2600

```
# more nn
#!/bin/sh
port=3111
while true; do
        netstat -na | grep $port >/tmp/$$p
        grep ESTABLISHED </tmp/$$p >/tmp/$$E
        recipfound=$?
        if [ $recipfound -eq 0 ]
        then
                where=`awk '{print substr($2,1,length($2)-5)}'
</tmp/$$E`
                finger @$where >/tmp/$$w
        cat /tmp/$$p /tmp/$$w | /usr/ucb/Mail -s $port-$where
pager@seiden.com
        date; cat /tmp/$$p
        sleep 15
        else
        sleep 10
        fi
done
```

The Hacker Quarterly

VOLUME TWELVE, NUMBER ONE!

$4 ($5.50 in Canada)

SPRING 1995

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tampruf

"There are an estimated 35,000 hackers in the U.S. and their community is growing by an estimated 10 percent annually. They are not isolated individuals, slaving away in a vacuum; hackers have established formal operations within every metropolitan city in North America. Hackers communicate via compromised Internet gateways, long-distance calls stolen from corporate victims and through about 1,300 underground bulletin boards across the U.S. This infrastructure collects and disburses a constant flow of stolen calling-card information, corporate voice-mail-access data, compromised PBX DISA-port numbers, hackable modems, cloned cellular telephones, and stolen cellular-phone IDs.... The threat to U.S. businesses also has recently taken a new direction, due to hackers' growing numbers and maturity. Security investigations have confirmed that known hackers are employed within Fortune 500 firms, which know nothing about the individuals' prior activities. The risk to U.S. businesses is clear: What will happen when one of these hacker's employment is terminated? Will the individual destroy or damage the company's voice/data networks, release vital information about these networks to other hackers, or plant the seeds of future destruction in company systems? Time will tell." - unbridled paranoia from The Organized Hackerhood, part of McDonnell Douglas' internal security newsletter leaked to us by an inside hacker.

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitnick, NC-23, The Plague, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.
Network Operations: Max-q, Piotrus, Sarlo.
Voice Mail: Neon Samurai.
Technical Expertise: Rop Gonggrijp, Joe630, Phiber Optik.
Shout Outs: Glenn Case.

READ

YOU HAVE ALWAYS BEEN HERE

***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 1984-1994 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**

The World vs. Kevin Mitnick

By this time, you would have to have been living in isolation not to have heard about the Kevin Mitnick story. Front page headlines and TV newscasts around the world announced the fugitive hacker's capture on February 15 in Raleigh, North Carolina.

If you read the opening paragraph of the *New York Times* on February 16, you would see Mitnick described as a "computer expert accused of a long crime spree that includes the theft of thousands of data files and at least 20,000 credit card numbers from computer systems around the nation." That portrayal is rather damning, to say the least. But let's look a little closer.

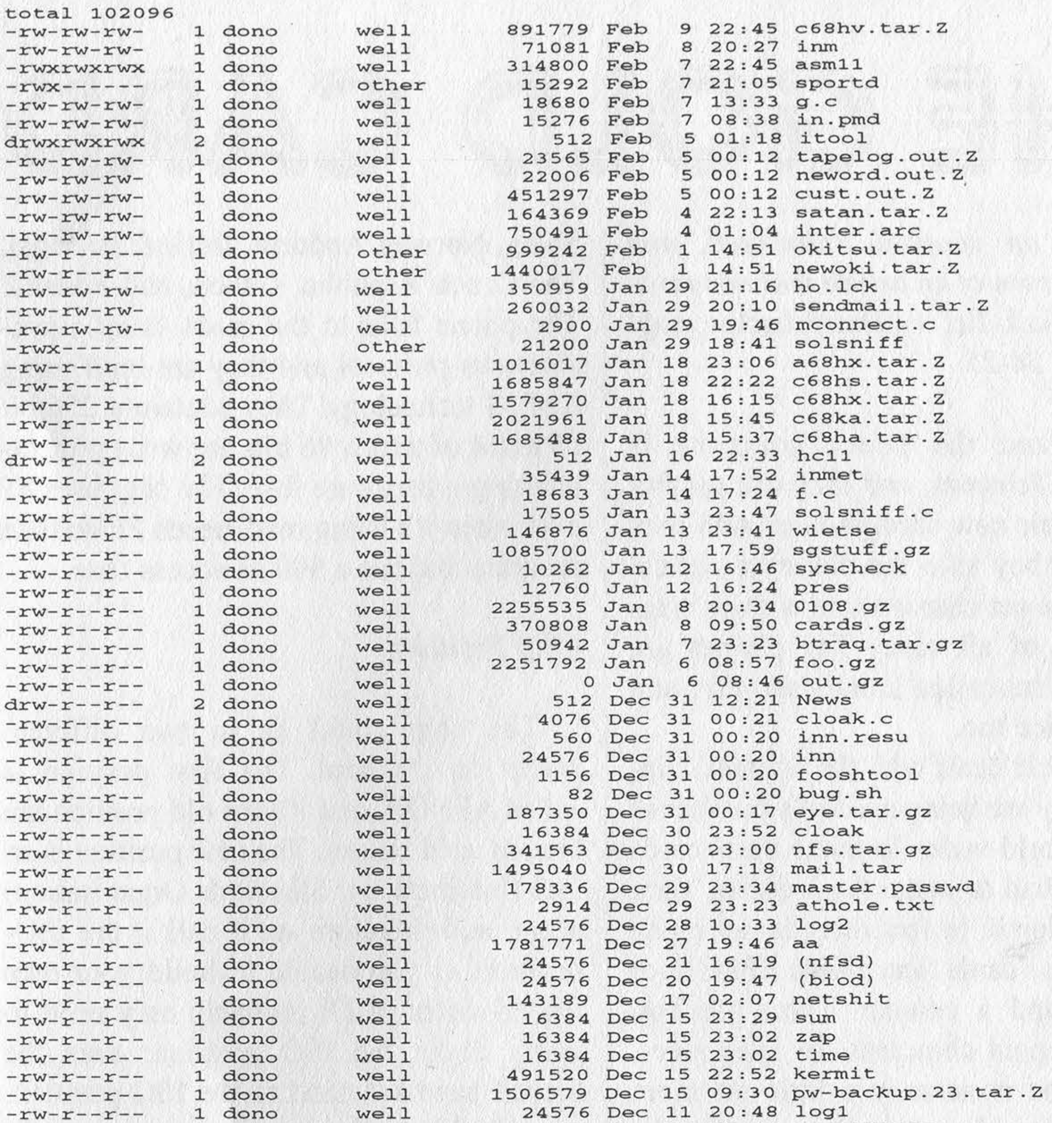
To the average person, the "theft of thousands of data files" would imply that somebody *took away* specific and valuable items as part of an elaborate plot. In reality, copying thousands of computer files is easy, quick, and, in most cases, relatively harmless. When put into this context, even if the files were of a sensitive nature, we can see how it's not necessarily part of an evil plot if someone comes along and copies them.

With regards to the credit card numbers, this is far more misleading. For one thing, only one computer system (Netcom) had its credit card numbers accessed, not "computer systems around the nation". And this compromise was not even news - the Autumn 1994 issue of *2600* reported it nearly half a year ago. Apparently, Netcom did nothing to secure the credit card numbers of its subscribers and, despite multiple warnings and basic common sense, kept this sensitive information online. And, as an ironic twist, Netcom claimed responsibility for helping to catch this most dangerous criminal in a letter to its subscribers entitled "Netcom Helps Protect The Internet".

Nearly every story ever written about Kevin Mitnick can be traced to one source: *New York Times* reporter John Markoff. Markoff was also the co-author of 1991's *Cyberpunk*, a book that focused on Kevin Mitnick (among others) and which was described by Mitnick (*2600*, Summer 1991) as having "many, many false statements, misrepresentations, and inaccurate stories". Mitnick believed Markoff and his wife (co-author Katie Hafner) were miffed at him for not helping with the book. And, as the years went by, it became clear that Markoff was still fixated on the Mitnick saga. In the summer of 1994 he penned a front page article in the *New York Times*, complete with Mitnick's picture, which announced to the world that he was a fugitive. The only substantive "crime" Mitnick was accused of was probation violation yet the *Times* saw fit to make this a front page story.

One week before his capture, Mitnick contacted us to express concern over information he had received indicating that Markoff was actively aiding law enforcement to help track him down. It seemed bizarre at the time but as events unfolded, it appeared that this is exactly what was going on. Markoff had been working with a friend of his (Tsutomu Shimomura) whose computer site had been compromised on December 25, resulting in another puzzling front page story that just didn't seem newsworthy enough to be on the front page.

(continued on page 46)



```
total 102096
-rw-rw-rw-   1 dono     well       891779 Feb  9 22:45 c68hv.tar.Z
-rw-rw-rw-   1 dono     well        71081 Feb  8 20:27 inm
-rwxrwxrwx   1 dono     well       314800 Feb  7 22:45 asm11
-rwx------   1 dono     other       15292 Feb  7 21:05 sportd
-rw-rw-rw-   1 dono     well        18680 Feb  7 13:33 g.c
-rw-rw-rw-   1 dono     well        15276 Feb  7 08:38 in.pmd
drwxrwxrwx   2 dono     well          512 Feb  5 01:18 itool
-rw-rw-rw-   1 dono     well        23565 Feb  5 00:12 tapelog.out.Z
-rw-rw-rw-   1 dono     well        22006 Feb  5 00:12 neword.out.Z
-rw-rw-rw-   1 dono     well       451297 Feb  5 00:12 cust.out.Z
-rw-rw-rw-   1 dono     well       164369 Feb  4 22:13 satan.tar.Z
-rw-rw-rw-   1 dono     well       750491 Feb  4 01:04 inter.arc
-rw-r--r--   1 dono     other      999242 Feb  1 14:51 okitsu.tar.Z
-rw-r--r--   1 dono     other     1440017 Feb  1 14:51 newoki.tar.Z
-rw-rw-rw-   1 dono     well       350959 Jan 29 21:16 ho.lck
-rw-rw-rw-   1 dono     well       260032 Jan 29 20:10 sendmail.tar.Z
-rw-rw-rw-   1 dono     well         2900 Jan 29 19:46 mconnect.c
-rwx------   1 dono     other       21200 Jan 29 18:41 solsniff
-rw-r--r--   1 dono     well      1016017 Jan 18 23:06 a68hx.tar.Z
-rw-r--r--   1 dono     well      1685847 Jan 18 22:22 c68hs.tar.Z
-rw-r--r--   1 dono     well      1579270 Jan 18 16:15 c68hx.tar.Z
-rw-r--r--   1 dono     well      2021961 Jan 18 15:45 c68ka.tar.Z
-rw-r--r--   1 dono     well      1685488 Jan 18 15:37 c68ha.tar.Z
drw-r--r--   2 dono     well          512 Jan 16 22:33 hc11
-rw-r--r--   1 dono     well        35439 Jan 14 17:52 inmet
-rw-r--r--   1 dono     well        18683 Jan 14 17:24 f.c
-rw-r--r--   1 dono     well        17505 Jan 13 23:47 solsniff.c
-rw-r--r--   1 dono     well       146876 Jan 13 23:41 wietse
-rw-r--r--   1 dono     well      1085700 Jan 13 17:59 sgstuff.gz
-rw-r--r--   1 dono     well        10262 Jan 12 16:46 syscheck
-rw-r--r--   1 dono     well        12760 Jan 12 16:24 pres
-rw-r--r--   1 dono     well      2255535 Jan  8 20:34 0108.gz
-rw-r--r--   1 dono     well       370808 Jan  8 09:50 cards.gz
-rw-r--r--   1 dono     well        50942 Jan  7 23:23 btraq.tar.gz
-rw-r--r--   1 dono     well      2251792 Jan  6 08:57 foo.gz
-rw-r--r--   1 dono     well            0 Jan  6 08:46 out.gz
drw-r--r--   2 dono     well          512 Dec 31 12:21 News
-rw-r--r--   1 dono     well         4076 Dec 31 00:21 cloak.c
-rw-r--r--   1 dono     well          560 Dec 31 00:20 inn.resu
-rw-r--r--   1 dono     well        24576 Dec 31 00:20 inn
-rw-r--r--   1 dono     well         1156 Dec 31 00:20 fooshtool
-rw-r--r--   1 dono     well           82 Dec 31 00:20 bug.sh
-rw-r--r--   1 dono     well       187350 Dec 31 00:17 eye.tar.gz
-rw-r--r--   1 dono     well        16384 Dec 30 23:52 cloak
-rw-r--r--   1 dono     well       341563 Dec 30 23:00 nfs.tar.gz
-rw-r--r--   1 dono     well      1495040 Dec 30 17:18 mail.tar
-rw-r--r--   1 dono     well       178336 Dec 29 23:34 master.passwd
-rw-r--r--   1 dono     well         2914 Dec 29 23:23 athole.txt
-rw-r--r--   1 dono     well        24576 Dec 28 10:33 log2
-rw-r--r--   1 dono     well      1781771 Dec 27 19:46 aa
-rw-r--r--   1 dono     well        24576 Dec 21 16:19 (nfsd)
-rw-r--r--   1 dono     well        24576 Dec 20 19:47 (biod)
-rw-r--r--   1 dono     well       143189 Dec 17 02:07 netshit
-rw-r--r--   1 dono     well        16384 Dec 15 23:29 sum
-rw-r--r--   1 dono     well        16384 Dec 15 23:02 zap
-rw-r--r--   1 dono     well        16384 Dec 15 23:02 time
-rw-r--r--   1 dono     well       491520 Dec 15 22:52 kermit
-rw-r--r--   1 dono     well      1506579 Dec 15 09:30 pw-backup.23.tar.Z
-rw-r--r--   1 dono     well        24576 Dec 11 20:48 log1
-rw-r--r--   1 dono     well         4621 Dec 11 20:45 passwdrace
-rw-r--r--   1 dono     well        13228 Dec 10 00:26 ns.c
-rw-r--r--   1 dono     well       637827 Dec  7 00:50 4004
-rw-r--r--   1 dono     well       257615 Dec  6 06:38 oldnw.tar.Z
-rw-r--r--   1 dono     well       184864 Dec  6 06:38 oldctek.tar.Z
-rw-r--r--   1 dono     well      8142621 Dec  5 04:26 nw.tar.Z
-rw-r--r--   1 dono     well      6813202 Dec  5 03:48 o.tar.Z
-rw-r--r--   1 dono     well        11185 Dec  3 02:04 vsr.gz.crypt
-rw-r--r--   1 dono     well        10402 Dec  3 02:04 tcpd.tar.gz.crypt
-rw-r--r--   1 dono     well        10247 Dec  3 02:03 ifj.c.gz.crypt
-rw-r--r--   1 dono     well       440996 Dec  3 02:02 marty.tar.gz.crypt
-rw-r--r--   1 dono     well         1024 Nov 30 22:38 aliases.pag
-rw-r--r--   1 dono     well         1336 Nov 30 11:15 foosh
-rw-r--r--   1 dono     well        90112 Nov 29 23:23 in.telnetd
-rw-r--r--   1 dono     well        16384 Nov 29 22:32 sss
-rw-r--r--   1 dono     well         1755 Nov 29 22:13 zap.c
-rw-r--r--   1 dono     well        60586 Nov 29 21:37 z
-rw-r--r--   1 dono     well           61 Nov 26 19:05 c.c
-rwxrwxrwx   1 dono     well        10112 Nov 26 13:25 zap2
-rw-r--r--   1 dono     well         3390 Nov 26 13:25 zap2.c
-rw-r--r--   1 dono     well        26444 Nov 24 20:48 portd.c
-rw-r--r--   1 dono     well        50599 Nov 23 21:53 key2.zip
-rw-r--r--   1 dono     well       607687 Nov 23 01:41 mbox.Z
-rw-r--r--   1 dono     well        48786 Nov 23 01:33 zipcrypt.zip
-rw-r--r--   1 dono     well       136912 Nov 23 01:33 zipcrack.zip
-rw-r--r--   1 dono     well       297223 Nov 22 01:55 zipstuff.tar.Z
-rw-r--r--   1 dono     well      5947301 Nov 22 01:53 kocher.tar.Z
-rw-r--r--   1 dono     well        13213 Oct 27 11:42 ss.c
-rw-r--r--   1 dono     well          150 Oct 27 11:37 unxor.c
-rw-r--r--   1 dono     well         4910 Oct 27 11:37 sniffer.c.gz
-rw-r--r--   1 dono     well        12646 Oct 25 13:44 sunsniffer.c
-rw-r--r--   1 dono     well       205725 Oct 24 20:16 1022csn.tar.Z
-rw-r--r--   1 dono     well       139047 Oct 23 18:33 tcpd.tar.Z
-rw-r--r--   1 dono     well         2139 Oct 23 17:45 passwd
-rw-r--r--   1 dono     well      1216403 Oct 23 17:32 lile
-rw-r--r--   1 dono     well          540 Jun 12  1992 mbox
```

If Kevin Mitnick was the mastermind behind it all, how come we were able to get ahold of one of his directories so easily after he was arrested and the directory deleted? These are the files he was accused of stashing on The Well, including 0108.gz, the Netcom credit card database. From the looks of it, lots of people were able to get access to this.

THE GOLD CARD

This is an adapted, translated, and updated version of an article that appeared earlier in Hack-Tic, the Dutch hacker magazine, issue 24-25.

In Holland the phone company is called PTT-Telecom, and they are mighty proud of their new card-phones. And they should be: they take the old style optical cards, the newer chipcards as well as magnetic cards of all sorts. The phones are built by a firm called Landis and Gyr and they look nice too.

This article deals with the prepaid chipcards as they are being used in a number of countries world-wide. To make these cards cheap they had to make them dumb. Very, very, very dumb. In fact there is not much more on these cards than a little EPROM or EEPROM and a counter. There are two types of prepaid chipcards for telephones, and one type is actually a little bit more intelligent than the other. Here is what the cards do.

Cards of Type 1

This is the oldest type of card. It comes in two varieties. One is being used in France and Monaco, the other in Sweden, Spain, Norway, Andorra, Ireland, Portugal, The Czech Republic, Gabon, and Finland. The phone talks to the cards using a synchronous protocol and they are built using NMOS technology. They contain a 256 bit EPROM of which 96 bits are write protected using a hardware fuse. The chip uses 85 mW when it's being read, needs 21 Volts to program and has a 500 ns access time.

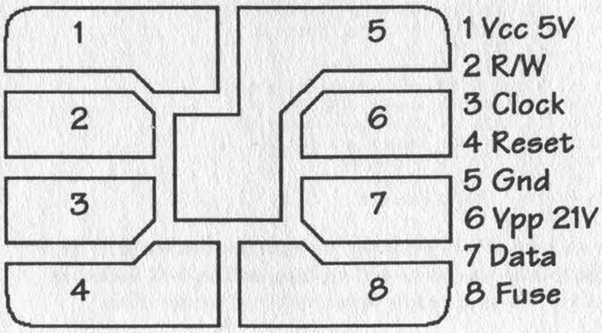
Chip Position

The chip could be in two different places on the card. The first position is called AFNOR, and it's the old position the French used to use . The new position is an ISO (International Standards Organisation) norm, and therefore we'll call it the ISO-position. If you decide to build your own reader-writer you'll probably only need to worry about the ISO position: even the French have switched to the ISO-position, so AFNOR cards are becoming rare. To read the drawings: the cards are being held with the chip in the upper left corner, contacts facing up.

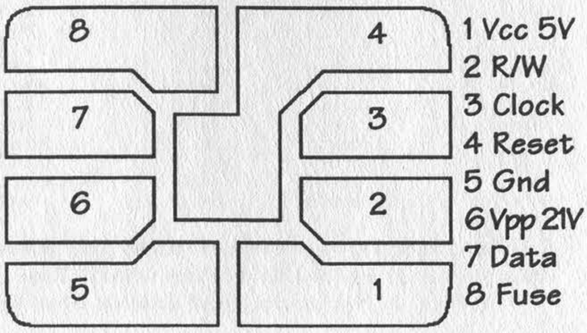
What They Do

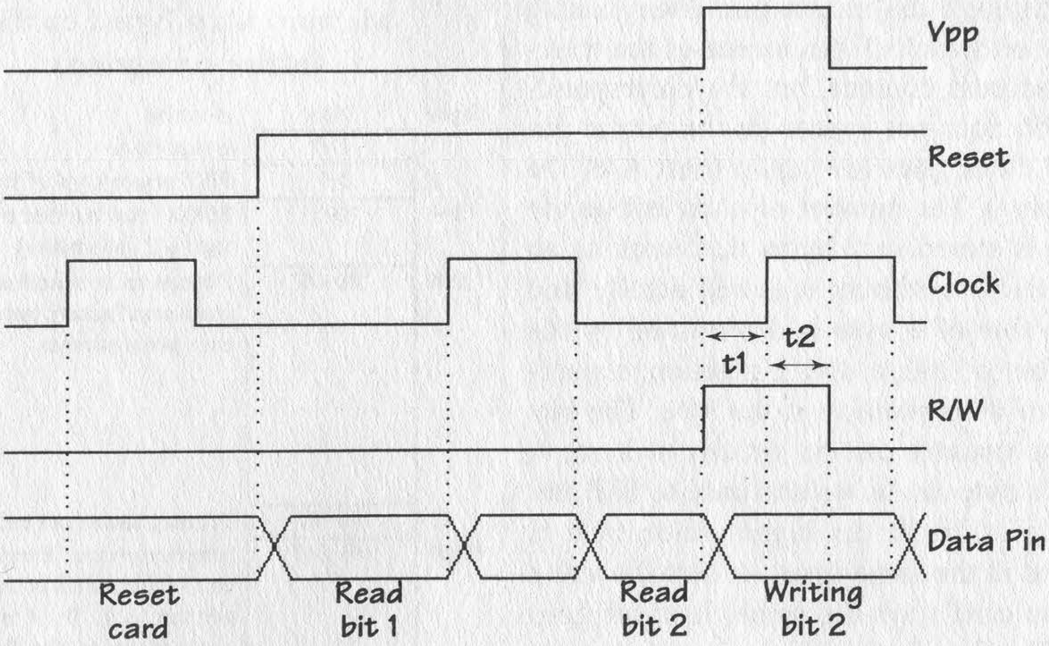
The next drawing is a timing diagram,

Type 1 Cards, ISO position



Type 1 Cards, AFNOR position





which shows you what the communication with the card should look like. If you read it you'll see that if reset is pulled low and clock is pulsed then the card's internal counter resets. If reset is then brought high you can "clock out" the data bits to the output pin one by one. If you raise not-read-write and put the programming voltage on the Vpp pin and pulse the clock you program the bit that you jumped to using only the clock. This bit will go from 1 to 0.

A few things to keep in mind: all signals in this drawing except Vpp are TTL-level. That means a low is 0 volts, a high is 5 volts. The cards of this type that we tested with all run perfectly fine off the 3.3 volts coming out of a notebook's printer port. The Reset, Clock, and R/W input pins can be directly connected to a PC's parallel port. Vpp is switched between 5 and 21 volts. The t1 and t2 time durations in the timing diagram must both be between 10 and 50 ms. When reading the card, Vpp and Fuse must be at 5 volts. The next two drawings show the memory contents of this card's two varieties.

Security

The chip on the card does not let you write bits back to 1, so raising the value of your card through normal interaction does not work. Because the whole chip is EPROM you could try to erase it. This is going to be tough, because the plastic that the chip is embedded in is totally opaque at ultraviolet wavelength. If you do succeed you'll have to re-write the first 96 bits containing country-code, card-type, etc. This is also not easy, because the card has a hardware fuse that is quite literally burned. Conclusion: filling up empty cards is not easy.

