2600

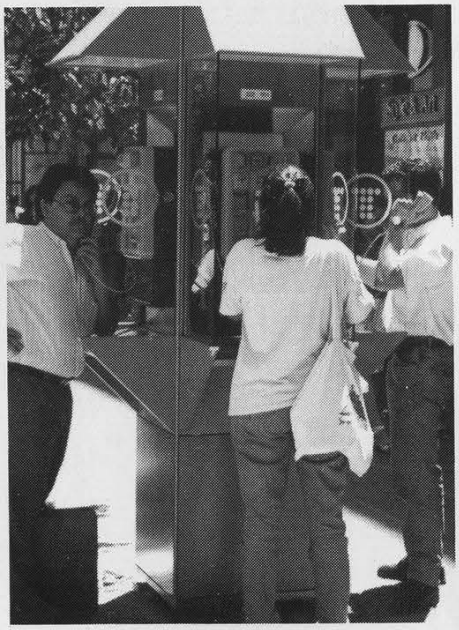
The Hacker Quarterly

VOLUME ELEVEN, NUMBER ONE

$4 ($5 in Canada)

SPRING 1994

PAYPHONES OF ARGENTINA

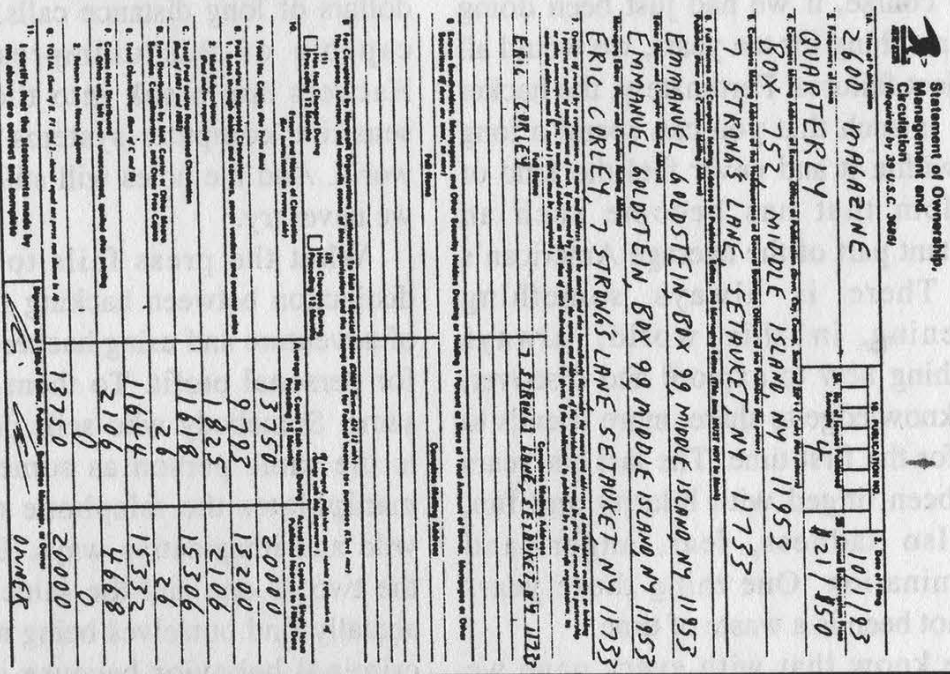


Argentina has two phone companies: Telefonica in the south and Telecom in the north. Buenos Aires is divided between the two. Both companies use the same tokens but their cards aren't compatible. See if you can guess which phones belong to which companies. See if you can guess which one we're not sure about.

Photos by Edward Stoever

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. TAKE US WHERE WE HAVEN'T GONE!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 1994 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1993 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**



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

1A. Title of Publication: 2600 MAGAZINE
1B. PUBLICATION NO.
2. Date of Filing: 10/1/93
3. Frequency: QUARTERLY
3A. No. of issues published annually: 4
3B. Annual subscription price: $21/$50
4. Complete mailing address of known office of publication (Street, City, County, State and ZIP+4 Code (Not printers): BOX 752, MIDDLE ISLAND, NY 11953
5. Complete mailing address of the headquarters or general business offices of the publisher (Not printer): 7 STRONG'S LANE, SETAUKET, NY 11733
6. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor (This item MUST NOT be blank)
Publisher (Name and complete mailing address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Editor (Name and complete mailing address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Managing Editor (Name and complete mailing address): ERIC CORLEY, 7 STRONG'S LANE SETAUKET NY 11733
7. Owner (If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Item must be completed.)
ERIC CORLEY, 7 STRONG'S LANE SETAUKET NY 11733
8. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities. If none, check box → None
Full Name: ERIC CORLEY
Complete Mailing Address: 7 STRONG'S LANE, SETAUKET, NY 11733
9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates (DMM Section 424.12 only)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes (Check one)
Has Not Changed During Preceding 12 Months
Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

10. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
A. Total No. Copies (Net Press Run)	13750	20000
B. Paid and/or Requested Circulation		
1. Sales Through Dealers and Carriers, street vendors and counter sales	9783	13200
2. Mail Subscription	1825	2106
C. Total Paid and/or Requested Circulation	11618	15306
D. Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies	26	26
E. Total Distribution (Sum of C and D)	11644	15332
F. Copies not Distributed		
1. Office use, left over, unaccounted, spoiled after printing	2106	4668
2. Return from News Agents	0	0
G. TOTAL (Sum of E, F1 and 2 - should equal net press run shown in A)	13750	20000

11. I certify that the statements made by me above are correct and complete.
Signature and Title of Editor, Publisher, Business Manager, or Owner: OWNER
PS Form 3526, January 1991 (See Instructions on reverse)

SQUISHED STAFF

Editor-In-Chief
Emmanuel Goldstein
Office Manager
Tampruf
Artwork
Holly Kaufman Spruch
Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Kingpin, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Tommy The Cat, Mr. Upsetter, Dr. Williams, and everyone else who never seems to fit in.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Earle, Jackrippr, and the bots.

Crime Waves

A decade is a long time to be doing anything. When we first started this project back in the summer of 1983, nobody could have predicted our growth, or even our existence in 1994. It's pretty strange to look back at the early days when we literally snuck around in offices and alleyways to get our first issues printed. And today you can find us in chain stores. Reality has always been weird to us.

Of course, if we had just been doing the same thing for ten years, we would all be abject failures. Fortunately, the hacker world is such that you can spend a long time within it and never feel the kind of boredom that has become such an important part of the average American's life. There is always something happening in this world, always something new to explore and discover, more knowledge to share, more friends to meet for the first time. The last ten years have been tinged with hilarity and fun, but also sadness, fear, anger, and determination. One thing these years have not been is a waste of time.

We know that with every page we turn, there is a risk. The most obvious of these include pissing off the powerful corporations and their law enforcement drones. Each and every time we share knowledge, we engage in a conspiracy of some sort. We risk having our lives disrupted by our accusers, our very means of learning taken from us by large armed men. We risk being chastised by our friends and family for being different and ostracized in school for not asking the proper questions or memorizing the standard answers.

These are the obvious risks of who we are and what we do. Most of us have come to recognize them. But there is a far greater risk facing us and it's one that many of us could fall victim to with little or no warning.

Over the years, we've tried to dispel the myth that hackers are criminals. This has been most difficult. As the tabloid press loves to scream, hackers *can* get into your credit file. But so can anybody else. Hackers *can* make thousands of dollars of long distance calls. Anyone is capable of this unimpressive feat. Hackers *can* break into thousands of sensitive computer systems around the world. And the holes will still be there if we never try.

What the press fails to see is the distinction between hacking for the sake of adventure and using hacker knowledge for personal profit. To them it's all the same. Somebody who sells phone codes is the same person as somebody who manipulates the telephone network in wild and imaginative ways. By defining the two as one and the same, we could actually find ourselves being nudged into criminal behavior because it's what's expected of us.

With this in mind, the massive growth of the hacker community is cause for concern. Many people are being drawn into our fold through these very same media perceptions. People have shown up at our meetings assuming that we're there to sell or buy codes. A disturbing number of people who engage in credit card fraud, that is, the stealing of actual physical, tangible merchandise, are trying to ingratiate themselves into the hacker community. It's not surprising. And they might actually be able to prey on our

temptations and suck some hackers into their midst, thereby learning a few new tricks. And by calling *themselves* hackers, they manage to justify what it is they do. Ironically, their technical prowess oftentimes doesn't extend beyond knowing how to operate a red box or punch in a code.

This kind of thing was inevitable, given the growing awareness that the mainstream world, and hence the mainstream criminal world, has developed for hackers. Carrots are being dangled in front of our faces. Our brains are suddenly in demand. You might say that society has finally found a use for us.

Knowing this, the most important thing as individuals is to realize why we do what we do. Is it that we want to find out things and spread knowledge around? Or do we want to get what we feel the world owes us? Are we trying to survive and get access to a locked world? Or are we intent on selling our knowledge to the highest bidder?

Truthful answers to these questions are more valuable than anything else. Once we understand our motivation, we can at least be honest with ourselves. Those who use their hacker knowledge to embark upon a life of crime can at least admit to themselves that they are now criminals, thereby salvaging some self respect. The rest of us will have some sense of where we draw our lines.

But how do we know what constitutes criminal behavior and what does not? Regrettably, the law no longer seems an accurate definer. With many of us, we just *know* when something doesn't feel right. And in such a case, trusting your instincts is always a good idea.

To be a hacker, your primary goal must be to learn for the sake of learning - just to find out what happens if you do a certain thing at a particular time under a specific condition. A good way to know if you're a genuine hacker is to look at the reaction of the non-hackers around you. If most of them think you're wasting your time doing something incomprehensible that only you can appreciate, welcome to the world of hacking. If, however, you find yourself being trailed and hounded by a bunch of drooling wannabes with a list of plots and schemes to make your knowledge "pay off" in a big way, you're probably on the verge of becoming a criminal and leaving the rest of us back in the age of innocence.

Obviously, embarking on such a journey en masse would mean the end of the hacker world. We would play right into the hands of our enemies and criminalize hacking by definition, rather than by legislation. Nothing would be better for the anti-hacker lobbyists. As a curious side note, in more than one instance, people who were found to have been helping the government prosecute hackers have been caught actively encouraging criminal behavior among hackers. We have to wonder.

We hack because we're curious. We spread what we find because segregated knowledge is our common enemy. This means that some opportunists will get a free ride and run the risk of giving the rest of us a bad name. The only surefire way to keep this from happening is for us to behave like the phone companies and restrict knowledge. Not likely.

It's not our job to catch criminals. But it is our moral obligation to keep our noble, if somewhat naive, aspirations from becoming subverted by those who truly don't understand.

build a dtmf decoder

by Xam Killroy

When I saw the product review of the TDD-8 DTMF Decoder in the Summer 1993 issue of *2600,* the last line got me thinking: "A pity that like a lot of good tools it's so expensive." So I designed this decoder around the Teltone 8870 DTMF Receiver IC, the same part used in the TDD-8 product that was reviewed. Originally, I intended to make a tone decoder that would display the current digit and simultaneously send it out over a serial line. No problem, I thought. So I started bread boarding it together, and soon realized it would actually take two shift registers, a stable clock generator, a custom burned PROM (to translate from four-bit binary to ASCII phone-pad symbols), and an RS-232 voltage level driver (because RS-232 voltages are different than TTL voltage levels).

"What I want," I thought in annoyance, "is a cheap computer to do all this conversion and communication and logging crap for me." And I had just such a thing sitting in my closet gathering dust. Years ago, the Commodore 64 was a very popular consumer computer, and there are millions of them floating around. They have a current street value of about $50, because they can't compare to any of the current computing muscle out there, but they are still enormously useful as a hacker's tool. They're durable, self-contained, and if you do blow one up experimenting, you don't feel nearly as bad as you would if you had just fried your $1400 486 or your $2000 Macintosh. And for bit manipulations and other "hacker applications", the C-64 is actually much *easier* to use than a "real computer."

The Mac and PC are designed to be used by people who should never need to get to the guts of the computer. Running applications is easy. But if you want to write code, you need to get a compiler, write a source file, compile it, link it, and then run it. If you want to build your own I/O devices, you'd better be a very good hardware designer. But when you turn on a Commodore 64, you are immediately in a BASIC interpreter, and getting to machine level from there is not very difficult. If you want to read a memory value, you just PEEK at it from BASIC. And there are multiple I/O ports to play with, all very easy to get to.

In this article, I'll show you everything you need to build a stand-alone DTMF decoder, with a one digit display. You can even order all the parts as a kit (see sidebar) and solder it together in about 20 minutes. And then if you want all the logging capabilities of a much more expensive dedicated DTMF decoder, I'll show you how to interface this project to a Commodore-64, or even a VIC-20 Computer (street value: about $10). With this DTMF decoder as an input device, you can decode and list touch tones from any audio source, and you can even make other applications that use touch tone control. With a telephone input, you can feed commands to your application remotely with a touch tone phone. With a radio input, you can make an amateur radio repeater controller. The applications are limited only by your imagination.

Some people might look at this and say, why a Commodore 64? There are several reasons I chose this particular computer. It's easy to use, especially for these sorts of projects. Lots of people have them already, and if you don't have one you can probably pick one up at a garage sale (I've seen them for as little as $20). Please understand, I'm not advocating retrograde technology. There is no substitute for a Pentium when you're playing X-Wing or running Crack on someone's password file, but there are also applications that don't need all that power, and with this project you can once again get use out of those "toy computers" which currently serve as door stops. If there is enough reader response to this project, I'll continue to design applications that you can add to your hacker's tool box. And perhaps these

projects will also give you some ideas, so you can design and build your own custom tools.

Of course, if you don't have and don't want to use a Commodore 64, and you know enough about the hardware interface, you can always hook this DTMF decoder to any computer of your choice, even a PC or Macintosh. The operation and outputs are explained below. The rest is left as an exercise to the reader.

Circuit Description

This section is for anyone who really wants to know what every part of the circuit is doing. If you don't really care, this is isn't vital and you can skip to the next section, "Circuit Construction".

The schematic diagram for this project is shown in Figure 1. The three major components are the DTMF Receiver IC (IC1), the display driver IC (IC2), and the seven-segment LED that displays the current digit. All the other parts provide power, support, and input conditioning for the circuit.

The capacitor in the audio input path (C1) is to block any DC in the audio input signal. The resistors (R1 and R2) form the audio amplifier feedback loop, which in this circuit (R1= R2= 100K) sets the gain of the internal differential input amplifier in the 8870 to unity. The crystal used by IC1 to generate its internal clock (X1) is a standard 3.58 MHz colorburst crystal. Finally, R3 and C2 form an RC timing delay that determines how long a tone must be present on the input to be considered valid, and then how long it must be off before the next tone is considered a "new" tone. With the values chosen here (R3= 330K, C2 = .1uF), the time for a tone to be considered valid is about 40 milliseconds.

The four-bit decoded output of the 8870 goes to a seven-segment decoder/driver, which is IC2, a 7447. The use of an off-the-shelf part like the 7447 is convenient and cheap, but provides one problem: the decoder IC doesn't output a binary 0 for an input touch tone digit of "0". Furthermore, all the other non-numeral digits (#, *, A, B, C, D) are also rendered as symbols by the decoder IC. See "Circuit Operation" section below. The 7447 drives a common anode seven-segment display on which the decimal point serves as a power-on and valid-tone indicator. Resistor R4 limits the total current that the LED can draw. Because the 7447 has internal limiting resistors, R4 can be left out, and the display will be much brighter but still not burn out. The disadvantage to having R4 in place is that the display will get dimmer when there are more segments on. For example, a numeral "1", which has only two segments, is considerably brighter than a numeral "8" which uses all seven of the segments. The advantage to having R4 however, is that it limits the current drawn by the entire circuit and makes the total current drain more uniform over time. This is particularly useful if you intend to power the circuit from the host computer bus, where current drain may be an issue (see "Computer Interface" section).

When operating without power from the host computer, or in a stand-alone configuration, power is provided to the circuit by a voltage regulator (IC3) which sources 5V from any input voltage between about 7.5V and 20V. The circuit is intended to be used with a 9V battery (attached to CON1).

Circuit Construction

You will need several tools to begin: wire cutters, wire strippers, a low-wattage soldering iron, and some rosin core (*not* acid core) solder. You will also want a heat sink (such as an alligator clip), and a well-lighted workspace where you can drip solder.

The entire circuit can be build on a single-sided printed circuit board 45mm x 65mm. The artwork for the board is shown actual size in Figure 2. This shows the copper traces as they should actually appear on the underside (opposite from component side) of the circuit board. The best way to fabricate the circuit board is photographically, but walking through the entire process of etching and drilling circuit boards is beyond the scope of this article. Because there are traces running in between IC pins on this board, the layout tolerances are fairly tight. If you have never made a printed circuit board before I strongly suggest you purchase the pre-fab

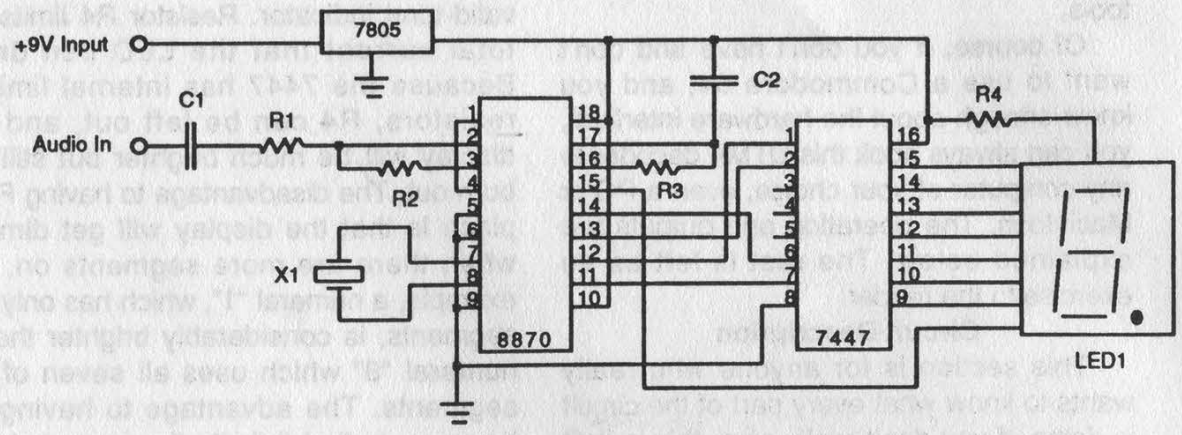


Figure 1 - Circuit Schematic

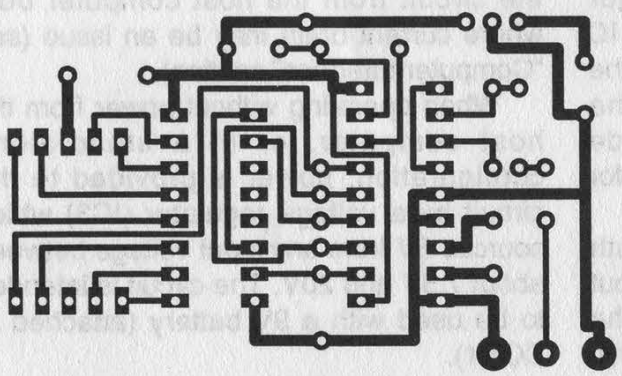


Figure 2 - Printed Circuit Board Artwork (Actual Size)

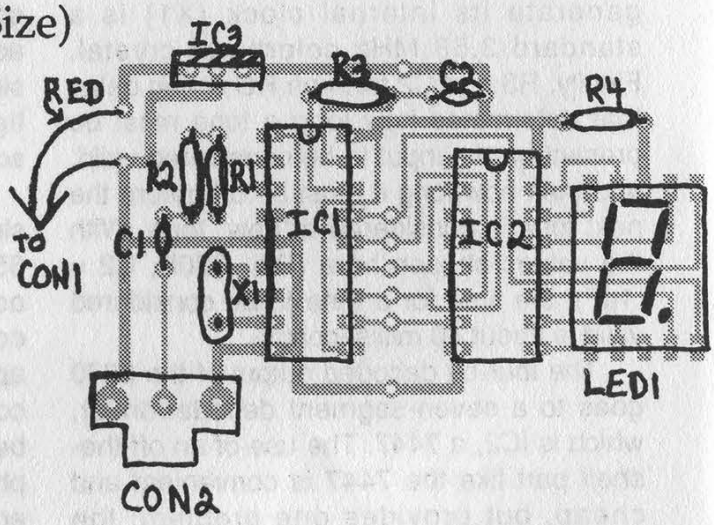


Figure 3 - Component Layout Guide

board, or the entire kit (see sidebar). The circuit is also simple enough that you can assemble it on perf-board, using the schematic in Figure 1, without the printed circuit board, but it won't be as durable or reliable.

