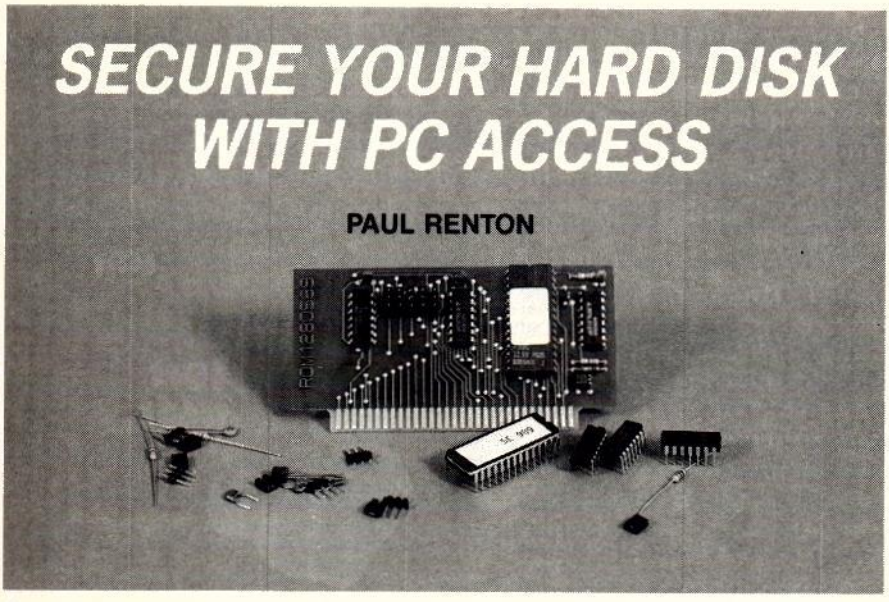
# SECURE YOUR HARD DISK WITH PC ACCESS

PAUL RENTON



Computer security may seem like a problem only for large corporations or the government. However, small businesses and home computers often contain sensitive information that should be protected. For example, if you have a small business, your payroll records may not seem to be the most sensitive information in the world, but a competitor would certainly love to see them! And you wouldn't want your babysitter to boot your PC and get into your checking-account data!

There are many approaches to PC security, but the one offered here is a combined hardware/software solution. PC Access provides one master password, which enables access to the password list and to other functions, and fifteen user passwords. An EPROM on a small expansion card contains a BIOS extension that hooks PC Access into your PC's boot procedure. The circuit is simple and inexpensive to build; a kit is available for less than $35.

PC Access provides several extras, including a hold function that allows the user to suspend computer access by pressing a hotkey. The computer then idles until the correct password is entered. The hotkey combination can be configured for compatibility with various memory-resident programs. In addition, you can maintain an audit trail of who logs onto the system. The audit file is encoded, hence meaningless when viewed with a DOS TYPE command. A program provided with the kit decodes the file into ASCII format.

## How it works

PC Access works by altering DOS's normal boot procedure in several ways. First, PC Access forces the system to boot from the hard drive by disabling access to floppy drive A during the boot process. Thus, you can't disable PC Access simply by booting from a floppy.

In addition, a software driver must be loaded via CONFIG.SYS and processed by DOS in the usual manner, otherwise the system will not boot. That means that you can't boot the PC by de-

*continued on page 73*

*continued from page 69*

leting the software driver or by changing the contents of CONFIG.SYS. Thus it is impossible to gain access to a secured PC without removing the PC Access card.

Further, PC Access locks out the use of the Ctrl and Alt keys on the PC keyboard, so pressing Ctrl-C or Ctrl-BREAK will not halt the boot process.

Additionally, some computers have monitor or setup functions that can be accessed before DOS has booted. Those setup routines are typically entered by pressing some combination of Ctrl, Alt and some other key. Locking out Ctrl and Alt provides a means to prevent unauthorized access to those functions during boot.

At boot time, PC Access's device driver (SECURITY.BIN) prompts the user for a password and optionally for a user ID as well. The passwords and user ID's are stored in an encoded form inside the device driver. If no valid password is entered in three attempts, access to the computer is denied until it is rebooted. A new password prompt appears each time the computer is rebooted.

After a valid password has been entered, the device driver restores access to drive A, re-enables use of the Ctrl and Alt keys, and returns control to DOS so that it can execute the remaining CONFIG.SYS commands and give user access to the PC.