Cards of Type 2

Of the two outdated systems, this is the newest one. Cards are being used in Holland, Germany, and Greece. They don't need 21 volts anymore and they're just a little smarter than the type 1 cards. The chips are always in the ISO position.

What They Do

When looking at the timing diagrams you'll notice the internal counter going back to zero when a clock pulse happens within a reset pulse. As soon as reset goes low, the corresponding memory bit is output through the output pin. Every rising flank on the clock pin increases the internal address counter, but the corresponding bit does not appear on the output pin until clock goes low again (part A of the drawing). The number of units left on the card is stored in 5 bytes that work as an abacus. The amount is stored octally, and the value of a byte is determined by the number of bits at the 1 position, regardless of their position in the byte. The bits in the counter can be written to zero. A whole byte can be written back to $FF, but only if a bit in the higher-value byte is erased at the same time. At best the value of the card stays the same, it never goes up. The first byte of the counter contains only 4 usable bits, the first bit (64) is a card-enable that is zeroed out when the card initializes. The next three bits (65-67) are sometimes used for tests in the counter-area suring production. The maximal value for the card thus becomes 5 x 4096 = 20480 units. In Holland a unit is a cent (guilder/100), in Germany it's a Pfennig (Mark/100), and in Greece they are actual telephone cost-pulses.

Memory Map Type 1 cards (France and Monaco)

byte	bits	meaning
1	0-7	Issuer code
2	8-15	$03: France / Monaco
3-11	16-87	9 bytes to be specified by manufacturer. Factory batch, maybe even serial number.
12	88-95	Total number
13-31	96-247	Telephone-tics. Every time a unit is used a bit in this area is written to '1'. The first 10 units are written in the factory to test the card. Cards are 40, 50 or 120 units or $05 for 40 units.
32	248-255	$FF when card is full

Memory Map Type 1 cards (other countries)

byte	bits	meaning
1	0-7	Issuer code
2	8-15	$83: phone card of this type
3-4	16-31	$8XXX total number of units on card + 2 (see below)
5-11	32-87	7 bytes to be specified by manufacturer. Factory batch, maybe even serial number.
12	88-95	Country code (see below)
13-31	96-247	Telephone-tics. Every time a unit is used a bit in this area is written to '1'. The first 2 units are written in the factory to test the card. Cards are 10, 22, 25, 30, 50, 80, 100 or 150 units. The value in bytes 3-4 is BCD coded. Examples: bytes 3-4 say $8012 for 10 unit card, $8152 for a 150 unit card. Valid country codes: $1E Sweden $22 Spain $30 Norway $33 Andorra $3C Ireland $47 Portugal $55 Tchechia (or whatever...)
32	248-255	$00

If the phone booth wants to write a bit to zero it clocks there and then it does a reset pulse followed by a clock pulse. The reset pulse means a write-operation is in progress and the next clock pulse should not be used to increment the internal counter, but to do the actual write instead (B in timing diagram).

The phone could also write a bit and write all the bits in the byte below that back to 1. This is done by just going through the write operation twice. The first time it does the write time, the second time signals the card to set the byte below the current one to $FF (C in timing diagram). This operation is called "erase" in all the documentation we have. Both during write and erase the clock should be on for at least 10 milliseconds.

The next drawing shows the memory content for this card type. The issuer code is always $80 in Holland. The byte with "Specific Data" is EEPROM that can only be written to by the manufacturer. The documentation is cryptic, but it's rumoured to have to do with chip testing. The byte is $FF in all cards we've seen so far. The 5 bytes that are issuer-determined could be anything. In Holland the first one gives you the manufacturer ($CA Gemplus, $2A Solaic). The second byte is the value when bought. $22 is 10 guilders (1000 units), $42 is 500 units (5 guilders), and $62 is the 25 guilder card. There can be no more units on the card than this maximum.

Manufacturing

The data that we have on this type of chip tells a few things about the state in which the PTT's get the cards. The cards are locked for transportation using a "transport code" of three bytes. Only if you know these three bytes can you program the chip and turn it on to become a phonecard.

The memory map in the "transport state" is as follows: 0-23 are static, 24-71 cannot be erased, there is "enable memory" (?) in bits 72-79 and the transport code is in bits 80-103. These bits cannot be read however. It seems the code has to be clocked in (!) though the output pin and the chip compares and acts accordingly.

Security

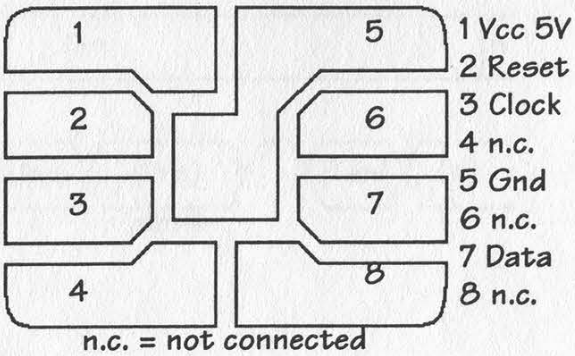
Although this card does allow you to set bits back to 1 again, the card is smart enough not to let you do that unless you reset a bit in a higher register, so the effect is neutral at best. We tried to fool the card, but all the obvious stuff doesn't work. Maybe something works using UV-light, but it's not very likely.

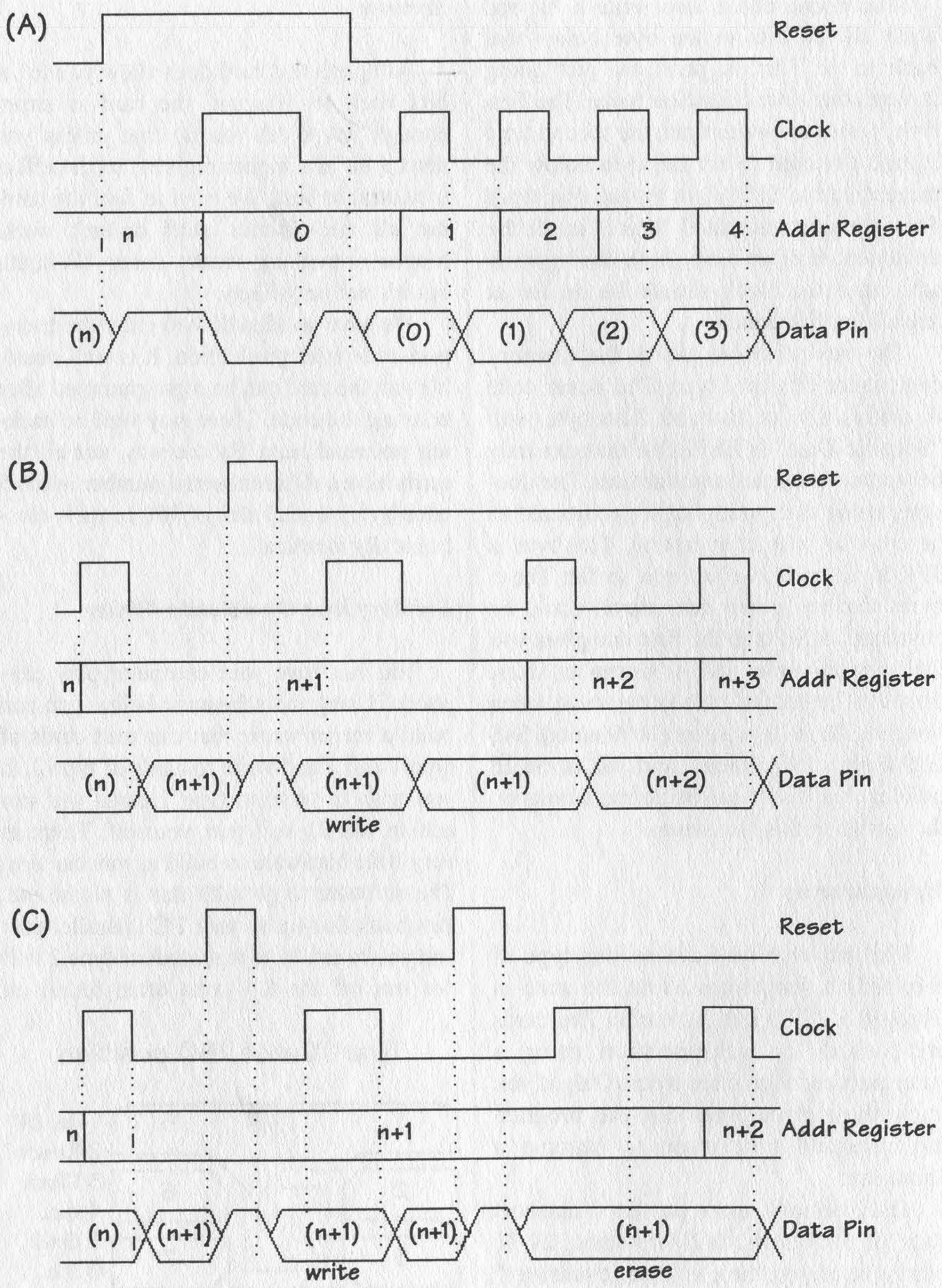
We have no idea how to enter the transport code after production. It is well possible that the card can be reprogrammed after entering the code. There may well be hacking potential here. By the way, not all the cards have a different serial number in the 5 telco bytes: each batch of 100 cards is electronically identical.

Building Your Own Reader/Writer

You can have your computer play payphone. Using the schematic below you can build a reader/writer that can read cards of type 1 and 2 and write to cards of type 2. If you wish to write to type 1 cards you can add in the 21 volt part yourself. There is very little hardware to build as you can see. The software to go with this is phone.exe. Just hook this up to your PC's parallel port and you're set. Note that cards of type 2 will not run off the 3.3 volts often found on

Type 1 Cards, ISO position




(A)
Reset
Clock
n
0
1
2
3
4
Addr Register
(n)
(0)
(1)
(2)
(3)
Data Pin
(B)
Reset
Clock
n
n+1
n+2
n+3
Addr Register
(n)
(n+1)
(n+1)
write
(n+1)
(n+2)
Data Pin
(C)
Reset
Clock
n
n+1
n+2
Addr Register
(n)
(n+1)
(n+1)
write
(n+1)
(n+1)
erase
Data Pin

notebook printer ports. The card-detect contact can be left out. Our software will also think a card is inserted when you press a key.

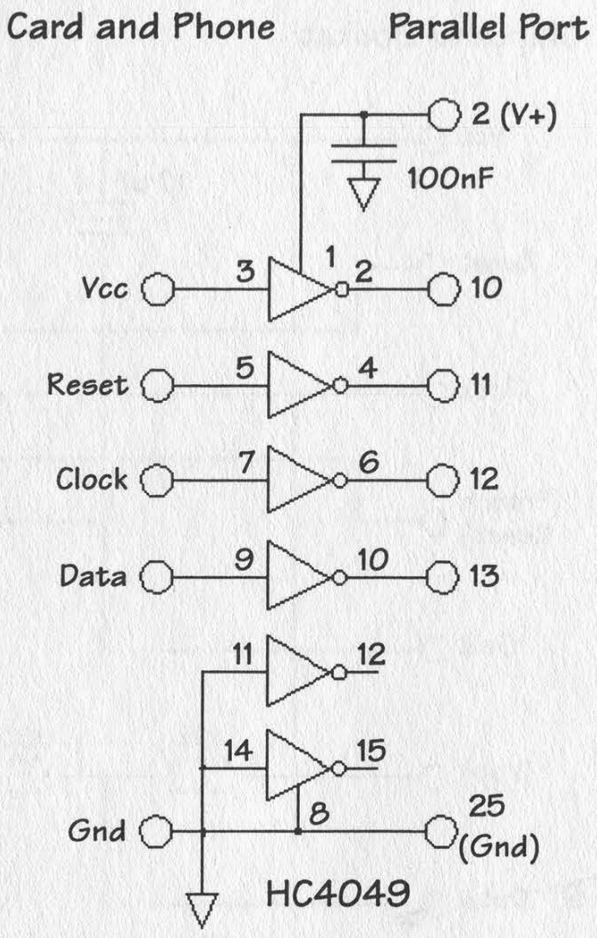
At the end of this article there is a source called phone.c. If that is compiled using Borland C++ with options -O2 -2 or with Microsoft C 6.0 with options -G2r -Ozax then you can do everything the phone can: read the entire card (-v for more information), writing (-w<bit>) or erasing (-e<bit>) bits. You could of course modify the program so that a new (lower) value is programmed in just one step, but that is left as an exercise to the reader. Phone -t brings you in a test mode: keys "p", "r", "c", and "f" toggle Power, Reset, Clock, and French reset respectively. A real phone reads the card in a rather peculiar way. Option -r simulates this behaviour.

Listening In

With the help of this "snooper" schematic, you can get your PC to listen in on the conversation between a card and a phone. You can write a program to monitor what happens on the printer port bits in real time. Takes at least a 386 to be fast enough to see what is going on. This will work also on notebooks with the 3.3 volt printer port. The left part of the schematic is hooked up in parallel with the phone and card, the right goes to the printer port on the PC.

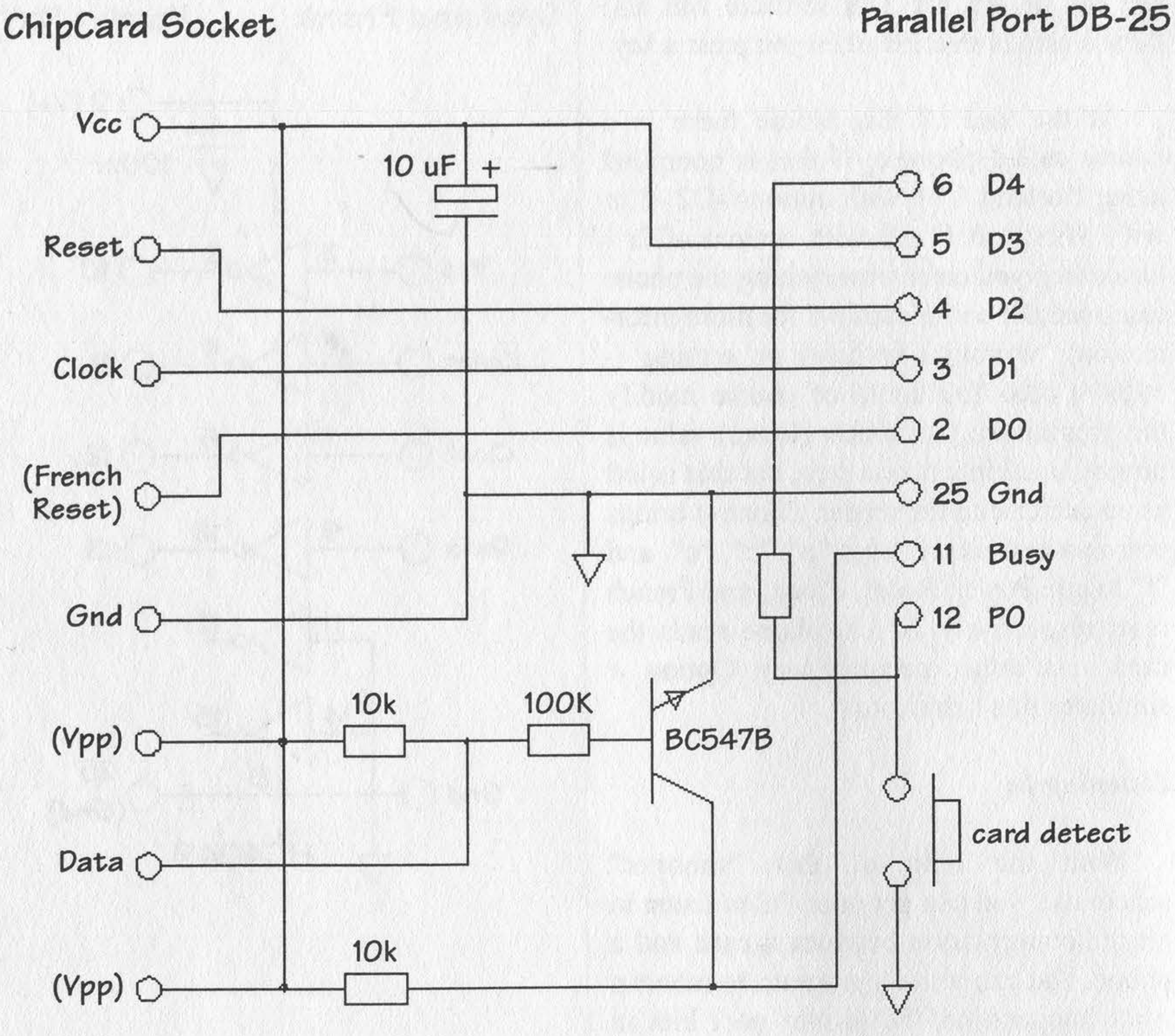
Goldcard

Many countries have these nasty steel doors that close behind the card as you insert it. The Dutch, being naturally paranoid and miserly, only insert their card in the phone if they can still see it. So the Dutch phonecards stay in sight during the conversation. This makes it very possible to build a fake chipcard that has wires coming out in the back and then simulating the



Memory Map Type 2 cards

byte	bits	meaning
1	0-7	Issuer code
2	8-15	country code
3	16-23	'specific data'
4-8	24-63	5 bytes 'card data', could be production codes, etc. Valid country codes: $2F Germany $3B Greece $77 Netherlands
9-13	64-103	x 4096 x 512 x 64 Octal counter, number of bits set to '1' in a register determines value of that byte



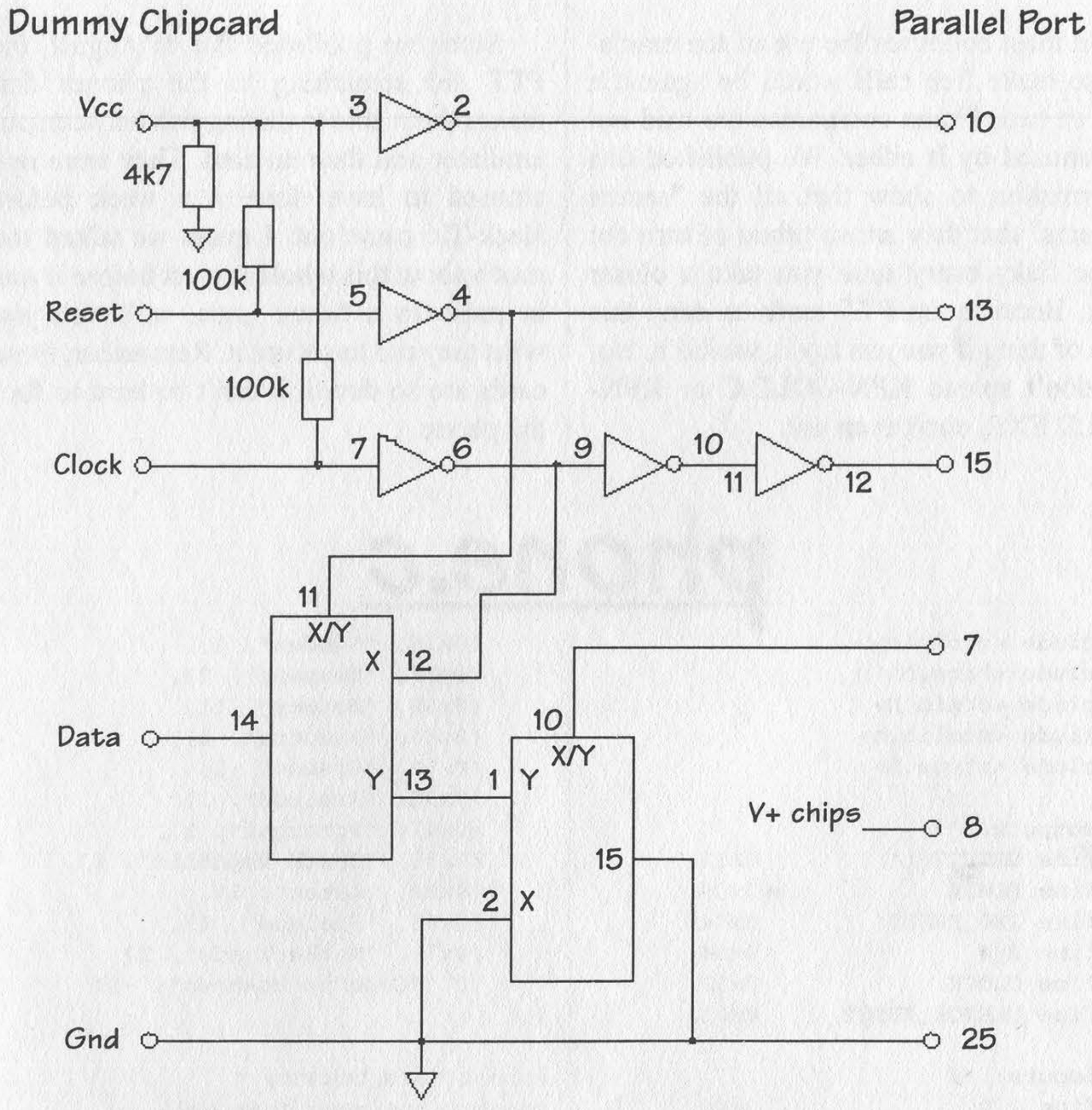
entire chipcard from a notebook computer. This potentially gives you an "always full" phonecard. The program must however do exactly the same thing as the real card. We made a fake chipcard by peeling the chip out of an empty card and soldering (careful, not too hot!) thin transformer wires to the contacts.

The program we made is called KPN-GOLD.EXE, and it reads a dumpfile in the same format as made by PHONE.EXE. Of course the program also participates in the whole abacus countdown routine. But as soon as power drops (card removed from telephone), the card goes back to its original value. You can also use this combination of fake chipcard and software to test your own chipcard reader-writer. We have been playing with three PC's. One as phone, one as card, and one as snooper, to tap the conversation.

The V+ in the emulator schematic is attached to pin 1 of the 4049 and pin 16 of the 4053. Pins 14 and 8 of the 4049 and pins 3, 4, 5, 6, 7, 8, and 9 of the 4053 are attached to ground. In the vicinity of the chips you put a 100 nF capacitor between V+ and ground.

Security Logic?

Supposedly the cards have a special



"security mechanism" that keeps the phone from accepting an emulator as the real card. We only read about this mechanism after we had successfully emulated the card, but we did notice something funny. At the end of the first reading cycle the phone issues a very fast reset of only a few microseconds, and it expects the card to do the correct behaviour. We solved this by having the entire reset behaviour done by a bit of hardware in the emulator. Maybe we hacked the "security mechanism" this way. Ah well....

More Intelligent Cards

There are also chipcards out there that have complete microprocessors with RAM and EEPROM on them. These cards are used in the new PAN-European GSM mobile telephone system for instance. In Germany these cellular telephony cards also work in payphones: the call shows up on your cellular phone bill. All the Dutch phones can do this too, and rumour has it that there will be a whole range of specialised chipcards. There may be cards that can only call one number (nice business card). This type of card can be secured much better with the use of challenge-response tricks and cryptography. Maybe we'll write about all this in a future issue.

The Law

In most countries the use of the emulator to make free calls would be against a law or two. Phone companies are said not be amused by it either. We published this information to show that all the "secure systems" that they are so proud of turn out to be flaky every time you take a closer look. Because the PTT tends to deny this type of thing if you just say it, we did it. No, we don't spread KPN-GOLD.C or KPN-GOLD.EXE, don't even ask.