The component layout on the top (blank) side of the circuit board is shown in Figure 3. Insert each component in the board, and then solder it in place and trim its leads off. It's easiest if you begin with the resistors, because the board can rest on them while you solder them in place. The rest of the components can then be inserted in order by height, from shortest to tallest, starting with IC1 and IC2, and ending with the voltage regulator (IC3).

Make sure that the board surface is clean before you begin soldering. Rubbing it down with rubbing alcohol and then wiping off any excess will insure that there is no grease from your fingers. When you solder the parts, remember that the components, particularly the ICs and the LED, are susceptible to thermal damage if you get them too hot. This means that you should use a heat sink (such as an alligator clip connected on the component side) on the leads of the ICs as you solder them. You should make sure that you only apply the soldering iron to the component leads for the minimum time needed to get a good clean solder joint.

Also make sure that you get the ICs in the board with the correct orientation. They will fit in two different directions, but you *must* have the end with the notch toward the edge of the board with the voltage regulator. The voltage regulator also has only one correct orientation, which is with the front (the labeled side) facing toward the ICs and the metal tab facing the edge of the board. If you put it in backwards, the circuit will not work. The decimal point on the seven-segment display should be toward the edge of the board. Make sure you put the red lead on the battery connector (CON1) in the hole closer to the voltage regulator (IC2). If you are not certain of the correct orientation of any of these parts (IC1, IC2, IC3, LED1, or CON1), study Figure 3 and make sure you have them oriented correctly before you solder them in place.

When the circuit is finished, there should be seven unfilled holes between IC1 and IC2 (which is where the computer interface is connected, see below).

Circuit Operation

Once you have built the circuit, turn it on by connecting the 9V battery. The decimal point on the LED should light up. You're now ready to decode DTMF tones. Connect a tone source to the audio input. When the circuit receives a "valid" touch tone, it displays the value on the seven-segment display. When a valid tone is applied to the input, the decimal point will turn off. Once a tone has stopped, the decimal point will light again, and the number will remain on the display until the next valid tone is received.

One quirk of using an off-the-shelf display driver (the 7447) with the 8870 DTMF receiver is the way a touch tone "0" is displayed. Because the 8870 doesn't output a binary 0 for the tone "0", it is actually displayed as one of the non-numeral symbols. A touch tone "D" is what is displayed as a "0" on the seven segment LED. Table 1 shows all of the touch tone inputs, their binary outputs, and the symbol displayed on the seven-segment LED for each.

Computer Interface

Although this tone decoder can be used as a stand-alone device, it is difficult to catch multiple digits, because they are only displayed on the seven-segment display until the next tone comes along. Furthermore, if the same touch tone digit is received twice in a row, the only way you will tell from looking at the display is by seeing the decimal point blink off as the next valid tone arrives while the number or symbol displayed remains the same.

This decoder becomes really useful when you hook it to something that can record the digits as they occur, and keep them in memory or display them to a multi-digit display (like a screen). All we need is a computer with a binary input port. For this project, I used the user port on the Commodore 64. This is the card edge on the far right as you look at the back of the computer. The six holes on the decoder

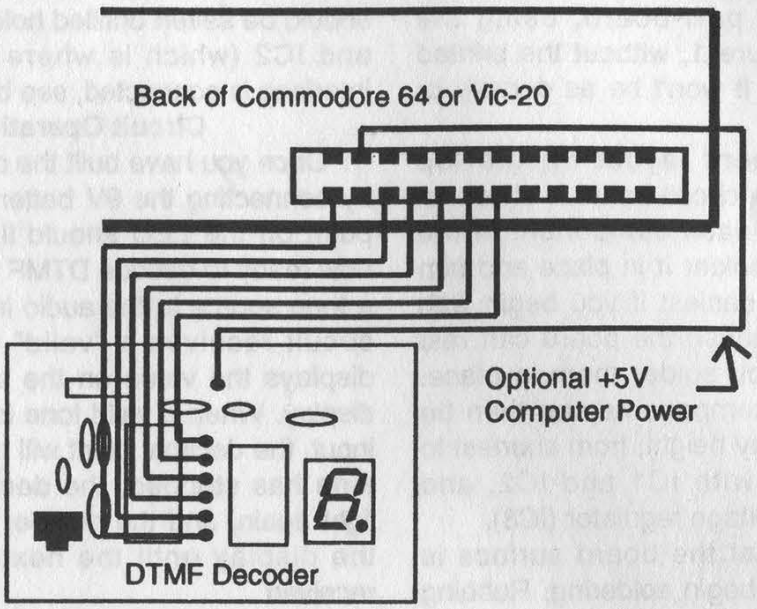


Figure 4 - Commodore 64/Vic-20 Interface Pinout

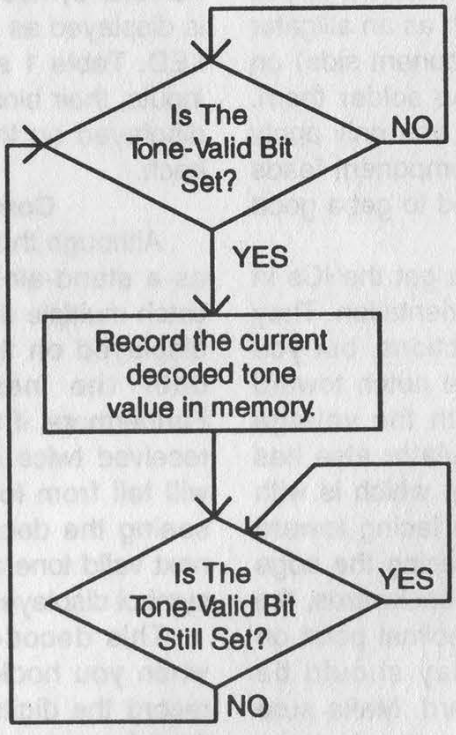


Figure 5 - Flowchart of Simple Decoder Polling Algorithm

circuit board between IC1 and IC2 are where you connect the board to the user port. The seventh hole (at the top of the Decoder) is an auxiliary power input, if you want to power the decoder circuit from the computer (and eliminate the need for batteries). Figure 4 shows which pins on the connector are connected to which holes on the board. The bottom-most hole on the board is the ground connection, the middle five holes are the four bits of the decoded digit and the valid bit. By connecting them to the user port, the state of the DTMF decoder is now reflected by the user port data byte in the computer's memory.

The algorithm for reading a digit in from the DTMF decoder is pretty straightforward. We just keep "polling" (checking the value of) the user port. If the valid bit is low (0), we check again. We look until the valid bit goes high (1), and then we record the current digit from the four-bit binary input. Then we wait for the valid bit to go low again before we start the whole process over. Figure 5 shows a flow-chart of this process. The Commodore 64 is a very slow computer by current standards, but it is still blazingly fast compared to the speed that DTMF digits can arrive. So a program written even in the glacially quick language of BASIC is plenty fast for our needs.

The sample program in Figure 6 is a DTMF number logging program. It scans for digits. If a digit is received, it prints it to the screen and waits for the next digit. If it gets a whole stream of digits, it will print them all on the same line. If it gets a "#" sign, or if there is a delay of more than three seconds until the next digit, it will skip to the next line and print any subsequent digits there. Numbers are not stored in memory, so once they scroll off the top of the screen, they are lost.

The code for the BASIC number logging program is broken down into subroutines and commented to indicate what is happening where. You can use this as a guide to writing your own code, or you can just copy sections of this program into your own. The possibilities of what you can do with this are limited only by your imagination. It's up to you.

And now you have a DTMF decoder. It's cheaper than an equivalent commercial product, and it offers a chance to start your own hacker's tool kit, in the spirit of the earliest pioneers who built all their own equipment. Good luck and have fun.

SIDEBAR

Part List, Kit Ordering Information

Many of the parts for this kit are available at Radio Shack, and have Radio Shack part numbers in parentheses next to them. The rest are fairly common and can be found at electronic hobby supply stores or from parts distributors. I've also contracted with Millennium Systems to provide all the parts and the printed circuit board in kit form. They also sell just the printed circuit board, if you prefer.

R1, R2 - 100K Ohm (271-1347)

R3 - 330K Ohm (This part value can be varied widely, so you can substitute at 470K Ohm resistor, Radio Shack part number 271-1354)

R4 - 330 Ohm (271-1315)

C1, C2 - .1 microfarad (272-1069)

X1 - 3.58 MHz Colorburst Crystal

LED1 - Common Anode Seven-Segment LED

IC1 - Teltone 8870-1 DTMF Receiver (You can call Teltone at 1-800-426-3926 to find your nearest distributor.)

IC2 - 7447 Display Decoder IC (276-1805)

IC3 - 7805 +5V Regulator IC (276-1770)

CON1 - 9 V Battery Clip (270-325)

Optional

CON2 - Female RCA Phono Plug for Audio Input (274-346, but this is not the printed circuit board mounted part that the circuit board art is designed for)

CON3 - 24 Pin (12 pin/side) card edge connector, .156" spacing (for connection to the Commodore 64 User Port)

Printed Circuit Board and DTMF Decoder Kits

Printed Circuit Board Only - $15

Complete DTMF Decoder Kit (Circuit board, components, and CON1 & CON2) - $28

Complete Kit + 24 Pin Card-Edge Connector for C-64 or VIC-20 User Port (CON3) + 5.25" Disk with number logging software - $42

Send orders, payable to:
Millennium Systems
P.O. Box 70868
Sunnyvale, CA 94086

You can also send comments and feedback to this address. If you have an application you'd like to see added to the hacker's tool kit, send it in.

```
10 GOSUB 10000: REM INITIALIZE VARIABLES
20 GOSUB 5000: REM SET FOR COMPUTER TYPE
30 GOSUB 4000:REM INITIALIZE THE PORT
100 REM MAIN PROGRAM LOOP
110 GOSUB 1000: REM GET A DIGIT
120 GOSUB 2000: REM PRINT DIGIT TO SCREEN, UPDATING LAST DIGIT TIME
130 GOSUB 3000: REM WAIT FOR THAT TONE TO END
140 GOTO 100: REM CONTINUE MAIL LOOP
1000 IF PEEK(DREG) AND 16 THEN GOTO 1020
1010 GOTO 1000: LOOP UNTIL VALID BIT GOES HI.
1020 DTMF=PEEK(DREG) AND 15
1030 RETURN
2000 IF TIME-LAST > 180 THEN PRINT
2010 PRINT OUT$(DTMF);
2020 RETURN
3000 IF PEEK(DREG) AND 16 THEN GOTO 3000
3010 LAST=TIME
3020 RETURN
4000 POKE DIR, 0: REM SET ALL BITS TO INPUT
4010 RETURN
5000 IF (FRE(0)-(FRE(0)<0)*65536)<5000 THEN GOTO 5040
5010 DIR=56579: REM DATA DIRECTION REGISTER ADDRESS FOR COMMODORE 64
5020 DREG = 56577 :REM USER PORT DATA ADDRESS REGISTER FOR COMMODORE 64
5030 RETURN
5040 DIR=37138: REM USER PORT DATA ADDRESS REGISTER FOR VIC-20
5050 DREG=37136: REM USER PORT DATA ADDRESS REGISTER FOR VIC-20
5060 RETURN
10000 DIM OUT$(16): REM DIMESIONS OUTPUT SYMBOL ARRAY
10010 READ CODE,SYMBOL$
10020 OUT$(CODE)=SYMBOL$
10030 IF CODE <> 15 THEN GOTO 10010
10040 LAST=0: REM TIME LAST TONE ENDED
10050 DTMF=0: REM DECODED DTMF VALUE
10060 DREG=0: REM DATA ADDRESS REGISTER
10070 DIR=0: REM DATA DIRECTION ADDR. REG.
10080 RETURN
15000 REM DATA FOR EACH POSSIBLE DTMF INPUT AND IT'S CORRESPONDING SYMBOL
15010 DATA 0,"D",1,"1",2,"2",3,"3",4,"4",5,"5",6,"6",7,"7",8,"8",9,"9",10,"0"
15020 DATA 11,"*",12,"#",13,"A",14,"B",15,"C"
```

Figure 6 - Commodore 64/Vic-20 Sample Code

Key	F_{Low}	F_{High}	Q4	Q3	Q2	Q1	Symbol
0	941	1336	1	0	1	0	c
1	697	1209	0	0	0	1	1
2	697	1336	0	0	1	0	2
3	697	1477	0	0	1	1	3
4	770	1209	0	1	0	0	4
5	770	1336	0	1	0	1	5
6	770	1477	0	1	1	0	6
7	852	1209	0	1	1	1	7
8	852	1336	1	0	0	0	8
9	852	1477	1	0	0	1	9
*	941	1209	1	0	1	1	-
#	941	1477	1	1	0	0	U
A	697	1633	1	1	0	1	F
B	770	1633	1	1	1	0	E
C	852	1633	1	1	1	1	
D	941	1633	0	0	0	0	O

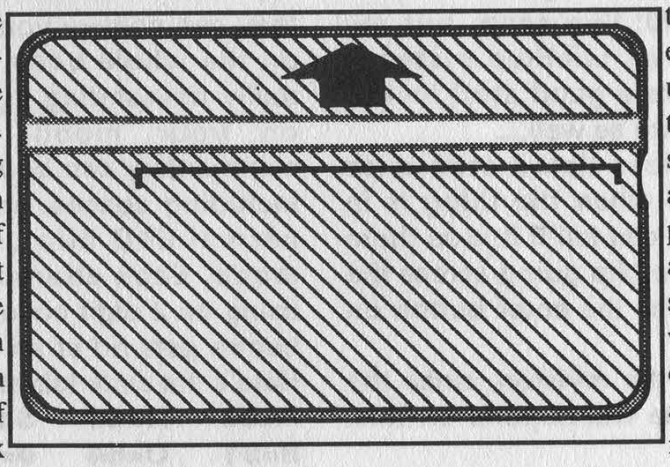
Table 1 - Keys, Frequencies, Decoder Outputs, and Displayed Symbols

The Nynex Change Card

by Kevin Daniel

Nynex is currently testing a supplement to coin-operated telephones in New York City based on a disposable card technology called the Change Card. This article represents an analysis of this system based on information inferred from the dissection of several cards, and trials using the Landis and Gyr Type BTK1290-4 telephones installed in one of Nynex's test sites. Your mileage may vary.

The Change Card is a plastic card identical in size to a credit card which is dispensed from a vending machine, costs $5.00, and has an initial value of $5.25. As calls are made using the card, the telephone subtracts value from the card and the value remaining is displayed both on the phone and the card. Billed as freeing the customer from the burden of carrying a pocket full of loose change, I can imagine this system has a host of benefits for Nynex such as: reduced consumer fraud, reduced employee fraud, calls paid for up front, and the transference of some billing operations from the central office to the individual telephones.



The Change Card is made from reflective infrared reader and electrical discharge writer technology. On the face of the card is a highly reflective metallic strip covered by a protective layer of white infrared-transparent ink. It is on this strip that all card validation and value information are encoded. Validation bits are encoded as a series of areas of high and low reflectivity in the left-most 2 centimeters of the stripe. Value information is encoded as the length of the high reflectivity area starting from the end of the validation section and extending to the right-hand edge of the card. When a Change Card is first inserted into a telephone it is locked into place and scanned left-to-right by the phone's read/write head. If the validation fails the card is immediately ejected, otherwise the scan continues until it hits the next area of high reflectivity. A new card has a value stripe beginning at about 2.2 centimeters from the left hand edge and running 6 centimeters. Upon placing a call the phone will fire a spark across the write head converting the underlying area of high reflectivity to low and scarring the white protective layer displaying remaining value to the user. Value is removed immediately at the time of connection and then following each billing period until the call is terminated. The system protects against fraud by performing a read-after-write sequence, if the write has not occurred the phone automatically and immediately terminates the call and ejects the card. The system also protects against card tampering/damage by skipping over value bits which have been damaged or blown out of sequence, reducing the value of the card to that of the next readable value. Other anti-fraud measures implemented on the test site devices include: physical capture of the card during calls, separation of the handset from the signal path prior to connection, and the blocking of 900 number calls.

The Change Card system is simple but highly evolved tamper resistant technology that would seem to have few possible areas of compromise. Although currently only available in units of $5.25, who knows what secrets the validation codes hold.

HOW TO HACK HEALTH

by MuscleHead

To quasi-paraphrase the lovable vice prez running OCP in Robocop, "Good hacking is where you find it." In this case, it's in a room of sweaty people wearing lycra. Most health clubs have aerobic equipment, and more often than not a stair machine is part of the collection. You can do more with these things than choose some workout routine and lie about your weight, you can *hack them!* They don't have that keypad and LED display just for the users, it's also there for techs and club owners to do things you (the sweating one) aren't supposed to know about....

All of the following refers to a Stairmaster 4000; I've seen, but my place doesn't have, LifeStep systems. Presumably, there's good stuff locked away in its firmware as well....

All codes unless listed otherwise must be entered when the thing is in attract mode; you can tell if it is as there will be an EKG-like blip going across the display. ENT means the enter button on the keypad.

First, find out the revision, since the codes you will use will depend on this. Hit **107 ENT 4**.

You should see something like this:

REV. D, REV. E, REV. M, REV. 1.1, REV. 1.2, REV. 1.3, REV. 1.5, REV. 2.1, or REV. 2.2.

If you get anything below 1.5, don't bother with it, most of the codes won't work.

Changing the workout time. Feel like you're not getting your fair shot on the stairs? Hit **1010 ENT**, enter the time (up to 45 minutes), and **ENT** again. Then, when Bobby Joe Steroid wants you to get off, you can tell him "Hey, the thing hasn't beeped and you *know* they shut off after fifteen minutes...."

Locking in the maximum time. Use your knowledge to protest goofy time limits. Note: this really *locks* in the max time; some poor Stairmaster tech will have to come out and use his/her magic wand if your club wants it changed after you do this. For 1.5 and 2.1 revisions: **1010 ENT**, enter the maximum workout time, **ENT**, system goes back to attract mode, **97405 ENT**, system displays time you just set, **ENT**. For 2.2 revision: **1010 ENT**, enter maximum workout time, **ENT**, system goes back to attract mode, **97405 ENT**. Now you can avoid the evil club's high-turnover setting and stay on the Stairmaster up to your God-given 45 minute limit!