## DOS's boot sequence

When an IBM (or compatible) PC executes its power-up routines, one chore is to search for BIOS extensions. The extensions are located in memory segments C000h through EFFFh. The BIOS searches that area in 2K steps, looking for the two-byte sequence, 55h AAh. If the BIOS finds that "signature," it then assumes that the next byte contains the length (in 512-byte chunks) of the routines contained in the ROM. Next the BIOS computes a checksum on the area described. The checksum must be zero for the extension to be recognized. Once the extension is recognized, the computer executes a far call to the fourth location in the ROM. That call is provided so that the ROM can perform any required initialization. The initialization routine should exit with a far return. The BIOS then continues searching for other extensions. Once all of the legal addresses have been searched, DOS is booted.

Part of DOS's boot procedure is to load the CONFIG.SYS file that is stored in the root directory, and perform any setup and configuration functions specified in the file. One advantage of using a device driver to request user passwords is that the passwords and user ID's can be stored inside the device driver rather than in the EPROM. Circuit cost and complexity would increase if that information were stored in EEPROM.

The software included in the PC Access EPROM sets up a new interrupt handler for floppy- and hard-disk access. The new routine allows DOS to boot from the hard drive, but not from drive A. A second interrupt is established that intercepts scan codes from the keyboard and disables the Ctrl and Alt keys.

## Circuit details

The PC Access EPROM is mapped into an 8K slot in the PC's address space somewhere between C000H and EFFFH. As shown in Fig. 1, decoding the desired address is accomplished with a 74LS30 eight-input NAND gate (IC1) and a 74LS04 inverter (IC2). When all eight NAND-gate inputs are high, then the output will be low; otherwise, the output will be high. A low output enables the EPROM's chip select ($\overline{CS}$) input (pin 20).

The address that is actually de-

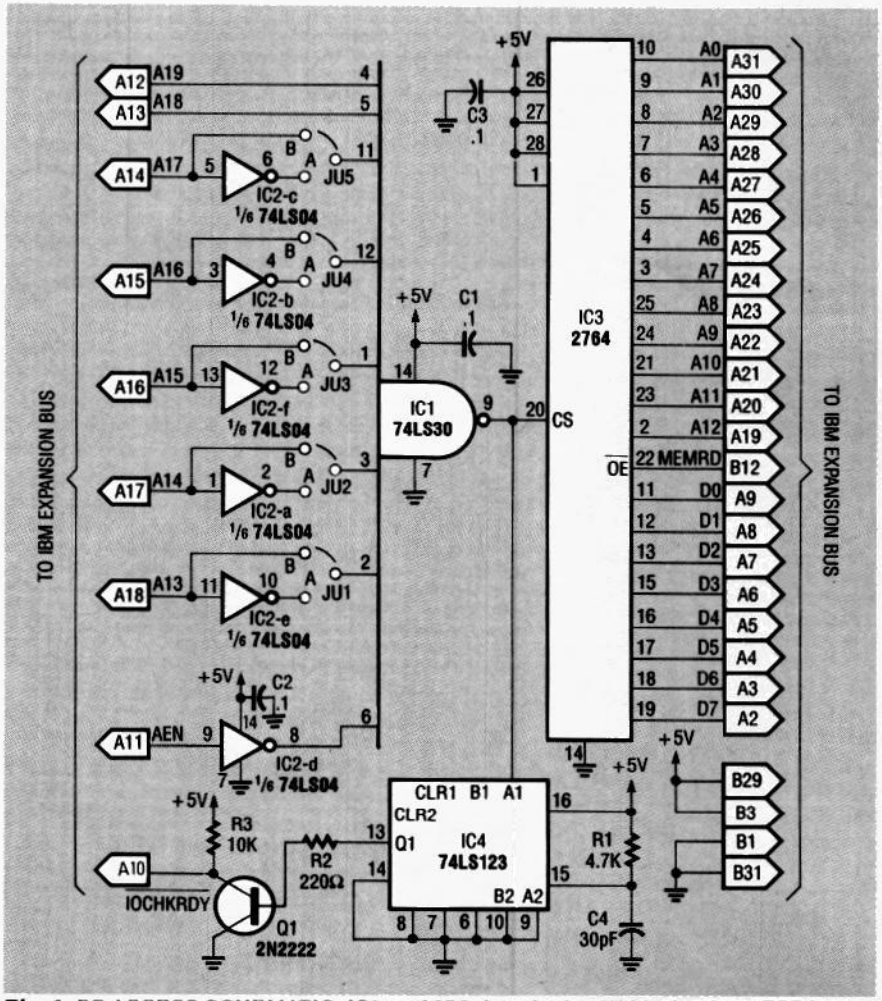



***Fig. 1.*** *PC ACCESS SCHEMATIC: IC1 and IC2 decode the 8K block where EPROM IC3 resides. The one-shot (IC4) and associated components extend the memory access cycle, thereby allowing slow EPROM's to be used.*