Update

Since we published this in August, the PTT did something to the phones that makes them able to distinguish between our emulator and the real card. They were real amused to have done it a week before Hack-Tic came out. I guess we talked too much about this whole project before it was in print. In a future issue, we'll tell you what they did to secure it. Remember, these cards are so dumb, it can't be hard to fool the phone.

phone.c

```
#include <stdio.h>
#include <bios.h>
#include <conio.h>
#include <stdlib.h>
#include <ctype.h>

/* outputs: */
#define DETECT              0x10
#define POWER               0x08
#define ISO_RESET           0x04
#define R_W                 0x04
#define CLOCK               0x02
#define FRENCH_RESET        0x01

/* inputs: */
#define I_O                 0x80
#define CARD                0x20

unsigned int          pp;
unsigned char         data[32];
unsigned char         bits[256];

int                   num_data;
int                   one = 0;
int                   verbose = 0;
int                   silent = 0;
int                   go = 0;

struct card_country {
     unsigned char    num;
     char             *name;
     unsigned char    type;
};

struct card_country cc[] = {
     {0x01, "Demoland", 1},
     {0x03, "France", 0},
     {0x1E, "Sweden", 1},
     {0x2F, "Germany", 2},
     {0x30, "Norway", 1},
     {0x33, "Andorra", 1},
     {0x3B, "Greece", 2},
     {0x3C, "Ireland", 1},
     {0x47, "Portugal", 1},
     {0x55, "Czech Republic", 1},
     {0x5F, "Gabon", 1},
     {0x65, "Finland", 1},
     {0x77, "Netherlands", 2},
     {0, "Country unknown", -1}
};

struct card_country *
country(unsigned char val)
{
     struct card_country *ccp = cc;
     while (ccp->num && ccp->num !=
val)
          ccp++;
     return (ccp);
}

unsigned char
_bits(unsigned char val)
{
     unsigned char    mask = 0x80,
count = 0;
     for (; mask; mask >>= 1)
          if (val & mask)
               count++;
     return (count);
}

void
initbits(void)
```

```
{
    int               i;
    for (i = 0; i < 256; i++)
        bits[i] = _bits(i);
}

unsigned int
bcd(unsigned char hi, unsigned char
lo)
{
    return ((lo & 0xF) + (lo >> 4) *
10 + (hi & 0x0F) * 100 + (hi >> 4) *
1000);
}

void
delay(unsigned int ms)
{
    unsigned long    tmp = 2000L *
ms;
    while (tmp--);
}

void
output(unsigned char val)
{
    outp(pp, val);
    delay(1);
}

unsigned char
input_bit(void)
{
    return ((inp(pp + 1) & I_O) ?
!one : one);
}

#define input_byte( )     (inp( pp+1
)&(I_O|CARD) )

unsigned char
card_in(void)
{
    return ((inp(pp + 1) & CARD) ? 0
: 1);
}

const unsigned char val[] = {128,
64, 32, 16, 8, 4, 2, 1};
void
read_data(int how)
{
    unsigned int    i, j;

    /* reset card */
    output(POWER);
    delay(10);
    output(POWER | ISO_RESET);
    output(POWER | ISO_RESET |
CLOCK);
    output(POWER | ISO_RESET);
    delay(10);
    output(POWER | FRENCH_RESET);

    /* clock bits in */
    for (i = 0; i < num_data / 8;
i++) {
        data[i] = 0;
        for (j = 0; j < 8; j++) {
            if (input_bit())
                data[i] |= val[j];
            /* clock next bit */
            output(POWER | CLOCK |
FRENCH_RESET);
            output(POWER |
FRENCH_RESET);
        }
    }
    output(0);
}

void
write_bit_iso(unsigned int index)
{
    unsigned int     i;

    /* reset card */
    output(POWER);
    delay(10);
    output(POWER | ISO_RESET);
    output(POWER | CLOCK |
ISO_RESET);
    output(POWER | ISO_RESET);
    output(POWER);

    /* clock bits in */
    for (i = 0; i < num_data; i++) {
        if (i == index) {
            if (!(data[i / 8] &
(0x80 >> (i & 7))))
                printf("wiping 0
bit!\n");
            output(POWER |
ISO_RESET);
            delay(10);
            output(POWER);
            delay(10);
            output(POWER | CLOCK);
            delay(200);
            output(POWER);
        }
        /* clock next bit */
        output(POWER | CLOCK);
        output(POWER);
    }
    output(0);
}
```

```
void
erase(unsigned int index)
{
    unsigned int     i;

    /* reset card */
    output(POWER);
    delay(10);
    output(POWER | ISO_RESET);
    output(POWER | CLOCK |
ISO_RESET);
    output(POWER | ISO_RESET);
    output(POWER);

    /* clock bits in */
    for (i = 0; i < num_data; i++) {
        if (i == index) {
            if (!(data[i / 8] &
(0x80 >> (i & 7))))
                printf("erasing 0
bit!\n");
            output(POWER |
ISO_RESET);
            delay(10);
            output(POWER);
            delay(10);
            output(POWER | CLOCK);
            delay(200);
            output(POWER);
            delay(10);
            output(POWER |
ISO_RESET);
            delay(10);
            output(POWER);
            delay(10);
            output(POWER | CLOCK);
            delay(200);
            output(POWER);
            delay(10);
        }
        /* clock next bit */
        output(POWER | CLOCK);
        output(POWER);
    }
    output(0);
}
char            *
bitstring(unsigned char val)
{
    static char     buf[9];
    char            *s = buf;
    unsigned char   mask = 0x80;

    for (; mask; mask >>= 1)
        if (val & mask)
            *s++ = '1';
        else
            *s++ = '0';
    *s = 0;
    return buf;
}

#define STEP    4
void
print_data(void)
{
    int             i, j;

    for (i = 0; i < num_data / 8; i
+= STEP) {
        if (verbose)
            printf("%3d - %3d\t", i
* 8, min(num_data, (i + STEP) * 8) -
1);
        for (j = 0; j < STEP; j++)
            if (i + j < num_data /
8)
                printf("%s ", bitstring(data[i + j]));
            else
                printf("
");
        printf("\t");
        for (j = 0; j < STEP && i +
j < num_data / 8; j++)
            printf("%02X ", data[i
+ j]);
        printf("\t");
        for (j = 0; j < STEP; j++)
            if (i + j < num_data /
8 && isprint(data[i + j]))
                printf("%c", data[i
+ j]);
            else
                printf(".");
        printf("\n");
    }
}

void
show_units(unsigned int burn,
unsigned int maxval, unsigned char
*p)
{
    unsigned int    val = 0;
    int             i = 20;

    if (verbose)
        printf("Value area:\n");
    do {
        if (verbose)
            printf("%s
(%02X)\t%3d\n", bitstring(*p), *p,
bits[*p]);
        val += bits[*p];
    }
    while (*p++ == 0xFF && --i);
    if (verbose)
```

```
        printf("\t\t===\n\t\t%3d out
of %d bits burned\n", val, maxval);

    printf("%u(+%u) units - %u units
left\n", maxval - burn, burn, maxval
- val);
}

void
show_units2(unsigned char *p)
{
    unsigned long    val = 0;
    int              i = 5;
    unsigned long    pow = 4096;

    if (verbose)
        printf("Value area:\n");
    for (; i; i--, pow /= 8) {
        if (verbose)
            printf("%s (%02X)\t%d *
%4lu = %5lu\n", bitstring(*p),
                    *p, bits[*p],
pow, pow * bits[*p]);
        val += pow * bits[*p++];
    }
    if (verbose)
        printf("\t\t
=====\n\t\t          %5lu
units\n", val);
    else
        printf("Value %lu units\n",
val);
}

void
print_type(void)
{
    unsigned int     val;
    struct card_country *ccp;
    unsigned char    cou;

    if ((cou = data[1]) == 0x83)
        cou = data[11];
    ccp = country(cou);
    printf("%s - ", ccp->name);

    switch (ccp->type) {
    case 0:
        switch (data[11]) {
        case 0x13:
            show_units(10, 130, data
+ 12);
            break;
        case 0x06:
            show_units(10, 60, data
+ 12);
            break;
        case 0x15:
            show_units(0, 40, data
+ 12);
            break;
        default:
            printf("value
unknown\n");
        }
        break;
    case 1:
        val = bcd(data[2] & 0xF,
data[3]);
        show_units(2, val, data +
12);
        break;
    case 2:
        show_units2(data + 8);
        break;
    default:
        printf("card type
unknown\n");
        if (num_data == 128)
            show_units2(data + 8);
        else
            show_units(0, 0, data +
12);
    }
}

void
dotestmode(void)
{
    unsigned char    nw, ow =
input_byte();
    unsigned char    ov = DETECT;

    if (verbose)
        printf("Test mode:\n");

    while (1) {
        output(ov);
        printf("\r%s - %s - %s - %s
: %s - %s",
                (ov & POWER) ?
"Power" : "     ",
                (ov & CLOCK) ?
"Clock" : "     ",
                (ov & ISO_RESET) ?
"I Reset" : "       ",
                (ov & FRENCH_RESET)
? "F Reset" : "       ",
                (ow & CARD) ? "
" : "Card",
                (ow & I_O) ?
"Output" : "      ");
        while ((nw = input_byte())
== ow &&
!_bios_keybrd(_KEYBRD_READY));
        if (nw == ow) {
            switch
(_bios_keybrd(_KEYBRD_READ) & 0xFF)
{
            case 'p':
                ov ^= POWER;
                break;
            case 'r':
                ov ^= ISO_RESET;
                break;
            case 'f':
                ov ^= FRENCH_RESET;
                break;
            case 'c':
                ov ^= CLOCK;
                break;
            case 27:
            case 'q':
                output(0);
                return;
            }
        } else
            ow = nw;
    }
}

void
usage(void)
{
    printf("phone [-cdfhirstv] [-
e<n>] [-w<n>] [<outputfile>]\n"
            "\t-c\tcontinuous
read\n"
            "\t-d\tignore card
detect\n"
            "\t-e<n>\twrite bit n
and erase next byte\n"
            "\t-f\tforce french
length\n"
            "\t-h,-?\tthis help\n"
            "\t-i\tinvert input
bits\n"
            "\t-r\tread as a real
phone\n"
            "\t-s\tsilent mode\n"
            "\t-t\ttest mode\n"
            "\t-v\tverbose mode\n"
            "\t-w<n>\twrite bit
n\n");
}

void
main(int argc, char *argv[])
{
    int             write_bit = 0;
    int             erase_bit = 0;
    int             wait_card = 0;
    int             real_read = 0;
    char            *of = NULL;
    int             test = 0;
    char            c;
```

```
    pp = *(unsigned int far *)
0x408;    /* look up LPT1: */
    num_data = 16 * 8;  /* default
128 bit cards */

    while (argc-- > 1) {
        argv++;
        if (argv[0][0] == '-') {
            while ((c =
*++(argv[0])) != 0) {
                switch (c) {
                case 'c':
                    go = 1;
                    break;
                case '?':
                case 'h':
                    usage();
                    return;
                case 'f':
                    num_data = 32 *
8;
                    break;
                case 'w':
                    write_bit =
atoi(argv[0] + 1);
                    break;
                case 'd':
                    wait_card = 1;
                    break;
                case 'e':
                    erase_bit =
atoi(argv[0] + 1);
                    break;
                case 'i':
                    one = !one;
                    break;
                case 'r':
                    real_read = 1;
                    break;
                case 's':
                    silent = 1;
                    break;
                case 't':
                    test = 1;
                    break;
                case 'v':
                    verbose = 1;
                    printf ("Phone
v1.0\t\t\t\t(C)opywrong 1994 by
Hack-Tic magazine\n");
                    break;
                }
            }
        } else
            of = argv[0];
    }

    if (verbose)
        printf("Reading on printer-
port 0x%X\n", pp);

    if (test) {
        dotestmode();
        return;
    }
    initbits();

    output(DETECT);

    while (wait_card && !_bios_key-
brd(_KEYBRD_READY));
    while (!card_in() && !_bios_key-
brd(_KEYBRD_READY));

    if (go) {
        while (inp(96) != 1)
            read_data(real_ read);
    } else {
        delay(20);

        read_data(real_read);

        if (!silent)
            print_data();
        print_type();

        if (write_bit) {
            delay(20);
write_bit_iso(write_bit);
            read_data(real_ read);
            if (!silent)
                print_data();
            print_type();
        }
        if (erase_bit) {
            delay(20);
            erase(erase_bit);
            read_data(real_ read);
            if (!silent)
                print_data();
            print_type();
        }
        if (of) {
            FILE            *f;
            if ((f = fopen(of,
"wb")) != NULL) {
                fwrite(data, 1,
num_data / 8, f);
                fclose(f);
            } else
                perror(of);
        }
    }
    while
(_bios_keybrd(_KEYBRD_READY))
        _bios_keybrd(_KEYBRD_ READ);
}
```

These are the guidelines for *2600* meetings:

1) We meet in a public area. Nobody is excluded. We have nothing to hide and we don't presume to judge who is worthy of attending and who is not. If law enforcement harasses us, it will backfire as it did at the infamous Washington DC meeting in 11/92.

2) We act in a responsible manner. We don't do illegal things and we don't cause problems for the place we're meeting in. *Most 2600* meetings are welcomed by the establishments we choose.

3) We meet on Fridays between the hours of 5 pm and 8 pm local time. While there will always be people who can't make this particular time, the same will hold true for *any* time or day chosen. By having all of the meetings on the same day and time, it makes it very easy to remember, opens up the possibility for inter-meeting communication, and really causes hell for the federal agencies who want to monitor everything we do.

4) While meetings are not limited to big cities, most of them take place in large metropolitan areas that are easily accessible. While it's convenient to have a meeting in your home town, we encourage people to go to meetings where they'll meet people from as wide an area as possible. So if there's a meeting within an hour or two of your town, go to that one rather than have two smaller meetings fairly close to each other. You always have the opportunity to get together with "home town hackers" any time you want.

5) All meetings *must* contact us to let us know how things are going even if nothing unusual is happening. If we don't hear from your city on a regular basis, we'll have to stop publicizing the site since telling people to go to where no meeting is really doesn't do anyone a service. You can email us at meetings@2600.com or call us at (516) 751-2600. We also need a way of getting back in touch with you.

Anyone can have meetings and set whatever rules they wish. However, if they're going to be affiliated with *2600*, we ask that these few guidelines be observed. Thanks.

Facts on ATM Camera security

by Kitsune

Here are some facts to clear up the many misconceptions on cameras at Automatic Teller Machines.

Myth: Every ATM has a camera, as required by law.

Fact: There are *no* national (U.S., Canada, Mexico, Japan, Australia, New Zealand, to name a few that I can confirm) or banking industry laws on requiring video or film.

There are *some* local laws (or laws in other countries) that have been implemented, but they are typically only for personal security in a vestibule.

Remember, the banking industry is *cheap*; they *do not* put in any more than they need. They are also unregulated - they can do anything they want with the cameras. There are no "camera police" to decide what is "allowed".

Their biggest loss is in fraud, and this is the *only* reason for them putting cameras in, *not* your personal security. If there is a vestibule with cameras in it, these are for security.

Myth: Every ATM has a camera, even if you cannot see it.

Fact: If there is a camera, you can see it. If the plastic is too dark for you to see through, the same is true for the camera.

Fish eye adapters (not lenses, but screw on adapter glass for the existing lens, which is typically an auto-iris type) cost bucks, as much as the camera in some instances. Pinhole lenses are even more expensive and the image sucks. They *do not* use them in ATM's. Period.

A one way mirror (like manager's office type) is too dark, so it is not used. Instead they use a mylar film. You can see through just as well as the camera, if there isn't too much reflected light on your side.

Myth: The camera can see me entering my PIN.

Fact: The banks couldn't care less if they see your hands entering the PIN - they want to see your face.

Myth: The camera can see me, and identify me and/or my car.

Fact: To get the best image of the user, the lens is picked and adjusted to make your face fill the screen when you use the ATM. This means setting the focal length/focus to around 20 inches. You cannot be identified at 20 feet with this setting, as either your face/license plate is too small, or it is out of focus.

Myth: Someone, someplace is watching that camera.

Fact: No one, no place is watching that camera. A "time-lapse" VCR is connected to the camera, and the VCR may be recording other cameras in the same bank in addition to the ATM camera.

Myth: The VCR records *everything*, just like my home VCR.

Fact: The "time-lapse" VCR is basically a "snapshot" recorder, and the images are therefore recorded every second or so. If the ATM camera is part of a larger camera system, the ATM camera is only recorded every few seconds (every second or so multiplied by the total number of cameras).

Typical speeds are:

NTSC: 2h (BETA-2 & VHS-sp), 6h (VHS-slp), 12h, 18h, 24h (0.2sec), 48h (0.4sec), 72h (0.6sec), 84h (0.7sec), 96h (0.8sec), 120h (1.0sec), 180h (1.5sec), 240h (2.0sec), 480h (4.0sec).

PAL: 3h (VHS-sp), 12h, 24h (0.18sec), 48h (0.34sec), 72h (0.5sec), 84h (0.58sec), 96h, 120h (0.82sec), 180h (1.22sec), 240h (1.62sec), 480h (3.22sec).

Myth: The banks review all the tapes, looking for suspicious activity.

Fact: Very few banks review their tapes, and those that do just review them for system operation (all cameras work? in focus? date/time correct? transaction data showing?). They do not watch the tape with any detail, unless they are looking for something.

Once they are looking for something, they search for the date and time of the audit trail on the tape, using the cue/review or VITC (vertical interval time code) search features of the VCR, ignoring all other activity on the tape.

Myth: The VCR is only activated when I put in my card.

Fact: The VCRs run 24 hours a day. Only one percent of them are "activated" by the card (there is too much time taken to get the tape up to speed after such an unloaded position, and if you stay in "still" forever, you trash the tape and heads).

It is also easier for the bank to just put it on a weekly exchange of the tape, then they do not have the possibility of running out of tape unpredictably based on ATM activity.

They usually have 15 to 30 weeks rotation of the tapes because it can take that long for them to find out that there is a problem with the account (three or more billing cycles).

Myth: There is a microphone, recording audio.

Fact: Very few VCR's can record audio. Of those, even less are ever used for audio. Audio recording only works in the 2hour or some 12hour/24hour speeds, on some VCR's. The banks do not use this feature. Some convenience stores however, do record audio to ensure ABC compliance.

Some Other Camera Facts

Most cameras now have CCD (charge coupled device) all electronic imagers. This makes the cost and maintenance go down in comparison to the vidicon tube cameras, but at a loss of resolution.

Typical resolution for CCD cameras are: black and white 2/3" imager: 512x492pixals 380horizontal; black and white 1/2" imager: 800x500pixals 570horizontal; black and white 1/3" imager: 512x492pixals 560horizontal; color 1/2" imager: 512x492pixals 330horizontal; color 1/3" imager: 752x852pixals 480horizontal.

Some Other VCR Facts

VCRs in use are BETA, Super-BETA, Ed-BETA (NEC), VHS and Super VHS (NEC, Sony, JVC, Panasonic, and many re-manufactured consumer decks), and a few 8mm's thrown in from Sony.

The BETA decks run at an odd fundamental speed (BETA 1.5 hour) and have same-angle heads (you cannot play your consumer BETA). The early VHS decks also had same-angle heads, and could not play your consumer tapes. The newer VHS/S-VHS decks have consumer compatible 2 or 4 head, and can play your two hour VHS tapes, but very few will play your six hour tapes (again because of the odd fundamental speeds). All use L500/T120 tapes. The L750/T160 tapes get eaten by the machines.

Tapes are good for about 10 to 20 passes before they are scored from the drum. The drums are good for 12 to 18 months if good tape (double coated, not too many passes) is used.

The decks cost the bank between US $1800 and US $2600. Many are RS-232C remote controlled, for programming/searching the tapes.

Typical resolution for VCRs is: black and white: 350horizontal, color: 240horizontal.

They will record color, but resolution and identification is better if you don't waste it on trying to reproduce color. Color cameras cost bucks too. Most cameras installed now are CCD.

Camera Hacks

Walk up to camera with the sun behind you. The auto iris lens usually cannot adjust for the bad contrast. Some cameras have image enhancers to fix such contrast problems, but they work only if the white to black area is about 3:1 or 3.5:1.

Walk up from the side. If you cannot see the glass of the lens, it cannot see you.

Walk up to the camera with a bright light glaring right into it. The auto iris will try to shut it out.

Cover the lens with cellophane. If it looks fuzzy and out of focus to you.... This has the added benefit of being unnoticed.

ATM Hacks

Myth: All the data is encrypted.

Fact: Some of the data is encrypted, just a few fields.

Myth: ATMs use dialup lines.

Fact: ATMs use direct connect, multipoint, or multidrop phone connections. Some are connected via satellite links, called Vsat. Some ATMs can be used in a dialback (ATM calls host) connection, for temporary sites, but not "temporary" sites as "permanent" as the fair, etc.

Myth: You could hack the modem line and make the ATM give you money.

Fact: The reason on the grand scale is protocol (typically SDLC/SNA, BISYNC, or async Poll/Select). These protocols exchange message numbers with each packet, so you would need to "become" the host after learning the sequences "right now", get the ATM to request from the host your withdrawal, emulate the proper *encrypted* sequence, based on the *encrypted* request, sequentially in real time.

There is no way for the host to "tell" the ATM to spit money. The host just grants approval for the request. ("Can I give this customer three $20's and a $10?" "...Sure!") Your next problem would be the audit trail kept in the ATM.

Some Other ATM Facts

If you disconnect the line, the ATM shuts down as if the service key was turned. Depending on the network, when you restore the line, reconnection can be automatic or need to be enabled by the host.

Those that speak of accessing the ATM when it is not communicating with the host are correct, to an extent. It all depends on the network and the software loaded (local approval for bank-owned accounts only, typically).

No, you cannot easily get into the vault of the ATM. I have seen them dragged off of walls with tow trucks (he ended up dragging it for about two blocks), they have been blown up (enough force to pop them also toasts the cash). They have however been cracked just like any other safe.

Typically, they are just attached to the floor, sticking out the hole in the wall.

Cash on hand is less than US $70k fully loaded with US $20 in a machine that has two bins, but usually they are a mix of two denominations.

The cash bins look like tall ammunition cases, and are also locked, and then locked into the machine (takes two keys even after the vault is opened). The bins have the feed mechanism built in, so when locked, they're sealed from "coathanger" prying.

If a card is captured, it is not "eaten, munched, or trashed". It is just tossed into a tupperware bin.

The deposit envelopes are checked only by humans for content; the machine cannot do this. The deposit envelopes are printed with the audit trail as they are accepted into the machine.

Our new Internet site is being constructed as we write this. Stay tuned for details on how it will change your life. In the meantime, please take note of these new addresses:

letters@2600.com - to send us a letter.
articles@2600.com - to submit an article.
2600@2600.com - if you just want to say hi.

And, in case things go awry, keep our old address - 2600@well.sf.ca.us. If you don't trust the net and have faith in the U.S. mail, write to us at 2600, PO Box 99, Middle Island, NY 11953. If you believe a fax is safe from prying eyes, our fax number is (516) 474-2677. And if you actually believe your phone calls aren't being tapped, you can call us at (516) 751-2600. The choice is yours.

h.o.p.e. scares away military

```
---------- Forwarded message ----------
Date: Mon, 8 Aug 94 8:33:13 MDT
From: [redacted] [redacted] [redacted].army.mil>
To: [redacted] [redacted] [redacted]-[redacted]-[redacted] [redacted]-[redacted]-[redacted] [redacted].army.mil>
Cc: [redacted] [redacted] [redacted]-[redacted]-[redacted] [redacted]-[redacted]-[redacted] [redacted].army.mil>,
    [redacted] [redacted] [redacted].army.mil>
Subject: Hackers
```

Good morning [redacted],

I'm writing to tell you that the First U.S. Hacker Congress is meeting in New York on Auqust 13 and 14. Groups like the Chaos computer Club, Hack-Tic, and Phrack will all be in New York doing what they do best (breaking into systems and yours is a prime candidate). The problem is even with the added security measures that have been taken on the network at WSMR, the hackers can still get into the system. When the sniffer program intercepted the passwords on the network the hackers built a dictionary from those passwords, this makes the systems on the network more vulnerable to attack (i.e. people tend to use the same type of password). The best advice I can give you on this matter is to take the WSMR network off the Internet (milnet) for the weekend.