Creating aesthetic commentary. This is the fun stuff. All those LEDs can be used for more than just displaying some simulated terrain or blipping a fake EKG; they can convey your deepest thoughts on the whole body image issue. Or a really devastating ego-nuke, depending on your mood. Your insightful commentary can be a max of 128 chars, including spaces, and will replace the normal EKG blip used in the attract mode. Each character is entered by using its 2 digit code; hitting the CLEAR button gets rid of an incorrect character. Here's the code table:

A=50	**N=63**	**Space=76**	**+=22**
B=51	**O=64**	**0=00**	**$=23**
C=52	**P=65**	**1=01**	**.=24**
D=53	**Q=66**	**2=02**	**%=25**
E=54	**R=67**	**3=03**	**?=26**
F=55	**S=68**	**4=04**	**'=27**
G=56	**T=69**	**5=05**	**"=28**
H=57	**U=70**	**6=06**	**_=29**
I=58	**V=71**	**7=07**	**#=30**
J=59	**W=72**	**8=08**	**heart=31**
K=60	**X=73**	**9=09**	**:=32**
L=61	**Y=74**	**!=20**	
M=62	**Z=75**	***=21**	

To program the message, hit: **7607 ENT**, enter your message, **ENT**. Remember, given the location, an ill-chosen message could push someone insecure with themselves into another five years of therapy. So, be a good neighbor....

Editing the message: **7607 ENT**

brings up the message. Use the up/down arrows to scroll through the message. **CLEAR** kills the rightmost character on the display, and anything you enter is inserted at the right.

Shutting message off: **2123 ENT**. It's still stored in memory though.

Turning message on: **2121 ENT**.

Turning "teletype" sound on: **40 ENT**.

Turning "teletype" sound off: **41 ENT**. Slot machine: this replaces the standard "You didn't die!" message you get when you slave all the way through a session. Not nearly as much fun as the message option, but it can cause amusing confusion in workout-numbed victims. **8089 ENT**, "DISPLAY ODDS" is displayed, enter number between 5 and 9999 depending on how unlucky you want everyone to be (higher is unluckier), **ENT**. Not too thrilling.

Turn off slot machine: **8089 ENT, 0, ENT**.

Cover your ass: **105 ENT**. This wipes the memory, and any chances a club owner has of proving you have curiosity.

Miscellaneous stuff: (all codes followed by **ENT**)

3121: Display current slot machine odds.

7703: Cumulative hours and floors.

9760: Change over to Imperial system.

9761: Change to metric system.

up arrow, 15: Display test.

107 ENT 5: Displays settings.

As an alternative to health clubs, many health equipment stores now carry higher-end toys like Stairmasters. Many of these stores also display them prominently at the front windows because "*Hey! LEDs!*" - Joe Customer will always be hooked by a lightshow! So, what better place to get across your opinion than a trendy health equipment store at a busy mall? Celebrate your public debut with a corn dog at Frank's Crisco Haus while you watch the nice owners handle the extra business you brought in....

For nearly two years, the 2600 Voice BBS has brought people from all walks of life together in a spirit of cooperation and sharing. While it might sound nauseating, it really can be fun. By dialing

(10288) 0700-751-2600

you will become part of a vocal band of explorers, their quest - to search the earth for strange phone numbers, their goal - to share tales of hacker adventure, their desire - to help others figure out the answer, and their purpose - to achieve all four.

BUT ALL OF THAT IS ABOUT TO

SOFTWARE PIRACY
Another View

by Roberto Verzola

Reprinted from the World Press Review, courtesy of the Third World Network Features agency of Penang, Malaysia

Many Manila computer users copy programs from computer shops or from the computer bulletin board systems that have proliferated around the city. They give copies of these programs to friends and colleagues who, in turn, give copies to other friends and colleagues. In the terminology of Western software companies, they are pirates: Copying commercial software and giving it away to friends and colleagues is called piracy.

I have seen pirates in movies, and they are a mean bunch. They are villains who steal, kill, and plunder. At the movies' endings, when these good-for-nothing pirates get their just due, the audiences invariably applaud, for the pirates get the punishment they roundly deserve.

It is no fun to be called a pirate. Or to be treated like one.

I have seen a number of people who come from or work for Western software firms. They come and visit this country of pirates and perhaps make a little study of how much they are losing from piracy in the Philippines. Quite a number of them, I would say, come to the country to do some pirating themselves. However, they do not pirate software. They pirate people. They pirate those who write the software. They pirate our best systems analysts, our best engineers, our best programmers, and our best computer operators.

There is quite a difference between pirating intellectual property and pirating individuals. It costs our country perhaps $10,000 to train one doctor. Training a second doctor would cost another $10,000. Training 10 doctors would cost $100,000. In short, given an "original" doctor, it would cost us as much to make each "copy" of the original.

When the Americans pirate our doctors, they take away an irreplaceable resource, for it takes more than 10 years to train a new doctor. The Philippines has approximately one doctor for every 6,700 citizens. When the U.S. pirates this doctor, it denies 6,700 Filipinos the services of a doctor. And every year, the U.S. takes away hundreds of our doctors. How many Filipinos have died because they could not get the services of a doctor in time?

What about a computer program? Whatever amount Lotus Corp. spent in developing its spreadsheet program, it costs practically nothing to make a second or third copy of it. When Filipinos pirate the program, they have not stolen any irreplaceable resources, nor would it take Lotus 10 years to replace the program, nor have we denied any American citizen the use of the program. It is still there for Americans to use. When the U.S. pirates our doctors, it does not take a copy and leave the original behind. Instead, it takes the original and leaves nothing behind.

Copying software is a benign case of piracy. Pirating doctors is a malignant case. We have been victims of this malignant form of piracy by Western countries for a long time. They should be the last to complain when they are affected by a benign one. This piracy debate will become even more important in the future, because advanced countries are now developing computer programs that can mimic what goes on in a doctor's mind. We can say with some certainty that the U.S. will raise a big row if we pirated this one program.

In truth, the terms "piracy" and "theft" of intellectual property are emotionally laden, but they are not very accurate descriptions of the act. Legally, one might be charged with violating the copyright or patent laws of a country, but this would normally be different from the crime of theft or actual piracy. Using these words, however, automatically connotes immoral action on the part of the copier. Thus, in the polemics against the Third World, "piracy" and "theft" are favorite terms among advanced countries, particularly the U.S.

The term "piracy of intellectuals" can likewise be used, if one wants to ascribe a sense of immorality to the act. This is not to imply, of course, that countries own their intellectuals. Both intellectuals and intellectual property have other important attributes, aside from simply being commodities on the market. Notwithstanding the fact that advanced countries normally encourage the best brains of the Third World to work for them through various incentives and enticements, these intellectuals have their own reasons for doing so. Perhaps the chances for personal and professional advancement are better. Perhaps the environment is more conducive to their own temperaments and predispositions. Perhaps they were persecuted in their home countries, and so on.

The Christian Bible tells of the miracle of the loaves, when Jesus and his apostles had only five loaves of bread and two pieces of fish to feed 5,000 people. Every time I give away a copy of my favorite program, I remember the miracle of the loaves. Indeed, 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?

YOU'LL NEVER CATCH 2600 RESORTING TO CHEAP GIMMICKS LIKE MULTI-PAGE ADS.

We prefer to devote our pages to the DIFFERENT projects that are ongoing. For those of you on the net, there are now two outlets to vent your hacker fervor.

On the 26th of each month, hackers from around the world converge on Internet Relay Chat Channel "#2600". If you're on the net, ask your system admin how you can access irc. If (s)he sputters and turns red, you will be able to easily identify them as a "hardass sysadmin" with no sense of fun.

Ongoing on the net is a newsgroup called "alt.2600" where hacker issues of the day are discussed from around the world. If you're still on speaking terms with your system admin, ask them how you can subscribe to this newsgroup. If they begin to convulse and speak in tongues, it may be time to consider another site.

coping with cable denial

by Cap'n Dave

There are three forms of denial technology in common use today. The first is the simplest: the negative trap. This is merely a filter placed outside of the home (usually on a pole, inside a pedestal, or in a box mounted to the house) that blocks out certain channels. The problems with this system are that a capital outlay is required for the homes that don't pay for the premium channels, and that someone has to come out to add or remove services. In addition, a converter may be required for non-cable-ready equipment.

These negative traps are cylindrical in shape, about five inches long and one inch in diameter. They are threaded with a male "F" connector on one end and a female "F" on the other. Each one may block out one or more channels (always contiguous though), and are often used in series. On channels where these are in use, your TV will show nothing, or a faint, "snowy" picture.

These could be removed, but the cable company will eventually notice and possibly get upset. Better yet, older-style traps can be opened and wired straight through. If they were then replaced, the cable company might never notice. A clever person might steal someone else's traps to experiment with. Newer traps are filled with epoxy and will have to be drilled out before being re-wired. The experimenter will probably have to destroy a few of these to get the technique down.

A note for apartment dwellers: the traps for every unit in the building are usually in a box somewhere on the outside of the building. This may (or may not!) have a lock on it. In any case, the next time the cable company comes out there is a small but finite chance that they will notice all the traps missing on one particular unit. To avoid this, drill out and rewire the traps, or remove every single trap in the box. Better yet, share the joy with some other buildings. This won't work for long, but it covers your tracks.

In the old days, the negative traps could be "burned out" by attaching 120V AC to the cable, and flipping it on and off a few times. *Do not do this!* It won't work anymore (the traps burn out and no longer pass signal) and it's real obvious to the cable company what happened. Melted co-ax is hard to hide. Also, it sometimes catches on fire. Kinda hard to explain to your insurance agent and/or the fire department.

The second common denial method is the interfering carrier. In these systems, a "jamming" carrier is placed halfway between the video and audio carriers (at a frequency 2.25 MHz above the video). This is removed by a "positive" trap placed inside the paying customer's home (threaded in line on the back of the box/VCR/TV. They look just like a negative trap, described above. In this case, the cable company only has to shell out for customers who are paying for the service. However, the interfering carrier obliterates some of the picture information, and the filter blocks out even more. This results in some degradation of the picture, especially the sharp details. Cable companies often get complaints about this.

These channels (more than one denial method may be in use on the same system) can be identified by the loud screeching noise emitted from the TV. Also, the picture should be flashing and/or full of lines. The actual "jamming" effects may vary from TV to TV. An article in the Spring 1993 issue described a crude method for blocking an interfering carrier. I have not tried this, and have no idea how well this will work.

The third method is to scramble the picture, and lease the customer a converter/descrambler to recover the picture. Not all converters can descramble! And one brand is *not* likely to descramble the competition's scrambling scheme. Also, unlike an earlier writer indicated, not all brands of converters have "booby traps" in them that activate on opening. Some do (especially Pioneer), but probably far less than half of non-Pioneer boxes are so equipped. If one were to "accidentally" trigger one of these, it would be prudent to return it and say the cat knocked it off the top of the TV. As long as there are no other anti-tamper methods in use (labels, etc), this will probably work. Especially if a female swapped the box. Women virtually never pirate cable. It's a man's game.

Scrambling is done in several ways. The most popular is to amplify the voltage of the horizontal sync signal. This prevents the TV from knowing when to draw the electron beam

back to the left side of the screen. Thus the picture "breaks up". Usually the audio is undisturbed. The cable descrambler lowers the voltage of the sync signal, and the TV again locks.

Now, about converters. These boxes come in three flavors: non-addressable non-descrambling, non-addressable descrambling, and addressable descrambling. The non-addressable non-descrambling converter is just a converter - it tunes the channels that non-cable-ready equipment can't tune, and converts them to channel 3.

The non-addressable descrambling converters can descramble and tune channels. But they must be programmed by the cable company via some contact method (i.e., not through the cable). They may have to open the box and program a chip, or use an infrared programming scheme.

The most sophisticated (and newest) form of converter descrambles and is addressable. That is, the cable company can reprogram the box over the cable. They will die, at least temporarily, if cut off from the data on the cable. These are the only kind of boxes used for pay-per-view.

Contrary to popular opinion, these boxes do not "spy" on the customer. They don't have tiny cameras or microphones in them. Cable operators have enough trouble getting a signal to you to worry about that sort of thing. In fact, the vast majority of cable systems are one way only, or at least one way over the cable. This means that the company has *no way* to tell if a box is cloned. On systems with instant pay-per-view (where the movie is bought from the box, not over the telephone) there are two ways of getting the data back to the cable company. Phone return is the cheapest. The box is attached to the phone line and it calls in, usually in the middle of the night. The more advanced systems send the data back over the cable. This system is gaining in popularity as the phone companies try to move into the cable business, and as they try to make the cable companies pay for using the phone lines. Both of these schemes are sometimes used to monitor what people are watching. (It's more like asking the box, "See what they are watching tonight at 7:00 pm and call me back." The cable operators can't find out every time you switch channels.)

The costs of these converters vary from $30 to $50 for the simplest up to $150 for a top-of-the-line addressable unit. "Wide open" units may often be purchased on the black market. Check the ads in the back of *Popular Science* or *Nuts & Volts*. (You *do* subscribe, don't you? All hackers should. Call 1-800-783-4624 now.) These are also good sources for replacement remotes, in case you lose yours. Remotes cost the cable company about $5 but they often charge $30 if you lose one, in addition to charging a couple of bucks a month. Talk about your return on investment! Remember, though, that it is illegal to own a converter box capable of receiving services to which you are not entitled.

Some "legitimate" cable companies are actually Mafia-owned fronts for obtaining converters. Stories constantly circulate about systems with 2,000 customers ordering tens of thousands of boxes. These converters are then diverted into the black market. With the government raiding these shops, it may or may not still be safe to order boxes, though remotes are probably still OK.

Positive traps can also be purchased from some of these suppliers, or can be built using parts from Radio Shack. Build a high order notch reject filter, and tune it for best picture quality. If there are several channels on the system blocked by an interfering carrier, a clever person might build and optimize (or buy) a single filter for channel 3 and use an inexpensive non-addressable converter to put the video out on channel 3.

Most converters can be opened easily, even though they often have some sort of "security" screws on them. The nastiest one I've seen uses a head that is slightly oval. You will know what I mean if you see one. These can be removed by heating a plastic tube and pressing it down over the head before it cools. Now you have a tool! Pens make good sources for such plastic tubes. Other kinds of security screws can be removed with improvised tools, or vise-grip pliers. Tools have also been advertised in *Nuts & Volts.*

Cable TV companies do have the ability to "look" down the cable and see what equipment is attached, and what channel you are watching. However, this requires skilled operators and expensive equipment (high frequency spectrum analyzers and TDR units). It must be done at the house (or pedestal, pole, etc.) and is not usually done randomly. This snooping can most likely be blocked by putting an amplifier before anything you don't want them to see. They will see the amp, and nothing past it. Higher quality amplifiers will do a better job.

Happy hacking!

PRODUCT REVIEW

Cellular Telephone Experimenters Kit
$125, Available for OKI 900
Network Wizards
PO Box 343
Menlo Park, CA 94026
voice: (415) 326-2060
fax: (415) 326-4672
Internet: info@nw.com
OKI Telecom
(404) 995-9800
(800) 554-3112
Review by Mr. Upsetter

Any technology that combines radio, telephones, and computers is sure to interest hackers. It's no wonder cellular telephony has received so much attention. Now exploring the system is a little easier for us. A company called Network Wizards has introduced an interface that allows control of an OKI 900 cellular telephone from a DOS PC via the RS-232 port. Their Cellular Telephone Experimenters Kit (CTEK) consists of an interface, four DOS executables for controlling the phone, and a C function library so you can write your own programs. Also included on disk are a user's manual, function library manual, and a short cellular tutorial.

The interface itself is contained in a small black box with a DB25 connector on one end. A cable with a specialized plug for connecting to the OKI is on the other end. Inside is a PIC16C54 microcontroller which converts data from the OKI to standard RS-232 data. The interface also has a mini stereo jack for connecting a microphone and earphone.

The DOS executables included with the CTEK allow you to perform numerous functions. The MENU.EXE program allows you to change any of the phone's five NAMs. (A NAM, or Number Assignment Module, consists of a telephone number, system ID, initial paging channel, access overload class, and group ID mark. This information, along with the ESN, identifies your phone in the cellular system.) This program also allows you to read, write, and edit the phone's 200 alphanumeric memories. The TEST.EXE program allows you to manually control the transmit and audio functions of the phone. You can turn the transmitter on or off and set the channel, SAT, and transmit power. You can also set the volume, mute the transmit, or receive audio as well as set the audio source to the earpiece, sounder, or external jack on the CTEK interface. The TEL.EXE program allows you to monitor the paging channel and displays all the forward control channel messages. It also allows you to place and receive a phone call while displaying the voice channel messages. The KEYCON.EXE program simply allows you to press keys on the OKI from the computer keyboard.

The programs provided with the CTEK certainly expand the functionality of the phone. But to do the really fun stuff, you need to write your own programs. Source code to TEL.EXE and KEYCON.EXE are provided to get you started with the CTEK function library. Although my C programming skills were a little rusty, I found it easy enough to write programs with the library. I wrote a cellular scanning program which had the following capabilities:

Scan for a paging channel and display the messages. If a voice channel is assigned, go to that channel and listen to the call.

Scan voice channels and listen to active channels.

Scan OMNICELL channels and listen to active channels.

While listening to a call, display the voice channel messages.

Automatically follow handoffs.

Decode DTMF, change the volume or audio source.

Automatically mute the audio and stop monitoring when the call is released.

Other functions in the library allow you to send reverse channel messages, get the received signal strength, control transmitter and audio functions, and read the phone's memory. Overall the function library is quite versatile. I had several other ideas for programs, for instance:

Log all messages and call information for certain cellular phone numbers. You could log paging channel messages, calls placed and received, call durations, DTMF digits dialed, cell channels used, etc.

Create a "spectrum" display of the cellular band by scanning all channels and recording the signal strength.

With a map of cell sites in your area, physically track a phone as it moves from cell to cell.

I had great fun exploring the cellular network while playing with the CTEK. But this kit isn't for everyone. To get the most out of the CTEK, you need to write your own programs. The executables provided in the kit really don't use the phone to its highest potential. Also, the OKI 900 isn't the cheapest phone in the world. It goes for about $400 to $450 new, perhaps $300 used if you can find one. Still, you could put together a great cellular monitoring system comparable to the ones designed for law enforcement for a few hundred dollars as opposed to a few thousand dollars. The CTEK is best suited for monitoring the cellular network rather than as a tool for fraud. You cannot change the phone's ESN with the CTEK. In fact, the library function which lets you send reverse control channel messages won't even let you send a bogus ESN.

Overall, the CTEK is a well designed product, both in hardware and software. While it's currently only available for the OKI 900, Network Wizards promises a version for the OKI 1150 soon.

Sample output of my cellular monitoring program (phone numbers have been masked)

Monitor system A or B?
Monitoring system B
Scanning for control channel
Monitoring Control Channel: 0337 System: B
Received Signal Strength: 46
(408) 482-01XX page scc=3, dcc=2
(415) 264-06XX page scc=3, dcc=2
(408) 671-19XX page scc=3, dcc=2
(310) 701-23XX non-autonomous reg: on scc=3, dcc=2
(805) 680-11XX reserved (13,6) scc=3, dcc=2
(415) 517-32XX page scc=3, dcc=2
(408) 499-03XX page scc=3, dcc=2
(805) 893-22XX reserved (13,6) scc=3, dcc=2
(510) 914-46XX page scc=3, dcc=2
(213) 500-44XX chan=526, vmac=0, scc=1, dcc=2
monitoring channel 526
audio on
hit any key to stop monitoring
Decoding DTMF. Press any key to resume.
3447555#706
audio off
(415) 971-86XX page scc=3, dcc=2
(707) 321-21XX page scc=3, dcc=2
OMNICELL Scan. Press any key to resume.
channel: 0358 RSSI: 10
channel: 0379 RSSI: 53
activity on channel 0379 RSSI 53
audio on
hit any key to stop monitoring
handoff msg: chan=465, vmac=0, scc=2, pscc=1
tuning to channel 465
handoff msg: chan=505, vmac=0, scc=1, pscc=2
tuning to channel 505
audio off
channel: 0400 RSSI: 11
channel: 0421 RSSI: 08

DID YOU MOVE?
ARE YOU EVEN THINKING OF MOVING?