coded is determined by the positions of five address-select jumpers, which are connected to address lines A13–A17. The jumpers determine whether the true or the inverted address lines from the expansion bus are routed to IC1. When a line goes directly to IC1, that line must be a high for the chip-select signal to occur. When the inverted address line is used, it must be a low.

Address lines A18 and A19 drive IC1 directly, because both will be high whenever an address greater than or equal to C0000 is accessed. The A13–A17 lines further decode the address; any available 8K slot from C0000–EE000 may be used. Jumper settings and corresponding addresses are shown in Table 1.

The AEN signal from the expansion bus shows whether the address and data busses are currently being controlled by the microprocessor or by the 8237 direct memory access (DMA) controller. The PC Access EPROM should be enabled only when the microprocessor is controlling the bus, so an inverted version of AEN is routed to IC1.

Data and address lines to the EPROM are connected to the corresponding data and address lines from the expansion bus. The EPROM's output enable ($\overline{OE}$) is provided by the memory read ($\overline{MEMRD}$) signal from the bus.

The 74LS123 is a one-shot that provides a 150-ns pulse at its Q1 output (pin 13) each time the EPROM is selected (i.e., each time $\overline{CS}$ goes low). The output of the one-shot drives Q1, a 2N2222 NPN transistor, which pulls low the expansion-bus signal $\overline{IOCHKRDY}$. That signal is used to insert a wait state into the memory access cycle, and is used to allow slow EPROM's to be used on a fast bus. Slow EPROM's (250 ns) are easier to buy and less expensive than fast (150 ns) ones.

Power for the card is obtained directly from the expansion bus.

## Construction

The hardest part of construction is fabricating the PC board. If you want to build your own PC board, foil patterns are shown in PC Service. You can also purchase a prefabricated PC board from the source shown in the Parts List. The commercial PC board has plated-through holes and gold-plated edge connections.

If you make your own board, remember that it's double-sided, so the wires must be soldered on both sides of the board.

After buying or building a board, install the components as shown in Fig. 2. The order of installation is not critical. Just keep polarities straight, and check your work carefully for shorts and opens before installing the board in your PC.

A socket may or may not be necessary for the EPROM. If you

TABLE 1—JUMPER SETTINGS

| | JU1 | JU2 | JU3 | JU4 | JU5 |
|---|---|---|---|---|---|
| C000 | A | A | A | A | A |
| C200 | B | A | A | A | A |
| C400 | A | B | A | A | A |
| C600 | B | B | A | A | A |
| C800 | A | A | B | A | A |
| CA00 | B | A | B | A | A |
| CC00 | A | B | B | A | A |
| CE00 | B | B | B | A | A |
| D000 | A | A | A | B | A |
| D200 | B | A | A | B | A |
| D400 | A | B | A | B | A |
| D600 | B | B | A | B | A |
| D800 | A | A | B | B | A |
| DA00 | B | A | B | B | A |
| DC00 | A | B | B | B | A |
| DE00 | B | B | B | B | A |
| E000 | A | A | A | A | B |
| E200 | B | A | A | A | B |
| E400 | A | B | A | A | B |
| E600 | B | B | A | A | B |
| E800 | A | A | B | A | B |
| EA00 | B | A | B | A | B |
| EC00 | A | B | B | A | B |
| EE00 | B | B | B | A | B |

Note: A refers to an inverted address line and B refers to a non-inverted address line.

