enjoyed your magazine and its many interesting articles! Keep up the good work!

I am, however, confused by the painting on the front cover of the Spring 1994 issue (Volume Eleven Number One). There does not seem to be a theme or meaning to the painting.

What is the purpose of the space suit? What do Babylon and Middle Island have to do with each other?

What is the number 17 that is prominent in what appears to be a green highway type of sign? What is the number that is on the sheet of paper behind the head of the person who is emptying the trash can full of passwords? I tried it on my phone and I get an intercept saying that the number is not valid.

The little doors in the background on the right, along with the dark figures are confusing. Is that supposed to be a public restroom in a park? Are the two figures in front of the door marked daemons supposed to be two homosexual men groping each other?

And finally, is that supposed to be a birthday cake in the foreground? If so, does it mean that this issue is the 10th anniversary issue?

Please enlighten us!

Clear Plastic Raincoat from Seattle

Space suits offer protection from vacuums. Babylon's elevation is only 15 feet whereas Middle Island's is 76. Highway 17 bypasses the New York State Thruway and offers a more scenic view. The number behind the head will get you nothing but trouble. We strongly believe in public restrooms. And once you recognize the two people in front of the door, their intentions should be very obvious. The "cake" you refer to is a spaceship with ten candles on it - at least that's how we remember it. The fact that it's our tenth anniversary is completely irrelevant. We hope we've been helpful.

Now what the hell is "Clear Plastic Raincoat from Seattle" supposed to mean?

On Piracy

Dear *2600:*

I think you people have a fabulous operation at *2600.* This publication got me started in hacking years ago when I was a youth.

I'd like to respond to Roberto Verzola's views in his article "Software Piracy: Another View."

Roberto takes the point of view as an opposite to the business interests invested in software development. He equates copies of programs to units of money.

In my view, software piracy is so vital to the software industry that without it, there would be no hit programs like Word or Lotus. Each piece of software gets its start as a beta copy. For every programmer who has a beta copy, fifty pirates have access to it via networks and the local BBS. When it its earliest stage, software is very dependent on word-of-mouth advertising. Unreleased software has no hype.

The many pirates who nab beta copies are interested in their newness. 0day WaRez are the most valuable and last for maybe a week on the pirate market. If it's a nice product, the pirates give it good reviews. If not, the beta copy is purged to conserve valuable disk space.

If the beta does well in the pirate circles, the pirates won't purchase them. But others will due to the word of mouth initiated by the pirate underground.

Another point of view Roberto seems to have missed is the pre-professional software user. As an art major at Stanford, my Mac at home is chuck full of pirate copies of graphic design software. Warez so expensive I could either pay my school tuition or buy them at the store. Yes, the software industry relies on pirates like me as well.

As I learn design in school, I need to practice on my own equipment, doing hobby type design: flyers, logos, dance tickets. All amateur work and no money involved - pure learning. When I start up a design profession, I will buy the software I have tried and tested for years.

SM
Morgan Hill, CA

On Honesty

Dear *2600:*

I am writing in regard to your article "How To Hack Honesty" as published in the Autumn 1993 issue. Some years ago, under an assumed name, I wrote *How To Beat Honesty Tests* as published by Loompanics Unlimited. In the course of researching this booklet, I took up an animated correspondence with Dr. Philip Ash, who was the chief designer of honesty tests at London House; I know he also developed an in-house test used by Supermarkets General Corporation and he probably designed other such tests as well. I asked him about "faking good" - and the actual terminology used by test constructors - and he told me that virtually all psychological tests are devised and normed with certain assumptions in mind. In the case of honesty tests, paramount among these is the assumption that everyone has at least a little larceny in his or her heart and that everyone has borrowed, misappropriated, or otherwise stolen something, somewhere along the line. Admitting to small thefts of things such as pencils or paper clips is good and feeling bad or guilty about these minor thefts reinforces your "honesty" when taking these tests. Questions your article designated as "control questions" do not ascertain whether you are "faking good" but make you more open to taking the test, convincing the gullible that there really is something magical about them. In actual practice, control questions can be even more innocuous than U.R. Source indicates ("Do you like animals?" has been seen on at least one form of the Reid Report). Ash himself defended their use.

Pencil and paper honesty tests do take the place of the polygraph in many cases at lower cost, but usually with no greater accuracy. One item Source's article fails to mention is that in trying to be all things to all people, honesty tests fail miserably at everything. One test claims to identify people who are more accident prone than average while also ferreting out those most likely to abuse workman's compensation claims! Dr. Ash also told me something interesting. If you are the most honest person possible, to the point that you have never stolen anything, and you are perfectly honest about it on the Reid report, you will fail because the test assumes you are faking good. Our society is test happy and we seem to like to quantify even the unquantifiable, such as one's honesty. It has come to this. Fret not, though. While polygraphs are illegal employment screening tools everywhere in the United States and Canada, the honesty test may be going the same route. Already in the Commonwealth of Massachusetts and the Province of Ontario, they are illegal in all applications. Similar legislation is pending in Rhode Island and in New York State they are still legal but cannot include any questions regarding substance abuse and the test results cannot be the "primary" reason for denying someone employment.

A.R. Weeks
New York, NY

Northern Hacking

Dear *2600:*

I am a new subscriber to *2600*. The back issues I requested came in a few days ago. I read every issue in a single sitting. The zine blew my mind. *2600* is phat! Since I am a new member to the hack/phreak community, I find some concepts in your magazine hard to understand. I've tried calling local boards, but the only users are kids addicted to MUDs. Because I'm a 16 year old kid living in a little Canadian hick town called Medicine Hat (dumb name, eh) with nobody to answer my questions, I decided to use our phucked up postal system to write to you guys. Now, onto the questions:

What the hell is a PBX and how do I find an access number into one? How do I find an authorization code for a PBX once I access one and what do I do with it? I'd like to get onto some LD boards, but I don't want to pay the high LD charges. I know you don't tell people to commit toll fraud, but you do tell how to. How would someone like me get toll-free planetwide calls? Your contributors write about how they get on computer systems. I live near an army base and I know they have a computer system. How do I access the computers? Do I just phone up the number in the phone book (403-544-4000) or what?

My telephone company is AGT but most of the equipment is made by Northern Telecom. My area code is 403 and an engineer at AGT told me that my province is the first completely digital telephone system in Canada. I'm wondering if you have any info on how I can have fun with my phone system?

DrP
Medicine Hat, Alberta

PBX stands for Private Branch eXchange and it's basically a phone system run by and for a company. Oftentimes, security lapses allow people on the outside to access dialtones, voice mail, computers, etc. On many occasions, these are reachable through 800 numbers. Methods of making free phone calls abound here and in many other places. But that doesn't mean it's a particularly smart thing to do. We understand how difficult it must be for you trapped in the middle of nowhere but you do have to be careful. Your "completely digital telephone system" could easily monitor your activities. Learning and exploration should be your primary goals, not **just** *getting things for free. Unfortunately, it's sometimes unavoidable to commit crimes, however small, in the process. You need to weigh the risks and decide what your priorities are. We don't suggest messing with your local military computer, at least not for starters. If there is a college in your area, do everything you can to get on the net. If you succeed, you will have eliminated the long distance charges and opened yourself up to an unlimited world of knowledge and contacts. We wish you luck. And don't give up on Medicine Hat - there are probably other hackers there too.*

Satellite Mystery

Dear *2600:*

This is the first time I have seen your very informative magazine. I was surprised to see it in my local Barnes and Nobles, right next to the other computer magazines.

The question I have is, most of the food stores around here have satellite dishes on the roof for whatever reason. Someone told me that they are for the checkout ATM machines. I was wondering if that is true. If I was to hook up that DTMF board (mentioned in your summer issue) to the satellite lead would I be able to get ATM account numbers and the pin numbers?

Alcatraz
Pt. Pleasant Beach, NJ

ATM's almost always use dedicated phone lines to transmit data - banks tend to be a bit sensitive about that kind of thing. The dishes you see are, in all probability, receivers for whatever music they wind up playing for the enjoyment of their customers. Sorry to disappoint you.

Red Light Cameras

Dear *2600:*

I'd like to give all you people in New York a little easier sleep. The "Facts" page of the summer issue listed a problem that we had here in California for a short time - machines that took pictures of a speeder's license plate (or for you a red-light-runner). Here's my advice: *Don't do a thing!* It will go away by itself. If anybody gets a moving violation, they have to sign it, saying that they will show up in court and answer to the charges. No big deal. But if anyone gets a ticket in the mail (assuming that the address listed with the DMV is still correct), consider this: did they ever sign anything saying that they would show up in court to defend themselves? *No!* That's what happened in Los Gatos, CA a couple of years ago. A man was arrested on a warrant for failure to appear on a mailed ticket. The case was thrown out of court, the CHP got a reprimand and were ordered to remove from service their millions of dollars of equipment they had just bought. In addition, the man won a civil suit (undisclosed amount) for false arrest and wrongful imprisonment. If it happened here, it will happen there. So have fun, run the lights, ignore the tickets, and get some money out of it.

An Unprintable Symbol

It's the American dream.