One of the Computer Scientists that should be executed.

[redacted]

Perhaps it would be a good idea to take White Sands Missile Range off the Internet altogether.

CELLULAR INTERCEPTION TECHNIQUES

by Thomas Icom
IIRG/Cybertek

In order to understand the techniques detailed in this article, a basic knowledge of cellular telephony is required. Instead of rehashing what has already been written, those in need of the required education should refer to a good g-file on cellular telephony. The ones written by Brian Oblivion/RDT or Bootleg are recommended by the author as well as Damien Thorn's articles from *Nuts and Volts* magazine, and the numerous articles that have appeared in *2600*. They should be considered required reading at this point.

Introduction

The Electronic Communications Privacy Act of 1986 (ECPA) prohibits the monitoring of cellular telephony communications except for network testing, equipment troubleshooting, interference tracking, or warrant-sponsored surveillance. It also mandates that the Federal Communications Commission deny Part 15 certification (which is required to sell radio equipment in this country) to "scanning receivers" which are "readily modifiable" to receive cellular telephony communications and 800 Mhz band frequency converters. This mandate does not apply to "test equipment" as technicians working in the cellular industry obviously need the equipment to troubleshoot problems. Nor does it apply to the phones themselves, for reasons which should be obvious. Kits are also exempt from this mandate, as Part 15 compliance is considered the responsibility of the builder.

So far, the response of the courts has been mixed in regard to enforcement of the ECPA. In 1986, the U.S. Department of Justice stated that they would not enforce the law, as doing so would be impossible. This was back in 1986 with an administration that does not exist anymore. The current administration might be a little less enlightened in regard to freedom of the airwaves. (They certainly are in regard to some other freedoms.) Some judges have held that since cellular telephony occurs over the airwaves, there is no "reasonable expectation of privacy". Others have maintained an opposite viewpoint. None of the judges with the former viewpoint have gone so far as to declare the ECPA null and void.

From a practical standpoint, despite whatever laws may be on the books, if it goes out over the airwaves one might as well shout it from a rooftop. Successful interception of unencrypted cellular telephone or any other form of radio communications is undetectable and requires only a basic level of technical expertise.

A Realistic Appraisal of Cellular Phone Security

It should go without saying that any unencrypted RF transmission is naturally unsecured, ECPA notwithstanding. With that in mind, even though your cellular phone conversation is being sent out for anyone to intercept and listen to, there are a few other factors.

The design of the cellular phone system doesn't give it half the range of the old IMTS system. The old IMTS system had a maximum range of 50-75 miles whereas a cell site might have an absolute maximum 20 mile range in a rural area where the cell sites aren't that close together. In an urban area, a cell site could have a range of *less than one mile*. The decreased range means less potential listeners.

The cell site is capable of adjusting its power output and the power output of a phone in relation to its proximity to the cell site. This can be as low as 30 milliwatts. What this means is that if one is close to a cell site, their signal's range will be decreased.

Scanners capable of 800 Mhz reception are still considered "high-end" pieces of equipment and therefore are generally purchased by serious monitoring enthusiasts. Among said enthusiasts, cellular is not considered a popular listening item, as they feel that 90 percent of the communications are "boring", and the continuous nature of cellular transmissions lock up the scanner and make it worthless for listening to anything else.

With 832 channels and many different conversations to choose from, a quick, innocuous sounding call will probably go unnoticed among the drug dealers, stockbrokers, and Verafone systems that inhabit the cellular airwaves.

All things considered, unless the phone's MIN is flagged for some reason or the cell site being used is flagged, the chances that a given cellular will be monitored are slim. If the user keeps their calls short and avoids having "interesting" conversations, potential listeners will either miss the conversation altogether, or monitor it briefly and go on to find a "less boring" conversation. If the phone's MIN is flagged, or the cell site being used is flagged, then expect the conversation to be monitored.

Usage Analysis

Cellular phones are used by anyone who feels they need instant phone communications despite their location, and can afford to have it. While this includes a lot of upper class housewives, yuppies, and corporate executive wannabes, there are some more interesting users.

Political organizations make use of cellular phone communications. The Democrats made extensive use of cellular phones during their last national convention. On the other hand, the Republicans were smart and banned the use of cellular phones in their national convention.

Police agencies are another cellular user, using them on the assumption that communications are a little more private than over their radio system. The NYPD uses them for non-emergency communications in their Precinct-Activated Response Program, and for their highway callboxes.

The various departments of transportation and public works departments also use cellular. Their highway radio advisory systems operating on 530 and 1610 Khz are often equipped with cellular phones for remote programming.

Flea Market vendors are mating Verafone systems with cellular phones in order to be able to validate credit cards and check purchases while working a show. The Verafone systems are basically 300/1200 baud modems.

Alarm system companies are mating alarm systems to cellular phones for use as a secondary (or even primary in a remote area) means of communication between the alarm system at the customer's site and the central station.

Recently, the Metro-North commuter rail service in the New York City metropolitan area started offering public phone service on their trains. These phones use the cellular phone network.

As one can see, the use of cellular phones has come a long way from some yuppie calling his wife to say he'll be staying at the office late, and then calling his mistress immediately afterwards to tell her what hotel to meet him at. Those who like to listen to real-life soap operas however will be relieved to know that such conversations still occur over the free and open airwaves despite all the other activity.

Equipment Availability

In addition to outrageously expensive pieces of surveillance equipment sold to law enforcement agencies (the Harris Corporation's "Triggerfish" being a prime example), there exist other types of equipment which can be used for interception of cellular telephony. Even if such a specialized function as tracking a specific MIN/ESN pair is required, the technical specifications of the cellular phone network are publicly available so any competent technician can design a piece of equipment to do the required job. An intercept station can be put together for about one-tenth the cost asked for by "law enforcement suppliers" and "spy shops".

Despite the ECPA, receivers capable of receiving cellular still abound. Readily modifiable scanning receivers made before the Part 15 revision are grandfathered, and the existing stock may still be sold. Since these units are "high-end" models and priced accordingly, they are still on the shelf waiting to be sold.

The specific wording of the new FCC Part 15 Regulations denies certification to "readily modifiable scanning receivers". Some of the new scanners put on the market since the Part 15 revision have been modifiable via a hideously detailed and complicated procedure. Apparently, a modification involving the desoldering and resoldering of multiple surface-mount devices isn't considered "readily modifiable". One manufacturer has taken a different approach on their new models. The cellular frequencies are locked out via the programming in the scanner's ROM, so no modification is available short of burning a new ROM for the scanner. There is however, a code sequence which can be entered into the keypad that loads test frequencies into the scanner's memory channels for diagnostic purposes. Some of these test frequencies are within the cellular phone band. From there one can then tune above or below the test frequencies and receive the entire cellular phone band.

Most scanners that have 800 Mhz capability will receive the cellular phone band via the image method. Due to the design of the receiver, a scanner will receive a signal at twice the intermediate frequency (IF) above the actual frequency. Most scanners have an IF of 10.7 Mhz, so one is able to listen to cellular by listening 21.4 Mhz above the cellular frequencies. If the signal is adequately strong, it will also be able to be received 10.7 Mhz (of whatever the scanner's IF is) below the actual frequency.

Obviously, cellular phones are exempt from this regulation. Cellular phones can usually be put into a diagnostic mode that turns them into a standard receiver/transmitter in order to be more easily tested during the troubleshooting/repairing process. The Oki 900 and Oki 1150 (also known as the AT&T 3730 and AT&T 4740 respectively), have software available for them from Network Wizards that will enable it to track a specific MIN.

MIN tracking can also be done with the CCS DDI (Digital Data Interpreter). Current versions of the DDI are unable to read reverse control channel ESN data in an attempt to prevent cellular phone fraud. They will still, however, read the forward control channel data. When used with an older Icom R-7000/7100 receiver, the DDI will automatically tune the Icom to follow the conversation.

Scanner frequency converter kits that enable non-800 Mhz capable scanners to receive the 800 Mhz band (including cellular) are still being sold. One can also make an 800 Mhz frequency converter out of an old UHF TV tuner that covers TV channels 70-83 - which are now the 800 Mhz band.

The Optoelectronics R10 near field receiver is a device which looks for nearby radio signals between 25 Mhz and 2 Ghz and automatically tunes them in. It will also display the received signal strength and frequency deviation. It is classified by the FCC as a piece of test equipment. If one were to get close enough to a cell site or an in-use cellular phone, the R10 would lock in to the signals from the transmitter in question. If one is monitoring a mobile unit which is handed off to another cell site, the

R10 is able to quickly reacquire the signal, as it is capable of searching through its entire 25 Mhz to 2 Ghz coverage in two seconds. By adding the optional cellular bandpass filter and/or attaching an antenna tuned to the cellular frequency range, the R10s effective range can be increased while also rejecting unwanted signals from outside the cellular telephone band.

Frequency counters are also a useful piece of equipment. After having experimented with the Radio Shack unit, I have discovered that using the supplied telescoping whip antenna, it will lock on a 3 watt phone running with a 5/8 wave antenna from a range of 50 feet. I'm sure the range could be increased by using a bandpass filter, amplifier, and/or cellular antenna. The Rolls Royce of frequency counters is the Optoelectronics Scout which was intended for SIGINT operations. Among other interesting features, it is equipped with an OS456 interface and will automatically "reaction-tune" an OS456-equipped receiver to whatever frequency the Scout picks up, and can send data on frequency acquisitions to a PC.

A laptop or palmtop PC will also be needed if one desires to use the DDI or Network Wizards Oki Kit. One should also have a copy of Video Vindicator's Cellular Manager software for reference purposes (converting frequencies to channels, finding what voice channels correspond to what control channel, and finding information about adjoining cell sites).

Interception Techniques

The most common intercept technique is to program the upper and lower limits of the cellular band into a scanner's search memories and use the search function to go through all 832 channels. With a scanner that searches at 25 channels per second, a complete search would technically take 33.28 seconds, not counting time spent initially listening to communications to determine if they contain relative content. This technique is adequate for highly-populated urban regions where there are a large number of frequency groups used for a given area. In a lesser-urban, suburban, or rural area this technique wastes too much time, as only a small fraction of the channels are used. It is also difficult with this technique to reacquire a target when it is handed off to another cell site.

A better approach is to program the frequencies being used in the area of operations into a scanner. Each control channel only handles 20 voice channels. So, if one has 10 control channels in their area of operations (equal to 10 cell sites in most areas), that's only 200 channels that have to be monitored. This technique will cut down on the number of frequencies that have to checked, and allow for more efficient coverage.

Those techniques are generally used for non-specific monitoring. Once an "interesting" conversation is noted, the target can then be identified and techniques designed to be aimed at a specific target can be employed. Typically, the control channel is determined by noting the voice channel being used by the target. Once the control channel is identified, the data stream can be monitored which enables easier tracking of the target during handoffs and easier acquisition of the target on the network.

Target specific monitoring falls into two categories. The first is a target with a known MIN. The second is a target which has been visually acquired and noted to be using a cellular phone.

Tracking a known specific MIN is generally a matter of having the right equipment and being in the same general area as the target. If the target travels over a wide area, one will have increased difficulty with monitoring. If such was the case, then the surveillance technician would have to maintain multiple listening posts in the various areas the target is known to frequent, or in the case of court-approved activity monitor the target at the MTSO. The tool of choice would be an Oki phone with the appropriate software, or the DDI unit hooked up to an older Icom R-7000/7100.

If one is on a budget and knows the target's voice, one can also manually scan through adjoining cell site frequencies until the conversation is reacquired. This will, however, result in losing part of the conversation.

For a target that one has visual acquisition on, one can determine the reverse channel frequency being used by means of a frequency counter. Once that is accomplished, the rest is easy. The forward channel operates 45 Mhz above the reverse channel. As the target moves from cell site to cell site, the frequency counter would indicate changes in operating frequency. The ultimate would be an Optoelectronics Scout sending frequency information to a PC which would then automatically tune two separate receivers to the forward and reverse voice channels.

Under normal circumstances, the forward voice channel will also repeat the reverse voice channel audio (this is called talk-around or side-tone). If, however, the target is using a hands-free unit there will be no talk-around so as to avoid feedback. The result is that one will only hear half the conversation: the landline talking to the mobile on the forward voice channel. This can be a problem if one's receiver has no reverse voice channel monitoring capability, or if one is too far away from the target.

Conclusion

For the cost of a good VCR or TV, one can listen in on cellular phone conversations and be able to track the phone's user as he goes about his/her business. Yes, it is illegal. Then again, so are certain types of sexual activity, but I don't see that stopping anyone. From a practical standpoint the identification of perpetrators violating the cellular provisions of the ECPA is virtually impossible.

We all know that a law isn't going to stop people from listening to radio communications. Various totalitarian states have tried throughout modern history with no success. Nevertheless, the retailers of cellular telephone equipment continue to placate potential customers with the lie of "No one can listen in. It's illegal." As a result, users of cellular phones are misled into thinking their conversations are as secure as they would be over their home phone. They then say things which open them up to victimization by a very small minority of individuals who monitor cellular communications in order to find potential marks. I don't see this ending anytime soon.

Some might argue that by providing this information I've clued in certain miscreants who might go out and do just that. This might be true, but I've also clued in people who use cellular phones to the fact that what they say over the air isn't private at all.

If one wants to take the attitude that talking about something encourages it, then perhaps we should pass a law banning the media from talking about murders, drunk driving, and a whole other host of unpleasant things that we'd like to discourage everybody from doing.

I didn't think so.

Thanks go to Bernie S. for his assistance with this article.

References and Sources

1. "Cellular Telephony" (g-file), by Brian Oblivion/Restricted Data Transmissions (RDT)

2. "Cellular Secrets" (g-file), by Bootleg

The above g-files should be available on any decent H/P system.

3. Introducing Cellular Communications, The New Mobile Telephone System, by Stan Prentiss, TAB Books

4. Network Wizards, POB 343, Menlo Park, CA 94026

Sells Oki Experimenters Kit.

5. CCS, POB 11191, Milwaukee, WI 53211

Sells DDI (Digital Data Interpreter).

THE BETTER LETTERS

More Bookstore Fun

Dear 2600:

I recently came across your magazine in a local bookstore while browsing in the rear. I had heard of *2600*, but I never expected to see it in a store. It was hidden off to the back with other magazines with a "questionable" background. The lady at the register had no idea what the magazine was about, but when I told her she responded with, "Well, isn't that a great thing to encourage." She basically pissed me off. Such comments show the general ignorance of society. People need to realize that hacking isn't a crime; it's simply knowledge. I've met so many people who believe all hackers are bad people. Most describe hackers as snotty-nosed brats. They don't realize that hackers are human. They're real people, with real lives (sometimes), who happen to be very intelligent. It makes me sick to see the stereotypes given by the general public to hackers.

Seventh Son

Piracy Proposal

Dear 2600:

I read the Spring 1994 issue of your magazine with great interest. I had never seen your magazine before, but when I found it for sale in a computer bookstore in a Jerusalem mall, I just couldn't resist.

I found the article "Software Piracy, Another View" by Roberto Verzola extremely thought-provoking. According to Verzola, if a company spends money and time developing a program, they lose nothing by having people pirate it (his word), as the pirates "have not denied [anyone] the use of the program". He says that the "'theft' of intellectual property... [is] not [a] very accurate [description] of the act, [which is] different from the crime of theft or actual piracy."

I have considered Verzola's point of view very carefully, and arrived at the following course of action, which I am sure that neither you nor he can possibly object to. Should you object, I expect both a registered letter to the above address, as well as an explanation in a future issue, with a copy of said issue sent to me by registered mail, as I doubt that I will have easy access to a future issue (I don't get to that computer bookstore very often).

I plan, therefore, on the following course of action:

1) I am going to sell Verzola's article to other magazines, under *my own name*, and keep all and any profits ensuing therefrom. According to Verzola, "using [the words 'piracy' and 'theft' of intellectual property] automatically connotes immoral action on the part of the copier." He also writes, "How can you be selfish if you can give things away and have more than what you started with? How can we deny a good friend if we can also keep it for ourselves?" Well, I assume that Verzola has made all the money he expected to make from his article, so if he gives the article away to me, he's also keeping it for himself (i.e:, he can also use it for himself). I'm certainly going to have more than what I started with, as soon as other magazines pay *me* for Verzola's article!

2) Here I'm making a small assumption, namely that editorially, you agree with Verzola's views (you certainly print no disclaimer). Therefore, I have decided to run off thousands of copies of your magazines and give them away for free, asking readers to reimburse me only for the cost of making the actual copies. Although, according to Verzola, "[I] might be charged with violating the copyright or patent laws of a country", he also feels that I will be doing nothing morally wrong. I can't believe you would try to prosecute me for following my conscience and doing nothing morally wrong. In fact, I shall be offering intellectual stimulation to people who could not otherwise afford to read your magazine!

Should you feel that anyone is being financially hurt by either (1) or (2) above, you're going to have to decide if copying a magazine is different than copying a computer program and, if so, how.

Daveed Shachar
Israel

It would be difficult to match the distance that you missed the point of this article by but, rest assured, you are not alone in your thinking. We don't expect to sway your opinion but we owe it to our readers to clarify your points. First, the issue of money was brought up by you, not by the article. The article dealt with the free distribution of a program, not reselling it and keeping the profits, as you apparently desire to do. The sole reason for this kind of distribution is because without it, there would be no access at all. Denying access because of financial reasons is distasteful to a large part of the hacker world, particularly when the pricing of this access seems to be so arbitrary. And, for the record, the article itself was given to us freely, to republish as we wished. What you suggest concerning our magazine has been taking place since our inception. It's called free exchange of information. Articles are xeroxed, passed around online, faxed, etc. All for the sake of spreading information, not just making a profit. As writers, our primary concern is to get people to read what we've written. To expect everyone who even glances at an article to pay a "licensing fee" would be selfish, unrealistic, and contrary to the purposes of writing in the first place. And for someone else to resell another's work without their permission is even more of an affront to the hacker ethic.

Eastern Europe Scene

Dear 2600:

I really don't believe it's been one year since I subscribed to *2600*. Well, as you Americans say, "Time flies when you're having fun." Well, I don't really want to waste your time writing crap but I really wanted to thank you for doing such a great job with your magazine.

I'm Bulgarian by origin but I've worked and lived in Hungary for more than five years now. I started doing computers eleven years ago. You guys can't even imagine what it was like at that time. The most exciting moment was when I sat in front of a real Macintosh (during the Communist regime, there were absolutely no Macs in Eastern Europe). There's still a lot to learn - the problem in Eastern Europe is the lack of good equipment. Can you believe that the Internet connection between Hungary and the outside world is a 64kbps line? Have you ever tried Mosaic together with a few hundred other users on a 64k line? Better not....

I would like to express my appreciation for having me as a subscriber (I received this year's magazine for free as an Eastern European subscriber). I'm curious if there are other Eastern European subscribers and what their opinion on *2600* is.

The MacMan
Budapest

For the record, we are still offering free subscriptions to people in Eastern Europe who write and request them. We hope this makes a difference.

Locked Up

Dear 2600:

I have been in federal prison for twenty months since I was arrested by the Secret Service for placing a phony ATM in a Connecticut shopping mall. Actually, the ATM was real - I just forgot to connect it to a bank - the Secret Service has no sense of humor.

I never knew your magazine was available before coming to jail. Maybe it was for the best - I probably would have gotten myself in more trouble - you have great articles. It takes me back to my high school and college days fifteen years ago when I lived to hack the DEC-10 and DEC-20.

As you have stated in several articles, the Bureau of Prisons (BOP) are major assholes. They do everything they can to keep me from your publication. I finally had a friend photocopy some old issues and staple a few pages of religious material on top and send the disguised copies in. This seems to get past the mail room hacks every time.

A word of advice to your readers: If you ever come face to face with the Secret Service, keep your mouth shut. Nothing you say will help you. They feed on intimidation and threats and can make an arrest a horror scene. They will then try the smooth and friendly approach to get what they want. They will promise you the world if you will just cooperate before it is too late. (It will not be too late - no matter what they say.) They will start with only wanting your help with your software or your little tricks of the trade. Don't do it! They lie! Someone will always have a superior who will overrule them when they are done with you. The government will *fuck you*. Keep your mouth shut and never never say anything without a lawyer.

The Secret Service promised everything they could to get all the copies of my ATM software along with the message protocols and technical manuals on the ATMs. They didn't want that shit on the streets. When they thought they had everything they wanted, the U.S. Attorney's Office proceeded with the fucking and their lies came out. *Don't trust - don't believe.* You'll regret it - I do.

ATM Bandit

This is a valuable lesson a lot of people have learned and one that even more will still have to experience. Many of us read about your ATM "hack" in the papers - while the idea was quite clever, setting it up and taking people's money was pure theft. Not bowing to this kind of temptation is one of the hardest challenges hackers face.

Dear 2600:

I recently read about your magazine in the December issue of *Details*. I now have the fall issue of *2600*, with which I am impressed. I would like to extend a big congrat to Phiber Optik on his release from the feds. I too am in federal custody at this time, have been since 1991, and have exactly one year to go. This too will pass. I would really like to see more Internet information in *2600*, although I can't really judge it by a single issue. I wish to have written correspondence with someone out there who is willing to give me an Internet e-mail account. There is information on the net I would like to receive, but I have no one to retrieve it for me. All I would require of this individual is to send me printouts and type in messages to friends I can't communicate with. If anyone out there in the real world would like to assist me in this way, respond in a future issue and I will write to you directly.

Phafnir

Dear 2600:

Today, for the first time in five years I had the opportunity to read *2600*! I very much enjoyed it - a true test of the First Amendment!

Unfortunately I am confined. Because of my past employment with Bell, I find myself being blamed by the U.S. Bureau of Prisons for every breach of their FTS system and put into the hole (solitary) regularly!

Even when a staff member lost his Token Ring access program for "Sentry" (this program unites an XT to the BOP mainframe), they again put me into the hole and went haywire - of course I *sued!* I won.

The Cryptic Prognosticator

Bits of Info

Dear 2600:

The 303 ringback is 99X-YYYY where X is any number and YYYY are the last four digits.

Zeek (Major)
Colorado

Dear 2600:

There's a simple way to avoid telemarketers using predictive dialers (Letters, Summer 94, page 42). The volume sensitivity is usually set so that it won't recognize that you answered unless you speak fairly loudly. I've gotten into the habit of answering the phone with a quiet "hello". Humans can hear it, but not the salesmen.

Skimmer
Cambridge, MA

Digital Correction

Dear 2600:

I just finished reading a friend's *2600* (Winter 1993-94) and I noticed an error. Page 38 describes a Digital lock, made by the "Lockey" company. They indeed are difficult to find in the U.S., however they are quite common throughout Southeast Asia. The error that was published is that the combination "is always five alphanumeric characters long". There are extra "key" tumblers that could render the combination four to six alphanumeric characters long. So you could continue to plod your way through all the combinations or you could buy a cheap chemical that is visible under ultraviolet light, spread it on the keys, wait for it to be opened, and check it out.