Let us know several weeks in advance. For some reason the post office doesn't forward magazines so you might miss an issue if you don't let us know about your new address. Also, to make sure it's actually you changing your address and not some mischief maker, we ask that you include your address label with any correspondence. If you can't find that information, then use an official address change card from the post office. Please don't leave address changes on our answering machine or through email without label info.

FOIA facts and fiction

by GateDancer and Shrike

Congress created the Freedom of Information Act and its sister, the Privacy Act, to guarantee citizens access to government files of interest or concern to them. This act is a law! This is supposedly a free country and therefore information should be readily accessible. Sounds good on paper, but as we all know, some government agency clowns seem to have a totally different point of view. Because of these mindsets, and the games that go with them, you need to know exactly how to submit your request.

The FOIA is intended to apply to any government agency. It does not apply to Congress, Federal courts, or the Executive office. There are also exemptions for Uncle Sam's banks and corporations held by the U.S. government. While the act is worded to provide access to agency records, this term is not really defined within the body of the law. The courts have, however, defined this to mean documents or *other information bearing materials such as photographs and computer tapes,* within both the possession and control of that agency. Any U.S. citizen, permanent resident aliens, foreign nationals, corporations, unincorporated associations, etc. (you get the picture) can make the request.

The Act requires an agency to respond within ten working days. If you're not happy with what you get, you can make an administrative appeal, to which they have 20 days to answer. In all cases, there's a Catch-22 where they can claim a need to get files from field offices, etc. But basically you should have some sort of response within a month to six weeks. There are a few instances where they can deny the request completely, but these are things like national defense or security, agency personnel, trade secrets, oil well locations, and the biggie, where it may interfere with law enforcement in an ongoing investigation. Sometimes they will try this load of manure on you. But just remember that it's a peon making that denial and exemptions are discretionary, not mandatory. You will usually get what you want with an appeal. Then a supervisor has to look at the matter and they usually give up the goods. Also, they cannot just claim that the information falls under some sort of exemption. They must state *exactly* why!

Now what does this cost? Well, the Act provides for a small fee to be charged for direct costs. That's copying, folks, not the man hours involved in tracking this stuff down. There are sometimes search fees, but they are pretty insignificant. Whatever this "search" line is, it isn't man hours. There's even a provision where these fees can be waived if it's in the public's best interest, but let's face it, they are mad enough at getting the request, so don't expect them to waive the fees unless you can get pretty creative with words and make them believe it's in the public interest!

Now let's get down to business and make the request. At first glance everyone may think that's easy. But perhaps some of us have more colorful backgrounds than others and want to target more than just one agency or branch office. The *United States Government Organization Manual* is probably at your local library. If not, call your local Congressional Representative. His office should help one get to you. (It's a nice way to make sure they are earning their paychecks!) Once you have targeted who you want to ask, then give their local offices a call and get the address for FOIA requests. If you're paranoid, make the call from a payphone. But the simple fact is they just don't have the manpower to investigate you just because of the call.

Again, the Act is vague about the request, saying that you must reasonably describe any records being sought. This only means that they want enough info so that an employee of that agency who is familiar with their filing system can locate the records with a minimum of time and effort. You *do not* have to explain why you want the information. Don't let them tell you that you do! But keep in mind that the more precise and accurate the request, the more likely you are to get a complete response (unless they just try to shine you on like the Secret Service is doing with the Pentagon City Mall trip). You should try to follow a basic request strategy.

Limit your request to what you really want. Don't just say "all files relating to...." or you are giving them an excuse to delay or soak you with copy costs.

State what your request includes and what it doesn't include.

Be specific about the search logic; use "and/or" to cover all the bases and not give them an excuse to manipulate your request.

Decide if you want to write to a regional office or the central one. Recent local investigations would probably be held in a local office.

If you know there have been newspaper accounts, then state that! These Government geeks can be pretty thorough and so should you.

Include dates and locations, as well as the names of specific goons (officers, agents, whatever) if you know them.

If you are asking about yourself, then make sure you give as much identifying data as possible, i.e. Social Security number, driver's license number, date of birth, place of birth, etc.

Now anyone can write a letter. And many people do. Not that they get what they want. But with a little effort, you will submit a masterpiece that will motivate them rather than allow them to ignore you. By all means type it. Date it. Keep a copy. Cite the statute: Freedom of Information Act, 5 U.S.C., section 552. If you are asking for personal files on you, also cite the Privacy Act: 5 U.S.C., section 552a. It's good to begin

your letter with those cites. Toward the end, remind them that you know your rights. *Nicely.* Let 'em know that if their response is not satisfactory, you will be appealing and ask that they include their name and the name of the person appeals would be directed to. If you are requesting personal files, you will need to get your request notarized. (Any bank or real estate office can do that for you.) Remind them that you're entitled to anything left over when they get done blacking out all the neat stuff. Because while they may blank out names, dates, and places, you can usually figure out the basics from what's left over. You also might want to ask that they contact you with an estimate of fees if you think there's going to be a lot of data involved.

Now when you do end up with a bunch of pages with most of the text blacked out, that's just one of their BS strategies and you should appeal. Appeals get you farther than you think. Also, if you do not get an answer by the time you think you should, then write again or call to let them know that you feel they are violating the time limits set forth by law.

They may claim that materials do not exist when in fact you know they do. True, they may just be playing you, but most often they are so disorganized that you will need to be even more specific than you already have been. Some of these goons get so mistrusting of each other that they carry on their own little investigations and actual agency records may not even exist. Be specific. Get names of goons, dates, offices, etc. *2600* has already printed a listing of Secret Service offices (Winter 1992-93), and we've included one for FBI field offices as well.

If you are still running into trouble, then write your district Congressman or Senate representative. There are even a couple of Congressional committees responsible for overseeing the lawful workings of the FOIA.

For more information, sample forms, and lots of help addresses, there is a booklet called "Using The Freedom Of Information Act - A Step By Step Guide" available from the Center For National Security Studies, 122 Maryland Ave., Washington DC 20002 for only $2. They have some other pretty informative books as well on national security and surveillance.

Happy hunting!

City	Address	Telephone
Albany, New York 12201-1219	5th Floor, 445 Broadway, USPO & CH	518 465-7551
Albuquerque, New Mexico 87102	301 Grand Avenue, N.E.	505 247-1555
Alexandria, Virginia 22314	Room 500, 300 North Lee Street	703 683-2680
Anchorage, Alaska 99513	Fed. Bldg., Room E-222, 701 C Street	907 276-4441
Atlanta, Georgia 30302	275 Peachtree Street, N.E., 10th Floor	404 521-3900
Baltimore, Maryland 21207	7142 Ambassador Road	301 265-8080
Birmingham, Alabama 35203	Room 1400 -2121 Building	205 252-7705
Boston, Massachusetts 02203	John F. Kennedy Federal Office Building	617 742-5533
Buffalo, New York 14202	Room 1400, 111 West Huron Street	716 856-7800
Butte, Montana 59702	115 U.S. Court House and Federal Bldg.	406 782-2304
Charlotte, North Carolina 28217	6010 Kenley Lane	704 529-1030
Chicago, Illinois 60604	Room 905, Everett M. Dirksen Bldg.	312 431-1333
Cincinnati, Ohio 45202	Room 9023, 550 Main Street	513 421-4310
Cleveland, Ohio 44199	3005 Federal Office Building	216 522-1400
Columbia, South Carolina 29201	Suite 1357, 1835 Assembly Street	803 254-3011
Dallas, Texas 75202	Suite 300, 1801 North Lamar Street	214 720-2200
Denver, Colorado 80202	Room 1823, Federal Office Building	303 629-7171
Detroit, Michigan 48226	P. V. McNamara Bldg., 477 Michigan Ave.	313 965-2323
El Paso, Texas 79901	Suite C-600, 700 E. San Antonio Avenue	915 533-7451
Honolulu, Hawaii 96850	Room 4307, Kalanianaole Federal Bldg., 300 Ala Moana Boulevard	808 521-1411
Houston, Texas 77002	6015 Federal Bldg. and U.S. Court House	713 224-1511
Indianapolis, Indiana 46204	Rm. 679, 575 North Pennsylvania Street	317 639-3301
Jackson, Mississippi 39269	Suite 1553, Fed. Bldg., 100 W. Capitol St.	601 948-5000
Jacksonville, Florida 32211	Oaks V, 4th Fl., 7820 Arlington Expwy.	904 721-1211
Kansas City, Missouri 64106	Room 300, U.S. Court House	816 221-6100
Knoxville, Tennessee 37919	Room 800, 1111 Northshore Drive	615 588-8571
Las Vegas, Nevada 89104	700 E. Charleston Boulevard	702 385-1281
Little Rock, Arkansas 72201	Suite 200, 10825 Financial Centre Pkwy.	501 221-9100
Los Angeles, California 90024	11000 Wilshire Boulevard	213 477-6565
Louisville, Kentucky 40202	Room 502, FOB, 600 Federal Place	502 583-3941
Memphis, Tennessee 38103	841 Clifford Davis Federal Building	901 525-7373
Miami, Florida 33169	16320 2nd Ave., N.W., N. Miami Beach	305 944-9101
Milwaukee, Wisconsin 53202	Rm. 700, Federal Bldg. & U.S. Court House	414 276-4684
Minneapolis, Minnesota 55401	392 Federal Building	612 339-7861
Mobile, Alabama 36602	One St. Louis Centre	205 438-3674
Newark, New Jersey 07102	Gateway 1, Market Street	201 622-5613
New Haven, Connecticut 06510	Federal Building, 150 Court Street	203 777-6311
New Orleans, Louisiana 70113	Suite 2200, 1250 Poydras Street	504 522-4671
New York, New York 10278	26 Federal Plaza	212 553-2700
Norfolk, Virginia 23510	Room 839, 200 Granby Street	804 623-3111
Oklahoma City, Oklahoma 73118	Suite 1600, 50 Penn Place	405 842-7471
Omaha, Nebraska 68102	Room 7401, Federal Bldg., USPO and CH, 215 North 17th Street	402 348-1210
Philadelphia, Pennsylvania 19106-1611	8th Floor, FOB, 600 Arch Street	215 829-2700
Phoenix, Arizona 85012	Suite 400, 201 East Indianola	602 279-5511
Pittsburgh, Pennsylvania 15222	Room 1300, Federal Office Building	412 471-2000
Portland, Oregon 97201	Crown Plaza Building	503 224-4181
Richmond, Virginia 23220	200 West Grace Street	804 644-2631
Sacramento, California 95825	Federal Building, 2800 Cottage Way	916 481-9110
St. Louis, Missouri 63103	2704 Federal Building	314 241-5357
Salt Lake City, Utah 84138	3203 Federal Building	801 355-7521
San Antonio, Texas 78205	Room 433, Old P.O. Bldg., 615 E. Houston	512 225-6741
San Diego, California 92188	Room 6S-31, FOB, 880 Front Street	619 231-1122
San Francisco, California 94102	450 Golden Gate Avenue	415 553-7400
San Juan, Puerto Rico 00918	Rm. 526, USCH & Fed. Bldg., Hato Rey, P.R.	809 754-6000
Savannah, Georgia 31405	5401 Paulsen Street	912 354-9911
Seattle, Washington 98174	Rm. 710, FOB, 915 Second Avenue	206 622-0460
Springfield, Illinois 62702	535 West Jefferson Street	217 522-9675
Tampa, Florida 33602	Room 610, Federal Office Building	813 228-7661
Washington, D.C. 20535	FBI Washington Field Office	202 324-3000

LETTERBOX

Comments

Dear *2600:*

As an avid reader who uses *2600* strictly as a tool to improve corporate security, I thought I would comment on a few items found in your Winter 1993-94 issue.

Concerning tone operated equipment, there are other "services" which use tones to activate equipment, etc. Living near a nuclear power plant, one of the joys is the monthly siren test. One day I happened to be listening to the scanner when the tests were taking place and, lo and behold, the local law enforcement agency was broadcasting some tone groups which seemed to coincide with the sounding of the sirens. A trip to the local police department the next test day revealed a box on the radio room wall, labeled accordingly, with test and reset buttons on the front. When the test began, each test button was pressed in sequence, followed minutes later by each reset button being pressed. Why someone hasn't recorded these tones and maliciously set off the sirens is beyond me....

Concerning password procurement, one of our pastimes in college was taking advantage of beginning computer science students by writing a CICS transaction to simulate a logon screen, and running it on one of the terminals in the computer lab. The students would attempt to logon and, when they did not succeed, would figure the terminal was dead and try another. Little did they know we were recording their ID and password for later use. Of course, we ran our little scavenger transaction from one of the lab assistant's accounts to shift suspicion in the unlikely event anyone ever caught on.

Even telephone service providers are not beyond using fraud to rape their customers. Several years back, when alternative long distance providers began to offer their services, little boxes with pads of raffle tickets began appearing in restaurants offering a free truck or some other expensive prize for merely filling out a free entry form. Unfortunately, hidden in the fine print was a statement authorizing the change of your long distance service to brand XX. It was really a shock to get your phone bill and notice a new long distance provider. The upside was that after complaining to Baby Bell and getting the service switched back to the old provider, AT&T, we were treated as a "new" long distance customer and sent a $5 gift certificate. Along this same line, I heard of a lady who filled out one of these raffle tickets using her work address and phone number. Supposedly, it cost the company big bucks to switch back to their normal carrier, and it cost the lady her job.

Another thing we discovered in our adventures with the IBM mainframe computers in college was the output queue. For those unfamiliar, all printing jobs go into temporary storage, where they are routed to their respective printers or other areas as they become available. One of the areas, which was faster than waiting for a printout, was to have the job printed to the screen. This gave the programmer immediate access to the program error listing and output. Supposedly there is an operator running batch jobs and monitoring the computer system for various events such as programs stuck in endless loops - a big job with beginning students on the system. Usually the operator is away from the terminal and is not aware of a problem until someone calls in. The trick is to write a program (or convince a beginning student to do it!) which will loop and generate pages upon pages of output. Not wanting to waste paper, the output is directed to the user's terminal. Unless the operator catches the problem, the job keeps on running. Suddenly the system begins to slow down and finally stops processing. There is suddenly no place for any output to go, as the loop program has generated thousands of pages of output, filling the output queue. I am not exaggerating the amount of output either! One hot-dog lab assistant wrote some bad code which generated 12,000 pages of 132 column output before the system choked and died.

Big Wind

Hacker Understanding

Dear *2600:*

Just picked up your Winter 1993-94 issue (I love the looks my local bookstore clerks give me whenever I buy it), and I must commend you upon another first class effort. I first came into contact with it thanks to the meetings in my area, which are always excellent. Of course, since I started going to them, I have become known as a weirdo who goes to hacker meetings by my normal friends. They always say "hacker" as if they are literally spitting out the word. Ah, well, if we were all made to suffer fools gladly, why did they invent mental institutions?

Your journal is one of the magazines I most look forward to and the best thing to ever happen to the H/P community. What annoys me to no end is that most of those who are coming into the fold now are only in it to make free phone calls and get pirated games. There seems to be very little desire to learn any more. That is one of the things that makes your magazine refreshing.

Scudder

There are lots of us who are in this to learn and spread our knowledge. As we all know, there are kids who just want a free ride, criminals who just want a new scheme, and reporters who just want an easy story. Either we ignore them or attempt to reach them on our terms - anything so long as we don't join them.

Novell Nosing

Dear *2600:*

In your Autumn issue I noticed that there were several readers who were concerned about Novell Networks not letting you know whether the user ID or the password was wrong when you tried to login. It is true

that the system does not tell you if you are using a valid user ID or not, but if you look a little more closely at how the system reacts to the user IDs you type in, you may find what you are looking for. The network I use runs Netware 4.0. All the stations are 486's. Most of the users on this system have three digit (alphanumerical) user IDs. The others are Supervisor, Guest, etc. Anyway, let's say I try to login using my user ID that I know is valid but I enter my password wrong on purpose. What happens? The software checks to see if my user ID is valid. This takes only a second. Next, it checks my password. This takes more time because the program must access the bindery files and search for my user ID and password. Since I entered the wrong password, the system kicks me out with a nasty "Access Denied userid/server" message.

Now if you look at how much time the system takes to kick you out, then you have the key to finding valid user ID's. My user ID was valid, so when I entered the wrong password it took about four seconds to look up my correct password, determine the one I entered was wrong, and exit. Had the user ID been incorrect, Novell would have kicked me out almost instantly. Try it. You can write a simple program in BASIC that will try all letter and number combinations by saving the user ID you wish to use and a stupid password like "aaa" to a file, then starting the login program with a line like "LOGIN<FILENAME.XXX". Time how long it takes for the program to return. If it takes a long time to return, then chances are you've got a live one. If not, then the user ID is not valid and the program should return almost instantly. Be sure you include a line to log off the network in the event you find a user ID that is not password protected. You will be surprised how many you find. I can't claim this will work on all networks, but it sure has worked on mine.

Digital Enigma
Cottonwood, CA

Nynex Negativity

Dear *2600:*

I recently moved to the 10009 section of 212 and ordered Nynex Voice Mail (so I could access my messages from a PBX system at work). This outrageous system charges for monthly use and for *both* each call you make to access your messages *and* each incoming call you get. The caller leaving you a message also pays for a call, so I see it as charging twice for each incoming call.

But because 10009-land has wiring that does not have the capability of letting Nynex count the number of incoming calls, subscribers in my neighborhood will get unlimited service for the monthly service charge plus the cost of four calls.

I was told subscribers would get 30-day notice of a change in the service to per-call counting. (I'll probably drop the service before my 30-day free trial is over.)

Happy in 212 Land

Why anybody would want Nynex to handle their messages instead of an answering machine is beyond us. Apart from the cost factor, there are privacy and dependability issues. As long as people don't buy into their pricing scheme by using this service, it will either go away or come way down in price. The ball is sitting in our court.

Reader Abuse

Dear *2600:*

This letter is in response to the letter titled "Bookstore Trouble" in the Autumn issue. I think another reason why this publication might not sell well is because bookstores hide it. I get my *2600* from a local Barnes and Noble. I asked them if they subscribed to this magazine. The person in charge said "I don't know" and "We don't have our magazines listed so I can't find out". I stepped back and pretended to be looking at another book a little ways from her. A man came up to her and asked if they had another magazine. She pulled out a list and told him "yes" and where to find it. It was pure luck that I found *2600*. There were at least ten of them hidden in a rack where I had to feel around to get one. I complained to an employee about the location of *2600* but the next time I came in they were in the same place.

I am interested in test loop numbers for the 209 area code. Does anyone know any?

Guy At The Desk
Sysop of The Office BBS
(209) 474-8829
(not a hacker board but hackers are welcome)

Please let us know the exact names and locations of any stores that feel compelled to display us behind other magazines. It would be interesting to find out why they carry us in the first place. Regarding loop numbers, if they still exist out there, they would probably be hidden somewhere in the 00XX suffixes.

Questions

Dear *2600:*

Is the algorithm for figuring the last digit of a credit card account number discussed in a back issue of *2600*? If so, which one? Also, are you still selling a list of Mastercard and Visa numbers that identify the issuer?