Security Concerns

Dear *2600:*

I remember reading a few issues back you stated that the official *2600* subscriber mailing list was secure and would not be shared with any other parties. However, is it true that the post office (and/or some other government agencies) is recording the name and destination address of every issue of *2600* that is being sent out? And the simple fact that both you and I believe in true

(continued on page 42)

LIVING ON THE FRONT LINE

(gathered from internet posts)

On July 6, at slightly after 2 am local time (PDT, 7 hours west of UTC), an intruder installed a TCP/IP-sniffing daemon on one of the machines at a2i communications (domain rahul.net). The sniffer was discovered and disabled on the evening of the same day, about 18 hours later. During this time, the daemon collected data including passwords.

Here is a summary of the intruder's tracks discovered in combination on the hosts bolero.rahul.net [192.160.13.1] and jive.rahul.net [192.160.13.2]. Both are SPARC machines running SunOS 4.1.3.

1. A number of setuid-root programs, which would instantly yield a root shell when executed. We found these with the command:

```
find / -fstype nfs -prune -o -perm -04000 -print
```

2. Processes, one listening on UDP port 891, another listening on UDP port 937. We could detect this bound ports with the 'lsof' program.

3. A daemon that monitored the '/dev/nit' device, keeping the Ethernet interface le0 in promiscuous mode, and recorded the first few bytes of each telnet, ftp, and rlogin session, apparently to collect passwords. Output was collected in a log file. We could detect the promiscuous mode of le0 with the command '/usr/etc/ifconfig le0', which printed information similar to this:

```
le0: flags=163<UP,BROADCAST,NOTRAILERS,
RUNNING,PROMISC>
```

4. A daemon listening on TCP port 3011 which would accept a connection (no password needed) and immediately provide a root shell. The intruder could later connect to this port and use the root shell to collect the contents of the log file. We could detect these bound port with the 'lsof' program.

5. We were able to monitor the local network and observe incoming connections to port 3011 from the following hosts:

```
joe.me.uiuc.edu 7:05 pm PDT July 6
athena.brynmawr.edu 6:54 am PDT July 8
```

We believe that during the connection at 7:05 pm on July 6 from joe.me.uiuc.edu the intruder was able to collect the contents of the log file. The connection attempt at 6:54 am on July 8 was benign, because the intruder's processes were no longer active.

From the log file collected by the intruder's daemon, we have made a list of potentially affected hosts and it is given below. A numeric IP address indicates failure of the SunOS 4.1.3 gethostbyaddr routine to resolve the name – this usually means that either reverse resolution failed, or that reverse resolution yielded a name that could not be resolved back to the original IP address.

A quick script has been used to filter out from the log file entries for ftp sessions in which the target user was 'anonymous' or 'ftp', and entries for connections not involving any host external to our network. All other host names recorded by the sniffer are included in this list. Site administrators at all these hosts are advised to search their systems for possible intrusions. They should assume that if their users accessed a2i, or if any a2i user accessed their site, a password might have been logged. We are mailing a warning message to postmaster at each affected host. The message includes specific entries found for that host in the intruder's log.

A script was run to attempt to telnet to port 3011 on each host in the attached list, attempting to find out if a similar intrusion was in progress anywhere. No active port 3011 was reached on any of these hosts. There is, however, no guarantee that the intruder will always use port 3011.

All sites should look at their logs and search for connections to and from the domain rahul.net and/or from any host on the network 192.160.13.0, at any time before approximately 11:00 pm July 6. All cleartext paswords used in such sessions should be considered suspect.

For safety, it may be wise to assume that any password transmitted during the last 8 weeks has been compromised – since it cannot be guaranteed that previous undetected intrusions did not happen.

It is not yet clear by which mechanism the intruder gained access.

The general format of the intruder's log is shown below.

```
===== begin sample log entry =====
- TCP/IP LOG - TM: Wed Jul 6 03:47:55 -
PATH: name.of.source.host(source_port) =>
name.of.destination.host(dest_port)
STAT: Wed Jul 6 03:48:34, 48 pkts, 128
bytes [DATA LIMIT]
DATA: < data bytes here >
 : < data bytes here >
 : ...
 : < data bytes here >
===== end sample log entry =====
```

LIST OF POTENTIALLY COMPROMISED HOSTS
(POSTMASTER AT EACH SITE – PLEASE CHECK YOUR INCOMING MAIL)

```
079a1.phy.ohiou.edu
129.108.1.10
129.198.2.40
129.71.44.224
130.99.32.69
131.128.123.13
131.241.16.4
134.53.8.55
138.119.20.47
138.13.16.203
138.43.160.87
140.175.7.143
144.26.45.1
146.68.173.106
147.160.30.23
155.16.192.32
156.98.25.50
158.234.18.74
158.234.24.60
```

```
165.113.242.2
165.173.38.9
192.204.164.33
192.84.232.107
193.227.31.2
198.147.181.1
198.211.41.35
198.62.89.50
198.78.71.51
199.182.70.2
199.8.30.50
ACC.WUACC.EDU
ACF6.ACF.NYU.EDU
ACUVAX.ACU.EDU
BLOOM-PICAYUNE.MIT.EDU
BUDZICHO.NAVSSES.NAVY.MIL
C208BN21.sunydutchess.edu
CORNELLC.CIT.CORNELL.EDU
CSA.BU.EDU
DEPAUW.EDU
GOPHER.UPENN.EDU
HDSF17.Houston.WIRELINE.SLB.COM
Joyce-Perkins.tenet.edu
LIB.IS.TCU.EDU
LibL19.LIBRARY.ColoState.EDU
MILANESE.MIT.EDU
MOSS3.TAMU.EDU
NIC.DDN.MIL
NTP-MASTER.ALMADEN.IBM.COM
Ruth.Butler.EDU
SALLIB.SALS.EDU
SUMEX-AIM.Stanford.EDU
SVAPPL04.MDC.COM
Sony.COM
Sun.COM
VAX.DICKINSON.EDU
VULCAN.LIBRARY.CMU.EDU
a100.ucs.usl.edu
acad.drake.edu
access1.digex.net
acs1.byu.edu
aed.pica.army.mil
amazon.csc.liv.ac.uk
ampere.mee.tcd.ie
anlnpb.ep.anl.gov
annex1.net.ubc.ca
antares.tymnet.com
awesome.hq.Verdix.COM
bart.starnet.com
blue.weeg.uiowa.edu
bode.ee.ualberta.ca
bodie.cs.unc.edu
brahms.udel.edu
bruno.cs.colorado.edu
btissue.chem.vt.edu
bubble.yonsei.ac.kr
buffalo.ny.ts.psi.net
cabell.vcu.edu
calamari.storage.tandem.com
caliph.intellicorp.com
camelot.acf-lab.alaska.edu
canyon.ATMOS.ColoState.EDU
carson.u.washington.edu
cathy.ijs.si
cbunnell.lerc.nasa.gov
central.co.nz
chameleon.cc.metu.edu.tr
cirrus.com
clark.net
clevxd.CPL.ORG
copernicus.isi.com
crl4.crl.com
crl5.crl.com
csl.biosci.Arizona.EDU
csws15.ic.sunysb.edu
csws2.ic.sunysb.edu
cube.clas.suffolk.edu
cuplvx.ap.columbia.edu
dandelion.com
dante.NMSU.Edu
default52.usa.cerfnet.com
dns.global.com
dorfsr.b17d.ingr.com
dorsai.dorsai.org
dracman.cray.com
dschmit.wa.ATK.COM
dunlop.cs.ucdavis.edu
dutikos.twi.tudelft.nl
echonyc.com
ecoli.harvard.edu
elf1.Stanford.EDU
enterprise.america.com
forsythe.Stanford.EDU
ftp.iitb.fhg.de
ftp.technion.ac.il
ftpserv.c-cube.com
garnet.Berkeley.EDU
gatekeeper.qualix.com
gemsgw.med.ge.com
gomez.intel.com
gpu.srv.ualberta.ca
grind.isca.uiowa.edu
grumpy.usu.edu
gryps1.rz.uni-greifswald.de
gucis.cit.gu.edu.au
gw1.octel.com
halon.sybase.com
hestia.arc.nasa.gov
host0.colby.edu
howe.cs.ucdavis.edu
hpcea.ce.hp.com
ibm.com
ics.soe.umich.edu
igw.merck.com
infoserv.utdallas.edu
ingate.microsoft.com
isr.harvard.edu
jarthur.cs.hmc.edu
jfrank.jfrank.com
jmch.demon.co.uk
jobe.shell.portal.com
k2cc.sos.clarkson.edu
kafka.network.com
kelly.teleport.com
kublib.kub.nl
kwilkins.NPD.Provo.Novell.COM
kwme6.nerc-keyworth.ac.uk
leif.ucs.mun.ca
leo.nmc.edu
lfs.cyf-kr.edu.pl
library.wustl.edu
llwhro.whro-pbs.org
luciano.ee.adfa.oz.au
m205b.cc.uch.gr
mac-nincehelser.tri.sbc.com
maelstrom-ether.Berkeley.EDU
maestro.maestro.com
maggie.jpl.nasa.gov
magma.com
mail.evansville.edu
mail.infinet.com
mars.dcs.fmph.uniba.sk
marsh.cacs.usl.edu
math.uwaterloo.ca
medusa.gs.gov.bc.ca
milpitas.adaptec.com
moab.me.iastate.edu
monk.fel.duke.edu
mri-gw.mri.com
ncb.gov.sg
nessie.cc.wwu.edu
netcom.netcom.com
netcom11.netcom.com
netcom12.netcom.com
netcom2.netcom.com
netcom3.netcom.com
netcom4.netcom.com
netcom7.netcom.com
netcom8.netcom.com
netcom9.netcom.com
netmail.microsoft.com
newt.com
nic.funet.fi
nic.uakom.sk
ninja.jp.borland.com
nowaksg.chem.nd.edu
ns.bmd.SAIC.COM
nx44.mik.uky.edu
ocean.ocean.com
ohstpx.mps.ohio-state.edu
orion.sil.nrc.ca
osage.den.mmc.com
oven.ccds.charlotte.nc.us
panix.com
parry.lance.colostate.edu
pc-78-73.ipxrarp.Virginia.EDU
pdavispc1.uk.mdis.com
phobia.phys.lsu.edu
phscpc1.ucs.uoknor.edu
picard.infonet.net
pinchy.micro.umn.edu
pirx.cs.purdue.edu
port4.buffalo.ny.pub-ip.psi.net
psulias.psu.edu
psulib.cc.pdx.edu
pure3.pure.com
pv022c.vincent.iastate.edu
quad4.phx.mcd.mot.com
quip.eecs.umich.edu
rcasciel.beva.blacksburg.va.us
renegade.lerc.nasa.gov
rhoda.fordham.edu
ring28.cs.utsa.edu
risc.ce.utep.edu
rkadw1.ple.af.mil
sabre.afit.af.mil
sandcastle.cosc.BrockU.CA
sauza.math.lsa.umich.edu
scooby.bme.ri.ccf.org
sequoia.northcoast.com
server.netcom.com
sescva.esc.edu
sgigate.SGI.COM
slip1-17.acs.ohio-state.edu
slon.labs.BrockU.CA
sluava.slu.edu
smartva2.svi.org
solomon.technet.sg
sowebo.charm.net
sparc5.sunbim.be
spectrum.xerox.com
starbase.NeoSoft.COM
sugar.NeoSoft.COM
sunset.ma.huji.ac.il
sv05wld.wldelft.nl
swootton2.NSD.Provo.Novell.COM
teacups.San-Jose.ate.slb.com
telesciences.com
thorin.uthscsa.edu
tigger.StCloud.MSUS.EDU
tollbooth.vnet.ibm.com
trump.cts.com
twnmoe10.edu.tw
ubvmsa.cc.buffalo.edu
uhunix.uhcc.Hawaii.Edu
ukanaix.cc.ukans.edu
ulinf0.unil.ch
unbvm1.csd.unb.ca
unidui.uni-duisburg.de
univax.fhda.edu
unknown-pc-28.bf.umich.edu
upr1.UPR.CLU.EDU
ursula.ucdavis.edu
utsw.swmed.edu
uxa.cso.uiuc.edu
v5119.tvrl.lth.se
vax.sonoma.edu
vector.ucsb.edu
vixen.cso.uiuc.edu
vm2.cis.pitt.edu
vms.huji.ac.il
vmsb.is.csupomona.edu
watt.engin.umich.edu
wcarchive.cdrom.com
welch.ncd.com
worf.qntm.com
wuarchive.wustl.edu
www0.cern.ch
zeus.apsu.edu
```