Spook

Intercept Tones

Dear 2600:

A use for those "recorded intercept" tones mentioned in the Summer 94 issue (the tones that precede "the number you have dialed is no longer in service"): I read in a very old Bell Technical journal in our company library that these tones allow Bell switches to automatically track statistics of what percent of calls do not go through. However, I have seen the phone installers in action and they routinely take a phone off hook for extended lengths of times when they're reprogramming the local switch. This causes the "time allotted for dialing" recording to trigger, followed after a minute by the loud brapping tones (0dBm vs. normal -20dBm). After several cycles of this, they get tired of hearing it so they redial a non-existent number just to get rid of the brapping. If you think of how many repairmen do this every day, you get to wondering what statistics they really end up keeping (like productivity stats of their repair crews).

Scott

Buena Park, CA

What's really amazing is the fact that the vast majority of intercepted numbers (out of service, disconnected, or changed) never hang up! For toll-free silent numbers, these can't be beat.

Monitoring Mail

Dear 2600:

Paranoia's concerns regarding mail monitoring (Autumn 1994) are understandable, but overstated. The surveillance he envisions would not work with most post box services or apartment buildings. For example, my city has several private mailing centers which offer post boxes. The bar codes I decoded for them indicate that the delivery point is only their street address, and does not code for the individual "sub-addresses" inside. Thus the same postal code applies to hundreds of individuals. It is barely feasible to code the delivery points for the required number of sub-addresses under the current system without reassigning the whole area's zip+4 codes. There are, after all, usually more than 100 post boxes in these places, with only two digits to represent them all, including the neighbors within the +4 area.

The word I got from my helpful post office was that each block of house numbers has two of its own +4 codes, one for the even and one for the odd side of the street. Each time the numbers progress from one hundred to the next, the code changes. If a block of 600's were separated by an intersecting street, the two subsets would have unique +4 codes.

A list of all the +4 codes can be obtained from Semaphore Corp. at (408) 688-9200, in a database format compatible with Apple Hypertext. The product is designed to clean up the addresses in your database and standardize them for a discount in bulk mailings. The price in 1993 was $125.

Drew
62901

Red Box Problem

Dear 2600:

I have been an avid follower of your magazine and have always turned to it for advice. Now I have a couple of questions to ask. Recently I built a red box. It worked great for a while. Then, for some unknown reason, it stopped working! I didn't change the box or the tones. But now, whenever I try and use the box on a phone, an operator comes on the line. I'll be in the middle of playing the tones and all of a sudden I hear: "This is AT&T. How may I help you?" What happened? I live in the 206 area code. I have one other question - what are the chances of getting caught while using extenders? I've been using a local one for a while now and nothing has changed. What are the chances of me getting caught?

Pestilence

Hardware and software upgrades are making detection of red box tones easier and more reliable. If you get the same results regardless of location, your box clearly isn't good enough to fool the system. As for getting caught, this really depends on how blatant you are - phone companies have historically put in little effort to track down red boxers.

ATM Fun

Dear 2600:

While at my local Citibank I was playing around with one of the ATMs (with a touch screen pad thing). Pressing the screen on the bottom where the words are underlined a few times got me into the diagnostic mode. When you try to use the diagnostic mode it makes some weird sounds and goes back to normal.

Kilobyter
Flushing, NY

If you have in fact stumbled upon a diagnostic mode, there must be a proper way to use it. Keep experimenting and you'll find it.

True Hackers

Dear 2600:

Although I have known about your publication for years (your mag has been referenced in hundreds of text files on hacking and phreaking), I have only recently acquired it through our new Barnes and Noble Bookstore. I was almost shocked to see it on the same shelf as the computer mags! I didn't think it was even still being published, but am very glad that it is. The Winter 1994-95 issue is only my second copy, but I must say that *2600* is everything everyone said it is.

In reference to several letters in the above mentioned issue, I was happy to hear your opinions on destructive hacking and phreaking. JL of Highland, CA was nothing but destructive by erasing that hard drive and uploading a virus. JL is the type of "hacker" that gives us all a bad reputation and pisses off the media. A *true* hacker would never think of doing such a stupid thing as destroying data or inserting viruses. A true hacker hacks to see if he or she has the necessary skills to do it, looks at things, then gets out! JL should not be proud of this accomplishment at all, but be sorry and promise never to do it again or completely give up hacking. Cat in the Hat from Warner Robins, GA was also wrong to even think of cutting wires in that terminal can. How would the Cat like it if the phone lines to their residence were cut or tampered with? Or, would the Cat like a $500 phone bill where all calls were undoubtedly made from his phone number? I doubt it.

Edison Carter

Mystery Computer

Dear 2600:

Here in California, Pacific Bell uses a special prefix for their company phone numbers - 811 - which I think is dialable from all area codes in California since some of the numbers reach northern California and some reach San Diego when I dial them from Los Angeles. These numbers are always toll free, even from payphones and most COCOTs, and are *not* dialable from other area codes outside California. Many of the numbers are assigned to Customer Service and printed on people's phone bills to call in for billing questions, etc. However, there are many *other* numbers for special offices, and some Pacific Bell employees even have their own voice mail numbers with dial out capabilities! While exploring these 811 numbers, I came across a computer. The computer voice greeting says, "Port 3, Module 1. Notice: This is a private computer system. Any unauthorized access will be investigated and prosecuted to the full extent of the law. Lurgin." My guess is that "lurgin" is an industry variation of "login". Also, the port and module number probably vary depending on where you're calling from. It is not a dial-up. It is accessed and used by touch tone entries. After entering eight to ten digits and hitting #, the system responds with "password". After entering another eight to ten digits and #, the system responds with "passcode invalid". Any ideas what this is? DEPAC computer for installers? The number is 811-1200.

William Tell

The "lurgin" you hear is no doubt a strange computerized pronunciation of the word "login". As for the purpose of the system, we can only theorize that it's something phone repairmen would use while on the road since virtually every other telco employee would have access to a "real" terminal. Keep a close eye on the next repairman who works on your phone.

Source of Income

Dear 2600:

Recently I was at a payphone and I needed to make a call. I deposited a coin and tried to make my call but as soon as I had dialed the last number the line just went dead. This pissed me off because I didn't get my quarter back. So I called the operator and told her what happened. She then happily said she would send me a check in the mail. This got me thinking - how could she possibly know how much money I put in the phone? So about 15 minutes later I called a number in Washington without inserting money (I was calling from California). The message came on and said that I needed to insert $2.70. Then I hung up and called the operator and told him the same story that I told the other operator. About four weeks passed and, just when I was beginning to think that the checks would never get here, I found two checks in the mail, one for 25 cents and the other for $2.70! I've been doing this for about six months off and on and so far I haven't seen any white vans parked outside my house.

CMS
Santa Rosa, CA

You never see the white vans until it's too late.

Strange Numbers

Dear 2600:

I just picked up the Autumn 1994 issue of *2600* and loved every page. I read the news article about the 800 number for the House of Windsor catalog and how it would tell you the address of the person you sent it to even if their phone number was unlisted. Since I have an unlisted number, I decided to give it a call to see if I could send myself a catalog. Wouldn't you know it, the article was right about there being gaps in the database - like the whole state of Idaho!

Last night I was scanning six digit numbers trying to find an ANAC number for my area when the number 115742 came up. After the fourth number was dialed, it started to ring. It turns out that when you dial 1157 you get a recording that says "The last number called to your phone has been traced and a $1.00 service charge has been added to your bill. If this is an emergency, hang up and call 911 or call 1-800-

582-0655 to have the charge removed." Is this some form of caller ID? And if a caller dials *67 before they call, will it disable the feature?

Jason
Boise, ID

*We're told the House of Windsor number now connects you with a human, so looking for gaps will be a bit trickier. What you're connecting to by dialing 1157 is the same as if you had dialed *57. This phone company "feature" really doesn't accomplish anything and is a great way for the telco to make money from harassing calls. By law, they are required to trace these calls without charge through their Annoyance Call Bureau. Anyone with access to features like Call Return (*69) or Repeat Call (*66) can use *57. *67 will not keep it from working.*

New Technology

Dear 2600:

I'm writing you from a cafe in Palo Alto, CA. I am using a small, battery powered communicator that is able to send messages over the Ardis (digital cellular) network.

This device, which runs the Magic Cap operating system and will cost less than a laptop, can send images and sound to anyone running the Magic Cap software. I can send/receive ASCII-only messages with folks on the Internet, Compuserve, AOL, Prodigy, and just about anyone else with inter-networked email.

There are many open security questions in digital cellular communications that need to be solved. I encourage *2600* readers to get a scanner, cell phone, or digital modem and experiment!

Bitslicer

Conscientious Trashers

Dear 2600:

Here is a copy of a letter we sent to NYNEX:

"To Whom It May Concern at NYNEX:

"We were recently going through certain central office and switch dumpsters and were shocked to discover the amount of recyclable and reusable materials that were being discarded as ordinary landfill fodder.

"For instance: hundreds of brown manila envelopes mixed in with the coffee grounds and Dunkin' Donuts wrappers. These envelopes can easily be reused for new files, and the discarded contents contained in them should be recycled instead of thrown in ordinary trash. Approximately twenty feet away from this particular switch's dumpster is a huge recycling bin, with containers for paper, plastic, cardboard, aluminum, and glass, which is consistently empty.

"Corporations and individuals send millions of tons of recyclable materials to the landfills *every year!* The corporations such as yourselves are the largest contributors to this eco-waste, and *must* do their part to help stop this growing trend.

"We realize we can't exactly boycott you for irresponsible environmental crimes, but we think you can see the advantages of cooperating anyway, because as we *all* know, the media is indeed a powerful tool. It's not like we're asking you to lower rates or anything (although that would be nice too), just to be responsible stewards.

"Thank you for your careful thought and consideration.

"Hackers for a Cleaner Planet"

Satellite Theory

Dear 2600:

About Alcatraz from Pt. Pleasant Beach, NJ in Autumn 1994 Letters - the little satellite dishes atop his local food stores are possibly/probably for inventory. If they're chain stores or subsidiaries of larger companies, they're probably using the dishes to transmit sales to the central office/headquarters. A list of purchases goes from the register to the dishes to the main company who then know what to order. Immediate gratification for Vons.

Anyone with your credit or debit card number can probably cut in and get an exact list of *what* you're buying, not just *where* you're buying. Not just food stores do this, most high-volume chains have automated inventory control through wires or satellite dishes. If *you* want to do this, I can't really help, but I'd recommend getting into the computers at a particular location, and intercepting data from there.

Daughter of a Satellite Engineer

A Fun Project

Dear 2600:

I got a friend to buy me a copy of the Autumn 1994 *2600* and I am truly impressed. I had heard about your magazine a long time ago but this is my first issue and it's great. My one gripe, however, was the article "Breaking Windows". In my opinion, most of the information set forth in this article demonstrated basic DOS and Windoze knowledge, nothing difficult enough to be included in an article in a magazine of this calibre.... However, I do have a suggestion for anyone who might try these tips: If you do bring a disk with you, keep a copy of attrib.com on it. A lot of stores will make their windoze files +rs and then delete attrib, making it impossible to change them back (most will also delete winfile.exe). I always have fun changing the color scheme to something like hot dog stand, making the win.ini +rs, then getting rid of attrib and winfile!

Quasinym

Mystery Number

Dear 2600:

In Volume 11 Number 3 Zappy from Atlanta asked about dialing any number in area code 404 with a 666 prefix and getting a strange series of DTMF tones returned. After a bit of playing around here is what I found. A 15 digit series is repeated over and over. It consists of the following: #4*400———-*5. Replace the seven dashes with the number you called from. I tried this from three different lines with the same results. It always starts with #4*400 then the seven digits of your number followed by *5. Ever heard of this?

Tony Sharp

Whatever this was, we can no longer reach it from our area.

TV Garbage

Dear 2600:

A couple of weeks ago, I was flipping through the channels of my TV set and saw a commercial for a show about "Hackers". It looked interesting to me, so I decided to check it out. After about an hour of boring World War II footage, the show finally came on. I was so disgusted! They showed hackers as evil people trying to take down all the computer systems in the world. It even had so-called "real" hackers on the show who had destroyed people's systems. They told their stories about how they erased all their valuable information and other insane stuff like that. I hate these so called "real" hackers who stereotype *all* hackers in the world as evil criminals. I have never erased *any* data or wrecked any computer network in all my years of hacking. When I do "get in" or find a back door or hole, I report my findings to the system operator so he can fix it.

The show kept going on and on about how evil hackers are. I was about to hit my TV when the *2600* editor came and set it right. "Most hackers know where the line between good and bad is... and most hackers don't cross it." I would have liked to have heard more, but they cut him off to go on to all the evil stuff. I would just like to say thanks! We've got to get rid of the stereotypes!

You also saved my TV set.

Puppet Master

Hacking Airphones

Dear 2600:

A couple of months ago, I flew on Delta Airlines. I hadn't been on a plane in three or four years so I was surprised to see that they have public Airphones that are easily accessible now, and they had one for every three seats. Well, I immediately looked up the charges in the brochure, and of course they were sky high (no pun intended). I think it was about $2 a minute for domestic calls... worse than payphones if you can believe that.

Anyway, I noticed that directory assistance was *free!* So I wanted to call it because I thought it would be exciting to make a phone call in flight. (It doesn't take much to amuse me.) The thing was - the phone required a credit card for billing. Being cardless, I asked my friend next to me if I could use his credit card to make the call and told him he wouldn't be charged. Well, he was wary and skeptical of my goal so he refused to lend it. So, I rummaged through my purse looking for any card with a magnetic strip. I found my bank card. Picking up the phone, I swiped my bank card through the reader to see what would happen. Next thing I heard was a bunch of DTMF tones, then the automated operator voice saying "This is an invalid credit card."

I think it reads all the numbers off a magnetic strip and plays them back in DTMF tones! Now, if I were to have recorded them and had a clear enough recording... maybe I would have been able to decode them and find out what's on my bank card.

The Airphones have much potential and leave much to be explored.

Empress
Georgia

Mac Attack

Dear 2600:

I've recently seen quite a bit of material on the Mac program AtEase, and some complicated and roundabout methods to get by it. When I was using an AtEase "protected" system at school last year, we had a very simple method to get around it when we wanted to get to the finder. Simply go to the "Find File" option, and look for "AtEase Preferences". Open it up and look at it with the file finder viewer. The Finder password is stored, unencrypted, in the preferences file, in a predictable place. I don't remember where exactly, but the pronounceable passwords that most people choose will stand out like a sore thumb among the metacharacter crap. Remember this password, and use the "Go to Finder" option of AtEase. Whoopee! You're free, no mess, no traces of your intrusion, and you can remember the password for future access. It's a method hardly even worthy of being called a "hack".

Rev. Mr. DNA

Computer Numbers

Dear 2600:

In your Winter 1994-95 issue of *2600* on page 27, Paul of New Jersey mentioned an NXX-9901 number that was dialed on the November 23 show of *Off The Hook.* I have found that the following numbers in the 201 area code yield some interesting results: 337-9902 - "ENTER PASSWORD", 848-9920 yields no output, 848-9901 - "ENTER PASSWORD: WRONG", 694-9901 - "ENTER PASSWORD: WRONG" These all connected at 1200 baud. What are they? Switches? Also, how would I found out what type of switch I'm on?

The Phantasm

We're not aware of a uniform switch announcement for New Jersey; your best bet, believe it or not, is to ask your business office - repeatedly. As for the computer, it's quite possible this is some kind of passworded modem that leads to something else. A switch would most likely ask for a user name as well as a password.

Fun With Cordless Phones

Dear 2600:

A few months ago I read an article in your magazine about monitoring cordless phones in the 46 and 49 Mhz area. I am new to phone and computer hacking, but I have been frequency hacking for years and I think your readers will enjoy the information I have to offer. The following information will enable the hacker not only to listen in on, but also *transmit* on cordless phone frequencies. You will need to purchase an amateur radio. I have found that the best radio for the job is the Kenwood TM-742 or its predecessor, the TM-741. These are amateur dual band radios that are designed to be used on the 144 Mhz and 440 Mhz band. These radios are modular so the band modules can be removed, but they can also hold a third band module. The band module you will need will be the 6 meter (50 to 54 Mhz) band module. The TM-741 is an older version of the 742 and can be bought cheaper than a new 742 (around $300.00). A new 6 meter module goes for about $100.00, about $50.00 used. You will need to have the radio modified to transmit and receive out of the amateur band. The mods are very simple and can be done by almost anyone with a little soldering experience and a 15 watt soldering iron. The mods are readily available from any amateur dealer and in most cases the dealer will modify the radio for you if you buy it from him or her. But the mod consists only of removing two surface mount resistors on the 741 and moving two surface mount resistors on the 742, real easy stuff. After the modification has been done and the 6 meter module installed in the radio, all you have to do is enter the cordless frequency in memory and you can transmit away. I would rather not be specific about the uses of this, but I'm sure we all see the possibilities. Also, as a note, most police frequencies are in the 460.00 Mhz area around the country. If you have the 440 Mhz module, the mod lets you transmit there as well. The possibilities are endless. Good luck and i hope this helps.

Radio Man, Tom

HACKING IN BRAZIL

by Derneval

Before talking about hacking here, it's good to describe the conditions of living. Right now, the country is a mix of Belgium and India. It's possible to find both standards of living without travelling long distances. The southern part of the country is where most of the industry is concentrated, while in the west one can find the Amazon jungle. There are many Brazils, one could say.

Hackers and computer enthusiasts have several different places for meeting. When "War Games" came out, the real places to meet hackers and make contacts were the computer shops, game arcades, and "Video-texto" terminals. The computer shops were a meeting place because many of those "hackers" had no computers of their own and the shop owners would let them play with theirs as part of an advertising tool to encourage people to buy one for their kids. Today that is no longer needed, since prices have dropped down and hackers meet at schools or sometimes just join a BBS (most people who buy a modem end up thinking about setting up a BBS). By the way, most schools are advertising computer training as part of their curricula, to charge more, and like everywhere, I guess, people no longer learn typewriting, but computer-writing, and many Brazilian newspapers dedicate a section on computer knowledge once a week, with advertising, hints, general info, and even lists of BBS's.

A few years ago, the "Video-texto" terminals were also big meeting places. That was part of an effort to make popular the use of a computer linked by modem to get services like msx-games, info on weather, bank account info, and so on. Just like the Net, one could do e-mail, and perform some fancy tricks and other things that could be called hacking. The difference was that it was created by the state-owned telephone company and each time the trick was too well known, it was changed. The real trick was keeping in touch with the people who used the system like hell. It's no different than what happens with the computer gurus. The protocol used for that system (X-25) is the same as is used for the banking money transfers, but it wasn't possible to do anything more than checking how much money one had and a few other things. People who used that at home (not too many, since the company didn't think it would be such a hit, and didn't provide for it) could spend their fathers' money discovering funny things about the system, like messing with other people's phones and such. One could also use the terminals at the Shopping Centers to make phone calls to their friends without paying. The guy at the other end would be heard by the small speaker.

Phreaking here in Brazil is something secretive. Apart from the trick described in the section "Letters To Read By" in the Summer 1994 issue of 2600, where one would call through locked rotary telephones, little is known about phreaking. One thing is that people who enrolled in Telecommunications Engineering could call Europe and USA with ease, but they would not tell you how. It must be said that all public phones have metal cables around the wires and that the phone machines are quite tough to break down. I guess it wasn't for beauty.

The phones use some sort of metal coin called fichas, which must be bought somewhere. The trick is to use a coin with a string, so it would not be collected. But if the police caught you.... The police don't follow rules for things like this. Either they would fine you, or arrest you for vandalism, or whatever else they can think of at the moment. It is a hassle.

My friend who was doing Electrical Engineering told me that boxing in Brazil was impossible. The system is just not good enough to be boxed. Other friends of mine told me that in the Northeastern part, the phone system can be boxed. The phone company doesn't admit any knowledge about that.

Internet access is something quite hard to get today. Until a few weeks ago, it was impossible to create an Internet site that was not part of some research project. So only universities and the like were capable of putting people in the Net Universe. In the University of Sao Paulo, people in the post-graduation courses could get access with ease, but graduating students would have to show some connection to a research project. That was because the students found out that one could use the IBM CDC 4360 to telnet without an Internet account. Also, all the faculty had computer rooms full of 386's which were linked by fiber optic to this computer. Another one did the file transfers between the accounts and the computer at the computer rooms and ftp was also possible without an account, but only to a few sites. That lasted for about a year, until it was fixed in the router, but only at the Politechnik School. Legend has it that the guys were downloading too many GIF and JPG pictures of top models from an ftp site nearby. That used so much bandwidth that the site started to complain and two things happened: the site stopped storing GIF's of wonderful women in swimsuits and the router was fixed to prevent ftp without an Internet account. One can still today connect to the outside world via telnet and many people have accounts in Internet BBS's like Isca BBS, Cleveland Freenet, and the like. The Bad Boy BBS was "in", until it went out of business. This kind of access is not good, though, for it is very slow. Also, it is hard to download something bigger than 60 kbyte. The way I devised, downloading the file inside the BBS and uuencoding it, you could list the file and capture the screen listing, uudecode it after some editing and have a working .exe or .zip file.

By these means one could, inside the campus, do all the downloading one wanted, from anywhere in the world. Outside the campus, it is possible to do it by phone lines, but the modems will not go faster than 2400 without character correction (no Zmodem at all), which makes it quite hard to download compressed files. To try doing anything but read letters by modem is some kind of torture. The real thing is to do it by "linha dedicada", a special line for computer transmission. It's much more expensive though, but if you have the money....

Perhaps the best way to get access to an Internet account though is to be part of the research project "Escola do Futuro" that, among other things, gets schools linked to the Net. That's what I did and they pay me quite well to search for data in the Net for the students of those schools. The University of Campinas is said to give all students an Internet account regardless of knowledge. Of course, here there's BITNET also. That's doomed for extinction, but for this or that reason, people haven't closed it down. Most teachers use it; guess there's even some post-graduation work written about that. It's easier to access via modem, also. Old habits die hard.

Outside the campus, for common people, there are few opportunities. The only thing you can get, at least until the opening of commercial Internet sites, something about to happen one of these days, is access by mail. You join one BBS with Internet access, and your mail is sent over the Internet later in the day. This is not direct access, as one can see, but it is easy to access by modem. Problem is that you have to pay if you use it too much. The BBS's that do it don't do it for free, also. Connection to Compuserve is also possible, but it costs a lot of money.

Because of the newspapers, knowledge of the Internet is spreading fast and the number of sites is growing the same way everywhere else in the world. Even the military people are starting with it. There are plans to enhance it and make better connections, and some informative material is being translated into Portuguese, like "Zen and the Art of Internet" and made available in the gopher.rnp.br. There are many mirrors from many famous sites, like Simtel20 and at least one Internet BBS, the "Jacare BBS" (Alligator BBS, available by telneting bbs.secom.ufpa.br - 192.147.210.1 - login bbs). World Wide Web sites are becoming sort of popular also, but still available only to a few people who are lucky enough to get the access. Brazilian hackers are not very fond of sharing the knowledge of how to get access and other things, sometimes because of fear of losing it, sometimes because the demand would overload the system. There are no hacker magazines here yet, and very few people confess their curiosity about hacking for fear of not finding jobs. Most would-be hackers either get a job and stop hacking for fun or keep their activities secret in order to pursue their objectives.