BO
Cortlandt Manor, NY

We have a list of Mastercard BINs (Bank Identification Numbers) that we offer for $5. However, this list is practically three years old. We recommend waiting until we get our hands on a new one. We never did get a Visa list. As for the credit card algorithm, we discuss that in our Autumn 1990 issue. It's really quite simple so we'll explain it here: on cards with an even number of digits, double the odd digits (first, third, fifth, etc.). If doubling the digits brings the digit over 10, then subtract 9. Add all of the digits up and the sum should be divisible by 10. On cards with an odd number of digits, do the exact same thing, except double the second, fourth, sixth, etc. digits instead of the odd ones. If this seems at all difficult or confusing, you just need to practice a few times with a valid card.

Dear *2600:*

This mail is in reference to an old *2600* article that

had a 101-digit sequence that could be used to remotely access an answering machine. I have a question about access codes for two and three digit remote access answering machines. Assuming that we are dealing with a "semi-smart answering machine", one that listens to only consecutive numbers yet doesn't hang up after two wrong digits, the 101-digit string is necessary to guess a two digit code. Is there a formula that was used to come up with this sequence? And if so what would be the formula to generate a sequence to access an answering machine with a three digit code?

Leroy Chism

When we get it, we'll print it. We promise.

Dear *2600:*

Has anyone figured out a way to hack those automatic car washes at gas stations, where you enter a code? It would be nice to be able to wash the car daily....

Randy Ramone

There are just so many things to hack these days....

The Dark Side

Dear *2600:*

I read your publication for only one reason - to try and keep up with the enemy. I am responsible for a number of large PBX's, many with voice mail systems. One of my biggest problems is keeping irresponsible hackers and thieves out of my business. You publish on the premise that those who want to know have a right to know. I don't dispute that until they start poking around in my voice mail system (or anyone else's) often with less than honorable intentions and do damage or steal from me. They may have a right to know, but they have no right to explore my system or use it for anything other than what I want it used for.

We spend time and money securing our systems. Features we would like to use are turned off because a thief might discover them and could potentially steal from us at the rate of thousands of dollars an hour. I would rather have my technicians doing productive work.

In your last issue, you put the naive kid from Puerto Rico in his place because it is obvious he only had larceny on his mind. Unfortunately, this same kid is going to be educated in how to achieve his objective by your publication. You reinforce (and implicitly encourage) his notion that it can be done and gotten away with. Many of the articles you publish are reports of crimes committed and how it was done by the perpetrators in enough detail to repeat the act, not simply information about how to get behind the locked door. Often you cross over the line to the side of irresponsibility.

Thanks for listening. I am sure if you publish this letter, thieves and hackers everywhere will discover they offend me (and others) and stop doing what they do. I won't have to waste time securing my systems. The world will be saved.

Pissed Off in Houston

While we understand your frustration, we feel compelled to suggest that you seek another line of work. If securing your systems is a waste of time to you, you're not doing anybody any favors. The reason you can't use those features you want to use is because they're lousy features with gaping holes you could drive a bus through. Be glad you haven't fallen victim to them and the outrageous billing schemes the phone companies slap on their customers.

We print facts on weaknesses and vulnerabilities. It's what we've been doing from the start and we're not about to cut off the information flow because information can be misused. It would be a very scary precedent to set. The information we print can be used by smart people to prevent their becoming victims. Unfortunately, too many think that ignoring what we say or keeping us from saying it will make everything unpleasant go away.

The Far Side

Dear *2600:*

A pattern of events has occurred that I feel have continued for too long. I would like to mention at the outset that while I agree in principle with *some* of your beliefs, I disagree with the methodology in which you carry out most of these beliefs. Normally it is not my concern how others run their lives but when their actions have an impact on my life I must take corrective action.

Over a year ago I was reminded that you were still publishing *2600* when I caught a broadcast of WBAI. On that show you mentioned a computerized CNA telephone number. You said on the air that the telephone number would appear in the next issue of *2600*. I sent *2600* a U.S. postal money order, my return address and a note printed on my laser printer in which I requested that my subscription begin with the above mentioned issue. I used a laser printer and a very legible font to avoid confusion from my handwriting. The issue with the CNA information in it *never arrived* and my subscription started *several months later* with naturally a different issue. After several more months I wrote to you at *2600* on *two separate occasions* to request your help. I *never* received so much as a postcard much less any help or the missing issue. I did however receive three of the four issues of *2600* where the last two issues reminded me to pay up for next year. Of the three issues that did arrive, two were so badly *mangled* that they were almost unreadable. While I am aware that the responsibility for this mutilation can be attributed to our *wonderful* postal service, I want to point out that other magazines replace mutilated issues when notified. *2600 never did.* The fourth issue never arrived. I tried calling your offices. While I am not satisfied with the exorbitant rates Nynex charges, I am even less pleased by the devious manipulation by *2600*. I refer to *2600* leaving a very lengthy outgoing message on its answering machine. Ostensibly this was done to be informative and helpful to the caller while in reality encouraging the caller to become a party in your scheme to defraud the telephone company in not paying for the incurred overtime charges. All the while maintaining its "plausible deniability". (I wonder how many pay telephones have been removed from service and lives made more difficult because of such behaviors?) I know the alternatives are to: 1) pay Nynex its outrageous rates (which I'm also opposed to) or

2) attempt the impossible and try to leave a coherent yet highly compact message in the *microscopic* time you have left available before the Nynex overtime message activates. Writing to you is pointless and only serves to litter the streets after you have discarded this letter. No mention or provision is *ever* made on the *2600* outgoing message about when an actual human being is present and your answering machine is not screening your calls.

The final action that repulsed me was that subscription money was used to essentially pay for the editor's *personal* vacation to Holland thinly disguised as a reporter on a fact finding trip. This is as shady an action as those you describe on the radio. But this last part is all a matter of deniability and perspective. I offer the following illustration. If the point of view is first taken from that of a taxpayer, then illegal payoffs from that tax revenue are reprehensible. If the point of view is then taken from the recipient of the same payoffs then it's a job "perk". The usual argument made to defend such a theft is that the "perk" is being taken "for the greater good". What's next, getting Ed McMahon's picture on a *2600* subscription gimmick?

In short, *2600* has taken on the tactics of the corporations it *professes* to fight. Ultimately, I have decided to fight fire with fire and take up your tactics. I've decided to vote with my dollars and: 1) *not* renew my subscription to *2600* (yes, I know you are disappointed); 2) listen to you on my Walkman whenever I can free of charge on WBAI and not subscribe to them either. A copy of this letter will end up there; after all there's nothing like using a little pressure from both ends as you know; 3) encourage others to follow my example; 4) tell them of my experiences. In case you decide to read this on your show or to publish it in *2600*, I suggest you do so *in its entirety* and comment if you feel so moved after you have presented the facts as fairly as you are able.

Please note that I am purposely omitting my return address to avoid any further complications.

One very displeased former subscriber

Let's start by addressing your subscription problems. Since the issue you wanted to start your subscription with never arrived, your "first" issue showed up several months later, and you only got three issues in total, it stands to reason that the issue you wanted was in reality your first issue and for one reason or another, it never made it to you. By your own admission, you didn't notify us until several months after you received your first issue, which in turn was several months from when you ordered a subscription. So how many months passed before we could find out there was a problem? Six? There's no way we could have solved your problem if we weren't even aware of it. When you did notify us (not knowing who you are there's no way we can verify any of this), we probably sent you a replacement copy. Again, it apparently didn't arrive. This, coupled with the poor condition of the copies you did receive, leads us to believe your post office is extremely incompetent or malicious. We do replace mangled copies but we have to be told about them. A complaint of this magnitude would have been remembered and there is no recollection here of such a thing. And, for the record, our labels don't tell people to pay up - each label contains the date of the last issue of the subscription, so that people know when their subscriptions end. The label of your last issue will say "Renew!". Nobody has ever taken offense at this before.

We will readily admit that our "customer service department" sucks. We're not Time Magazine. But we never ignore complaints and, while we may be a bit slow sometimes, everybody gets what they order. We just cannot answer every individual question we get and we certainly can't return every non-problem-related phone call that comes in. Getting the magazine out and making sure people get it are our highest priorities. So if somebody leaves a message on our answering machine asking how to subscribe, they probably won't get a call back because all they have to do is listen to the answering machine! We're not trying to be nasty - we just don't have the time.

Now to address the irrational hysterics that constitute much of the second part of your letter: do you honestly believe that our answering machine message is part of a conspiracy? As we mentioned above, we provide information to people who call. The idea is to be helpful. And we don't make a secret of the fact that you can hit a star to skip the message entirely. Of course, encouraging people to use touch tones probably implicates us in yet another conspiracy.

As for your concluding accusations, we'd be insulted if we weren't so confused. What exactly are you accusing us of? Paying people? Well, we kind of have to do that sometimes. 2600 is a business after all, even though you seem to prefer that it not be. Where do you get the impression that subscribers are subsidizing these luxurious lifestyles you've conjured up? Or is it just wishful thinking?

Payphone Fun

Dear *2600:*

I've just started reading your mag. It's pretty good. I thought at first it would be infantile skater crap. But no! It's well written and really professional in its attitude.

I've found something interesting at two payphones at a nearby restaurant. Both payphones can make long distance directory assistance calls toll free! You know, area code plus 555-1212. These are Wiltelco 6000 models using AT&T long distance. Using the 800 number on page 45 of your Summer 1993 issue, I found both numbers. I won't disclose them now for obvious reasons. Any comments? (The restaurant is right across from a US Sprint operating center.)

Neophyte 1138
Ohio

It's called bad programming. We've seen this sort of thing before where information calls are accidentally (or out of nostalgia) programmed as free calls. The programming is done at the phone in this case, since the phones you describe are COCOTs.

Dear *2600:*

The payphones in the Days Inn at 1630 Canal Street, New Orleans, LA kept returning my quarter for local calls

no matter how long I talked. No complaints, but why is this so? Was it a defect in the phone? It was a Bell phone.

Tim
San Diego

In your case, the problem was most likely mechanical. If this consistently happened with more than one phone, then the problem is definitely - unusual.

Dear *2600:*

Hi. I've been reading your mag for a few issues and I personally think it's the greatest thing in print (next to the First Amendment, but it seems like nobody knows what that is anymore). Anyways, a strange thing happened to me at my local mall. See, they've got these "strange" payphones, which I imagined to be COCOTs. (No telco logos, some generic LD carrier, LED displays that say "DIAL" when you pick up the phone and then a timer of how much time you have left after you insert the money....) I tried out one of the methods for getting an unrestricted dial tone on a COCOT, namely calling a 1-800 number and waiting for them to hang up, then "hissing" in the receiver when it tried to reset. Well, I tried this about three times and it led nowhere, it would just get the "hang up and try your call again" message after the 1-800 hung up, so I left it alone and walked away. About five minutes later, however, I came back to the area and was absolutely shocked to see about six or seven spams (mall cops) hanging around the phones, asking people if they'd seen anyone fooling around or if the phones had been "acting funny". I'm positive nobody saw what I was doing, since it was in a vacated part of the mall early in the morning, and I had my credit card out and faked (quite well in my opinion) that I was making a regular call - fake talking and everything. My only conclusion was that somehow I set off some kind of security measure or something by this activity, or the mall cops were monitoring the phones. Either way, it's scary - has anyone ever heard of a COCOT that monitors calls to make sure they're not "cheated" and lets someone know if they are? Or are mall phones and the like being monitored constantly?

TcP

When you're in a mall, all logic remains outside. Particularly when it comes to security guards. We'd just love to hear them explain why it's against mall policy to hiss into a phone.

Dear *2600:*

I thought you guys might like to know about this. Recently I was watching a coin collector from PTC, and he dialed an interesting phone number before emptying the coin box. The number was #9667, and the cocot will say "Service Entry 14, Collection". You then hit 1 and it will read off the current total of money in the phone, and the amount of money made by the phone since installation. If you hit 2 while the phone is reading the totals, it will reset the current total to $0.00!

Death Adder

The COCOT industry will not sleep well tonight.

Quarter Variations

Dear *2600:*

This letter is regarding the "Quarter" device printed in the Summer 1993 issue. I'm sure you have gotten comments about this before. After building the "Quarter" I noticed that sometimes, the tones would freak out and come out in groups of three (equivalent to a 15 cent piece), and the timing would be a bit out of whack. I did a few modifications to the circuit and came out with something a bit "cleaner". Instead of using a 9-volt battery or three AAA batteries (4.5 volts), I chose to use two CR2025 3-volt Lithium batteries. With 6 volts, it did the job and took up less space. I changed the value of R1 (originally 470 kohms) to equal 460 kohms - the 10 kohms decrease makes a *big* difference in timing and spacing. Since I couldn't find a resistor of that value in my collection, I just used one 240 kohm and one 220 kohm in series. With these simple changes, the "Quarter" became a bit smaller, and the timing error was changed to make the pulses always be 5 (25 cents), and the tones are produced in quicker succession, making it sound more realistic. The only downfall of using the two 3-volt batteries is that the volume is a little bit decreased, but it doesn't make a difference when the speaker is held to the phone.

Kingpin - 617
Boston

Prison Phone Report

Dear *2600:*

I know some ingenious person has the answer to these problems:

1) Our phones in the prison system here in Michigan are quite weird. They are payphone-like in appearance but have no change slot or information printed on the outside of the metal housing. In effect they are those crippled calling-card-only types that you see in the airport. The problem is that they are connected to some weird pulse system that MCI is running just for our incarcerated friends. The system does not require you to dial a zero before your number but an automatic computer generated voice comes on and asks whether you'd like your collect call to be person to person or a plain old garden variety one. It then prompts for your name and tells you to wait while it connects. It then asks the person who picks up the phone on the other end if he or she will accept a collect call from (inserts your recorded voice) and if the answering person pushes 1 in tone mode you get connected. If you listen carefully after you've given your name you can hear other people's pulse numbers as they dial their family or whoever. Is it possible that this system is some combination of tone *and* pulse generated switching? When they first installed this system I found that all I had to do was cover the mouthpiece when it asked me for my name. It would stall for a few seconds and then put me through to the correct party, *but not as a collect call!* For some reason, doing this allowed you to call anywhere in the world *free of charge,* but not the 313 area code where the prison is located. They've since

updated the system so that this little trick won't work.

2) The county jail's phone system is a little different. I'm going to go down there in a little while so I'm hoping someone can figure this out for me. The jail's phones are regular payphones that accept money but don't allow you to use your calling card. I haven't tried dialing 10288 for an AT&T operator, but I *do* know that trying to get an operator the old-fashioned way (0) won't work. You also *can't* call outside the 313 area code. Weird, huh? Any ideas, people?

Oh, by the way, I seem to recall a Usenet newsgroup called alt.illuminati that dealt with the whole New World Order paranoia thing. Hope that helps Almost Anonymous.

Wog

The phone system uses pulse dialing to get to the MCI automated operator. Perhaps some paranoid prison official thought inmates could hit touch tones and accept their own collect calls, so they disabled the touch tones. In any event, the pulse system has got nothing to do with MCI - it's simply how your call gets placed by the local company. There are an almost unlimited number of possibilities with your county system - 800's, 950's, carrier access codes, collect calls, green box tones from the called party, maybe even black boxes if you're in a primitive area. If you do manage to get an operator, the trick is to make sure she doesn't see the class of service, which is undoubtedly showing up as a prison phone. It's not easy and it's different in every area.

Government Data

Dear *2600:*

I just bought the Autumn 1993 *2600 Magazine*. I love it!

Maybe I am too "old" to be a real hacker (I am 46) but I am very close to this world, being a programmer involved in the computer security field (Access Control, Passwords, etc.). I just heard recently that President Bill Clinton is a real pusher of the information superhighway technology and there is a BBS system - an email front end line to the White House. Can you please provide me with this number to send messages and to be in touch with these folks?

AO
Arizona

It's not exactly a BBS. It's a way to send feedback to the government over the Internet. The addresses are president@whitehouse.gov and vice.president@whitehouse.gov. Don't think for a second that this mail will ever be read by its recipients. Don't believe either that you can remain anonymous on the net. If you're real lucky, you'll get a form letter back.

Cellular Chatter

Dear *2600:*

The Autumn 1993 article on "More Cellular Fun" started out good but it was soon obvious Judas Gerard didn't know all that he was talking about. The Uniden phone uses a BR93C46 located in an eight pin socket to store the ESN. On the CP1200 it's located at IC107 next to the firmware. The only downfall with Uniden phones is that you need a Uniden "NAM writer" handset to change the MIN to math the ESN.

I should be writing an article soon on converting the standard handset into a "NAM writer". On the Motorola the patch kit does exist and makes editing the ESN a snap. On the older Mitsubishi the ESN is able to be edited from the keypad.

I would not recommend trying to do an ESN change on phones newer than 1992. Most new phones have a habit of destroying themselves, especially Motorola and NEC phones.

Tech-No Wiz
Columbus, OH

More Corporate Outrage

Dear *2600:*

It has come to our attention that you have published one of our business marketing 800 numbers in your quarterly and also in a hacker's bulletin board. The number you published is 1-800-775-55XX.

Our service is a commercial caller identification which operates throughout North America and provides needed information to law enforcement agencies and major businesses.

By publishing one of our lines as a novelty number to call for "fun", your disclosure is causing wasted time by our staff and costing not only their time, but also the long distance fees we pay while our lines are in use during your subscribers' games.

You are hereby given notice to *cease and desist* the publication of our business number, immediately remove it from bulletin board postings and, in the bulletin board, publish the posting that an 800 number had been published by your service which demonstrates commercial caller identification service and is not to be called for entertainment or curiosity purposes and that such calls may create civil and/or criminal prosecution for interference with interstate telecommunications.

You are also hereby notified that all calls to this number are being identified and callers will be contacted regarding their abuse of this number, and your company will be invoiced for the call activity at a rate of $1.00 per call.

We hope in the future you will take more precautions when encouraging your readers to entertain themselves by disrupting business services.

James E. Walker
President
Tel-Scan
2641 N. Taft
Loveland, CO 80538
(303) 663-1703
FAX (303) 663-1708

If this isn't the height of arrogance and condescension, we may never know what is. First off, guess what? We didn't even publish your stupid 800 number! In fact, we just protected your valuable seven digit goldmine by blocking out part of it. We'll await your letter of thanks. Next, what appears on our voice

mail system, which we assume to be the hacker bulletin board you mention, is entirely legal. If somebody posts an 800 number there, we are under no obligation whatsoever to erase it. We don't allow codes or credit card numbers because they can be used to commit fraud. Calling an 800 number is not, by any stretch of the imagination, an instance of fraud. However, if you try to bill someone for calling your 800 number, you will be the one guilty of fraud. If a person repeatedly calls your number after being asked not to, it's a clear case of harassment. But that's not what you're talking about here. You've got one hell of a nerve assuming that our readers do nothing but make frivolous calls and disrupt communications. Our readers have designed systems like the one you use and, if you weren't so stuck up, you might have actually gotten some real, legitimate customers out of this unique group of people. Since you've made your feelings about them so clear, we fervently urge our readership to never do business with this company. That should make us all happy.

Individual Outrage

Dear *2600:*

I just don't understand why the hack/phreak community has anything to bitch about when it comes to getting busted by the law enforcement. I am a published author of a book *Con-Artist Games On You.* I have started a second book named *The Underground Road Map Through Cyberspace.* The edition will present the point of views, lives, religion, morality, of both the law enforcement (cyberangers) and the hack/phreak Americans. So far I have had very little response from the H/P community. The only group here in Phoenix, the NSA, has offered some information.

As it stands, the American public perception of H/P people are Snotty Nose Spoiled Little Brats that are a menace to society, and should be spanked or locked up in a reform school. With this brand, it would seem logical the H/P would jump at the chance to give their viewpoints out. Maybe their I.Q. is not high enough to accomplish this? Maybe they are brain dead, due to their computer has done all of their thinking. For some reason, they are only talking among themselves and not to the public where it counts the most.