"If someone's hacked our system, we'd certainly like to know about it, although it's very doubtful; more likely, this is just someone trying to make you nervous" - Netcom admin, *2600*, Summer 1994

Date: Wed, 13 Jul 94 18:22:12 PDT
Subject: Hacker Break In CERT#12804
Status: R

Hi;

We were one of many systems that was attacked this past weekend. Unfortunatly my system was compromised. The attached is a description of the Hackers dirty work and a suggested plan to try to prevent future attacks. I am sharing this because it is amazing how everyone seems to clam up if they are attacked and/or broken into. It of course hurts the 'professional' pride to be hacked, but the only way to stop this is to spread the information. The 'head in the sand' reactions are not going to make this problem go away. This particular hack used several 'textbook' methods to try to break in and it still worked, suprisingly enough an d suprisingly well. I am running a Sun and PC network with a PPP link to the internet. Hope this can help somebody else not get caught unprepared.

Subject: Response to the Hacker attack of July 8th-11th 1994.

Synopsis of the Break in:

On Friday July 8th 1994 at 23:09, an incoming mail message was received by IRT's mail server. The message came in from Netcom (machine: netcom11.netcom.com). This message was carrying a shell script which exploited a security hole in the 'sendmail' program. THe mail was interpreted and run by the 'sendmail' program. The script copied source code contained within itself into the '/tmp' directory and using standard UNIX commands compiled and started a daemon process on Port number 7002. An outsider telneting in to this port would have bypassed all logins and logging facilities. Netcom alerted IRT on July 11th at 16:13 that IRT had possibly been compromised. Upon checking, I discovered the daemon running on our system. According to Netcom's log we had been telneted to from their system at 23:13 on July 8th. The record shows it was at most 4 minutes before the offending session was ended. This is the last recorded information available. Once the port was established we were accessible to anyone who knew about the port and we could have been visited again from anywhere without any record.

The daemon source code was found in the mail queue and removed for analysis. The process was killed and removed from the '/tmp' directory. We were **disconnected from** the Internet and a search **was made to see if** any traces could be found. On Tuesday July 12th at 11:59, three(3) files appeared on the system. In the '/'(root) directory a file of zero size appeared with the name "1776_July_4" at the same time two zero size files appeared in the '/tmp' directory. The file names were "tmp.7105.foo" and "tmp.7105.bar". The time stamps and file names ending in "foo" and "bar"(a well known acronym) are very suspect. No further strange occurances have surfaced. Netcom has not been able to provide anymore information on the hacker. They report he hacked into an account on their system and was able to work undetected for an unknown period of time. Netcom was alerted by complaints from System Administrators who detected the break in attempts.

What Failed:

- Sendmail was thought to be patched and wasn't.
- The security package(COPS) I ran did not have checks to alert for this problem with sendmail.
- PPP packet filtering created a false sense of security. Running a high level of filtering was not enough.

Recommended Actions:

All users must be forced to change their passwords. In the future, any accounts with passwords that can be broken will be disabled and the user will need to see administrator to have it re-enabled. It was also recommended that the whole OS be reinstalled from scratch if you are comprimised.

Sendmail needs patching with the latest software patch from Sun Microsystems(Sendmail Jumbo Patch #100377-15) or Upgrade to version 8. Sendmail also needs to be set up to use a restricted shell(SMRSH) that was obtained from the Computer Emergency Response Team(CERT) ftp site. In addition, obtain the following programs for installation to try and thwart future attempts to break in:

tcp_wrapper - Package to monitor and filter incoming requests for variety of services. (info.cert.org)

tripwire - A tool for monitoring a designated set of files for and directories for changes and/or corruption. (info.cert.org)

securelib - Tool to control access to network daemons not under inetd control or which serve more than one client. (eecs.nwu.edu /pub/securelib.tar, securelib.ps)

netlog - A tool to passively watch all TCP and UDP traffic on a network. (net.tamu.edu: /pub/security/TAMU/) Also look at TIGER(COPS like program)

swatch - A process to watch the log files **in real time and associate arbitrary actions with patterns. (sierra.stanfor.edu: /pub/sources)**

crack - A program to try to crack passwords.(info.cert.org)

Recent reports indicate that Netcom's credit file, stored online and containing information on all their customers, has been compromised.

news items

You wouldn't know it walking around in the streets and malls but our nation is facing an incredible crisis. Phone numbers are running out faster than anyone expected. New area codes are being created almost weekly. And, in what is bound to be a first, one area code is on the verge of exhausting its supply of numbers before anyone has even used it. According to Bellcore, exchanges in the new 500 SAC (Special Area Code) for personal communication services are being assigned so quickly that at least one more code will probably be necessary in the very near future. (We're told it definitely won't be of the X00 format.) AT&T is currently offering three exchanges: 346, 367, and 677. They say they won't be discontinuing their 0-700 EasyReach service but it's pretty obvious they want their customers to switch to their new 500 service called True Connections. They say it will have better features, like Call Scheduling, Call Sequencing, and Voice Mail and, unlike 700 numbers, it won't be necessary to dial into the AT&T network to reach the number.