Hacking the Tandy/Casio Pocket Computer

by Sam Nitzberg

The PC-6 is a pocket computer that was produced by Radio Shack and also by Casio under another name. It is programmable in BASIC, with 10 areas in which programs may be stored, has a memo-pad area for notes, equations, phone numbers, and the like. A trapdoor is a secret entry point to code. A Trojan horse is a subversion of a program which results in the program performing some function other than the one intended by the user. The PC-6 does allow passwords to be used, but is vulnerable to the attacks mentioned; this is not addressed in the PC-6 documentation.

The PC-6 has a memo pad area and a set of 10 program areas. The memo pad is normally used to store functions, financial information, phone numbers, and assorted notes. Normally, the memo pad may be browsed, and the contents of any program area may be viewed. The memo pad may be accessed directly via keys on the PC-6 keyboard, or the memo pad may be accessed via programs. If a password is set by using the PASS command, any attempts to read the memo pad directly or obtain program listings are denied, and the protect error (Error 8) is returned. While the password is set, programs may still be executed.

This is the trapdoor and Trojan horse vulnerability: once a password is set, the user is locked out at the command level from accessing program listings or the memo pad data. Programs can still be executed, and they may manipulate and access the program area. That is, a user cannot read memo pad contents with the password enabled, but if that user has modified a program present to display or manipulate memo pad contents, that program will execute properly and without restriction.

An example follows. Suppose this is a program in one of the 10 program areas:

```
 10 CLEAR
 20 INPUT A
 30 GOSUB 100 : REM Perform some
    function
 40 PRINT A
 50 END
100 A=A+1
110 RETURN
```

This is not an exciting program. But it may be used to subvert the password mechanism all the same. To covertly provide memo pad access, all that is needed are a few minor code changes. Someone having physical access to the PC-6 only once without the password being set could change the code to the following:

```
 10 CLEAR
 20 INPUT A
 30 GOSUB 100 : REM Perform some
    function
 40 PRINT A
 50 END
100 A=A+1
105 IF A=-9999 THEN FOR Z=1 TO 10:
    READ# $ : PRINT $ : NEXT Z
110 RETURN
```

By adding line 105, the memo pad is subverted. To create the trapdoor, the value of -9999 has been chosen. Presumably the legitimate user will not enter this figure. A subversive user would enter the value -9999 when running this program to activate the Trojan horse property which has been installed. The commands READ# $ and PRINT $ are used to read a single record from the memo pad, and display the record. The net result is that line 105 will cause the PC-6 to display the first 10 records in the memo pad whether or not a password has been set, the Trojan horse. Other than this all programs will behave properly. Similarly, attacks feasible against the memo pad may delete one entry at a time or write over entries. One would be limited only by how many ways there are to manipulate data present in the possibilities of what could be done with the memo pad data.

While this is a simple example, it demonstrates the problem with the password mechanism. Any person who is using a PC-6 is vulnerable to this attack. The only countermeasure besides the obvious - not letting anyone access the PC-6, and always having a password set is to periodically review all source code on the PC-6. If a person who owns one of these does not use passwords and someone were to apply the above technique, it would not matter if the individual

(continued on page 40)

Hacking the Tandy Zoomer/Casio Z-7000 ZPDA

by Enigma

Recently, I purchased a personal digital assistant. I chose the Tandy/Casio model over the Apple model partly because I was familiar with the 8088 and GEOS operating system (I figured I could write software and hardware hacks much more easily), but the big driving force of my decision was a nice employee discount!

Those who own the ZPDA and are already familiar with the IBM world can vouch that it is very similar to a PC - all the way down to the A:\AUTOEXEC.BAT and CONFIG.SYS. This got me to thinking about how to hack its software and firmware.

The File Manager is one of the most important parts of the ZPDA in my personal opinion. It lets you see which files are located in which directory. It verifies the existence of AUTOEXEC.BAT, CONFIG.SYS, and various *.INI files. The key to hacking into the Zoomer lies in these files - but how to get to them?

Something that Casio and Tandy did NOT tell you is that a simple text editor exists for the standard, stock ZPDA. It's part of America Online's Compose Mail feature. Just launch America Online, select File Open, and use the dialogue box to pick (almost) any file. Try looking at A:\AUTOEXEC.BAT right now. This batch file and its complement CONFIG.SYS are executed when you first turn on the ZPDA and when you press the reset button in the battery compartment. The big problem with this, though, is that these essential files are located on the ROM disk. You can change them on-screen, but when it comes to saving them, you will not be allowed to. So we can't change these. What now?

There are still all those *.INI files lurking about. Can we change these? Try it. The answer is: not directly. There are two main .INI files: B:\GEOWORKS\GEOS.INI and A:\NET.INI. You can open NET.INI and see all kinds of nifty things to play with, but nothing that can be changed - alas, it's on the ROM drive. When you try to open the other file (GEOS.INI), you will get a file error. After some experimentation coupled with my programming experience, I concluded that this .INI file is "in use" by the GEOS operating system itself. Because of this, GEOS will stop you from using that file. At this point, we know that we have to change the contents of A:\NET.INI, but there does not seem to be a way to do that. Oh, dreck! So close and yet so far....

Look through the AUTOEXEC.BAT again and see that it makes a call to a little batch file named MKRAM.BAT. This batch file checks the existence of B:\GEOWORKS\GEOS.INI. If it isn't there, one of the ROM files, A:\LOCAL.INI, is copied to B:\GEOWORKS\GEOS.INI, in effect creating the proper .INI file. This gives us a lead into what is contained in GEOS.INI. Open A:\LOCAL.INI and you will see a simple two-line configuration that points to A:\NET.INI. Hmmm, interesting. GEOS.INI is on the RAM disk (i.e., it, theoretically, can be modified) and points to a config on the ROM disk. We will need to do two things at this point: (1) copy NET.INI to the RAM disk, allowing us to modify it and (2) change GEOS.INI to point to our NEW NET.INI. With the GEOS operating system restrictions, this doesn't seem like an easy task.

The first thing to do is load up the File Manager. Copy A:\NET.INI to B:\NET.INI. This is the easy part. Now we have a NET.INI that resides in RAM which can be easily modified. Don't edit this file yet, though, as you don't know what you're doing and can potentially mess something up.

The second step is a little more tricky. Somehow we have to change the second line in GEOS.INI from "ini=A:\NET.INI" to "ini=B:\NET.INI". Because GEOS won't let you edit the file directly, this is easier said than done. You may have noticed that there is a file in the File Manager, SDISK.EXE, that will completely reset your ZPDA to factory defaults, clearing all memory. If you run this by double clicking, it looks like GEOS shells to DOS and then executes the program. You may also notice that SDISK.EXE has a slightly different icon. If you rename SDISK or if you create a batch file and try to execute it under the File Manager, the ZPDA spews out an error message. Now, with this information, take a look at the NET.INI config file. Under the entry "[fileManager]" are a few lines - specifically one mentioning

SDISK.EXE followed by, presumably, an icon name. You'll also notice that lines exist for PENRIGHT.BAT, ZDRIVER.EXE, ZDRIVER.COM, and ZDRIVER.BAT. This means that ANY non-GEOS file named one of these five things can be executed directly from the File Manager. Another practical advantage of this icon execution is that when GEOS shells out to one of these files, it closes all of its data files (including GEOS.INI). A batch file can then delete or overwrite this all important .INI.

Now, how to specifically do this? Simple. Use File Manager to make a copy GEOS.INI called, say, TEMP.INI. Use America Online to modify the string "A:" into "B:" in your TEMP.INI file and save it. Now use America Online to create a new file called ZDRIVER.BAT and fill it with this line: "COPY B:\GEOWORKS\TEMP.INI B:\GEOWORKS\GEOS.INI" and save it. Jump back over to File Manager, and double click on your ZDRIVER.BAT file and it will install your own, personal GEOS.INI. You can delete TEMP.INI now, if you wish to free a little disk space. You will now be able to modify your own B:\NET.INI to your heart's content! Take note, though, that the only time GEOS will reread this configuration file into memory is when the ZPDA is rebooted or when GEOS returns from a shell. Rebooting is accomplished by hitting the reset button in the battery compartment while the unit is on (be sure that you are NOT holding down the A and B button while doing this or else all of your data will be wiped). So, after you edit NET.INI, you will have to hit the reset button. This can be gotten around, though, by creating a ZDRIVER.BAT file with just the single line that does not do anything (REM or ECHO or EXIT).

A word of caution before we continue. Any time you screw with a computer's configuration, especially if you do not know what you're doing, you are going to lose something. When your ZPDA locks up beyond hope because of a faulty .INI, the only way to fix it is with a total reset (both action buttons and reset). I have found this out the hard way several different times. If you are going to play with your ZPDA's configs, be prepared to lose something. A null modem cable or a serial cable with a null modem adaptor plug will only cost about $25. The "official" transfer software for the ZPDA costs about $100 and something similar can be found on America Online (and who can't get a 5-free-hour-voucher for AOL these days?). To put it bluntly, if you have important information, be sure to back it up because it will get wiped.

Now that we can get to and change the configuration, let's look at what can be done. NET.INI contains many different things to play with. Some of the more stable ones I've found (title followed by variable) are:

[system] (fontSize) and [motif] (fontSize): These two variables are, by default, equal to 10. If you have good eyes, you can change them to a smaller value to make the screen less cluttered. You can also make them larger.

[ui] (screenBlanker): This is usually set to "true". You can change it to "false" if you don't want the screen blanker to ever kick in.

[hardIconBar] (app0...app5): These are the filenames of applications to run when you tap on the hard icon bar. I've found that it's a little more convenient to change the World Clock icon so that it will run the File Manager (in my opinion, much more useful!).

[fileManager] (filenameTokens): This section seems to contain information about what non-Geoworks (DOS) programs and batch files the File Manager will let you run. You can add entries here to fool the File Manager into letting you run your own little programs.

Have fun figuring this stuff out! I've ordered the Zoomer Software Development CD and the service manual for myself, so I may have some more useful information in a future article. Before concluding this article, I would like to pose a question to my fellow 2600 readers. Organizers (such as the ZPDA, the Casio BOSS, etc.) have a password feature. Does anyone know how secure those passwords are? Or more exact, does anyone know a specific way to bypass the password in one of these gadgets? Obviously, there must be SOME sort of back door that the technicians can use to get into the organizer without wiping the data. Happy hacking!

(continued from page 38)

later started to use passwords. Unless a manual review was done of all code in the program areas,the attack would be effective. If a person regularly uses passwords, one lapse and the PC-6 could be rendered vulnerable indefinitely.

EXCHANGES IN 500 LAND

HOME OF PHONE NUMBERS FOR LIFE

202	ALLTEL SVCS CORP
220	DIAL CALL
221	MICROCELL 1 2 1
223	CABLE & WIRELESS COM
224	BELL ATLANTIC NSI
224	SOUTHWESTERN BELL
225	TIME WARNER COMM
226	BELL ATLANTIC MOBILE
227	AMERITECH MOBILE
228	CINCINNATI BELL
229	CABLE & WIRELESS COM
230	PCC MANAGEMENT
231	PCC MANAGEMENT
233	COLONIAL COMM SYS
234	CN COMMUNICATIONS
235	TRIAD MN CELLULAR
236	NORTHEAST TEL CO
238	ADVANCED RADIO TECH
241	VANGUARD CELL SYS
244	TELEPHONE ELECTRONIC
246	COMM GATEWAY NET
247	U S CELLULAR
249	GTE SOUTH INC - KY
254	UNITED TEL CO INC
255	VBI
256	ALLNET COMM SVC
257	BELLSOUTH TELECOMM
258	BELL ATLANTIC MOBILE
259	UNITED TEL CO CAROL
262	ALLTEL MOBILE
264	BELLSOUTH WIRELESS
265	MCI COMMUNICATIONS
269	AMERITECH MOBILE
272	APC
273	BATON ROUGE MSA
274	AMERICAN PAGING
275	PAGE MART
276	LDDS METROMEDIA
277	ARCH COMM GROUP INC
279	ARCH COMM GROUP INC
280	UNITED TEL CO MINN
282	U S WEST NEW VECTOR
283	CENTURY TEL CO
286	CENTRAL TEL CO NV
287	WILTEL INC
288	AT&T
289	PAC BELL MOBILE
291	LAKEDALE TEL CO
292	BRAZORIA TEL CO
294	CABLE & WIRELESS COM
299	NYNEX MOBILE
300	DELTA COMMUNICATIONS
302	MORRIS COMM
303	BELL MOBILITY
304	CHESTER TEL CO
306	SASKTEL MOBILITY
309	CHESTER TEL CO
320	UNITED TEL CO OF MO
321	MICROCELL 1 2 1
323	SCHNEIDER COMM
328	BC TEL MOBILITY
332	FREEMAN ENG ASSOC
334	CANADIAN VALLEY TEL
340	UNITED TELCO OF OHIO
342	PAC BELL MOBILE
345	AIRTOUCH CELLULAR
346	AT&T
349	OMEGA CELLULAR
357	PAGING SYSTEMS INC
367	AT&T
368	PAGING SYSTEMS INC
369	BELL ATLANTIC NSI
373	PAC BELL MOBILE
375	PIONEER TEL COOP INC
377	CENTRAL OKLAHOMA TEL
380	RADIO CAR DAKOTA CEL
382	ELKHART TEL CO INC
386	JEFFERSON TEL CO
393	CABLEVISION SYSTEM
395	AMERICAN SHARECOM
400	AIRTOUCH COMM
404	COMM INNOVATIONS COR
405	TRIAD OK L P
412	N PITTSBURGH TEL CO
421	ADVANTIS
422	ADVANTIS
424	CGI CORP
426	WIRELESS ONE
430	MCCAW CELLULAR
431	MCCAW CELLULAR
432	MCCAW CELLULAR
433	MCCAW CELLULAR
434	CHEROKEE TEL CO
436	GEOTEK COMM INC
437	AT&T
438	ACCESSLINE TECHNOL
442	AT&T
443	AT&T
444	ONCOR
445	AT&T
446	AT&T
447	AT&T
448	AT&T
449	AT&T
454	WIRELESS ONE
456	UNICOM CORP
463	CROSS TEL CO
464	EDWARD A SMITH
476	CIMARRON TEL CO
480	GTE MOBILE COMM
483	GTE TELOPS
484	TELECOM USA
486	GTE MOBILE COMM
487	US INTELCO NTWKS INC
488	AT&T
499	CAL ONE CELLULAR
503	AWESOME PAGING INC
510	ONE COMM
522	STANDISH TEL CO
526	POKA LAMBRO COMM
528	LUFKIN TEL EXC INC
529	U S CELLULAR
535	HORRY TEL COOP INC
543	PAGE MART
546	TELECOMM PREMIUM SVC
556	WILKES T & E
567	PEOPLES TELCO INC
581	IDB MOBILE COMM
587	HUTCHINSON TEL CO
588	LINCOLN TEL & TEL CO
599	TWO WAY RADIO OF NC
600	AIRTOUCH COMM
614	SPRINT CELLULAR CO
620	TRILLIUM CELLULAR CO
622	MAINSTREET COMM
624	OMNIPOINT
626	PARKWAY COMMUNICATNS
628	NB TEL MOBILITY
638	NEW CELL
639	NEXTEL COMMUNICATION
641	DEADWOOD CELLULAR
651	UNITED TEL CO OF NJ
654	HOOPER TEL CO
655	AMERICAN SHARECOM
659	UNITED TEL CO OF NJ
661	AMERITECH MOBILE
662	ROGERS CANTEL
666	NATIONWIDE WIRELESS
672	NPB TELECOM
673	AT&T
674	AT&T
675	AT&T
677	AT&T
678	NYNEX MOBILE
679	AT&T
682	NATL TEL CO OF AL
684	PTI COMMUNICATIONS
687	MTS MOBILITY
688	MT&T MOBILITY
691	MOBILETEL INC
693	LAFOURCHE
700	AIRTOUCH COMM
720	SW BELL MOBILE
721	SW BELL MOBILE
723	RADIOFONE INC
724	PITTENCRIEFF
725	PITTENCRIEFF
726	OMNIPOINT
728	COMSAT MOBILE
729	UNITED TEL CO OF PA
732	WILTEL INC
733	RED ROSE SYSTEMS
734	ISLAND TEL MOBILITY
735	NEWTEL MOBILITY
737	PAGE NET
738	PAGE NET
742	BIXBY TELEPHONE CO
746	AMERITECH MOBILE
749	DURANGO CELLULAR
752	POINT COMMUNICATIONS
753	COMCAST CELL COMM
754	METRO CALL
755	U S CELLULAR
757	SPRINGWICH CELL LTD
758	AMSAT
760	AMSAT
762	RESERVE COMPUTER
763	SO NEW ENGLAND TEL
764	PREFERRED NETWORKS
767	ED TEL MOBILITY
769	OHIO STATE CELLULAR
770	VIRGIN IS TELE COM
771	E T COMMUNICATIONS
772	MESSAGE CENTER USA
774	SNET PAGING INC
777	COMCAST CELL COMM
782	ROANOKE TEL CO INC
784	RAM TECHNOLOGIES
786	SPRINT CENTEL FL
787	FIRST PAGE USA
788	UNITED TEL CO OF TX
789	WEST IOWA TEL CO
792	CAMPTI-PLEASANT HILL
800	AIRTOUCH COMM
801	TRIAD UT L P
806	TRIAD TX L P
808	PAC WEST TELECOM
826	VANGUARD CELL SYS
827	THUNDER BAY MOBILITY
828	UINTAH BASIN TEL
832	BAY SPRINGS TEL CO
835	QUEBECTEL MOBILITE
840	NATIONWIDE PAGING
841	GTE TEL OPERATIONS
843	COX ENTERPRISES
846	GTE MOBILE COMM
855	UNION TEL CO - WY
862	USA MOBILE
864	UNITEL
865	CROCKETT TEL CO INC
866	ISLAND TEL CO LTD
867	NEWFOUNDLAND TEL
868	NEW BRUNSWICK TEL
869	SASKATCHEWAN TEL COM
870	MARITIME TEL LTD
871	ALBERTA GOV TEL
873	MANITOBA TEL SYS
874	BELL QUEBEC
877	SPRINT LDD
878	BRITISH COLUMBIA TEL
880	ADVANTIS
881	ADVANTIS
882	CENTRAL TEL OF VA
883	TELECOM USA
884	UNITED TEL OF IN
885	UNITED TELCO MO - KS
886	UNITED TELCO OF OHIO
887	TELECOM USA
889	TELECOM USA
892	EVANS TEL CO
899	POTTAWATOMIE TEL CO
907	GCI CORP
937	US INTELCO NTWKS INC
945	WILTEL INC
946	CENTRAL TEL CO OF NC
947	QUESTAR COMM
957	RESERVE TEL CO
966	WIRELESS ONE
968	CENTURY TEL CO
973	USA MOBILE
987	AGT MOBILITY
988	WEST TENNESSEE TEL

The two biggest questions remain: who will win the battle for 224 and who the hell is Edward A. Smith (464)?

PAGER MAJOR

by Danny Burstein

This article has been put together to answer some of the more common questions about pager systems. It is primarily focused on the U.S. and Canadian arrangements, but other countries are not forgotten.

What is a Pager Anyway?

As usually described, a pager is a portable unit, generally about half the size of an audio cassette box, which can be signalled to send a one way message to the pager owner. (There are lots of versions available. For example, Motorola offers up the Sensar which is shaped like a flattened out pencil. There are also extra thin credit card units, pcmcia cards that fit into computers, etc.)

What Types of Messages?

The earliest units, usually called beepers, simply gave a tone alert. This was a signal to the wearer to, for example, call the answering service.

The next step was units which could display numbers. While the most common use is to send it the phone number you want the person to call, you can, of course, add code numbers to mean anything else you'd want.

For example, the number xxx-yyyy-1 might mean to call the xxx-yyyy number at your leisure. Xxx-yyy-9 might mean call ASAP.

The most recent units, called alpha-numerics, display complete written messages. So, for example, the pager could show the message: "Please call home, you have a letter from the IRS."

There are also *voice* pagers which will let you actually speak into the phone and have it come out the person's pager. These are pretty rare. Typically these are used within local areas, i.e., in a factory. They are also used, on occasion, by groups such as volunteer fire departments.

How are Messages Sent to the Pager?

Messages are sent by radio. Actually, it's a bit more complicated than that. Let's take a look at how a pager actually works: The pager is a small sized radio receiver which constantly monitors a specific radio frequency dedicated to pager use. It remains silent until it "hears" a specific ID string which tells it to, in effect, turn on, and then listen up for, and display, the forthcoming message. (Again that could be a numeric or other string.) This ID is called (in the US) a CAPCODE. It has *nothing* to do with the phone number you call or the ID you give to the page operator (see below). (The ID number you associate with the pager is actually merely "column a" of a lookup table. The pager radio service uses it to get the capcode, which is in "table b", and sends the capcode over the air. These tables can and are modified each time a new pager is added to the database.)

So the key point is that the pager company radio transmitter is constantly sending out pages, and your specific unit will only activate when it hears its ID/CAPCODE over the air.

How Do I Send Out the Message?

This depends on your pager vendor. Let's take the most common examples:

Alert tone only (the old style): You call up a phone number assigned to the pager. You'll hear some ringing, then a signal tone. At that point you hang up. Shortly afterwards the pager transmitter will send out the individual unit's capcode and it will go off. (Note that earlier models, some of which are still in practice with the voice pagers, don't use a capcode but instead use a simple tone sequence. Since these give a very limited number of choices, they are pretty much phased out except, again, for things like volunteer fire departments.)

Touch tone entry: You will call a unique phone number dedicated to the specific pager. It will ring, then you'll hear a signal tone. At that point you punch in, using touch tone, the number you want displayed on the pager. A few seconds later the transmitter will kick out the pager's capcode, followed by the numbers you punched in. Then the pager will give its annoying alert tone, the person will read it, and call you back. (Note that there is a variation on this in which the company uses a single dial-up phone number. You call it up, then punch in the pager's ID number, and continue as above. This is often used by nationwide services with an 800 number.)

Alpha-numeric: With this one there are various ways of getting the message to the system. *Via an operator:* The pager company will have you dial up their operator. When they answer, you give them the pager ID number and the message. They'll type it into the computer and shortly afterwards the transmitter will send out the capcode and the message. *Using your computer:* Most pager companies with alphanumeric have a dial-up number you can call yourself. Some of these will work with regular comm programs, while others require proprietary software. If you call the tech department chances are they will give it to you. (They'd rather have your computer call their computer than have you call a person.) The most common method is to have your computer dial up the number, then you type in the pager ID, followed by the message. Again, a moment later, the system will transmit it over the air, etc. (There are also various software packages that automate some of this.) *Special terminals:* Because of the popularity of this type of system, there are various stand-alone terminals specifically designed for this purpose. The most common one is the Alphamate (tm Motorola) and it's pre-programmed with many of the functions. It's basically a half-decent keyboard with a two line display, and is set up with the phone number of the company, etc.

How Large/Long a Message Can I Send?

This depends on a few key items. This is of most concern with an alpha-numeric, although it has some relevance with numeric ones (i.e., if you're giving a long distance number, extension, and code....). In no particular order these are:

The design of your sending computer or pre-programmed terminal. For example, if you get an Alphamate, chances are it will be pre-set to 80 characters. (You can reset it, provided the next two items work out)

The design of the pager transmitter system. It will place a limit on the maximum length message it will send over the air. This can vary dramatically. Generally (with a BIG YMMV) you'll get at least 15 numbers with a numeric, and at least 80 characters on an alphanumeric. Some systems will allow up to 225 or so alpha characters.

The design of the pager. Especially a problem with alphanumerics. Many of the ones on the market will only hold 80 characters so anything above that will be lost.

My company has given us pagers, and I notice that I have both an individual ID and a "group" number. When we page out to the group, everyone's unit goes off. How does this work?