I myself have put my *ass* on the line! I live in the land of gestapos. This includes Gail Thackeray (also known as the Hacker Tracker), the deputy processing attorney for the State of Arizona. Thackeray is responsible for many convictions brought about, due to Operation SunDevil during 1990. By showing any consideration toward the evil hack/phreak/pirate community, you are labeled an enemy of the state. I am probably at the top of Thackeray's list. We also have a *bad ass* cyberanger from the International Association of Computer Investigative Specialists Howard Schmidt. Thank *God* I am an author and have the First Amendment on my side (so far).

It just upsets me to think that these so-called chicken-shit hackers/phreakers are hiding in the safety of their bedrooms doing a lot of *big talk* (that is all it is) and not willing to fight for freedom in cyberspace. So, as the American public passes more and more laws that will have a damaging effect on the H/P community, they sit there, with their thumb stuck up their ass.

If any of your readers would like to respond to the comments made here, they are able to reach me at 6611 W. Peoria Suite 5-111, Glendale, AZ 85302 or my BBS (602) 846-4470 Fido 1:114/191. I don't need to hear their lame bullshit crap on how good of a hacker/phreaker they are by the things they have done or can do. As far as I am concerned, it is not a fact until I see it with my own eyes. I am interested in any newsletter, stories of people being busted, authors of real hacker programs, etc.

I hope you respond to this open invitation to make a difference in cyberspace. If not, then you have only yourselves to blame.

Richard Finch
Computer Justice
Glendale, AZ

Forgive us for saying this but maybe you're going about this the wrong way. You need to be more confrontational. If you keep being so nice to us, we're liable not to respect you at all.

By the way, Thackeray hasn't worked for the State of Arizona for years. You can sleep easy now.

Exiled Hacker

Dear *2600:*

I've written to commend you for continuing your publication for so long. I myself used to be involved with things you print about. Unfortunately, I was another unlucky character who got caught by the law. It was also very tempting to begin again after I got your most recent issue, but thought twice and decided against it. However, I will continue to read your publication and hope you continue to print it.

Ares
Hacker's Hospice
(1986-1989) RIP

Please give yourself some credit. You don't have to engage in illegal activity to be a hacker. As long as you keep an active interest and imagination, you'll be a compatriot.

Pointers

Dear *2600:*

Regarding the letter in the Autumn issue seeking a BBS with information on the New World Order, there are a number of sources available (besides your local library). Try Logoplex BBS (804) 741-9671. There used to be a BBS dealing especially with the NWO run by William Cooper, an ex-Navy Intelligence officer, who currently has a shortwave radio program on WWCR (World Wide Christian Radio) broadcasting from Nashville. The show occasionally gets "bumped" or edited, even in the middle of the program and the broadcasting tower was burned down last spring but has been rebuilt. This is how much certain parties would like to discourage this information from being made available. Get it while you can. Also, if you

haven't read it yet, find "Privacy for Sale" by Jerry Rothfeder.

Trout

Fighting Back

Dear *2600:*

Here's one for your Atlanta phreaks!

Sitting in my midtown apartment one recent afternoon, trying to come up with someone or something to phreak, the perfect invitation came in straight through *my* phone.

The phone rang, I answered, the caller said nothing, then hung up after about 20 seconds. Well, I've had Caller ID for a couple of months now so I checked the box to see who it was. It was 404-572-6400. I also noticed that I had gotten many hang-up calls (no message on my machine) from that general number range, 6400 to 6450, in the past few weeks.

Well, if someone calls me a bunch of times (16 to be exact) and hangs up I consider it a challenge. I called that number and several others in that range and I would always be connected to some type of device that would just sit there for about 30 seconds then disconnect. Finally, it occurred to me that I was calling into some system's outgoing trunk group and that the device was not really answering but accessing an outward trunk and waiting for a dial tone. Well, I gave it a dial tone from one of my archives of cassette tapes. Guess what? It didn't hang up this time but started dialing. At this point I decided to connect my Radio Shack DNR (dialed number recorder) to see what it was the device was calling. It would dial a different number every time, sometimes even ten digit toll numbers, but they always started with a "9".

I was still puzzled as to what had been dumped on my doorstep just waiting to be ripped open. I decided that the trunk must be a Centrex line because what else would be dialing a "9" towards the local CO?

Now it was time to let the mystery call get answered. I went through the sequence and, after the device had dialed a number, I played a ringback tone from another one of my archived tapes. Nothing happened. It just kept listening to the ringing tape. After about seven rings it would hang up. And if I played a tape of a busy signal or reorder it would hang up immediately.

Well, I thought, maybe it's looking for a voice answer. So after two rings I said "Hello". It took the bait! Immediately someone came on and said, "This is Joe-Bob from the *Atlanta Journal and Constitution* and I'd like to tell you about a subscription offer...." I now had it pegged - the device is an auto dialing system that randomly calls numbers, waits for a ring and a voice answer, then connects to a sales operator so that they don't have to do the dialing and they never get a busy or no answer!

The time that it called me with no one there must have been an occasion when the sales operators were too busy to get my connected call. Pretty slick gadget! But the sales operators sure are surprised that *I'm* always the person who answers no matter what number their system calls! I just act like it's the first time I've gotten a call from them, but they sure act funny when they recognize my voice.

Now I've found ways to get through to the sales operators without using the tapes. The calling system has a wide allowance for dial tone and ringback frequencies. If you press the 1 and 2 buttons together on most touch tone phones you get a single 697 Hz tone. The device accepts this as a valid dial tone. The device doesn't really wait to hear a ringback tone but will connect to the sales operator after hearing any spoken voice, as long as it *doesn't* hear a busy signal or SIT (special information tone - doo-dah-dee....). All this can be done from any telco payphone.

What's next with this thing? First I'd like to know what it's called. And, since most Centrex lines have call transfer and three-way calling, there must be a way to go in, then get back out through their system. Any ideas?

Bellsouth Baboon
Atlanta, GA

It isn't necessarily a Centrex system. After all, many phone systems require a 9 to get out. Apart from that, we must compliment you on an ingenious hacking expedition. If we learn more about this kind of thing, we'll pass it on.

Governmental Suggestion

Dear *2600:*

Just wanted to drop you guys (and gals?) a line and say thanks for publishing such informative stuff. My friends and I look forward to every issue. It seems that your publication is fairly popular here in Fort Worth, Texas, as it is usually sold out. Looks like we may have to subscribe!

After reading the article "Congress Takes A Holiday", and reading further, finding "Bookstore Trouble", you may have, unknowingly, made a very good suggestion. I do not know what this would cost you, but here goes. Why not send a copy of *2600* to every congressman each quarter? If not to *every* one, then how about to the "troublemakers"?

It may not give any of them a clue, but it just might open up their minds. And, yes, I'm not holding my breath! Do you know of any potential meetings taking place in the Dallas/Fort Worth area?

Randy815@Dallas

We just started Dallas meetings - look for details on page 46. Sending issues to congressmen is an interesting idea. We'd like to get more input on this.

Phiber Parallel

Dear *2600:*

Your editorial on the fate of Phiber Optik was dead-on. Your statement that "Basically, they succeeded in sending a few friends to prison for trespassing" sent a chill of recognition down my spine. A few years ago, after getting off a late shift, a friend and I were arrested while walking alongside some railroad tracks owned by Southern Pacific. The short version of our story is that the sheriffs had nothing better to do, and needed a "big" arrest for their records, so they charged us with *felony* attempted train derailment. They stole personal

(continued on page 40)

Blue Boxing Revisited

A CCITT SYSTEM #5 INTERPRETATION

by Kevin Crow

This article will attempt to teach the reader basic CCITT-5 International signalling. More technical readers may enjoy reading the original CCITT-5 "RedBook", and can use this as a supplement.

During the time I've been working on this article, the ITU has changed the names of a few departments. CCITT is now known as the ITU-T, however for the sake of avoiding any coining in terms, I will still refer to the signalling as "CCITT-5", or "C5".

CCITT-5 signalling is still known as the international signaling standard. CCITT-5 is related to R1 signalling, a substandard used from within North America. A highly stripped down version, R1 doesn't include any trunk signalling involving 2400Hz, and I won't be discussing it in this article. R2 Signalling, another substandard, is widely used in Europe, however I will not be covering R2 signalling in this article.

I have heard over and over again that C5 is no longer available for use in the United States, "since being the well-advanced country that we are" we have moved on to bigger and better things, such as CCIS, and eventually SS7, and its Digital Hysteria. I find it amusing that the UK has had ISDN for far longer than we have, I still prefer vinyl over CD's, and I've been able to get near-perfect connections with C5 that sound *better* than the new stuff (although this is strictly medium dependent, it's still worth mentioning). The reason I am addressing this issue is simply to remove any sort of beliefs you might have because of AT&T's propaganda over the years — boxing is possible from *anywhere.*

Back in 1976, when CCIS started hitting the scenes, there were many problems that immediately crept up. AT&T's breakup in the 80's didn't make the transition phase any easier, and in parts of the new Baby Bells (even today) you can find R1 Signalling. AT&T has since scrapped their implementation of CCIS and is now using SS7 wherever it is possible. Do not let this confuse you however — no matter what switch you're on, or how you're being routed to/through a C5 connection, in most cases you will still be able to signal yourself. On with the show....

C5 signalling is broken down into eleven major groups of Signals. It is with these signals that all the necessary operations and functions are executed for (almost) error-free international switching. For two switches to communicate with each other they require the ability to send signals, as well as receive them. They need to know which signals are being sent, and they need to know what to do with them. For the scope of this article, let us assume that all signals being sent from the originating switch are known as "forward signals", and likewise, all signals being received by the originating switch (or sent by the switch on the other side) are known as "backward signals". Of the eleven signal groups, six are signalled in the forward direction, and the remaining five are signalled in the backwards direction. The dialogue that happens between these two switches is really quite primitive, and therefore can be mimicked with $20 worth of parts, as in the case of the blue box.

Let's take a look at the signal groups:

1. *Seizing Signal* — The seizing signal is sent in the *forward* direction by the *originating* switch. Its purpose is to initiate circuit operation at the incoming end of a circuit. It "seizes" the equipment for switching the call.

2. *Proceed to Send* — This signal is sent *back* in response to the seize, and indicates that the equipment is now ready to receive the numerical set of signals.

3. *Start-of-Pulsing* — Also known as (KP). The KP signal is a *forward* signal. KP is actually broken down into two types of signals. KP1 is "terminal", that is, it is used in placing *domestic* calls. The KP2 signal is a "transit" signal, and is used in International Signalling. The purpose of the KP signal is to prepare the incoming switch's registers to let it know what kind of

call it will be handling.

4. *Numerical Signal* — This signal is also a *forward* signal, and it provides the information necessary to effect the switching in the desired location. The numerical signal includes the actual phone number of the desired location, as well as some extra information that will be discussed later on.

5. *End-of-Pulsing* — This is also known as the ST (start) signal. It's a *forward* signal, and its purpose is simply to show that there are no more numerical digits to follow. In a sense, at this point, the call has "started switching".

6. *Busy-Flash* — This is a *backward* signal, and it is sent to the outgoing exchange to show that a) the route or b) the *called* subscriber is busy. The International Transit exchange sends this signal after the register association to indicate that there is congestion at that exchange, or the appropriate outgoing routes. This signal is optional if there is congestion beyond that exchange. Upon its receipt, there is usually an indication to the outgoing operator or to the calling subscriber that causes the sending of a clear forward signal by the outgoing exchange to *release* the connection. This signal is never supposed to be sent after an answer signal, and only after a proceed to send signal (see below).

7. *Answer Signal* — Another *backward* signal, this one is sent to the outgoing exchange to indicate that the called party has answered the call. In a semi-automatic working, it also has a supervisory function, that is, it begins the initiation of watching over the connection. In automatic working, it is used to a) start metering the charge to the calling subscribe, and b) to start the measurement of the call duration for accounting purposes. Receipt of this signal also permits discrimination between the busy-flash and clear back signals. It also must never be sent after a busy-flash signal (see below).

8. *Clear Back* — Obviously a *backward* signal, it is sent to the outgoing exchange to indicate that the called party has cleared, or "hung-up". In semi-automatic working, it performs a supervisory function as well, and must not permanently keep the speech path from being open at the exchange. In automatic working, if the calling party has not cleared within one or two minutes of the clear back signal, arrangements are made to clear the connection, stop charging, and stop measurement of the call duration. It should also only be sent after the answer signal.

9. *Clear Forward* — This signal plays a very important role in both exchange signalling, and blue boxing. In exchange signalling, it is sent at the end of a call a) in semi-automatic working when the operator at the outgoing exchange pulls her plug, or if an equivalent operation is performed and in b) automatic working when the calling subscriber hangs up or otherwise clears. It is *also* sent after the receipt of the busy-flash signal by the outgoing exchange and when there is a forced release of the connection, or when an abnormal release of an outgoing register occurs. The clear forward signal must be acknowledged by a release guard signal under all conditions of equipment, including its idle condition (blue box enters, left stage). It also may be sent from an outgoing end at any time to initiate the release of a circuit. It is completely overriding, and it will break any other signal sequence.

10. *Release Guard* — This is a *backward* signal, and is sent in response to a clear forward. It also serves to protect a circuit against subsequent seizure. It will do so as long as disconnection operations (controlled by the reception of the clear forward signal) have not been completed at the incoming end.

11. *Forward Transfer* — The forward transfer signal is sent to the incoming exchange when an outgoing operator wants the help of an inward operator at the incoming exchange.

You may have already noticed a few laws that must exist in order for this whole procedure to work. These "laws" are known as the "Signal Code". I will spare you the boring drudgery of these laws, and will not go into too much detail, except where is needed.

General information on Signal Code

In the early days, you may not have

heard much about the 2400 Hz signal behind the famed 2600 Hz signal, since most people were boxing domestically from within the US using R1. The 2400 Hz signal plays a very important role in international signal-coding arrangement, and for reference is known as frequency f1. 2600 Hz is known as frequency f2. These signals may be transmitted individually or in combination. With today's high-technology DSP's and signal generators, there is no reason at all why these signals should be transmitted individually. Yet, the specs allow for them (an example of drudgery). The purpose of these *two* tones being played in tandem (no pun intended), or simultaneously, is to increase the immunity from what is known as "false release by signal imitation". Hopefully this doesn't include you Amiga lamers. One of the most important aspects of the signal code is what happens when these laws aren't followed, or something goes wrong. In events such as a "double seizing", f1 is seen as being transmitted by both sides. This condition is usually detected, and according to the holy redbook, if it persists attention must be given. Obey your laws.

Finally, the signalling *frequencies* and operating limits. I'm going to quote right out of the redbook, since it's fast, and quick(er). This information may or may not be useful to you:

2.3.1 Signalling Frequencies

2400 Hz (f1) and 2600 Hz (f2). These frequencies are applied separately or in combination.

... stuff cut out

2.4.3 Efficiency of the guard circuit

The signal receiver must be protected by a guard circuit against false operation due to speech currents, circuit noise, or other currents of miscellaneous origin circulating in the line. The purpose of the guard circuit is to prevent:

a) signal imitation. (Signals are imitated if the duration of the resulting direct-current pulses at the output of the signal receiver is long enough to be recognized as signals by the switching equipment);

b) operation of the splitting device from interfering with speech.

To minimize signal imitation by speech currents it is advisable that the guard circuit be tuned. To minimize signal interference by low-frequency noise it is advisable that the response of the guard circuit falls off towards the lower frequencies and that the sensitivity of the guard circuit at 200 Hz be least 10 dB less than that at 1000 Hz.

An indication of the efficiency of the guard circuit is given by the following:

a) during 10 hours of speech, normal speech currents should not, on the average, cause more than one false operation of the f1 or f2 signal circuit lasting more than 90 ms (the minimum recognition time of a signal liable to imitation is 100 ms);

b) the number of false splits of the speech path caused by speech currents should not cause an appreciable reduction in the transmission quality of the circuit.

Note: Since Signalling System No. 5 and V.22 modems (among others things) are using the same frequency, additional tests where speech is replaced by data transmission should be performed so that the connection is not released at the start of data transmission.

... stuff cut out

3.3.1 Signalling Frequencies

[The Publishing "error"]

Freq. (Hz) Digit	700	900	1,100	1,300	1,500	1,700
1	*	*				
2	*		*			
3		*	*			
4	*			*		
5		*		*		
6			*	*		
7	*				*	
8		*			*	
9			*		*	
C10				*	*	
ST3P,C11	*					*
STP, C12		*				*
KP1			*			*
ST2P, KP2				*		*
ST					*	*

Simple graph showing forward signal frequencies

A signal shall consist of a combination of any two of these six frequencies. The frequency variation shall not exceed 10 Hz of each nominal frequency.

3.3.2 Transmitted signal level

-7 +- 1 dBm0 per frequency.

The difference in transmitted level between the two frequencies comprising a signal shall not exceed 1 dB.

...

3.3.3 Signal duration

KP1 and KP2 signals: 100 +- 10 ms

All other signals: 55 +- 1 ms

Interval between all signals: 55 +- 1 ms

Interval between cessation of the seizing line signal and transmission of the register KP signal: 80 +- 10ms

3.3.4 Compound signal tolerance

The interval of time between the moments when each of the two frequencies comprising a signal is sent must not exceed 1 ms. The interval of time between the moments when each of the two frequencies ceases must not exceed 1 ms.

...

Now that you've seen the laws behind C5 signalling, you may be interested in knowing that there are some interesting switch "characteristics" that become apparent when you break some of them. Crossed-lines, and "dropping in" on conversations have been known to occur during such errors. There is a wide variety of non-dialable numbers that become "dialable", operators who actually know what they're talking about can be reached, and other random phreaks of nature have been known to occur.

Earlier on I sketched out the plans for the "numeric" digits, but never went into much detail. Some countries have additional digits in their numeric field to represent different situations that occur. For instance, during a time of war, or serious network congestion, there are usually open connection paths that are accessible through special routes. Other countries have devised ways to allow for international dialing via KP1 routes (perhaps for lower level compatibility reasons, or accounting). Oftentimes there is an additional routing number that can provide extra security for abused [MCI] networks. Having additional routes also allows companies to use a variety of pathways for connecting calls (cross-Atlantic, satellite, copper, fiber, etc). I have heard rumors that indicate a formula exists for locating "important" customers to make sure they're routed through the cleanest way possible. If you're getting a 1.5 second delay on your conversations, perhaps you should find another way.

On the whole, countries must have a continuity in signalling, otherwise we wouldn't be able to communicate. As in the case of the metric system vs. America, there exist differences even in signalling (however minute). The actual routes involving operators, and operator-assisted calls, vary (Code 11 vs. 121) but overall the damned thing works out pretty well. I don't expect CCITT SS5 to disappear anytime soon.

Now that you've learned a little about what's been going on for the last couple of decades, you may be interested in learning a little more about the way things work firsthand. Even without a box to generate tones, you can do a few things simply with the hookswitch of your telephone (those of you with 3-way calling may experience a little difficulty with this experiment). Below are a handful of 800 numbers that are available to citizens of foreign countries while they stay in the States. These have been termed "country direct" numbers, and can be found by dialing 800 information, or by speaking with the international division of AT&T.