Speaking of AT&T's EasyReach service, there have been some changes. For one thing, we're no longer using our (10288) 0-700-751-2600 number for access to our voice BBS. You can dial direct at (516) 473-2626. But we are using the 0-700 number for all kinds of other things, including AT&T's newest feature. You can now forward your EasyReach number to go to almost anywhere in the world. Callers to the number, however, are warned that they are about to be charged for an international call to [insert name of country here]. Apart from the joy of hearing the recording speak the name of funny-sounding countries, it is now possible for anyone in this country to give others a huge phone bill just by having them call into their EasyReach number. (EasyReach call forwarding works differently than regular call forwarding - EasyReach bills the original caller while normal call forwarding bills the person forwarding their phone.) For example, if you were to call our 0-700 number anytime in the near future, you could wind up with a phenomenal bill very quickly because we've forwarded it to Inmarsat Atlantic West (country code 874). This is the most expensive long distance call you can make - the rates are $30 for the first three minutes and about $1 per six seconds thereafter. You have to hit a couple of touch tones to verify that you really want to do this but no international access is necessary. And, no, we don't make anything from calls to that number - in fact we have to pay $7 a month to keep it. And we are not encouraging anybody to call it, except maybe to hear the funny warning recording.

700-460-1000 (via AT&T) is a toll-free number to make appointments to call Cuba. However, the only time you can make appointments is between 9 pm and 11 pm Eastern Time. We're not sure why they have to use a 700 number for this when an 800 would have sufficed. By the way, did you know there are only two phone lines from the United States into Cuba and they go by way of Italy? Seems the whole thing is the result of a squabble between the two governments over surcharges for collect calls. Negotiations are under way to increase that number to several hundred.

You can now access via modem Bellcore's vast database of documents and search for specific titles and product numbers. To access the system from the Internet, telnet to info.bellcore.com and login as cat10. If you don't have net access, you can call (201) 829-2005 and type "telnet info" at the "annex:" prompt. You can then login as cat10. No password is required.

Look for new numbers in the 555 exchange to start showing up soon. Historically, 555-1212 has been used for directory assistance and every other number in the exchange has either gone unused or also was connected to directory assistance, sometimes without incurring a charge. Now the 555 exchange is being opened up to all sorts of public information services. Numbers can be for one area code, multiple area codes, or nationwide. They've even considered what to do about fictitious numbers like the kind seen in films and on television. Currently almost any number in 555 can be used. But under this new system, only 100 numbers would be usable: 555-0100 through 555-0199. Anyone interested in obtaining application forms can call 201-740-4645.

The good news is that directory assistance rates are going down by 45 percent. The bad news is that it's not in the United States but in the United Kingdom. It seems all of this automation is saving them money so they're passing it on to the consumer. Calls from payphones or by disabled persons to directory assistance will continue to be free. Charges for information were introduced in April 1991.

Wiltel has sunk to a new low in finding ways to collect large sums of money for phone calls. By dialing 10658-0-416-444-2222, you're connected with a sex line that charges $3.99 a minute. The Wiltel 10555 prefix also works in this manner. And what's even worse is that any phone line unfortunate enough to select Wiltel as its primary carrier need only dial 0-416-444-2222 to be charged a huge amount. Up until now, 0+ calls implied operator assistance. Thanks to Wiltel, you can now be charged a lot extra without ever coming into contact with an operator. But the real icing on the cake is the fact that the ten digit number in real life has no relation to the ten digit number that

Wiltel has concocted. Result: some poor person in Toronto is getting tons of calls from slobbering sex callers in the States who think that Wiltel's number corresponds to the actual number. We would love to know what Wiltel was thinking when they introduced this service. Also, how on earth would someone make a 0+ call to that 416 number if Wiltel were their primary carrier?

According to a former government official quoted in *Federal Computer Week,* "on any given day DOD literally does not have control of five or six of its computer systems; the hackers do." Password sniffers that capture the first 120 keystrokes of a session seem to be the biggest cause for concern. According to Michael Higgins, a DOD official, hundreds of thousands of passwords, perhaps millions, have been captured in this manner. And they say that hackers are even getting in through fax machines! If the fax is connected to an office LAN or is also a network printer, access to the network through the fax is possible. With stories like this circulating, we can only wonder what the ultimate "reaction" will be.

BI PROFILE is one of the automated check-in systems used for people on probation. Callers dial 900-737-6781, enter a personal identification number and a password. According to the pamphlet that comes with this "service", "a charge for this service appears on your home telephone bill. This is part of your supervision that you are expected to pay." The system uses touch tone or voice recognition and asks the following questions: Has your home address changed since you last checked in? Has your phone number changed since you last checked in? Have you changed jobs since your last check-in? Have you had any trouble with the law or been rearrested since you last checked in? Are you following the requirements of your supervision such as court-ordered payments, treatment, counseling, or other conditions? If your answers indicate anything other than normalcy, you'll be asked to go into detail. The system tells you when to call again. But the most important part is a lesson in courtesy we can all benefit from. If you hang up before the computer says "Goodbye", your call will not count at all.

The FCC has finally started to take action to prevent certain 800 toll-free numbers from charging customers. (They really know when to take a stand, don't they?) But there still may be some of these ripoff numbers operating. Don't dial: 800-468-3825, 800-949-1661, 800-444-6749, 800-873-7036, 800-697-7877, 800-568-8955, 800-877-3655, 800-288-9377, 800-733-7877, 800-766-6614, 800-927-9377, 800-759-4688, 800-568-8596, 800-723-5016, 800-758-4297, 800-767-4475, 800-846-2303, 800-285-9049, 800-944-9249, 800-468-4475, or 800-433-0069. A couple of other exchanges that could be trouble are: 719-898-xxxx and 303-960-xxxx.

Speaking of ripoffs, we must advise you never to use phones inside hotel rooms except for making internal hotel calls. Here's an excerpt from the billing page of the Omni Shoreham Hotel in Washington, DC: "Local Calls: Billing commences after 45 seconds. A $1.10 charge will be added to your account for each local call, third-party call, and credit card or collect calls." In other words, even if you think you're billing it to your calling card, you'll wind up paying twice. "Long Distance Calls: $1.50 + Daytime AT&T charges." In addition to a surcharge, you won't even get a time of day discount. "Information: $1.76." There are no words to describe that outrage. Finally, the kicker - "Toll Free Calls: $1.50." And they wonder why people steal the towels.

How do cellular companies handle fraud? Not as effectively as they could, according to what we've seen. From United States Cellular Corporation: "The cellular industry is engaged in a constant battle against tumbling ESN fraud. At present, there are three alternatives available to minimize the negative impact of this problem. 1) USCC can ask a roaming partner to deny roaming privileges to a MIN that is tumbling its ESN, 2) USCC can deny roaming privileges to all roamers temporarily by deleting our exchange from a roaming partner's switch, 3) Cellular carriers can implement pre-call validation systems designed to detect tumbling ESN's and shut down fraudulent roamer calls in progress. Unfortunately, this last alternative is in many cases cost prohibitive. The most commonly used solution is to deny roaming privileges to all roamers on a temporary basis...." "If fraudulent calls do appear on your customer's bill, instruct your billing or customer service representative to review the Billed ESN Mismatch Report. This report details all calls that passed our roamer call edit. Remember that our roamer call edit searches the MIN and the first three digits of the ESN. It does not check the entire ESN. If a fraudulent user programs a phone with your legitimate customer's MIN and with an ESN that matches the manufacturer's code of your customer's phone, the calls will appear o n your customer's bill."

Here are steps that one cellular company takes against four types of fraud:

1. Tumbler Fraud

A. Customer disputes roaming charges appearing on a bill.

B. Check the current Billed ESNMismatch report for customer's MIN.

C. If customer's MIN appears on the Billed ESN Mismatch report along with the disputed call, review the past three bills for calls placed to disputed telephone number.

D. If review of past three bills does not show calls to disputed number, credit customer's bill with Disputed Roamer Charge Adjustment voucher code.

E. Contact the Corporate Fraud Control Analyst if the disputed dollar amount exceeds $250. Have photocopies of disputed charges, three previous bills, *and voucher ledger available to send to Corporate Fraud Analyst upon request.*

2. Cloning Fraud

A. Customer disputes roaming charges appearing on a bill.

B. Check the current Billed ESN Mismatch report for customer's MIN.

C. If customer's MIN does not appear on the Billed ESN Mismatch report, contact Corporate Fraud Control Analyst immediately for further instructions.

D. Have photocopies of disputed charges and three previous bills available to send to Corporate Fraud Control Analyst upon request.

E. Do not credit customer's account before speaking to Corporate Fraud Control Analyst.

3. Subscription Fraud

A. Welcome package is returned as undeliverable and two attempts to locate the customer are unsuccessful - or - unable to locate a customer who has an outstanding balance.

B. Suspend the customer's ESN/MIN in the switch - or - begin the collection procedures.

C. If unable to contact customer or collect an open balance, finalize the customer's ESN/MIN.

D. Pull ESN/MIN out of the switch.

E. Notify Corporate Roaming Department of ESN/MIN non-pay status.

F. If outstanding account balance is unusually large or anything seems out of the ordinary, contact the Corporate Fraud Control Analyst for further instructions.

G. Do not credit customer's account before speaking to Corporate Fraud Control Analyst.

4. Stolen Phones

A. Customer enters office to activate a used cellular phone (customer provided equipment).

B. Phone's ESN is found in the switch's local deny file - or - circumstances surrounding the activation seem out of the ordinary.