Remember that a pager is basically a radio receiver that is constantly monitoring for its capcode. You can get pagers which listen for more than one. In this case (which is quite common) your personal capcode might be yyyy, while your boss's might be yyzz. In addition, both pagers will be listening for the capcode zzzz. When zzzz is detected, all the pagers with that capcode will go off. (Alternatively the pager company's computer may be smart enough to take a group id and translate it into capcodes xxyy, xxya, xxzz, etc., and send out fifty sequential messages. There are some software tricks that reduce overhead here so it doesn't actually send the same message 50 times.)

I keep hearing about sports or news services available by pager. How do they work?

Keep in mind that pagers work by constantly monitoring the radio channel for their capcode. So if you have ten pagers, or a hundred, or a thousand, all with the same capcode, they will *all* go off at the same time.

The service company will have someone (or perhaps, a smart computer) monitor the news broadcasts/radio channels for something interesting. At that point they'll send out the message to the group ID/capcode subscribing to that information. This way the news company sends out one message and it gets displayed by all subscribers. (Again, they can also send out the capcodes for the 500 subscribers. It gets into a security/cost/radio time equation as to which method they'll use).

So if I find one of these sports-news pagers on the sidewalk I can use it for free?

Umm, kind of. As long as the company providing the service keeps using the same group code, your pager *will* continue to receive the messages. But the individual pager ID will probably be changed immediately so you won't be able to use it for your personal messages. Note also that some pagers *do* have the ability to be turned into a lump of clay over the air. Very few systems have actually implemented this security feature (which is called "over the air" shutoff), but it is there.

I've found a pager on the sidewalk and would like to use it. What can I do?

Not much. Keep in mind that you need an account with the paging company for them to send out the radio signal. So unless you keep paying them, the pager will soon be a paperweight. You might as well turn it in for the reward.... (On the other hand, if you *already* have a pager, you may be able to get this new one cloned to your first one, which will allow you to have a duplicate unit. See below.)

Speaking of that pager on the street, it's got all sort of numbers on it. What do they mean?

There will be a lot of items printed, some by the manufacturer, some by the dealer. In no particular order these will include (usually in *very* small print)

a) the pager frequency;

b) the pager's serial number;

c) the capcode programmed into it.

Very frequently, especially with numeric units, there will also be the phone number assigned to it. And, of course, there will be the dealer's name, the local supplier, an "if found here's the reward number", and other housekeeping. Note that often the capcode will *not* be printed on the unit, but will only be readable via the programmer.

Can I listen in/monitor pager channels?

Kind of. The frequencies are readily known and the data is a digital stream going over the air. There are various vendors of equipment to decode the material and display it or feed it into your computer. Some of these folks advertise in communications magazines such as *Popular Communications*. However:

The federales and the pager companies don't like you doing this (see the ECPA).

The volume of traffic is quite high. If you figure a 1200 baud channel in use 75 percent of the time, well, you can work out the math.

By the way, the numeric units do *not* use touch tone over the air. Some did way back when, but I doubt any do these days.

I have a pager for which I'm paying big bucks every month. I miss a lot of pages since I'm in the subway a lot. What can I do about this?

There are several things:

Some of the pager companies will re-send messages on request. Basically you call up their phone number, punch in a security code, then go through a menu which tells them to resend the last, say, five hours worth of messages.

You can get a second pager unit cloned identically to the first. Leave this one at home or in your office. When you get back you can compare its messages to the one on your belt. While the message may be a few hours late, at least you'll be getting it.

Actually, most pager companies will refuse to clone your unit for you. However, there are many third parties which will do it. Check out the ads in technical and communications magazines.

What are the prices and services offered?

These vary dramatically by area and company. Unfortunately there is no central database keeping records on this. Generally the following factors get counted in determining what you'll be paying:

How sleazy the company is.

Which type of pager and service you get. Again, the most common are numeric (cheaper) and alphanumeric (more expensive).

Level of usage. You may get, say, 25 free messages a month and then pay $0.25 for each additional.

Whether you own the pager or lease it.

Insurance, etc.

Area of coverage. Smaller area means less expensive.

Speaking of coverage, what's this satellite nationwide paging?

Well, it's not quite what they're telling you. It's *not* a single satellite covering the nation. Rather, what's done is: You call up the paging company. It then signals transmitters in the top 500 cities to send out your capcode. Shortly afterwards you get the message. Note that you are *not* receiving a satellite transmission.

What's in the Pipeline?

Two key features are slowly filtering down.

Much more pager memory/longer messages. Most pagers are severely limited in the amount of material they can hold, with a typical maximum being about 20 messages. Units with much larger memories, or even better, units that are hooked into palmtop or laptop computers, are making it to market.

Two way communications. In its simplest form this allows the pager to verify reception to the transmitter. Also on the way is complete two-way communication which would basically be wireless email. These systems are still a bit limited, but are rapidly gaining footholds in industry and should soon be consumer level. Take a look, for example, at what the Fedex folk carry.

Update suggestions should be sent to dannyb@panix.com.

MITNICK

(continued from page 4)

When Shimomura concluded that the intruder was "probably Mr. Mitnick", the hunt was on. Shimomura had all the help he needed - he programmed for the NSA and the FBI was almost as interested as Markoff. Using cellular tracking, it wasn't too difficult to track down Mitnick. Less than a week later, Markoff and Shimomura signed a $750,000 book deal, no doubt to be called something like *Cybersleuth*, pitting good hacker against evil hacker.

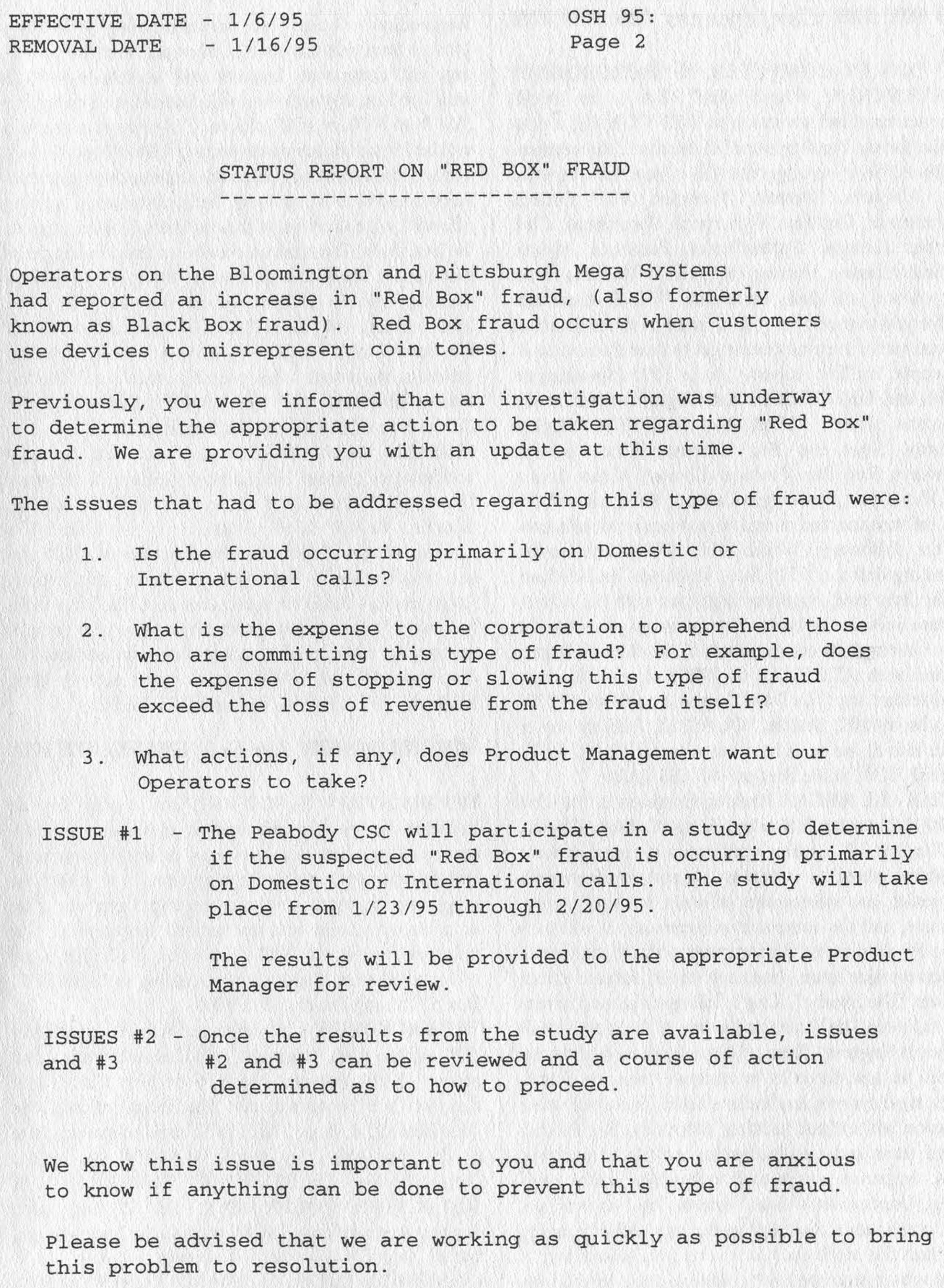
But how much do we actually know? Obviously, enough for a classic cat and mouse bestseller. But what will happen to those facts that don't fit in quite so neatly? Will the awkward questions ever be answered?

What was Mitnick wanted for in the first place, besides the nebulous "probation violation"? Markoff reported that Mitnick was suspected of wiretapping the FBI while a fugitive. But we never hear how such a conclusion is reached beyond pure speculation. The recent charges appear to be nothing more than a smokescreen, designed to demonize Mitnick and make him appear to be a threat to everyone's privacy. Little mention is made of the fact that not one of the 20,000 credit card numbers lying around on Netcom was ever used by Mitnick, nor was he ever suspected of benefitting financially or causing any damage. Mitnick was also accused of leaving taunting messages on Shimomura's voice mail. Upon closer examination, it's fairly obvious that Mitnick was not at all involved in this - for one thing a new message appeared *after* he was apprehended! As for the "sensitive" files, Mitnick was certainly not the only one who had access to them. In fact, serious doubt can be cast as to whether he was the one who figured it out in the first place. The fact that we were able to track down a copy of the directory he was supposedly using tells us that many people already had access. Does this suggest a closely knit conspiracy? Hardly. In classic hacker fashion, word of one person's discovery got out and spread throughout the net. After all, who could keep quiet about a password sniffer designed for the NSA that could run on virtually any machine? So far, the press has.

A 23 count indictment handed down on March 9 charges Mitnick with possessing device-making equipment, possessing unauthorized access devices, and 21 counts of using a counterfeited access device. We assume this to mean reprogramming a cellular phone in order to remain hidden. The government says that this indictment only covers a period of several days before Mitnick's arrest, the implication being that there will be many, many more charges added to cover the years that he was on the run. This is a spiteful and vindictive approach - these "crimes" came about *because* of Mitnick's fugitive status; it's simply not possible to be a fugitive and live one's entire life on the books. Any damage or outright theft should naturally be followed up on but in this case such actions seem practically nonexistent. It's becoming clear that the government intends to punish Mitnick over and over again for getting away. And we may never find out why he was running in the first place.

How long Mitnick will be imprisoned for is really anybody's guess. Judging from the way some influential people are talking, it could be a very long time. We have to get the facts so that we can judge for ourselves what "real world" crimes we're talking about. The potential to learn from this still exists but the desire to punish and make an example threatens to thwart that.

RED BOX FRAUD!



EFFECTIVE DATE - 1/6/95
REMOVAL DATE - 1/16/95

OSH 95:
Page 2

STATUS REPORT ON "RED BOX" FRAUD

Operators on the Bloomington and Pittsburgh Mega Systems had reported an increase in "Red Box" fraud, (also formerly known as Black Box fraud). Red Box fraud occurs when customers use devices to misrepresent coin tones.

Previously, you were informed that an investigation was underway to determine the appropriate action to be taken regarding "Red Box" fraud. We are providing you with an update at this time.

The issues that had to be addressed regarding this type of fraud were:

1. Is the fraud occurring primarily on Domestic or International calls?

2. What is the expense to the corporation to apprehend those who are committing this type of fraud? For example, does the expense of stopping or slowing this type of fraud exceed the loss of revenue from the fraud itself?

3. What actions, if any, does Product Management want our Operators to take?

ISSUE #1 - The Peabody CSC will participate in a study to determine if the suspected "Red Box" fraud is occurring primarily on Domestic or International calls. The study will take place from 1/23/95 through 2/20/95.

The results will be provided to the appropriate Product Manager for review.

ISSUES #2 and #3 - Once the results from the study are available, issues #2 and #3 can be reviewed and a course of action determined as to how to proceed.

We know this issue is important to you and that you are anxious to know if anything can be done to prevent this type of fraud.

Please be advised that we are working as quickly as possible to bring this problem to resolution.

This memo comes from AT&T Megasystems in Kansas City and is addressed to all of the other Megasystems out there: Pittsburgh, Bloomington (Indiana), Dallas, Seattle, San Diego, New York City, and Denver. Our source tells us the code for coin fraud is '06'.

2600 Marketplace

Conferences

DEF CON III COMPUTER "UNDERGROUND" CONVENTION. What's this? This is an initial announcement and invitation to DEF CON III, a convention for the "underground" elements of the computer culture. We try to target the (fill in your favorite word here): Hackers, Phreaks, Hammies, Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, Artists, Criminally Insane, Hearing Impaired. WHO: You know who you are, you shady characters. WHAT: A convention for you to meet, party, and listen to some speeches that you would normally never get to hear from some k-rad people. WHEN: August 4, 5, 6 - 1995 (Speaking on the 5th and 6th). WHERE: Las Vegas, Nevada at the Tropicana Hotel. SPECIAL EVENTS: Hacker Jeopardy, Spot the Fed Contest, Voice bridge, Giveaways, Red Box Creation Contest, Video Room, Cool Video Shit, Scavenger Contest, Who knows? For more information and complete convention details contact the following: World Wide Web: http://underground.org/defcon; FTP Site: ftp.fc.net /pub/defcon; mailing lists: mail majordomo@fc.net with the following statement in the body of your message: subscribe dc-announce; voice or voice mail: 0-700-826-4368 from a phone with AT&T LD, or 10288 it; e-mail: dtangent@defcon.org (The Dark Tangent); snail mail: 2709 E. Madison #102, Seattle, WA, 98112; BBS system to call for info if you don't have net access: 612-251-2511; new DEF CON Voice Bridge: 801-855-3326.

ACCESS ALL AREAS. Hacking Conference, 1st - 2nd July, 1995 (Saturday & Sunday), King's College, London, UK. The first UK hacking conference is aimed at hackers, phone phreaks, computer security professionals, cyberpunks, law enforcement officials, net surfers, programmers, and the computer underground. It will be a chance for all sides of the computer world to get together, discuss major issues, learn new tricks, educate others, and meet "The Enemy". King's College is located in central London on The Strand and is one of the premier universities in England. There will be a large lecture theatre that will be used for talks by computer security professionals, legal experts, and hackers alike. The topics under discussion will include hacking, phreaking, Big Brother and the secret services, biometrics, cellular telephones, pagers, magstrips, smart card technology, social engineering, Unix security risks, viruses, legal aspects and much, much more. Technical workshops will be running throughout the conference on several topics listed above. A video room, equipped with multiple large screen televisions, will be showing various films, documentaries, and other hacker related footage. The conference facilities will also include a 10Mbps Internet link connected to a local area network with various computers hanging off of it and with extra ports to connect your laptop to. Registration will take place on the morning of Saturday 1st July from 9:00 am until 12:00 noon, when the conference will commence. Lectures and workshops will run until late Saturday night and will continue on Sunday 2nd July from 9:00am until 6:00pm. The price of admission will be 25 pounds (approximately US $40.00) at the door and will include a door pass and conference programme. Accommodation in university halls of residence is being offered for the duration of the conference. Special prices for British and Overseas university students, holding current student identification, are also available. To make a booking, call the following numbers: +44 (0)171 351 6011 (voice), +44 (0)171 352 7376 (fax). If you would like more information about Access All Areas, including pre-registration details then please contact one of the following: Telephone: +44 (0)973 500202, Fax: +44 (0)181 224 0547, e-mail: info@phate.demon.co.uk.

PHRACK MAGAZINE and Computer Security Technologies present The Summer Security Conference "Summercon" June 2,3,4 at the Clarion Hotel, Atlanta, Georgia. 404-659-2660. Admission: 10 dollars. The Clarion Hotel is a block from the Peachtree MARTA station, and is also on the airport-downtown shuttle route. Room rates for conference attendees are 65 dollars a night for single or double occupancy. Parking is also complimentary for conference attendees. For more information: Email: scon@fc.net, WWW: http://www.fc.net/scon.html, Mail: 603 W. 13th #1A-278 Austin, TX 78701.

For Sale

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.

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! Also, ELECTRONIC SURVEILLANCE **DETECTION EQUIPMENT,** for RF and telco devices from retiring TSCM specialist. Complete set, $4500. Send SASE or fax # for complete details.

LOOKING FOR THAT 6.5000 MHZ CRYSTAL? We have them for $4 (US), cash or money order only. Send your order to Durham Technical Products, P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@sdf.saomai.org) Three or more crystals only $3 each. Also available: rotary lineman's test sets (orange, blue, and black) for $65.00 (Touchtone test sets available soon); 8870 or SSI-202 DTMF decoders or M957 receiver $4; 556 timers for $1.50; 555 timers for $1.00. Same day service on most orders. A current listing of the products we carry is available by snail mail or e-mail.

FUTURECRIME. Get Steve Aylett's "The Crime Studio" from Inland Distribution, PO Box 120261, East Haven, CT 06512. Orders 800-253-3605. $11.95. The law is where reality goes to die.

UNAUTHORIZED ACCESS. The hacker documentary by Annaliza Savage, as reviewed in 2600 Winter 93-94 issue now available from Savage Productions, Suite One, 281 City Road, London EC1V 1LA, U.K. with a cheque or money order for $25.00 or 15 UK Pounds. NTSC VHS unless otherwise requested.

GRAY AREAS #7 has Internet Liberation Front interview, HOPE and DEF CON reviews. #6 has computer viruses, Erik Bloodaxe interview, and CFP. #5 has a phone phreak, WELL break-in, PumpCon and HoHoCon. $8 each ($10 foreign) to: Gray Areas Inc., PO Box 808, Broomall, PA 19008.

VIDEO: "HOW TO BUILD A RED BOX". VHS 72 min. Complete step by step instruction on how to convert a Radio Shack tone dialer into a red box. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch and more! Best investment you'll ever make! Only $29 US. $5 for shipping and handling. DIGITAL RECORDING KEYCHAIN. Records ANY tone you generate onto chip. Very small. Fits in pocket for easy access. 16 second capacity. Includes 3 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherwood Place, Englewood, NJ 07631.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector: ANSICHK9.ZIP. Send $3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St NE #430, Atlanta, GA 30308.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus automated Tempest module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM and energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $5 (no free catalog): Consumertronics, P.O. Drawer 537, Alamogordo, NM 88310.

"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 & only 1/4 inch thin! Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. $39 each, 2 for $75, 4 for $140. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & 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 & wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35 POSTPAID, each additional crystal only $3 POSTPAID. All 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.

Info Exchange

DATA INTELLIGENCE CORE (503) 697-7694. An information exchange for intelligence matters. Handles H/P/A subjects as well as espionage. Need information on Russian Intelligence. Send e-mail to idres6e7@pcc.edu.

INFO EXCHANGE. Please send any hack/phreak/scam/controversial info. Especially looking for info that is relevant to the United Kingdom. Need info to start UK hack mag. Send info and return address (not compulsory) to: London Underground c/o Terry Boone, 120 Chesterfield Rd., Ashford, Middlesex, TW15 2ND, England.

WANTED: Any information on cable hacking or ANSI bombs. I need to know what exactly an ANSI bomb does, where I can get one, and how it works. Also need any other BBS or cable hacking info. Will exchange knowledge with anyone. Send info to The Dominus, 4302 West Azeele St., Tampa, FL 33609-3824. Will exchange knowledge!

NEW ENGLISH HACKER requires contacts in order to learn and explore the arts of hacking and phreaking, will provide a 100% reply to any other hackers who will take the time to reply and supply information. Send all correspondences to: The Net_Jester, 16 Frida Cres, Castle, Northwich, Cheshire, CW8 1DJ, England.

Help Wanted

NEED HELP TO CLEAR MY CREDIT REPORTS. Please respond to PO Box 6308, Chicago, IL 60680.

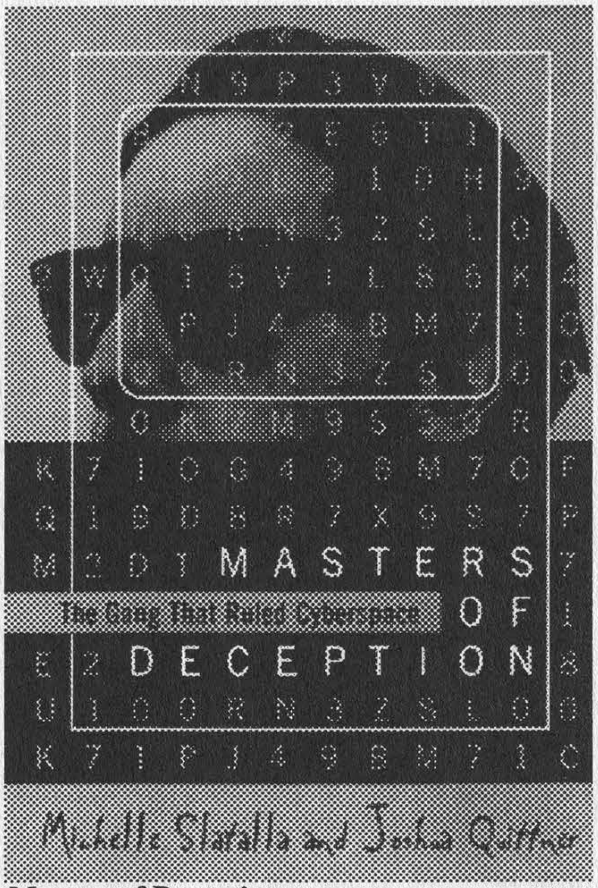
Hacker Boards

TIN SHACK BBS. True hackers and hacker files only! Around for over 6 years! Free IMMEDIATE access on first call! Special deal for 2600 readers, elite access for half the regular rate! Just mention 2600 Magazine! 300 to 14.4! 3+ gigs of files! (818) 992-3321.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Call (214) 289-8328 by modem.

Marketplace ads are free to subscribers!
Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion.
Deadline for Summer issue: 5/15/95.

West Side Hacker


MASTERS OF DECEPTION
The Gang That Ruled Cyberspace
Michelle Slatalla and Joshua Quittner

Masters of Deception
by Michelle Slatalla and Joshua Quittner
$23.00, HarperCollins, 225 pages
Review by Scott Skinner

One of the first things that comes to mind after completing Slatalla and Quittner's *Masters of Deception* is Sergio Leone's classic western: *The Good, the Bad, and the Ugly*. Not that the two have much in common, mind you. They don't. Only I couldn't help but recall that the three character's from Leone's film - far from following their titled namesakes - are all downright bad. They all rob, steal, and kill with alarming simplicity and regularity. They all commit crimes. Yet there are, nonetheless, subtle distinctions of badness which allow the audience to draw markedly different conclusions concerning the morality of each of the characters. So it is that in *Masters* we meet some teenagers, all of whom commit crimes (at least, in the legal sense), all of whom belong to an exclusive hacking group, yet each retaining an individual moral sense in both spirit and action of what the hacker ethic entails. It is in terms of these two realms - that of the individual and that of the group - that *Masters* attempts to deconstruct the story of MOD, sometimes stressing one over the other, sometimes integrating the two, but always implying that both are integral to understanding what has become the most notorious network saga since that of Robert Morris and the Internet worm.