### Parts List

**Resistors**

*All resistors are ¼-watt, 5%, unless otherwise noted.*

**R1** ..... *4700 ohms*
**R2** ..... *220 ohms*
**R3** ..... *10,000 ohms*

**Capacitors**

**C1–C3** ..... *0.1 µF disc or monolythic*
**C4** ..... *30 pF disc*

**Semiconductors**

**IC1** ..... *74LS30 8-input NAND gate*
**IC2** ..... *74LS04 hex inverter*
**IC3** ..... *2764 EPROM*
**IC4** ..... *74LS123 dual retriggerable monostable multivibrator*
**Q1** ..... *2N2222 NPN transistor*

**Other components**

**JU1–JU5** ..... *3-pin header with shunt jumper*

### Ordering Information

**The following are available from Renton Products P.O. BOX 16271 Seattle, WA 98116 (206) 682 7341**

**Etched and drilled PC Board with gold-plated fingers ..... $14.**

**Complete kit of parts (including programmed EPROM and software on 5¼ inch diskette) ..... $34.**

**Assembled and tested units .. $59.**

**Please add $3 S/H to each order. WA residents add 8.1% sales tax.**

just want to use the board for security, you may want to solder the EPROM to the board. But you could use the board to prototype your own ROM BIOS extensions, in which case you'd want to use a socket.

### Installation

All of the software for PC Access, including a burned EPROM and a copy of the binary file for burning your own EPROM, comes with the kit of parts. (A hex dump of the EPROM is shown in Listing 1.) The software is also available on the RE-BBS (300/1200 8N1, 516-293-2283) in a self-extracting ZIP file called PCACCESS.EXE. You'll need about 160K of disk space to decompress the file.

The general procedure for installing PC Access is to copy all files to the root directory of the boot drive, add a line to CONFIG.SYS, set the card's address, and then install it.

The easiest way to install the software is to log onto your boot drive (C in most cases), place the distribution diskette in drive A, type *A:INSTALL*, and then press Enter. Doing so runs a batch file that copies all files into the root directory of drive C, and also makes the needed change to CONFIG.SYS. If you wish to install the software yourself manually, copy SECURITY.BIN and the *.COM files into the root directory. Then add the following line to your CONFIG.SYS file:

DEVICE = SECURITY.BIN

That must be the first line in CONFIG.SYS; do not put any spaces in the line. In addition, don't rename SECURITY.BIN.

The card has five jumpers that determine the address at which the EPROM resides. The default (factory) setting is D8000h, which should be fine for most systems. If there is a conflict, the computer system may not boot. If there are any problems, remove the card and select a new address using Table 1.

After configuring the jumpers, park your hard drive and turn the computer off. Then install the card in any empty slot.

With the card and the software installed, turn the computer on.