C. Contact the Corporate Roamer Hotline to verify that the phone has not been stolen.

D. If phone's ESN is listed as stolen in the Industry Negative File and a police report has been filed, do not activate the phone and do not say anything to the customer. Attempt to confiscate the phone. If you feel that you are in danger, calmly tell the customer that the phone cannot be activated due to industry regulations and that the phone will not be useable nationwide. If the customer does not wish to give up the phone, have a coworker contact the police. Obtain the customer's driver license number and vehicle license plate number. Be prepared to provide local police with detailed information about the applicant.

E. If phone's ESN is listed as stolen in the Industry Negative File and a police report has not been filed, activate the phone once the Roamer Hotline has confirmed that the stolen entry in the Industry Negative File has been restored.

Recently, one of our writers confused the hell out of Pennsylvania Turnpike tollbooth collectors when the magnetic strip indicator showed a timespan of several days for a trip of a couple of miles. This led to an extended discussion with tollbooth authorities who referred to a "maximum time formula" and an exchange of letters, excerpts of which follow: "As a frequent traveller on the Pennsylvania Turnpike, I would like to know the specific requirements that drivers such as myself are bound to so that I can achieve maximum compliance and enjoyment of the Turnpike in general." The Pennsylvania Turnpike Commission would not tell our writer what the maximum time formula was but "such information would certainly be provided to any motorist charged with such a violation." In other words, you'll find out what the law is once you break it and not an instant sooner.

Those of you capable of dialing Milo, Iowa can take advantage of immediate free Internet service with no validation. Dial 515-945-7000 for access. This system is only available as a dial-in but it has full Internet access in every other way. We don't know who's behind it or anything else about the system except that they use unshadowed passwords and the phone number you give them will show up in the passwd file which everyone can see. Apart from that, we'll reserve judgement until we learn more.

The following comes from an AT&T press release dated August 17, 1994:

AT&T has formed an investigative team to track the theft of business long distance service to the "hacker's hideout".

AT&T Global Business Communications Systems (GBCS) has created an investigative unit whose sole purpose is to monitor, track, and catch phone-system hackers in the act of committing toll fraud. The unit will initiate "electronic stakeouts" with its business communications equipment customers in cooperation with law enforcement agencies, and work with them to prosecute the thieves.

"We're in a shoot-out between "high tech cops" - like AT&T - and "high tech robbers" who brazenly steal long distance service from our business customers," said Kevin Hanley, marketing director for business security systems for AT&T GBCS. "Our goal is not only to defend against hackers but to get them off the street."

AT&T said hackers today are more sophisticated and organized than ever before. ***For example, a publication for hackers celebrated its 10th anniversary this past weekend by gathering hundreds of hackers in New York City to share their tricks of the trade.***

Although communications and computer companies continually educate business customers on protecting themselves from hackers, illegal access continues to cost billions of dollars in losses of long

(continued on page 40)

BREAKING WINDOWS

by The Camelback Juggler

When was the last time that you wandered into your local computer discount store to test drive that new Pentium based PC? Armed with a fresh stack of formatted 3.5" diskettes, you find your way to the hottest new machine in the store. As you approach the machine of your choice, you notice that flashy screen saver that's so familiar. However, as soon as you touch the mouse, that damn password verification window rears its ugly head. Now consider your options - you could hack away trying to guess the password, or you could go ask one of the customer service geeks to supply the password (he will probably give a demonstration of all the computer skill that he possesses). The first method is brute force and obviously time consuming, the second method works. However, now you have someone shoulder surfing so purloining files and roaming are not within the realm of possibility. The third method is a bit more elegant.

Your first goal will be to exit Windows. The best way to accomplish this is to simply hit the standard CTRL + ALT + DEL. If that does not work you may need to reset or cycle the power off and on. Try and observe what the computer does next. If the computer boots directly to Windows and the screen saver does not appear immediately, then you are in good shape and you don't need to worry about defeating the password. However, if the screen saver starts automatically after Windows starts, chances are a more computer savvy person set the machine up and you need to do a little more work.

If the screen saver begins immediately after Windows starts, reboot the machine. During the boot up cycle, press F5. This will circumvent the standard boot cycle and the computer will drop to the DOS level prompt. Next, you will need to start the MS-DOS editor by typing EDIT. Then, you will need to open the file, C:\ WINDOWS\ CONTROL.INI. Scroll down until you see a file which looks similar to the following:

```
[Screen Saver.Marquee]
PWProtected=1
Text=NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
Font=Wingdings
Size=72
BackgroundColor=128 128 128
TextColor=255 255 255
Speed=10
Attributes=00000
CharSet=2

[ScreenSaver]
Password=1237
```

At this point you will need to modify a couple of things depending upon what you want to accomplish. In this case the utilized screen saver is the marquee. By simply changing the line PWProtected=1 to PWProtected=0 the password will be disabled. Unfortunately, the password itself cannot be determined from the line Password=1237 because the password is encrypted. However, another technique would be to place a semicolon before the line Password=1237 (;Password=1237) and inserting the new line "Password=".

```
[ScreenSaver]
;Password=1237
Password=
```

By replacing the encrypted password with a blank, the screen saver password will still be active. However, when a password request occurs, simply pressing return will do the job. The above methods are, what I call, breaking windows with a glass cutter. There are some quicker and somewhat dirtier methods of accomplishing the same thing. These methods could be called breaking windows with a sledge hammer.

The faster method consists of getting to the MS-DOS prompt level as described above. Then, create a temporary subdirectory and copy C:\ WINDOWS\ CONTROL.INI into the temporary directory. Then delete the C:\ WINDOWS\ CONTROL.INI from the WINDOWS directory. Also, you can simply rename CONTROL.INI to something like, CONTROL.OLD. Again, this will accomplish the same thing as modifying the CONTROL.INI file. However, the computer will display errors when windows starts. So let the situation govern which method you choose.

Some machines use third party security systems. These systems usually consist of a front end for the standard Program Manager that comes stock with Windows. Packard Bell's Navigator is a good example of these security systems. The Navigator has a lock feature that requires a password to enter into the standard program manager. To get around this system you will need to get to the MS-DOS prompt level using previously described methods. Then create a temporary directory and copy C:\ WINDOWS\ STARTUP.GRP into the temporary directory and remember to delete the original. Again, you could rename STARTUP.GRP to STARTUP.OLD. This should defeat most third party password schemes.

Another trick that these retail outlets like to use is changing the attributes of the .INI files as well as related files (.GRP) to read only or hidden. Therefore, you may need to change all the files that you will be fiddling with to the standard archive format. To display attributes of all files in the current directory, type ATTRIB C:\ WINDOWS\ *.INI (or .GRP) <return>. Then use the ATTRIB command to change file attributes to archive. Example: to remove the read only attribute from all files in the Windows directory, type the following command: ATTRIB -R C:\ WINDOWS\ *.* /S <RETURN> the /s processes all files in the current directory and all subdirectories. Also, make sure the "Save Settings on Exit" option in Program Manager is enabled.

If there are many people around, you will want to accomplish all of this as quickly as you can. Try to copy all files that pertain to the task at hand onto floppies before you attempt to gain access, because some people like to delete the necessary files. Also, it may be a good idea to carry a system disk with you just in case you need to boot up clean. If you are creative enough you can make a .BAT file that will automate most of the procedures that I have described, the old EDLIN command should serve you well if this is your goal. However, .BAT files can be problematic unless you have analyzed all pertinent files on your target computer.

Normally you don't want to leave any evidence behind. Of course, I keep all changes that I make relatively innocuous. However, just for fun, I like to modify the Marquee screen saver. My favorite font is wingdings. If you use a capital N (wingding) the screen saver will display a skull and cross bones. Then I reestablish all security measures that were originally in place, so they have to drag out the guy who set the machine up to reset the machine. Keeps 'em on their toes. Have fun....

(continued from page 37)

news

distance service and proprietary information.

"We're working with our customers to beef up security to effectively battle well-organized hackers," Hanley said. "Our "SWAT" team can shut down some of the worst offenders, but businesses still must be as aggressive in protecting their communications systems as hackers are in attacking them."

As part of its equipment maintenance services, AT&T's Technical Service Center in Denver uses advanced "expert systems" to conduct security as well as maintenance checks 24 hours a day on AT&T business communications equipment. When system vulnerabilities are detected, customers are alerted and advised on how to increase security.

The new program takes this further. AT&T's investigators, using data collected by the expert systems, profile hacker activity. They then contact customers and work with them and law enforcement authorities to "stake out" the customers' vulnerable access points. When unauthorized access occurs, the team gathers information on the hacker and springs the trap for prosecution.

AT&T also offers a broad range of other security systems and services to protect business customers against toll fraud, such as AT&T's Hacker Tracker (TM) software for call accounting systems and NetProtect (SM) service, which monitors and alerts customers of suspicious calling patterns on their business communications systems.