In the same vein as *The Cuckoo's Egg* (1990), *Cyberpunk* (1991) , and *The Hacker Crackdown* (1992), *Masters of Deception* is yet another story about yet another group of hackers and the officials who eventually catch up to them. But whereas the subjects of these earlier works seemed content to use phone networks to hack computers on the Internet, the teenagers who comprise MOD go one step further and hack the telephone switches themselves. The implications of this are alluded to from the opening scene, that of the AT&T crash of 1990, which crippled long distance telephone service to millions of customers nationwide. The crash, which is a textbook case of AT&T's technical incompetence, is rather tactlessly used as an example of what MOD could accomplish, inadvertently or otherwise, at the height of their own technical prowess. *Masters* is also a unique work in its class for its portrayal of hackers not merely as individuals but as members of organized gangs with conspiratory goals and agendas. This is perhaps the most challenging aspect of *Masters*, as any depiction of a group will naturally detract from the individuality of its respective members. Far from achieving any dialectical synthesis, however, *Masters* accomplishes its portrayal mainly by ignoring the obvious conflicts inherent in such a task. For example, *Masters* is replete with sentences such as, "A group mind had already taken over. Something bigger than all of them had been born", notions that certainly suggest a sacrifice of individual ethics toward that of the group. But how, then, are we to interpret this "group mind" when *Masters* tells us that, "Mark is Mark...Whatever Eli or other MOD members did...they did on their own, without Mark's help or commiseration or even knowledge", and "If Eli called it 'The Mission,' Mark thought of it as 'The Project.' And Paul? He just wanted to know more"? Just as real people have an amazing capacity to hold mutually exclusive beliefs, *Masters*, it seems, has an equally impressive capacity to narrate and compartmentalize its own contradictory themes.

Masters is undoubtedly a good read. Ironically, however, it is precisely the ease with which one can surf through its pages which accounts for why so many of its finer points are lost. For example, MOD, we learn, is a gang. The authors like that term. Gang. Quittner even uses it in his articles on the same subject. After all, these hackers are all from the inner city, the spawning ground of gangs. Gangland, as it were. It is unfortunate that Slatalla and Quittner have latched onto this word, given the negative connotations that are now associated with it, and even more unfortunate that many readers will see the word and miss the meaning. What sort of gangs are we talking about here? *Masters* tells us, "Gang members on the electronic frontier don't live in the same states, wouldn't recognize each other if they were standing shoulder to shoulder on the same bus". Gee, that doesn't sound like any gang I know of. Sounds more like some national club. Perhaps that is why *Masters* describes Eli's room as "...the closest thing to a clubhouse that they'd ever have" OK. So MOD is both a gang (albeit a strange one) and a club. Anything else? The point is that the authors are using the term *gang* in an extremely broad sense, a fact that is likely to escape the attention of their readers as they riffle through this text. At one point, *Masters* even describes the LOD gang as being "just like any schoolyard pack of boys". Interestingly, *Masters* implies that MOD was somehow more ganglike than LOD despite the fact that MOD had neither the rules nor the parliamentarism of their Texas-based counterparts. In any case, I know of no better way to arouse confusion than to use relatively distinct terms as if they were synonyms. One thing I was hoping to find and never did was the rather innocuous term "friendship." The core of MOD was first and foremost a friendship (and, incidentally, where I come from, when you put friends together in one room, you get a group of friends, not a gang).

While *Masters* is indeed a fine book, it is by no means a great book, if only because it does what so many other hacker books have done before: attempt to explain hackers to an audience which has barely become comfortable with the idea of computers, let alone computer wizards. But this is 1995, and hackers have been around in their present incarnation for some 15 years now. Yet at times, *Masters* appears to have been written in an historical void. Missing are the countless points in history that would provide some context as to what the characters are doing. Missing are the references to the fact that - by the time MOD came into existence - a hacker culture had already existed and flourished around the world. To its credit, *Masters* does tell us that "To be a hacker in the late 1980s was to be a kid with a notebook stuffed with passwords for Unixes and VAXes, switch dialups, and all kinds of university mainframes". And *Masters* does have a token page or two acknowledging Robert Morris, Operation Sundevil, the Steve Jackson case, and other unquestionably important events in hacker history. But you will need a scanner and some OCR software to find these paragraphs because - wouldn't you know it - *Masters* does not have an index, or source notes for that matter. And it is precisely omissions of this nature that make one wonder to what degree this book should be taken seriously. Add to this the factual errors. While addressing these errors are beyond the scope of this review, one thing I found absolutely inexcusable was *Masters'* use of the moronic "house" paradigm to describe being locked out of one's corporate computer. Once again, for the record: being locked out of one's corporate computer is not like being locked out of one's own home; if anything, it is like being locked out of one's private golf course. Even worse, *Masters* makes this analogy even while drawing attention to other ridiculous analogies that were presented in the now famous Harper's forum on computer hacking. *Masters*, then, has a way to go before greatness. The fact is that there are a lot of characters in this story - a whole lot - and they all fit together in a myriad of complex ways. If *Masters* has any weakness, it's in trying to simplify a story that could fill volumes to something under 226 pages (to give you some perspective, Mark's indictment alone could fill volumes). While I certainly respect the magnitude of Slatalla and Quittner's undertaking, I sometimes cringe at the result: a sort of fun-to-read children's story for adults.

This review was written *without* the use of the following terms:

cyberpunk
cyberspace
digital highway
global network
infobahn
infoway
information superhighway
cracker
on-ramp

With a little effort, you can avoid using these terms as well.

The anonymous remailer in Finland used by thousands to transmit anonymous messages over the Internet apparently isn't so anonymous after all. Finnish police, aided by the good folks at Interpol, raided the anon.penet.fi site at the behest of the Church of Scientology and successfully got the real email address of a person who had posted sensitive information to the alt.religion.scientology newsgroup. According to the system administrator, he had the choice of giving up one name or the entire system. As far as we're concerned, there's not much difference. The Internet needs *real* anonymity to prevent this kind of scare tactic. Meanwhile, the Church of Scientology continues to pursue a lawsuit against Netcom for allowing people to post things that the Church finds objectionable. The CoS attempt to "shut down" the alt.religion.scientology newsgroup appears to have loudly backfired. In true democratic form, more people than ever are sharing ideas and information through that forum thanks to all the publicity.

Speaking of scare tactics, Internet users in Hong Kong experienced the power of government firsthand. Access to the net was all but cut off after a series of government raids that, depending on who you talked to, were designed to curtail unlicensed connectivity or prevent computer hackers from operating. Whatever the intent, the effect was most chilling as nearly all access to the net was cut off throughout the country.

According to the Canadian Alliance Against Software Theft (CAAST), two bulletin boards (Montreal's "90 North" and Toronto's "Legion of Death") were shut down and their owners indicted under the Canadian Copyright Act. They were fined a total of $22,500 after pleading guilty to having unlicensed software.

A brief story in the *Dallas Business Journal* says the Internal Revenue Service is "expanding a secret database it keeps on the lives of U.S. citizens" to include motor vehicle records, child support information, credit reports, news stories, and tips from IRS informants.

The *New York Times* claims that Big Brother "is definitely watching" in central Liverpool and in many other British towns and cities. "Local governments, civic associations, and law enforcement agencies are rushing to install elaborate video security systems, brushing aside any concerns about civil liberties in an effort to deter crime." The surveillance program cost $600,000 and is focused upon a busy half mile stretch of Church Street. The 20 cameras are perched on top of 20-foot poles several hundred yards apart and are individually controlled from a darkened room a few blocks away. Systems like this one are popping up all over the country with only a few people wondering what kind of effect this could have on such things as public demonstrations. In America, however, we can always depend on pure stupidity. Five teenagers in Florida are standing trial for vandalism and the main piece of evidence against them is a videotape. The difference is that they made it themselves for their own entertainment.

A Pennsylvania plumber ordered "ultra call forwarding" on the lines of five competitors and had their calls routed to himself. Apparently, Bell Atlantic never thought of this scenario. The competitors lost thousands of dollars in business and the plumber was charged with various crimes, the strangest one being unlawful use of a computer. That's right, you can now be charged with computer crime without ever actually using one yourself!

NYNEX has done it again - this time they slipped up when installing All-Call Restrict, the service that blocks your phone number from appearing on Caller ID displays. It seems that a large number of customers weren't actually being blocked when they thought they were. We'll never know how many people were ultimately affected nor will we find out what horror stories took place as a result. But we will be able to reaffirm that NYNEX continues to have major problems performing even the simplest of tasks for its hostage customers.

Some highlights from a recent NYNEX security publication called *SQAR* (Security Quarterly Activity Report):

"Security investigated a report that a Service Technician solicited and received $30 from a customer to install an additional unauthorized jack and wiring during a new line service connect. The allegation stated that the Service Technician claimed that this was new Company policy and payment should be made to him. A relative of the customer called regarding this policy and was advised to contact Security. The technician denied receiving any money. The customer, in a written statement, maintained that the technician returned the following day and suggested that the $30 be called a 'tip'. When the customer refused, the technician returned the money. The employee could not satisfactorily explain why the work was performed but no billing forms were submitted for the work. The employee was dismissed."

"Security received a report from the NYPD that the husband of a New York Telephone employee was arrested for the armed robbery of an armored truck delivering payroll funds to a Company location. It was also reported that our employee had prior knowledge of the crime. The employee made a video-taped interview, with the police, admitting that she was aware her husband planned to commit the robbery. She also admitted to spending a portion of the proceeds from the crime. The employee was dismissed."

"Security received an anonymous report that a New York Telephone employee was call forwarding customers' lines without authorization. During the investigation, Security observed an employee acting suspiciously while working in a terminal box. When questioned, the employee admitted to call forwarding six to ten lines per week to specified telephone numbers for weekly payments of $250. This has been occurring for over seven months. The employee also admitted to turning back some customers' lines in order to prevent them from knowing that the service was compromised. The lines were eventually used to place fraudulent third-party calls all over the world. The local D.A.'s office became involved; no arrests have been made to date and the employee was dismissed."

"A Service Technician was accused of defacing a religious article at a customer's business location. Security determined the allegation to be true. The employee made a formal apology, paid restitution of $300 and was also suspended for three days."

"The ex-wife of a New York Telephone Representative reported that the telephone records for her non-published service were being compromised. She alleged that her ex-husband was obtaining the records from his girlfriend who is a TRG Staff Manager. Security investigated and found that the TRG manager had accessed the records. When interviewed, she acknowledged accessing the records and stated it was done at the request of the ex-husband. The representative claimed that he made the inquiry at the request of his ex-wife, which she denied. Both employees were dismissed."

"Security investigated a report from a TRG manager that a fellow manager had made threatening statements concerning the Company, Vietnam veterans, guns, and explosives. The threats were made in the presence of other coworkers. The employee admitted to making the threats but claimed they were made in jest and he would never do anything to cause damage to the Company or his fellow employees. The employee had previously been placed 'at risk' under FMP but was able to keep his job. In a subsequent FMP, he was again identified 'at risk' and has been separated from the payroll."

"Security received a report that four orders for new telephone service were processed in a fraudulent manner. The orders were directly entered into the Service Order Processing (SOP) system, bypassing the Direct Order Entry (DOE) system, thereby avoiding the need for customer credit information. Security determined that the orders were processed from one specific RMO terminal. The employee assigned to the terminal was identified as a Business Office Representative and questioned. The employee at first denied any knowledge of the orders but later admitted the infractions when confronted with the evidence. The employee also alleged that this practice is widespread but would give no further information in this regard. The employee resigned."

"Security received an anonymous report alleging that a Special Representative permitted his daughter, a non-employee, to accompany him to work on Saturdays. It was also alleged that the daughter had access to Company records, and had assisted her father by performing various typing functions in the ICRIS (Integrated Customer Record Information System) and SOP systems. The employee admitted to bringing his daughter to work on one occasion but denied that she had performed any work in the data base systems. Security was unable to substantiate access into the systems. The employee was cleared of the charges and the Personnel Policies and Practices section dealing with access of unauthorized persons to work locations was reviewed with him."

"Security received a report from a subscriber that an employee offered to return after hours to install an additional jack for $70. Security identified the employee to be an Escort who had been temporarily promoted to Service Technician. When interviewed, the employee admitted that he had installed unauthorized jacks on other occasions and had solicited the complaining customer for the unauthorized installation of the jack. The subject also implicated another employee in the scheme but Security was unable to substantiate this allegation. The Escort was dismissed."

The bad news is that this is a quarterly publication and there are many more such stories involving only one phone company in one state. The good news is that it seems virtually anyone can get a job in a phone company these days.

LEAKING CABLES

In recent months a number of journalists on national newspapers have been anonymously sent a document labelled "private and confidential" and "not to be shown outside BT". It is an internal British Telecom briefing about the challenge from cable companies which, it says, "are literally digging themselves in across the country". The document spells out how much of a threat they could be and explains what BT is doing about it. For some reason no newspapers have published the document. BT representatives, playing down the leak, claim it is between a year and 18 months old and therefore not worth regurgitating but it makes fascinating reading. The company is worried and it shows that competition for the former monopoly is a real issue, not just a political promise.

Cable companies are digging up and laying down cable in 30 streets a day. There are currently 127 cable franchises, most of which have financial backing from major American telephone and cable groups. Most are ostensibly offering cable television but 26 of them are also offering phone services, with another 33 expected to jump on the bandwagon soon. The document says there are currently (whenever it was written) more than 17,000 cable business lines, an increase of 500 percent on the previous year. Such telephone lines are forecast to grow by 20,000 a month in the residential market and 3,000 for business.

"The threats which the cable challenge pose to BT must not be underestimated," warns the briefing, and lists those threats as follows: a large proportion of the residential market being "swallowed up" and pressure on the local business market; collaboration between cable companies, meaning cheap cable-to-cable calls and the potential of a national network, which could pull in larger customers; lost revenue for national and international calls where traffic is carried by Mercury; the loss of phone numbers if customers are eventually allowed to keep their own when they move; exploitation of the imminent national code change.

These are indeed serious threats to BT. Quite apart from the immediate loss of revenue, these factors could combine to make a serious dent in the company's image, which has been improving greatly since privatisation. I am not convinced its response is the most effective one, however. The document claims: "We can and will beat off the challenge by focusing on value rather than price... and by emphasising our quality of service." In America, for instance, where phone services are light years ahead of ours, phone companies compete for business by putting the emphasis on value, price, and quality. BT is relying on teething problems with cable companies and with Mercury, which there almost certainly will be, so that it can draw comparisons with its own slicker operation. But teething problems take less and less time to sort out these days, particularly for private companies with bright young technologists hoping to make a fortune. BT should remember, too, that only ten years ago it was a hopeless, shambolic dinosaur.

"Putting the customer first must be a reality, not a promise," the document continues. "We must help our customers choose to stay with BT by showing them that we value their business," it says, claiming that this should be achieved through the advertising theme "We Want Your Business". I could be wrong, but is an in-yer-face ad campaign starting "We Want..." really likely to convince customers that they are being put first? As for receiving "help to choose" the person offering the help, there's just a chance some customers might feel the advice was a touch biased.

So here, in its own words, are the five things BT staff have been told to concentrate on to fend off the opposition: "quality of service" (improving, certainly, but far short of potential); "depth of experience" (its depth of experience lies in running a poor service - good service is a new concept to BT); "breadth of portfolio" (big deal - nonsense words); "future technology" (already far outstripped in this field by the cable companies themselves); "understanding of business needs" (ditto). Then, bizarrely, it goes on to suggest BT people tell their customers: "No other supplier can offer such competitive rates, a wide choice of products and high quality of service that are all designed to meet every customer's needs." It would be interesting to see how, given what we have already read, they justify such a claim about competitive rates unless it is a purely subjective judgment along the lines of, BT is so marvellous that people should pay more. Read on, and you find that BT admits the cable companies' typical service record includes four-hour fault response and 24-hour fault repair, although it adds that there is some evidence Mercury lines get congested. There then follows a table comparing BT against its rivals on a series of subjects which, again, appear to make a nonsense of the response the company is telling its staff to dish out to disgruntled customers. The table shows that on price, cable firms are "cheaper overall"; on the network, cables have clearer lines and new technology while BT offers equivalents in "nearly all" business centres; on customer contact, cables have face-to-face and BT offers impersonal numbers like 151 for all but the biggest companies; on billing, cable calls are automatically itemised but BT's can only be supplied (on demand) on digital exchanges; on charging, where cable callers pay only for what they use and BT users pay in fixed-size units "which may make us uncompetitive"; on local service, where cable companies are leagues ahead because they are all locally-based.

Perhaps some of the contradictions in fact and claim can be explained by BT not wanting to panic its staff. But this is a gloomy document and BT is going to have to hit back with a lot more than slogans and a good sales pitch if, in its own words, it wants to stop the cable operators "cumulatively eroding a large proportion of the residential market and a significant percentage of BT's business base". As the company warns its employees: "Doing nothing is no longer an option."

2600 MEETINGS

NORTH AMERICA

Ann Arbor, MI

Galleria on South University.

Baltimore

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

Baton Rouge, LA

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

Bloomington, MN

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

Boise, ID

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.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

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

Cleveland

University Circle Arabica.

Columbus, OH

City Center, lower level near the payphones.

Dallas

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

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

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

Kansas City

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

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 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.

Nashville

Bellevue Mall in Bellevue, in the food court.

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

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

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

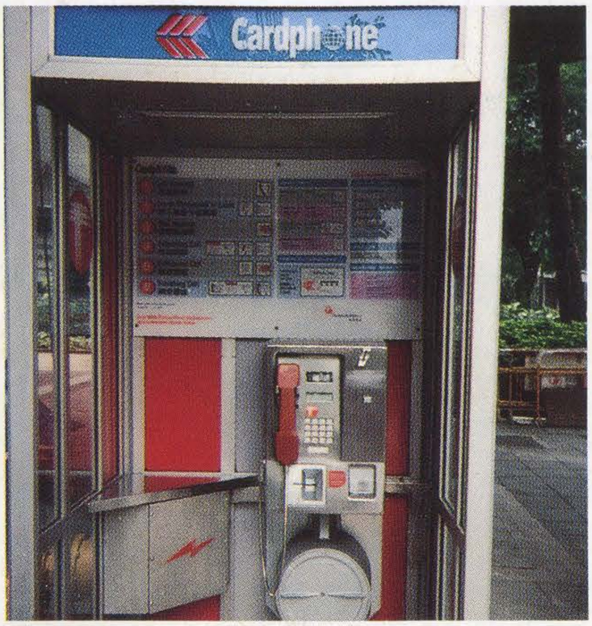
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

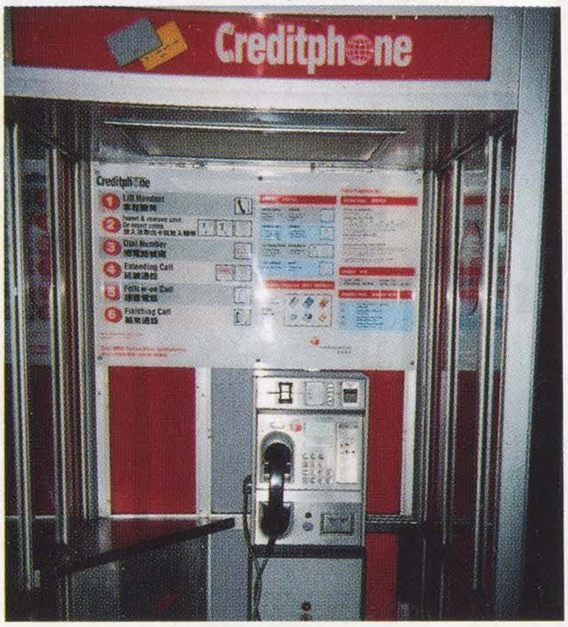
All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

PLEASE CHECK GUIDELINES ON PAGE 19

Payphones of the World

HONG KONG

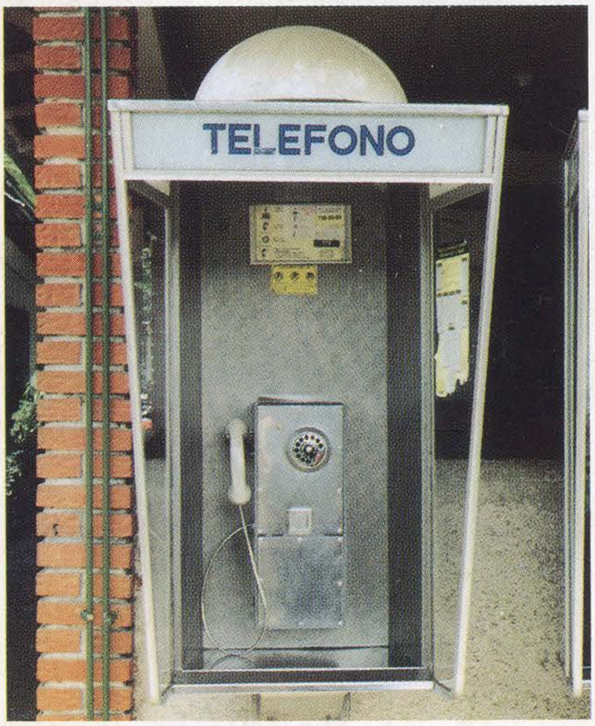




A Cardphone and a Creditphone. The Creditphone takes credit cards, the Cardphone takes phone cards. They both take coins as well.

Photos by Michael Pusateri

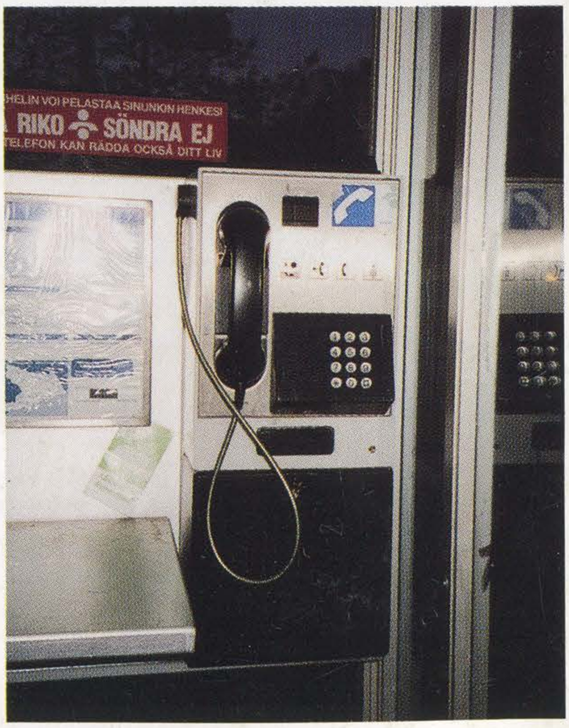
COSTA RICA



In the frontier town of Puerto Jimenez, Peninsula de Osa.

Photo by Martin Raminer

FINLAND


HELIN VOI PELASTAA SINUNKIN HENKESI
RIKO SÖNDRA EJ
TELEFON KAN RÄDDA OCKSÅ DITT LIV

Reminiscent of coin phones throughout Scandinavia. Card phones in Scandinavia are usually orange, coin phones are blue/silver.

Photo by Flippy the Squid