Belize: 235-1154
Brazil: 344-1055
Chile: 552-0056
China: 532-4462
Costa Rica: 252-5114
El Salvador: 422-2425
Germany: 292-0049
Greece: 443-5527
Guam: 367-4826
Hungary: 352-9469
Indonesia: 242-4757
Macau: 622-2821
Malaysia: 772-7369
Portugal: 822-2776
Panama: 872-6106
Uruguay: 245-8411
Yugoslavia: 367-9841 (having trouble)

If you actually make a call into one of these countries, one of the first things you will hear is a C5 Supervisory signal. Have the person at the other end experiment with the hook switch (make sure they don't hang up for more than a minute or so). You will actually hear the supervisory signals going off and on.

As in the case of the blue box, people have been able to trick switches into

thinking that they were another exchange somewhere off in the distance. This is basically accomplished by dialing through a C5 connection into another exchange (which is what happens when you dial those 800 numbers), and sending a *clear forward* signal. This will bring the switch out of *idle* mode (or whatever mode it was in). It will respond with a *release guard* signal notifying the boxer to proceed. The boxer then sends a *seize* signal, and again gets a response with a *proceed to send* signal. This is usually the hardest part for the boxer, since timing here is very critical. Countries differ in timings and sensitivity, so usually what works for one country won't for another. The *clear forward* sent by the Boxer usually consists of 2600Hz+2400Hz for 110-150 Milliseconds, followed by a *seize* of around 150-400 ms. Simply seizing a trunk on the other side isn't enough, however, since the boxer must also know the correct routing to get the calls through. Typically, International "transit" routes are of the most interest, and the boxer may send a traditional KP2 (indicating international call) + Country Code + 0 (for good luck) + City Code (or Area Code) + number + ST. Signalling numbers like KP2 12 415 121 ST will get them to an AT&T Inward operator, whose job is to talk with other operators and settle business by voice if it's not possible via direct routing. Alliance Teleconferencing used to be a big thing in the past, and is still dialable today via blue box.

I am not happy to say that blue boxing has gone into the wrong hands. Like all good tricks, they eventually become harder and harder to do until eventually they disappear — well, almost. Kids from all around the world have used the blue box for their own amusement, making calls to girlfriends they'll never meet, and to "warez" boards to do some software pirating. Even the great people who were at Apple Computers have been known to have played their part in releasing the beast. Now that the technology has fallen into the lower echelons, countries have had to make adjustments to their systems to combat these problems. The German Telecom has spent many marks on British Telecom "filters" that they've placed on C5 connections to try and stop some of the chaos — nice try. (The Germans have already figured out long ago that the systems on the other side will actually perform just fine out of spec, and, for example, instead of sending a 2600Hz or a 2400Hz signal, they'd send a 2650Hz or a 2450Hz - right out of the filtering bands.)

Slowly things are going towards SS7, and the signalling is disassociated. By the time C5 is completely scrapped, there will probably be new ways to approach this blue box mystique. I haven't even begun to cover R2 signalling which yields much more fascinating results, (faking ANI, billing to others) but, unfortunately, it is out of the scope of this article. Maybe next time kids.

WRITE FOR 2600!

SEND YOUR ARTICLES TO:

2600 ARTICLE SUBMISSIONS
PO BOX 99
MIDDLE ISLAND, NY 11953

INTERNET: 2600@well.sf.ca.us
FAX: (516) 751-2608

Remember, all writers get free subscriptions as well as free accounts on our voice mail system. To contact a 2600 writer, call 0700-751-2600. If you're not using AT&T, preface that with 10288. Use touch tones to track down the writer you're looking for. Overseas callers can call our office (516) 751-2600 and we'll forward the message.

A GIFT FROM HALLMARK

by Bernie S.

My heart's out to Fyberlyte for his efforts on The Magical Tone Box article in the Winter 1993-94 issue of *2600*. While his efforts deserve plaudits, the week after his article saw print it became obsolete!

Once again, the mass-market consumer electronics industry has succeeded in bringing down the cost of very sophisticated technology to ridiculous levels. Hallmark, Inc. (the greeting card company) has teamed up with Information Storage Devices, Inc. (who makes the chip Radio Shack sells which was used in FyberLyte's project) to produce the "Talking Greeting Card".

For a mere $7.95, you can buy a completely assembled digital audio recording device (complete with speaker and microphone) built into a greeting card. The idea is to record your 10 second voice greeting on the card and mail it to the person of your choice. The possibilities abound....

If you take the card apart, you'll find a plastic and cardboard frame inside containing a tiny 1" square circuit board, four 1.5V watch batteries, two switches, a piezoelectric microphone, and a decent 1.5" 16-ohm speaker. This is basically the same thing FyberLyte took pains to gather parts for and assemble, except it is *much* smaller, *much* cheaper, and ready to go!

My hacker friends and I have removed these modules and concealed them inside all kinds of unlikely containers: a chewing-tobacco tin, a Zippo lighter, a dental floss dispenser, even a coat collar! The voice-band fidelity is quite good, and it's excellent for recording (and playing back) ACTS coin-deposit tones, Sprint voice FONcard codes, call-progress tones, telco recordings, etc.

Thank you, Hallmark, for "caring enough to send the very best" in a cheap, accessible, and readily hackable device!

10XXX

by The Prophet

One of the most misunderstood and unused features of the post-breakup telconet is the tenex code (also known as 10-XXX code). Since there are very few tenex codes that work in all areas of the country, I have included only a very brief list of common tenex codes to get you started.

Tenex codes were instituted after the AT&T breakup in every RBOC in the vicinity of 1984-1985, and are continuing to be instituted in the non-RBOC (independent) areas of the country. In every area that has "equal access" long distance service, tenex codes are available. Your telco will tell you if you have equal access, but they will not give you a list of tenex codes for your area - you have to get those from your long distance carrier or by scanning.

A tenex code is useful because it permits you to use a long distance carrier other than the one that is primarily assigned to your account. For example, if Deathstar Ltd. is your primary long distance carrier, and you prefer to use Pizzacomm, you could dial Pizzacomm's carrier access (tenex) code in order to use Pizzacomm for the long distance call. This is useful if Pizzacomm has a lower rate to where you're calling, for example, or if you need to circumvent Deathstar for some reason. This is also useful if you need to access a number in the 0700 area for a service (such as a conference calling service) available only through Pizzacomm and not Deathstar. Calls placed through tenex codes are billed by your RBOC; however, if you use an obscure carrier (such as a carrier which usually deals only with COCOTs), sometimes you will not be billed for the call (the long distance carrier has to pay your RBOC to bill the call for them). Also, it can occasionally take a year or more for the call to be billed - it's usually several months.

Of course, there are many other uses for it. For example, some PBX's will block calls to a 1AC, but will not block calls to a tenex+AC. Also, it's useful to use the AT&T tenex when red boxing in some areas, to circumvent the RBOC and go over the AT&T network (which can be boxed when the RBOC cannot be), and in some very small telcos, it's possible to dial a tenex+ACN on a payphone and not be billed for the call.

The format for using a tenex is as follows:

Tenex+ACN

Example: To use AT&T to place a call to the *2600* Voice BBS:

10288-0-700-751-2600

Another example: To place a call to Vancouver using Sprint (Sprint has its own network into Canada so it is beneficial to use Sprint to bypass AT&T and other carriers which use AT&T lines during network difficulties and outages):

10333-1-604-662-6397

Brief List of Tenex Codes

These work in almost all equal access areas:

10288 - AT&T
10732 - AT&T private test network
10222 - MCI
10333 - Sprint
10444 - Allnet
10488 - Metromedia

NOT MUCH GOOD NEWS HERE

A trip to the library can reveal all sorts of fascinating items.

A publication called *Prosecutor's Brief,* described as the "newsjournal of the California District Attorneys Association" had some rather shocking advice in its Summer 1989 edition. (Too bad we didn't catch this one sooner.)

In the lead story, author Jerry P. Coleman proclaims, "Prosecutions of phone 'hackers' are not overly complicated, may be even fun, and can certainly assist your office's strained budget by providing a ready source of computer hardware."

According to California Penal Code section 502.7(g), "An instrument, apparatus, device, plans, instructions or written publication... may be seized under warrant or incident to a lawful arrest, and, upon the conviction of a person for a violation of subdivision (a), (b), or (c), the instrument [etc.] may be... turned over to the person providing telephone or telegraph service in the territory in which the same was seized."

But, according to the article, most of these companies will donate the equipment "right back to law enforcement". What a cozy arrangement.

Concerning monitoring, some of the revelations are pretty scary. It seems that pen registers operated by Pacific Bell double as partial wiretaps, and it's perfectly legal for them to record conversations without a warrant if it's part of a phone company investigation! The article states, "In the case of Pacific Bell, but not necessarily all other companies, the first 90-120 seconds of each call made from the trapped line is taped for the purpose of identifying the person(s) using the illegally hacked codes."

The article goes on to describe the ideal scenario: "If you are fortunate enough to receive the case before the search warrant has alerted the hacker to the investigation, your most important decision may well be the length of time the DNR stays on the targeted line. Weighing in favor of greater DNR time are the desires for obtaining at least a $400 felony loss, and identifying with certainty the hacker. Those considerations must be balanced against the risk that the DNR and its attendant call content taping will be suppressed as being an unreasonable privacy infringement, and the moral consideration of continued losses to the common carrier."

The "recorded salutations" on the tape are considered a key bit of evidence since they identify the defendant. In addition, "any notebooks containing handwritten authorization codes, phone numbers called, etc., can be compared to the known handwriting of the defendant (from booking slip and/or court-ordered exemplars). Don't neglect the seized computer's own memory banks - either its internal hard disk or any floppy disks may contain programs or files identifying the computer's user as the defendant."

District attorneys are also urged to look through the evidence for any "contacts among the hacker community" or BBS numbers.

Another "particularly fun" way of prosecuting a hacker is to look through his computer programs for games that have a listing of the top 10 scorers. "If your defendant's name appears close to the top of the list (or exclusively), it is quite reasonable to argue that, having had the most time to play the game this successfully, the defendant must own the computer."

Another absurdity concerns the justification for seizing telephones, described as "entirely appropriate within the statute, and serves to drive home rather graphically to the hacker just how serious this matter of criminal prosecution is."

It's pretty obvious how serious computer crime is to district attorneys in California. Here is our first solid piece of evidence that they consider hacker cases to be fun and easy ways of getting other people's computer equipment for themselves. A true mockery of justice.

The CDAA can be reached at 916-443-2017.

*

Another fascinating document was recently obtained by *2600* - the full transcript of last year's Congressional hearing which turned into a hacker bashing courtesy of Rep. Edward Markey (D-MA) and Rep. Jack Fields (R-TX). It's far too long to reprint here but you can get a full copy for $10 from the U.S. Government

Printing Office, Superintendent of Documents, Congressional Sales Office, Washington DC 20402-9315. Tell them you want the hearings on telecommunications network security, serial number 103-53, stock number 552-070-15676-3. You can order by credit card at 202-512-2470. There's hours of entertainment here.

*

For the last two issues, *2600* has actually been on sale at CompUSA, the computer superstore. For a while we were concerned that we were becoming too mainstream but our fears turned out to be unfounded. Apparently someone at CompUSA Central decided to read a copy. Result: They have decided to "permanently remove *2600* from their stores". The problem is, so many people found us at CompUSA that they're now being inundated with calls from people wanting to know why we suddenly disappeared. How do we know this? Don't worry, we know....

*

Trouble on the information highway: the biggest telecommunications merger in history will never be history now. Bell Atlantic and TCI, two of the biggest entities of any sort on the planet, decided to break off the engagement and blame it all on the FCC for regulating rates. If we only knew it would be that simple.... The Clinton Administration is becoming obsessed with monitoring citizens. On February 4th, the Administration rejected all of the criticism it has received on the Clipper Chip proposal and announced plans to move full speed ahead with its implementation - on a "voluntary" basis. The Clipper Chip would allow law enforcement to eavesdrop on phone calls that use the government standard of encryption. Civil liberties groups have strongly condemned Clipper and its companion Capstone (for data encryption) because of the potential for abuse and widespread monitoring of citizens. This technology is being developed with the help of the NSA, an organization that's *supposed* to keep its monitoring activities outside our borders. And that's not all. More recently, the administration reintroduced a digital telephony proposal that would require phone companies to provide real-time traffic analysis to all law enforcement agencies. Unlike a pen register, this is an ability that will always be there, one which simply has to be turned on. The data would then be sent to a remote monitoring post. According to the Electronic Frontier Foundation, such information amounts to more than just the numbers we dial. "As we all come to use electronic communications for more and more purposes," a recent press release says, "this simple call setup information could also reveal what movies we've ordered, which online information services we've connected to, which political bulletin boards we've dialed, etc. With increasing use of telecommunications, this simple transactional information reveals almost as much about our private lives as would be learned if someone literally followed us around on the street, watching our every move."

*

Some new area codes that will be debuting in 1995: 334 (Alabama), 360 (Washington State), and 520 (Arizona). These will be the first area codes not to have 1 or 0 as the middle digit. Look for many more.... We discovered quite by accident that Wiltel Communications passes Caller ID data across state lines and they seem to be a lot better at it than Cable & Wireless. For one thing, anyone can access Wiltel by using their carrier access code (10555). Cable & Wireless doesn't allow outside use of its code (10223). Customers who use Wiltel stand a very good chance of having their phone number passed on to the called party, regardless of whether or not they've blocked it.... Speaking of carrier access codes, get ready for a shock. After finally getting accustomed to the 10XXX system of using different long distance companies, it's all going to change. Yeah, no kidding. It seems a thousand possibilities are no longer enough. Strange, we never seem to have more than a handful of choices in any one part of the country. But someone out there is using all of these codes, so the rest of us must adjust. Starting in 1995, you will dial with the format 101XXXX. That's right, *seven* digits, not five. The 5000 and 6000 number ranges will be used for new carriers. If we assume that AT&T's new code will be 1010288 (no codes are known yet), the dialing instructions to reach our voice bulletin board will be: 1010288-0700-751-2600. This is really starting to get stupid.

LETTERS

(continued from page 31)

possessions from us during the booking procedure, set bail at an outrageous $5,000 each, and falsified the arrest records to support the felony charge. Of course, the prosecutor read the law and withdrew the felony charge; the charge was supposed to be applied to anyone who placed an explosive within 1000 feet of a switch!

The sheriffs did not want to be embarrassed, however, so they convinced the prosecutor to replace the felony charge with a misdemeanor trespassing. Now, the tracks we were walking along were only 20 feet from a major street, in an area that was not fenced off, posted trespassing, or sensitive in any way. Yet, we were technically trespassing, and we were prosecuted, coerced into pleading guilty (mostly because we couldn't afford a lawyer, and the public defender never even appeared at our hearings), and I actually served 30 days *jail time* and 1000 hours of community service. All this because I walked along some train tracks.... The negative ramifications of this event took years to overcome, and cost thousands of dollars in lost wages, bail bond fees, and legal fees.

The point is, once law enforcement officials begin an investigation or make an arrest, they will do almost anything to avoid the embarrassment of having all charges dropped or the "suspect" going free. Better to lock up a couple of kids for nothing than admit they shouldn't have arrested them in the first place. Unfortunately, when it comes to hacking, law enforcement is clearly as unjust and absurd as it is in the rest of America, if not worse. Phiber Optik has my sympathy, and the police have my contempt.

Racer X

Thanks for sharing that. Such experiences need to be told to others so we can all be on the lookout for injustice. And for those who want to stay in touch with Phiber Optik, his address is:

Mark Abene 32109-054
FPC, Schuylkill
Unit 1
P.O. Box 670
Minersville, PA 17954-0670

All incoming mail is read by prison authorities. The only things allowed are letters and non-hardcover printed matter. Only book publishers can send hardcover books.

Correction

Dear *2600:*

Just mailing you to point out an error on FyberLyte's "The Magical Tone Box" article that appeared in this past Winter edition of *2600*. At the end when he discusses the use on the Tone Box for blue boxing he mentions "So, to seize, hit 1, 2, dial on the phone's keypad (or your own dialer), then 3." Now anyone with basic blue boxing knowledge knows this does not work. Why? Because DTMF is not equal to MF. The tone pairs used for DTMF signalling of numbers are not the same as those used in MF, therefore you must also record those tones. Not that this is difficult with the Tone Box. I must say it's a great alternative to building a blue box using VCO's (Voltage Controller Oscillators). In any case, thanks for a good article.

Aleph One

Phone Company Charges

Dear *2600:*

I was just reading the letters page for the Autumn 1993 issue and I realized that if I did not comment on the complaint of SpOOf! about the cost of CID, I would be remiss. I do not mean to defend the phone company, but the cost of enabling CID does not pay for the "flipping of the switch" so much as it pays for the cost of paying someone to man the phones to answer the request. There are probably a lot of other hidden costs, including extra software to make CID work and upgrading of switches. If one does not want to pay for the expense, one does not have to. I'm tired of seeing hackers complain about cost without taking a holistic view of a situation.

In the Winter 1993-94 edition, Will Chung writes that total capacitance is added when caps are placed in series. Actually, in series, capacitance is calculated the same way resistance is calculated in parallel. To add caps in a linear manner, place them in parallel.

To sum up:

In parallel capacitors add as

Ctot = C1 + C2 + ... + CN

In series capacitors add as

1/Ctot = 1/C1 + 1/C2 + ... + 1/CN

This could prevent needlessly wasted debugging effort....

David

Thanks for the correction. As far as charges for Caller ID, we believe that is exactly what they want you to think. You do need to pay the people who answer the phones. But surely the monthly charges we all pay are sufficient for this. We doubt customer service representatives are demanding extra pay for every Caller ID request they process. Which leaves the cost of paying for the new technology. That is an investment by the phone companies. Their profits (of which there is a staggering amount) go into these investments and, if more people use more phones - which by every account is exactly what is happening, then the investment pays off. Charging fees in addition to this is sheer greed, an art the phone companies have mastered to perfection.

DO YOU HAVE A LETTER YOU HAVEN'T SENT US?

What are you waiting for?

2600 Letters
PO Box 99
Middle Island, NY 11953

2600 Marketplace

MANY TEXT FILES, on hardcopy or disk. Send for a free catalog. H/P/A/Virus related everything! P.O. Box 54, Elka Park, NY 12427. Internet Address: microwir@works.com

EXPLORE THE DARK SIDE OF COMPUTERS, full of forbidden knowledge from the H/P/C/A scene. Summer catalog with reduced prices out now!!! Send only $1 for our new catalog with new items to: SotMESC, P.O. Box 573, Long Beach, MS 39560. Books, disks, subscriptions, and more....

GENUINE CUSTOM 6.49 MHZ subminiature quartz crystals - the optimum frequency and size for your project! Only $5 postpaid, sent first class mail. 5/$20 or 10/$35. FREE detailed installation notes included. USPS money orders or cash shipped next day, checks allow 3 weeks. Free instructions only send SASE. Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector for only $3 (covers shipping and handling). Send $3 to: Patrick Harvey, 710 Peachtree St. NE 430, Atlanta, GA 30308.

WRITING HUGE TEXT FILE on cell phreaking, need info! Please send to Nicholas Singer, 6 Winsor Place, Purchase, NY 10577.

THE BLACK BAG TRIVIA QUIZ. On 5.25 360k DOS disk (only). Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining, very educational, and FREE! Just send two 29 cent stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

SMALL L.A. AREA H/P BBS needs aggressive, technically/socially conscious new users. Warez D00dz need not apply. 2 nodes, no waiting. (714) 525-4145 and (714) 525-4421.

THE ANARCHIST'S BBS. A computer bulletin board resource for anarchists, survivalists, mercenaries, investigators, researchers, computer hackers, and phone phreaks. Encrypted e-mail/file exchange available. Call 214-289-8328 by modem.

WANTED. Operation instruction manual for Western Electric 145A test kit and/or any current hacking and phreaking info! Send to: Gray Area Newsletter, PO Box 30286, Memphis, TN 38130-0286.