The first thing that comes to mind upon seeing this is that these people have really missed their calling. All this talk of stakeouts, SWAT teams, cops and robbers, and attacks makes you think these people really wanted to be cops but for whatever reason wound up in their air-conditioned corporate offices drawing huge salaries. Apart from the gross distortions of reality that they've claimed as fact in the past, it should be noted that the sole purpose of this press release was to get publicity for dubious new products that AT&T is releasing at, no doubt, a grossly inflated price. What better way to spur sales than to create an atmosphere of hysteria and anti-hacker fervor?

Speaking of the latest from AT&T, check this one out: 800-433-3210. What is it? Merely the latest in AT&T's "You Will" campaign to invade our privacy and sell information about us to anyone wanting it. The service allows you to have a House of Windsor catalog sent to anyone you choose. Just enter their phone number and off it goes. Oh, did we mention that the computer *tells you the address of the phone number you've entered?* There are gaps in the database but unlisted numbers don't appear to be treated any differently than listed ones. In other words, if someone can get your phone number - listed or unlisted, this 800 number, using AT&T's Infoworks product, will give them your address. Business addresses can also be obtained in this manner. AT&T appears to get this information from local phone companies and, judging from what we've seen, is taking no precautions to protect it against misuse.

Those of you with a copy of the new crime bill might want to look at the Computer Abuse Amendments Act of 1994. By changing the word "intent" to "reckless disregard", the number of hackers prosecuted could substantially increase. Another change broadens the type of computers that someone can be prosecuted for accessing from "federal interest computers" (banks, government agencies, etc.) to computers "used in interstate commerce". That basically means any machine hooked to the Internet.

Finally, here in 516, an era has ended. For the first time ever, effective September 24, we're now required to dial 1 before an area code when calling outside 516. The 516 and 914 area codes were two of the last areas where it was still possible to just dial an area code without a preceding 1. Since area codes will be indistinguishable from exchanges starting in January, it was necessary to adopt the same standard as everyone else. Please be patient while we try to catch up to the rest of the country.

New Area Codes for 1995

281	Texas
334	Alabama
360	Washington
423	Tennessee
456	International Inbound
500	Personal Communications Services
520	Arizona
540	Virginia
562	California
630	Illinois
954	Florida
970	Colorado

Please continue to send us interesting bits of news. Information yearns to be free!
2600,p.o.box 99,
middle island, ny 11953
2600@well.sf.ca.us
(516) 474-2677 FAX

2600 Marketplace

SOCIETY OF DOOM'S (SoD) Voice Mail System and Voice BBS: 518/725.FUCK, box SOD (763). Running custom software, plenty of H/P talk, and soon to have a BBS like interface w/message areas and lots of other fun stuff! Call today! The Liquid Sky BBS (SoD HQ) offers Internet mail and newsgroups, SoDNET, and lots more. Three 28.8 VFC lines. Call today: 518/725.9701. TOTALLY FREE!

INFORMATION IS POWER! Arm yourself for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supplement you with files, programs, manuals, and membership from our elite organization. Legit and recognized world-wide, our information resources will elevate you to a higher plane of consciousness. Send $1 for a catalog to: SotMESC, Box 573, Long Beach, MS 39560.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual .SYS/.COM program. 100% tested on PC, XT, AT, 286, 386, 486, & all DOS's. Only $29 US. Includes disks, manual. Ship anywhere free. Also: PC BACKGROUND KEYPRESS RECORDER. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to disk or RAM. Also stores key-press timings and key-hold duration. Can identify what's typed, when, and by whom (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite; GPO Box 343, Sydney NSW 2001 Australia.

GET YOUR COPY of the newest and best ANSI Bomb/Bad Batch File detector: ANSICHK7.ZIP. Send $3 to cover cost of disk, shipping, and handling to: Patrick Harvey, 710 Peachtree St. NE 430, Atlanta, GA 30308-1211.

STARTING AN H/P NEWSLETTER. Need writers. Send your articles to P.O. Box 54, Elka Park, NY 12427. If you would like to receive a newsletter, please send $3 for a one year subscription. The newsletter will be published tri-monthly.

BLUE RIDER looks for exchange information about hacking, phreaking, computer viruses, etc. Contact: P.O. Box 91, 43-200 Pszczyna, Poland.

GET THE COLLECTION, a collection of 5000+ viruses on a CD-ROM! Includes many new and undetectable viruses, about 10 megabytes of source and disassemblies, piles of newsletters and related info, databases, and shareware related to viruses. 157 megabytes total! $99.95 + $7 express shipping. American Eagle Publications Inc., PO Box 41401, Tucson, AZ 85717. (602) 888-4957.

THE ANARCHIST'S BBS. A computer bulletin board resource for anarchists, survivalists, mercenaries, investigators, researchers, computer hackers, and phone phreaks. Encrypted email/file exchange available. No ID verification required. 10 lines! Call 214-289-8328.

COHERENT SPECTRUM BBS. 401-435-6759, 3 nodes, 3 gigs storage, 2 online CD-roms. All H/P/V/A/C subjects covered. 24 hrs, 7 days per week. Sysop: VIRIIMAN.

THE UNDERGROUND is now offering membership. For diskette and info, send $10 cash or money order to: P.O. Box 1874, Lomita, CA 90717-5874.

"THE MAGICAL TONE BOX." Fully assembled version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size and only 1/4 inch thin! Records ANY tone you generate onto chip. 20-second capacity. Includes 4 watch batteries and warranty. $49 each, 2 for $95, 4 for $184. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping and insurance. "THE QUARTER" device - complete kit of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for 1, 2, or 4 kits for shipping and insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35 postpaid, each additional crystal only $3 postpaid. Orders from outside U.S., add $12 per order, U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

AUTOMATIC TELLER MACHINES. British 2600 reader wishes to access and/or exchange information with others who have interest/expertise/experience in the matter. ALSO, I am seeking access and/or exchange of scanning and password cracking software. ALSO, very happy to correspond with any other British or US fellow 2600 readers with the desire to increase knowledge. Write to: Aussie Nick, 4 St. Peter's Road, Luton, England LU1 1PQ.

NEED A 5089 DTMF GENERATOR? We have them for $5 US, cash or money order only. Send your order to Durham Technical Products, P.O. Box 237, Arlington, TX 76004. (Internet address: bkd@sdf.lonestar.org) Chips in quantity: 10 for $40. We also carry 6.5 Mhz subminiature crystals, only $4! Same day service on most orders. Write or email us for our parts list. It's your nickel.

NEUROZINES AND OTHER CULTURAL HACKER ZINES! A one-stop, cutting-edge, mail-order source for over 1,000 titles. Beautifully illustrated 120 page catalog includes alternative/fringe, science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3 to Xines, Box 26-1, 1226-A Calle de Comercia, Santa Fe, NM 87506.

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!

FREE INTERNET H/P BASED BBS. Melkors Domain, 10,000+ H-P-V-A-C files! HP CD-rom also! 3 nodes! 203-322-9447, 968-9148, 968-0927. No NUP, Inet access first call. Security specialists/hackers/phreakers/virus creators all welcome!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/94.

(continued from page 31)

vocals

freedom of the press is causing myself and other subscribers to be blacklisted? It seems trivial, but I am concerned about the principles behind this.

2600 has been published since 1984. Each issue contains quite a few good articles. However, if an individual is looking for a specific article, and thus a specific issue, s/he has nowhere to turn, other than sending in a letter to your magazine. Would it be possible for you or a third party to put together a *2600* Index of all the articles ever written?

lexis
cyberspace

While recording the name of every subscriber is possible, we don't believe it's very likely. The issues are thrown onto a truck as soon as we get them to our local post office. Very often, they're delivered the next day. And we never tell them when we're coming. If they're so efficient that they can record thousands of names under those conditions, we probably have a lot more to worry about. And if we were getting blacklisted for believing in freedom of the press, we'd be damn proud of it. Freedom carries a high price, even here. Concerning the index, you'll be happy to know that one has been completed. You can get a free electronic copy by sending us email (2600@well.sf.ca.us). We'll have more info shortly on paper distribution. (It's big.)

Security Lapses

Dear *2600:*

I have an Internet account at a small college. It's clear that the people running the system know as little as I do about running a secure system. On three different occasions I've called (each time around noon when there is a lot of modem traffic) and without even logging on I've gotten a screenful of line noise, followed by a PINE editor error message saying it can't reach my printer. If I wait a minute I find myself logged onto the computer in someone else's account inside the PINE editor. If I finger, I see that there is only one person logged in under whatever account I'm on, and that this person had been on for some time prior to my arrival. This raises two questions: 1) What the hell causes this? 2) Other than sending bogus email to Bill Clinton, what can I do once I find myself logged onto someone else's account? Specifically, can I find out their password while on their account?

Colostomy Bagboy
Washington

Apparently the person using the account tried to do something that confused the system and made for a very long delay which he couldn't get out of. So he lost patience and simply hung up. It's unusual for a system to allow a new caller to pick up within an account - this was common a decade or so ago. You can't find out the person's password unless you slip a program into their account that captures it and mails it to you or hides it until they do the same thing again and you get in once more. But that would be wrong.

Contradictions

Dear *2600:*

Our country has become so entirely hypocritical! If there is anything I've learned in college, it's how much the Computer Science Department hates hackers! I don't even care about that. But what I do care about is the fact that the little girl in *Jurassic Park* is made fun of by her little brother for being a computer hacker and at the end of the movie she saves everybody's lives by hacking a "UNIX" system. In *Sneakers,* they were all praised for being extremely intelligent. In the Disney movie *Blank Check,* the little boy uses his computer to hack his way in and cash a check for a million dollars! And this is something Disney made? There are several other movies where hackers come to save the day and everyone is happy. But if it is so glorified in this perspective, who the hell decided in reality that the penalties are completely the opposite? To be honest, I think it was Geraldo!

Problem Child
Las Vegas, NV

Hacker Sites?

Dear *2600:*

In addition to Frackville, PA, here are some "hack" towns: Hackleburg, AL; Hackberry, AZ; Hackett, AR; Hackberry, LA; Hackensack, NJ; Hackettstown, NJ; and Hacksneck, VA.

Roger Harrison
Long Island

And not one of them has a 2600 meeting.

Help Needed

Dear *2600:*

We're trying to find out all we can about RSA cryptosystems and their standards.

We read *2600* for the first time this spring. We love the anarchy! *2600* is democracy: pulling down the pants of the Bank faced institutions.

We're not hackers - we're a three man programming team. We aim to write a "secure modem" system for the Psion Series 3a pocket computer. Trouble is, it's hard work to find anybody sparky enough in Grey Britain who can explain ISO standards for Public Key Cryptosystems, or who knows what RSA is even.

We read in Britain's *New Scientist* magazine (11-June-94), that there's a product called "Pretty Good Privacy" floating around the Internet in the States. It's obvious to us that Public Key Encryption, having been explained in *Scientific American* back in '79, before Global Networks, will soon be as pervasive as the cold water tap. We wantto start on the Psion (a British company) right now, so other palmtops have to catch up.

So is there anybody out there who knows all about the Clipper's specifications, ISO standards, the latest unbreakable underground standards, algorithms for generating randomly distributed keys, people using Pretty Good Privacy, and anything else we should be asking about?

Lady Penelope
23 Triangle Place
Clapham Common
London SW4 7HS
England
+44 (0) 71-498-2843

Remember, every third call is probably a spook.

internet world guide

(or how to translate those two-letter domains into countries)

DOMAIN	CTRY CD	COUNTRY NAME
—	871	Marisat Atlantic Ocean
—	872	Marisat Pacific Ocean
—	873	Marisat Indian Ocean
—	874	Marisat Atlantic West
—	246	Diego Garcia
—	247	Ascension Island
AD	33	Andorra
AE	971	United Arab Emirates
AF	93	Afghanistan
AG	1	Antigua and Barbuda
AI	1	Anguilla
AL	355	Albania
AM	7	Armenia
AN	599	Netherlands Antilles
AO	244	Angola
AQ	672	Antarctica
AR	54	Argentina
AS	684	American Samoa
AT	43	Austria
AU	61	Australia
AW	297	Aruba
AZ	7	Azerbaijan
BA	387	Bosnia-Herzegovina
BB	1	Barbados
BD	880	Bangladesh
BE	32	Belgium
BF	226	Burkina Faso
BG	359	Bulgaria
BH	973	Bahrain
BI	257	Burundi
BJ	229	Benin
BM	1	Bermuda
BN	673	Brunei Darussalam
BO	591	Bolivia
BR	55	Brazil
BS	1	Bahamas
BT	975	Bhutan
BV	—	Bouvet Island
BW	267	Botswana
BY	7	Belarus
BZ	501	Belize
CA	1	Canada
CC	672	Cocos (Keeling) Islands
CF	236	Central African Republic
CG	242	Congo
CH	41	Switzerland
CI	225	Cote D'Ivoire (Ivory Coast)
CK	682	Cook Islands
CL	56	Chile
CM	237	Cameroon
CN	86	China
CO	57	Colombia
CR	506	Costa Rica
CS	42	Czechoslovakia*
CU	53	Cuba
CV	238	Cape Verde
CX	672	Christmas Island
CY	357	Cyprus
CZ	42	Czech Republic
DE	49	Germany
DJ	253	Djibouti
DK	45	Denmark
DM	1	Dominica
DO	1	Dominican Republic
DZ	213	Algeria
EC	593	Ecuador
EE	372	Estonia
EG	20	Egypt
EH	34	Western Sahara
ER	291	Eritrea
ES	34	Spain
ET	251	Ethiopia
FI	358	Finland
FJ	679	Fiji
FK	500	Falkland Islands (Malvinas)
FM	691	Micronesia
FO	298	Faroe Islands
FR	33	France
FX	???	France (European Territory)
GA	241	Gabon
GB	44	Great Britain (UK)
GD	1	Grenada
GE	7	Georgia
GF	594	French Guiana
GH	233	Ghana
GI	350	Gibraltar
GL	299	Greenland
GM	220	Gambia
GN	224	Guinea
GP	590	Guadeloupe
GQ	240	Equatorial Guinea
GR	30	Greece
GS	500	South Georgia and South Sandwich Islands
GT	502	Guatemala
GU	671	Guam
GW	245	Guinea Bissau
GY	592	Guyana
HK	852	Hong Kong
HM	—	Heard and McDonald Islands
HN	504	Honduras
HR	385	Croatia (Hrvatska)
HT	509	Haiti
HU	36	Hungary
ID	62	Indonesia
IE	353	Ireland
IL	972	Israel
IN	91	India
IO	—	British Indian Ocean Territory
IQ	964	Iraq
IR	98	Iran
IS	354	Iceland
IT	39	Italy
JM	1	Jamaica
JO	962	Jordan
JP	81	Japan
KE	254	Kenya
KG	7	Kyrgyzstan
KH	855	Cambodia
KI	686	Kiribati
KM	269	Comoros
KN	1	St. Kitts and Nevis
KP	850	Korea (North)

KR	82	Korea (South)
KW	965	Kuwait
KY	1	Cayman Islands
KZ	7	Kazakhstan
LA	856	Laos
LB	961	Lebanon
LC	1	Saint Lucia
LI	41	Liechtenstein
LK	94	Sri Lanka
LR	231	Liberia
LS	266	Lesotho
LT	370	Lithuania
LU	352	Luxembourg
LV	371	Latvia
LY	218	Libya
MA	212	Morocco
MC	33	Monaco
MD	373	Moldova
MG	261	Madagascar
MH	692	Marshall Islands
MK	381	Macedonia
ML	223	Mali
MM	95	Myanmar
MN	976	Mongolia
MO	853	Macau
MP	670	Northern Mariana Islands
MQ	596	Martinique
MR	222	Mauritania
MS	1	Montserrat
MT	356	Malta
MU	230	Mauritius
MV	960	Maldives
MW	265	Malawi
MX	52	Mexico
MY	60	Malaysia
MZ	258	Mozambique
NA	264	Namibia
NC	687	New Caledonia
NE	227	Niger
NF	672	Norfolk Island
NG	234	Nigeria
NI	505	Nicaragua
NL	31	Netherlands
NO	47	Norway
NP	977	Nepal
NR	674	Nauru
NU	683	Niue
NZ	64	New Zealand
OM	968	Oman
PA	507	Panama
PE	51	Peru
PF	689	Polynesia
PG	675	Papua New Guinea
PH	63	Philippines
PK	92	Pakistan
PL	48	Poland
PM	508	St. Pierre and Miquelon
PN	64	Pitcairn
PR	1	Puerto Rico
PT	351	Portugal
PW	680	Palau
PY	595	Paraguay
QA	974	Qatar
RE	262	Reunion
RO	40	Romania
RU	7	Russian Federation
RW	250	Rwanda
SA	966	Saudi Arabia
SB	677	Solomon Islands
SC	248	Seychelles
SD	249	Sudan
SE	46	Sweden
SG	65	Singapore
SH	290	St. Helena
SI	386	Slovenia
SJ	47	Svalbard and Jan Mayen Islands
SK	42	Slovakia
SL	232	Sierra Leone
SM	378	San Marino
SN	221	Senegal
SO	252	Somalia
SR	597	Suriname
ST	239	Sao Tome and Principe
SU	7	Soviet Union*
SV	503	El Salvador
SY	963	Syria
SZ	268	Swaziland
TC	1	Turks and Caicos Islands
TD	235	Chad
TF	—	French Southern Territories
TG	228	Togo
TH	66	Thailand
TJ	7	Tadjikistan
TK	690	Tokelau
TM	7	Turkmenistan
TN	216	Tunisia
TO	676	Tonga
TP	62	East Timor
TR	90	Turkey
TT	1	Trinidad and Tobago
TV	688	Tuvalu
TW	886	Taiwan
TZ	255	Tanzania
UA	7	Ukraine
UG	256	Uganda
UK	44	United Kingdom
UM	???	US Minor Outlying Islands
US	1	United States
UY	598	Uruguay
UZ	7	Uzbekistan
VA	39	Vatican City State
VC	1	St. Vincent and the Grenadines
VE	58	Venezuela
VG	1	Virgin Islands (British)
VI	1	Virgin Islands (US)
VN	84	Vietnam
VU	678	Vanuatu
WF	681	Wallis and Futuna Islands
WS	685	Western Samoa
YE	967	Yemen
YT	269	Mayotte
YU	381	Yugoslavia
ZA	27	South Africa
ZM	260	Zambia
ZR	243	Zaire
ZW	263	Zimbabwe

"—" under a category indicates no service.
"???" indicates a mystery to us. Please help.