PROTECT YOURSELF! Searing hot red pepper spray. 10% Oleorisin Capsicum, none stronger! Chosen by over 4000 law enforcement agencies, including NYPD and LAPD. Instantly disables attackers for 45 minutes. Proven superior to MACE. .68 oz., $19.95 plus $4.50 S/H. Money orders only. Cannot ship overseas. Send to: Vanguard Security, P.O. Box 1173-A, New York, NY 10028.

CELLULAR PHONES. Why pay for two phones? Have a car phone and a handheld portable with the same number. Modify ESN and NAM using your PC. Programs and instructions are available for: Motorola, Mitsubishi, NEC, Panasonic. US$ 49.95 per model plus S&H. Call our fax on demand number for more information: 011-356-310950.

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!

NEED A 5089 DTMF GENERATOR? We have them for $5 (US) + $2 shipping and handling each, cash or money order only. Send your order to P.O. Box 237, Arlington, TX 76004 USA. Same day service on most orders! Chips in quantity: 10 for $50, and each additional chip $4 - we pick up the postage. (If outside the continental U.S., please write for information on availability and our UPS shipping rate.)

ELECTRONIC SECURITIES LTD. World leading supplier of amateur and law enforcement grade surveillance equipment. We buy direct from over 300 manufacturers. Many exotic imported "bugs" such as spread spectrum, scrambled, subcarriers, plus tone activated carrier current infinity transmitters, mains, loop extenders, slaves, laser listeners, through-wall mics, scanners, DTMF decoders, fax, modem, and beeper interception kits, etc. All models of sub-miniature CCD cameras with a wide variety of pinhole lenses. Infrared and starlight night vision devices, long range parabolic and shotgun microphones. Plus a complete line of medium to high end countermeasures equipment, computer security and cracking software, cellular phone reprogramming kits, EPROM programmers, Van Eck tempest receivers, answering machine code busters, color box kits, lineman's handsets, telephone and facsimile scramblers, lockpicking equipment, phreaking and hacking technical papers. 150 page product reference catalog is $5 US Postal Money Order. Send to: Electronic Securities Ltd., 16 Watermill Way, Ridge, NY 11961.

"THE QUARTER" DEVICE. Complete kit of all parts, including 2x3x1 case, as printed in the Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29 or 2 kits for $50. Send money order for 2nd day shipping; checks need 2 weeks additional to clear. Add $4 for either 1 or 2 kits (foreign add $12 per order, U.S. funds only) for shipping and insurance. ALSO AVAILABLE: 6.5536 Mhz crystals in quantity: 10 for only $35 postpaid. Each additional crystal only $3 postpaid. For larger quantity discounts on either item, include your phone number and needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

GET THE ULTIMATE CD-ROM! The virus-base contains thousands of fully functional computer viruses, virus construction toolkits and virus related info. $99.95 + $7.00 express shipping. Better hurry! American Eagle Publications, PO Box 41401, Tucson, AZ 85717.

DETAILED CELLULAR TECHNICAL PAPERS. Full disclosure. Send $10 to: Marc M., 3026 Barnhard #361, Tampa, FL 33613.

THE EVIL DOMAIN BBS (518) 589-6044. The BBS where hackers abound! Many H/P/Anarchy text and utilities. All 2600 subscribers gain complete access. The biggest H/P board in 518. New User Password: PHAVCT.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Summer issue: 5/1/94.

MICHIGAN NUMBERS

Both MSUnet and Michnet allow access to telnet on a limited basis - only addresses in the format 35.x.x.x.

This includes burrow.cl.msu.edu, which allows access to gopher, which in turn ties you into a virtually unlimited database of information.

MSUnet

(517) 336-3200
(517) 353-8500
(517) 835-5490

Michnet

(313) 258-6811
(313) 283-8822
(313) 370-4310
(313) 370-4311
(313) 577-0321
(313) 577-0335
(313) 593-5335
(313) 722-1500
(313) 762-3311
(313) 762-3319
(313) 763-4800
(313) 763-6520
(313) 763-6521
(313) 827-7600
(313) 939-3370
(313) 998-1302
(313) 998-1303
(313) 998-1304
(517) 353-3500
(517) 774-3790
(517) 788-6300
(517) 797-2814
(517) 797-2822
(616) 387-2070
(616) 394-7120
(616) 539-0977
(616) 592-2041
(616) 627-2214
(616) 627-2220
(616) 771-9479
(616) 777-3944
(616) 941-9826
(616) 963-9975
(616) 983-1965
(906) 225-0222
(906) 487-1517

Ameritech Commercial Service

(313) 229-7411
(313) 255-0680
(313) 259-3365
(313) 263-6104
(313) 271-0205
(313) 271-2293
(313) 272-5661
(313) 282-3540
(313) 292-5610
(313) 332-2444
(313) 335-6481
(313) 335-7343
(313) 335-7357
(313) 335-7362
(313) 335-7417
(313) 335-7427
(313) 335-7486
(313) 336-8687
(313) 347-1184
(313) 352-8920
(313) 362-4277
(313) 420-2890
(313) 425-6250
(313) 433-0845
(313) 463-4973
(313) 475-9076
(313) 477-4422
(313) 482-4780
(313) 489-5928
(313) 495-0020
(313) 557-6216
(313) 565-2640
(313) 569-9706
(313) 575-9177
(313) 575-9243
(313) 581-8530
(313) 583-4370
(313) 634-6201
(313) 651-3804
(313) 662-0611
(313) 662-8838
(313) 662-8842
(313) 663-0008
(313) 663-0321
(313) 663-0520
(313) 663-0613
(313) 663-3677
(313) 675-5392
(313) 683-0467
(313) 699-9879
(313) 722-0460
(313) 739-0218
(313) 774-9147
(313) 781-0913
(313) 824-9462
(313) 832-4340
(313) 839-7389
(313) 841-8730
(313) 851-4591
(313) 852-8423
(313) 864-0755
(313) 865-8061
(313) 871-0005
(313) 881-9625
(313) 892-0920
(313) 898-6066
(313) 921-1690
(313) 934-0147
(313) 941-8450
(313) 963-2369
(313) 964-1327
(313) 973-7080
(313) 979-8718
(906) 225-0411
(906) 487-9007
(906) 632-3261
(906) 774-0585
(906) 789-2010
(906) 932-3219

Special thanks to Tonto of 517

hacker reviews

***Secrets of a Super Hacker* by The Knightmare**
Loompanics Unlimited
205 pages, $19.95
Review by Michael E. Marotta

"Third time's the charm." This is the third book on hacking from Loompanics and it is the best of the three. (M. Harry's *Computer Underground* is also a fine work.) The book has some hype, but overall *Secrets of a Super Hacker* presents a complete summary of what every hacker knows. And what every wannabe wants to know.

There was a time when hackers earned their power. Working alone, each one found neat stuff. When BBS's were invented, hackers could share, but sharing was based on exchange: to get something, you had to have something you found on your own. When Stoll and Hafner wrote about hacking they were careful to say enough to give body to their narratives. But not too much. They never gave out passwords. This book blows all of that away. It is the *Jurassic Park* of hacking.

In *Jurassic Park*, the mathematician who dies rambles on under morphine about how power corrupts. He notes that the karate master doesn't beat his wife because becoming a master entails mastering himself. But the JP, Inc. folk *bought* their technology wholesale. They didn't have to earn their power. So, it was in control of them. *Secrets of a Super Hacker* will deliver into anyone's hands for $20 what it took us 30 years to learn. The appendix includes rtm's list of common passwords - in case you want to be a hacker but don't know how to FTP. From shoulder surfing to tempest, from social engineering to dictionary attacks, it's all in here. He even covers dumpster diving. The best part is the lengthy section on getting data from damaged diskettes. And then imagine hacking a computer network by splicing your notebook computer into the light pen of a terminal!

The Knightmare maintains that as more and ever more people come online, there will always be opportunities for the hacker. Somewhere there is a username/password combination SMITH/SMITH. Somewhere there is a new manager open to the "dumb user" ploy. You just have to find them. What do you do then? Well, the hacker ethic says don't screw things up. But the hacker ethic also says to explore. The Knightmare says that once you are inside a computer, you can prove to yourself that you are really a hacker by changing its databases and not getting caught.

Secrets of a Super Hacker is very readable. Its colloquial American crams a lot of information into each sentence. It is a very dense narrative. The organization is commendable. The book is divided into three sections: Before Hack, During Hack, and After Hack. The book begins with The Basics (hardware, software, etc.) and The History of Hacking (*YIPL, TAP, 2600*). Subsequent chapters include: Researching the Hack, Passwords and Access Control, Social Engineering, Reverse Social Engineering, and What to Do When Inside.

Naturally, there is a chapter on How to Keep from Getting Caught. At 10 cents a page, you can't go wrong.

UNIX Security: A Practical Tutorial
By N. Derek Arnold, ITDC
McGraw-Hill, Inc.
ISBN 0-07-002560-6
Review by Simson L. Garfinkel

While there is suddenly a plethora of UNIX security books on the market, almost all of them are written from the point of view of the system operator, feverishly bent on keeping hackers out of his computer while not making life too terrible for the legitimate users. While these books make interesting reading, it takes a lot of work between-the-lines to get any useful info out of these tomes about breaking into UNIX systems.

Thankfully, such is not the case with Arnold's *UNIX Security*. This is a book aimed at the hacker community, with detailed, step-by-step instructions for finding and exploiting vulnerabilities on all kinds of UNIX systems. Although the book is filled with tips, most hackers will turn straight to Chapter 8, "Break-in Techniques." The advice is all sound: patience is a virtue (and necessary if you don't want to get caught); arrange for evidence that points at somebody else; search out log files and cover your tracks. In addition to good technical know-how, Arnold shares tips on social engineering as well.

The only confusing aside is Arnold's belief that hackers are hell-bent on getting sysops fired. To this end, he suggests sending insulting or harassing forged electronic mail, allegedly from the sysop, to the sysop's manager. What sensible hacker would do this? Besides being a great way to get caught, there are simply so many more rewarding things that a hacker can do once gaining superuser privileges. Sadly, Arnold's book is a bit shy in this department.

As an added jackpot, Arnold's book contains over 140 pages of program listings. While some of the programs are of limited utility, the hacker's pride and joy are the fairly sophisticated password cracking program, the UNIX computer virus for infecting a.out files, and a utility for groveling through /dev/kmem.

UNIX Security's heavy System V bias makes it of limited value for hacking into the university world, but makes it ideal for those interested in breaking into business. Perhaps his goal in publishing this information is to create more work for computer security professionals. (Arnold's company, ITDC, is a McGraw-Hill consulting firm which teaches courses in computer security; this book is largely taken from ITDC's course notes.) With *UNIX Security*, a good laptop with a cellular modem, and a few day's supply of batteries, a young aspiring hacker could go far.

trojans in the u.k.

by Veghead

Many installations, in the UK at least, now favour PC's as terminals to their UNIX machines. My college for example uses a large ethernet setup running Sun Microsystems PC-NFS to access their various UNIX machines, using a PC version of TELNET. I noticed a gapin' 'ole in the security:

As login authentication for the ethernet, PC-NFS has a DOS-based login program, similar to Novell's, that compares a given password to that found in /etc/passwd on a pre-specified UNIX machine. Stupidly, it'll take the uid and password from the command tail, so to login I could type:

net login myid mypassword

Trojanising this meant writing a bit of C code that would intercept the net command, save any interesting info (such as the uid and password) in a secret file, and pass the original parameters on to the original NET program, which would be none the wiser. This meant that to the user, nothing odd would have happened - no authentication errors to put them on the scent. In fact, it was marginally more complicated than this as the NET program interprets any parameter as "*" to mean "ask the user". For example,

net login *

will make the program respond with

Enter username:
Enter password:

But overcoming this wasn't really a problem; the Trojan would simply put the questions to the user and then pass them as parameters to the real one (not forgetting to kill the echo on the password!). It worked like a well oiled dream!

I was considering the idea of a "generic Trojan" that could be used in all manner of situations without the need for re-writing the actual code. What I came up with was a badly written bit of 8086 code (I called it Keyspy) that does the following.

1) When executed, hooks Int 15h and TSRs (terminates and stays resident).

2) Records the next forty keystrokes the user makes using the "Keyboard Intercept" interrupt. (So don't try and run it on old style keyboards - it *won't* work!)

3) Next time it's executed it dumps down the key-scan code info to a disk file, unhooks itself from the interrupt table and releases the 1K or so of memory it's been holding hostage up until then.

What use is this? Ok, what would happen if you run it before running PC-TELNET? The next user to come along would notice nothing wrong and would hopefully login. All the time, the program would be noting down everything the user was typing. Later on you go back, run it again and it will obediently supply you with a file containing the first forty scan-codes of the keys the user had hit.

One way of getting round traditional Trojans is to login in twice, firstly with a dummy password like "FUCKYOU", so if the program has been trojanised you don't get caught and the hacker gets a message. Even if the above user had done this, they would still get caught.

On our network all software is run using a networked copy of a DOS menu called Automenu. All that needs to be done is to insert a command to run Keyspy into the menu code before and after it runs TELNET. Then, when anyone uses TELNET from anywhere, Keyspy supplies a copy of their keystrokes to a centrally located file where I can pick them up from.

Ideally, you would have a program that would dump the info to a file itself, without having to be run again but it would make the code far more complex with loads of undocumented calls etc. and quite frankly, I couldn't be arsed.

Adventurous programmers could then adapt that program to allow it to wrap itself around an executable file, infecting it so to speak. That way it would be almost undetectable.

The other real downer is that it saves scan codes and not ASCII or anything useful like that. It's necessary to write a program that converts the alphanumeric scan-codes to ASCII for your particular keyboard.

The Chrome Box

by Remote Control

Emergency vehicles in many cities are now using devices called OptoComs. OptoComs are sensors on traffic lights that detect a pattern of flashes from vehicle-mounted strobe lights.

This flash pattern varies from city to city depending on the manufacturer of the equipment used. Often the sensors are installed only at major intersections. Nevertheless, the Chrome Box, which simulates these strobe patterns can often be used to give your car the same priority as an ambulance, paramedic van, fire truck, or police car.

Because of the varying patterns on different systems this article will outline a general procedure for making the Chrome Box.

Decoding Flash Patterns

First, you need to observe an emergency vehicle in action. You can wait until you encounter one by chance, running out to see when you hear a siren, or pulling over in your car to let one pass by. You might wait near a fire station for the next emergency to occur. Or, if you are very impatient, you can summon one by calling in a false alarm (not recommended).

If the OptoComs in your area are the kind with a pattern of single flashes at a steady rhythm, you have merely to buy a strobe light at Radio Shack and adjust the flash rate until you can induce a traffic light to change. If the flash pattern is more complex, you can videotape the emergency vehicle and then play back the tape in single-frame mode, counting the number of frames between each flash. Each video frame is 1/30th of a second. Using this you can calculate the time between flashes in the pattern. Another way is to count the number of flashes (or flash-groups) in one minute and use that to compute the rate. Counting video frames will give you a good idea of the spacing of the flashes in a complex pattern.

For really accurate information, call the fire station and ask them, or write to the manufacturer for a service manual, which will include a schematic diagram that you can use to build one. A good cover story for this is that you are a consultant and one of your clients asked you to evaluate Optocom systems, or you could pose as a freelance journalist writing an article.

Modifying the Strobe Light

You may not have to modify the strobe at all. But if you need a faster flash rate than your strobe allows, open it up and find the large capacitor inside. Capacitors are marked in microfarads, abbreviated as mf, mfd, or ufd. By replacing the capacitor with one of the same voltage rating (usually 250 volts or more) and a *smaller* value in microfarads, you can increase the flash rate. Halving the microfarads doubles the rate. The other component that can be changed is the potentiometer (the speed control device with the knob on it). Using a smaller value (measured in ohms or kohms, abbreviated with the greek letter "omega" or the letter K) will speed up the strobe. There may also be a resistor (small cylinder with several colored stripes on it, and wires coming out of each end). Replacing this resistor with one of smaller value will also speed up the strobe.

To generate a complex pattern, you will either have to design and build a triggering circuit using IC chips, or rig up a mechanical device with a multiple-contact rotary switch and a motor. It *has* been done.

To modify the strobe for mobile operation the simplest thing is to get a 110-volt inverter that will run off of a car battery by plugging into the cigarette lighter and running the strobe from that. Or, you can figure out (or find in a hobby electronics magazine) a strobe circuit that will run from batteries. Battery-powered strobes may also be available, either assembled or as kits.

Stealth Technology

Most light sensors and photocells are more sensitive in the infrared area of the light spectrum. Infrared (IR) is invisible to the human eye. Putting an infrared filter over the strobe light may allow the Chrome Box to operate in traffic undetected by police or other observers. IR filters can be obtained from military surplus sniperscope illuminators, or from optical supply houses like Dow-Corning or Edmunds Scientific Co.

Using the Chrome Box

Mounted on your car, the Chrome Box can guarantee you green lights at major intersections in cities that have OptoComs.

Handheld Chrome Boxes may be used to create gridlock by interfering with the normal flow of traffic. If you have access to a window overlooking a traffic light, you can play pranks by switching the signals at inappropriate moments, or you can plug the strobe into an exposed outlet at a laundromat or gas station.

Some Decoded Patterns

Torrance, California - standard large Radio Shack strobe lights are used. Moderately fast rate.

Manhattan Beach, California - flash-pairs in a 4:1 ratio, at a rate of two flash-pairs per second

Please send in any new patterns or info you discover.

2600 MEETINGS

Ann Arbor, MI

Galleria on South University.

Austin

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

Baton Rouge, LA

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

Bloomington, MN

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

Boise, ID

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

Boston

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

Buffalo

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

Chicago

Underground Coffeehouse, 3508 N. Broadway, (312) 327-2117.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

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

Columbus, OH

City Center Mall, outside the lower level entrance to Marshall Fields.

Dallas

Town East Mall (Mesquite), 3rd Level Food Court.

Danbury, CT

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

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

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

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Memphis

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

Nashville

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

New York City

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

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

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

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

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

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

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

Sacramento

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

San Francisco

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

Seattle

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

Tempe, AZ

Java Road Coffeehouse, 7th Street & Mill Ave. Payphone: (602) 967-9585.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

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.

*****

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.

The Shirt

❑ You won't find it in clothing stores. (We did, but that's a long story.) The 2600 hacker t-shirt could be the fashion statement of the nineties. After all, anything is possible. Two-sided, white lettering on black background, blue box schematic on the front, hacker newspaper articles on the back. $15 each, two for $26. M, L, XL

The Video

Actual footage of Dutch hackers penetrating a United States military computer system in the summer of 1991. This is not a secret videotape. These hackers filmed this to show everybody just how easy it really is. In fact, a small part of this tape was shown on *Now It Can Be Told*. This version tells the whole story and runs about 30 minutes. $10. VHS, NTSC format only. ❑

2600 SUBSCRIPTIONS

INDIVIDUAL

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

CORPORATE

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

OVERSEAS

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

LIFETIME

❑ $260 (also includes 1984, 1985, 1986 back issues)

2600 BACK ISSUES

❑ 1984 ❑ 1985 ❑ 1986 ❑ 1987 ❑ 1988
❑ 1989 ❑ 1990 ❑ 1991 ❑ 1992 ❑ 1993

$25 per year

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

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas - we don't have enough little boxes to check off so please figure out another way to convey this info.)

NAME, ADDRESS, SUBSCRIBER #, SPECIAL NOTES, ETC.

MAIL TO: 2600, POB 752, MIDDLE ISLAND, NY 11953

TOTAL AMOUNT:

documentation

OUR ADDRESS:

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

no one told
you when
to run