* - This country no longer exists but its Internet domain is still being used.

SOFTWARE REVIEW

The Supervisor Series
Handy Software for Privileged VMS Users
Review by Floyd Lloyd

This article presents a review of the Supervisor Series of utilities for VMS. The Supervisor Series is a collection of tools which give privileged VMS users the ability to intercept traffic between terminals and user processes running on the VAX. There are a few different flavors of how it works, which will be discussed later in this article. This software started life as a commercial product and was later released to the public domain. It can be found on the Internet at ftp.spc.edu/ anonymous/macro32/savesets via anonymous FTP.

Most of us who have had the privilege (and years) to remember hacking the DECsystem 20, have fond memories of the TOPS-20 operating system. It was a nice, comfy, friendly environment (my first impressions of VMS were not so complimentary). TOPS-20 offered two commands that I really missed in VMS: SPY and ADVISE. SPY's functionality should be obvious from its name; it let you watch what was happening on another terminal. You could see exactly what the other person was seeing, including their typing. ADVISE went a step beyond SPY. Not only did you get the display of the other person, but you also were allowed to type. ADVISE gave you the equivalent of two terminals hooked to the same process on the Twenty. The computer took input from either terminal and gave output to both, without discrimination. ADVISE was a great tool for teaching spastic users. It also helped out when two people were working on the same problem, but were at different locations.

I got very used to using SPY and ADVISE and missed them greatly when we migrated to VMS. Well, now they're back (for VMS) in the form of the Supervisor Series of software. The software seems pretty bulletproof - I demo'ed a commercial version of a package which did the same thing a few years ago. Within five minutes after starting to use it, it crashed the VAX! With the Supervisor Series, I've had none of these problems. The software is well organized, works like a part of VMS, and comes with complete sources and excellent documentation.

Using the Supervisor Series is very straightforward. The first problem to overcome is gaining access to a fully privileged account. Once you've cleared that first (and big) hurdle, the product installs like any other quality VMS application using the VMSINSTAL.COM procedure. I have two additional suggestions for the installation. First, I would not install this product in its default location; hide it down in some subdirectory where no one ever goes. Second, change the name of the .EXE from SUPERVISOR.EXE to MAIL.EXE or something innocuous; if someone FINGERs you and sees a program called SUPERVISOR in use all the time, they may get suspicious - nobody worries when they see someone running MAIL all day long. You'll also have to change the .CLD file to invoke the renamed .EXE. The installation of The Supervisor Series will require the insertion of identifiers via the AUTHORIZE facility on the VAX. If security auditing is enabled on the VAX, this action will set off alarms on the system console. Once the identifiers have been added, you must grant them to yourself. Once again, this can set off alarms on an audited system.

SUPERVISOR works in two basic modes which are analogous to SPY and ADVISE on the Twenty. SUPERVISOR by itself works like SPY; showing you what's happening on a particular terminal. SUPERVISOR invoked with the /ADVISE qualifier allows you to "join in" on someone's session. SUPERVISOR also has a "quiet mode" and a "notify mode", which are controlled by the /NOTIFY qualifier. If the /NOTIFY qualifier is specified, the target will get a message on his terminal letting him know that you're watching or advising. The default is /NONOTIFY, which is sufficient for most applications; there's no evidence that you're watching them.

Once the product is installed, using it is simple. The first step is to define the command to your process (the default installation location, which is not recommended for clandestine operations, is shown):

$ set command sys$sysdevice: [supser.exe]supervisor

Next, the program is invoked:

$ supervise LTA7: (To watch the user on LTA7:)

$ supervise/advise LTA9: (To advise the user on LTA9:)

$ supervise/advise/notify LTA9: (To advise the user on LTA9: and let them know about it)

It's that simple and it really works. The only thing that this product needs is the ability to monitor the RTAn: class of device. That inability is not a fault of the software; it is a limitation of VMS to provide this information. RTAn: terminals are created when users use the SET HOST command to connect to your local system across a DECnet network.

The Supervisor Series consists not only of SUPERVISOR, but also includes PHOTO. PHOTO (another long lost DECsystem 20 command) allows you to record your keystrokes and screen output to a file for later review. PHOTO used in conjunction with SUPERVISOR allows you to record the actions of someone else.

This software brings some real power to the user's hands, whether you're a system manager, hacker, or crasher. The software and documentation are first rate and well worth the cost of an FTP. So, I leave it up to the reader to do the hard work and gain a fully privileged account on a VAX. Once you have that, get The Supervisor Series and enjoy yourself.

2600 MEETINGS

NORTH AMERICA

Ann Arbor, MI

Galleria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

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

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

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

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

Coventry Arabica in Cleveland Heights.

Columbus, OH

The French Market in the Continent by the arcade and 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.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9995.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

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) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

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.

Memphis

Hickory Ridge Mall, Winchester Rd., in the food court. Payphones: (901) 366-4017, 4018, 4019, 4020, 4021.

Nashville

Bellevue Mall in Bellevue, in the non-smoking circle inside the mall in front of Dillards.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

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 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

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

Sacramento

The Capitol City Coffee Company, 1427 L Street, on the corner of 15th & L streets in downtown Sacramento. Payphone: (916) 442-9429.

San Francisco

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

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

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.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

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

*****

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.

TIME RUNNING OUT?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS OCCURS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (the dire threats on this page will never apply to you)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25
□ 1988/$25 □ 1989/$25 □ 1990/$25 □ 1991/$25
□ 1992/$25 □ 1993/$25

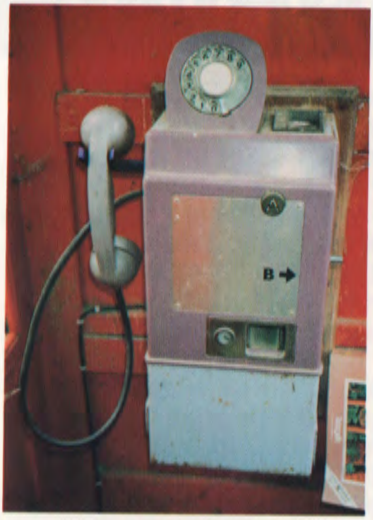
(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

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

TOTAL AMOUNT ENCLOSED: □

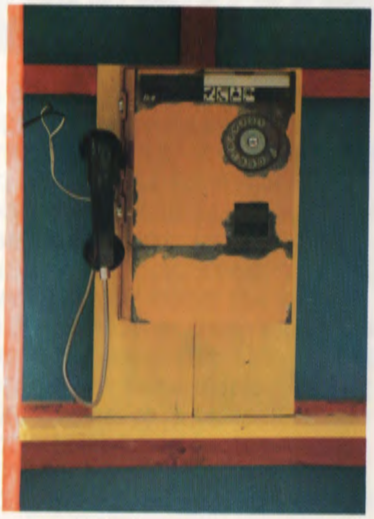
New Zealand



An "old model" coin telephone.

Photo by Kingpin

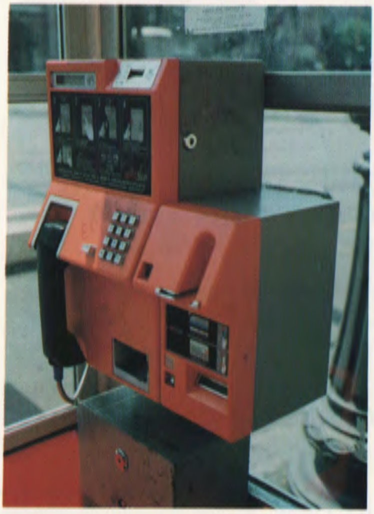
Myanmar



Another non-modern model in Yangon.

Photo by Julie Alperin

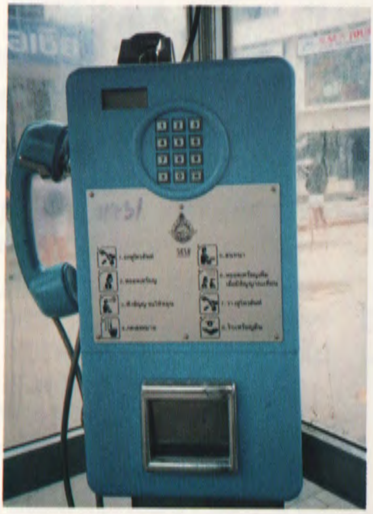
Italy



This phone in Rome does everything.

Photo by Davide D'Angelantonio

Thailand



In a town called Phuket. Really.

Photo by Chas Dye

FOREIGN PAYPHONE PHOTOS NOW COME TO YOU IN LIVING COLOR ON THE BACK PAGE! SEND YOURS TO: 2600, PO BOX 99, MIDDLE ISLAND, NY 11953 USA.