**Listing 1--PC ACCESS EPROM CONTENTS**

```
000000  55 AA 03 FA 8C CA 8E DA BA 00 00 8E C2 BF FF 01
000010  B0 EA 26 88 05 BF 4C 00 BE 00 02 26 8B 05 26 89
000020  04 47 47 46 46 26 8B 05 26 89 04 BF 04 02 B0 01
000030  26 88 05 BF 4C 00 B8 08 04 26 89 05 47 47 8C C8
000040  26 89 05 BF 24 00 BE 10 02 26 8B 05 26 89 04 47
000050  47 46 46 26 8B 05 26 89 04 BE 0F 02 B0 EA 26 88
000060  04 BF 24 00 B8 A6 04 26 89 05 47 47 8C C8 26 89
000070  05 FB B8 01 02 BB 00 00 B9 00 30 8E C1 B9 01 00
000080  BA 80 00 CD 13 BA 00 30 8E DA C7 06 27 10 00 00
000090  C7 06 29 10 00 00 C7 06 2B 10 00 00 C7 06 39 10
0000A0  00 00 BF BE 01 8A 05 3C 80 74 09 8B C7 05 10 00
0000B0  8B F8 EB F1 47 8A 05 8A F0 B4 00 A3 00 10 47 8A
0000C0  05 8A C8 B4 00 A3 02 10 47 8A 05 8A E8 B4 00 A3
0000D0  04 10 B8 01 02 BB 00 30 8E C3 BB 00 00 B2 80 CD
0000E0  13 BA 00 30 8E DA BF 0B 00 BE 06 10 B9 13 00 8A
0000F0  05 88 04 47 46 E2 F8 8B 0E 04 10 8B C1 F7 26 15
000100  10 8B D8 8B 0E 00 10 8B C1 F7 26 13 10 03 C3 8B
000110  D8 8B 0E 02 10 8B C1 03 C3 A3 19 10 8A 1E 0B 10
000120  8A C3 B4 00 F7 26 11 10 8B 1E 19 10 03 C3 A3 1B
000130  10 8B 1E 0C 10 8B C3 D1 E8 D1 E8 D1 E8 D1 E8 25
000140  FF 0F 8B 1E 1B 10 03 C3 A3 33 10 48 A3 1D 10 8B
000150  1E 15 10 8B C3 F7 26 13 10 A3 1F 10 8B 1E 1B 10
000160  8B C3 48 A3 31 10 FF 06 31 10 8B 1E 31 10 8B C3
000170  3B 06 1D 10 76 03 E9 BC 00 8B C3 BA 00 00 F7 36
000180  1F 10 A3 21 10 8B C2 BA 00 00 F7 36 13 10 A3 23
000190  10 8B C2 05 01 00 A3 25 10 8B 1E 25 10 8A CB 8B
0001A0  1E 21 10 8A EB 8B C3 D1 E8 D1 E8 24 C0 0A C8 8B
0001B0  1E 23 10 8A F3 B2 80 BB 00 30 8E C3 BB 00 00 B8
0001C0  01 02 CD 13 BE 00 00 8B C6 3D 00 02 75 03 EB 62
0001D0  90 56 BF D5 03 8C CB 8E C3 B9 0B 00 8A 04 26 3A
0001E0  05 75 1B 46 47 E2 F5 C7 06 27 10 FF FF 5E 56 8B
0001F0  C6 05 1A 00 8B F0 8B 04 2D 02 00 A3 2D 10 5E 56
000200  BF E0 03 B9 0B 00 8A 04 26 3A 05 75 1B 46 47 E2
000210  F5 C7 06 29 10 FF FF 5E 56 8B C6 05 1A 00 8B F0
000220  8B 04 2D 02 00 A3 35 10 5E 8B C6 05 20 00 8B F0
000230  EB 95 E9 31 FF 90 8A 1E 08 10 8B C3 B4 00 F7 26
000240  2D 10 8B 1E 33 10 03 C3 A3 2F 10 8B D8 BA 00 00
000250  F7 36 1F 10 A3 21 10 8B C2 BA 00 00 F7 36 13 10
000260  A3 23 10 8B C2 05 01 00 A3 25 10 8B 1E 25 10 8A
000270  CB 8B 1E 21 10 8A EB 8B C3 D1 E8 D1 E8 24 C0 0A
000280  C8 8B 1E 23 10 8A F3 B2 80 BB 00 30 8E C3 BB 00
000290  00 B8 01 02 CD 13 BE 00 00 BF EB 03 8C CB 8E C3
0002A0  BB 00 30 8E DB B9 15 00 8A 04 3C 61 72 06 3C 7A
0002B0  77 02 2C 20 26 3A 05 75 0A 46 47 E2 EB C7 06 2B
0002C0  10 FF FF 8A 1E 08 10 8B C3 B4 00 F7 26 35 10 8B
0002D0  1E 33 10 03 C3 A3 37 10 8B D8 BA 00 00 F7 36 1F
0002E0  10 A3 21 10 8B C2 BA 00 00 F7 36 13 10 A3 23 10
0002F0  8B C2 05 01 00 A3 25 10 8B 1E 25 10 8A CB 8B 1E
000300  21 10 8A EB 8B C3 D1 E8 D1 E8 24 C0 0A C8 8B 1E
000310  23 10 8A F3 B2 80 BB 00 30 8E C3 BB 00 00 B8 01
000320  02 CD 13 B8 00 30 8E D8 8C C8 8E C0 BE 0A 00 BF
000330  00 04 B9 08 00 8A 04 26 3A 05 75 0A 47 46 E2 F5
000340  C7 06 39 10 FF FF 90 8B 1E 27 10 0B DB 75 03 EB
000350  23 90 8B 1E 29 10 0B DB 75 03 EB 18 90 8B 1E 2B
000360  10 0B DB 75 03 EB 0D 90 8B 1E 39 10 0B DB 75 03
000370  EB 02 90 CB B4 0F CD 10 24 7F B4 00 CD 10 B4 02
000380  B7 00 BA 00 02 CD 10 8C CA 8E DA BF A5 03 8A 05
000390  0A C0 74 0F 57 1E B4 0E B7 00 B3 07 CD 10 1F 5F
0003A0  47 EB EB EB FE 41 43 43 45 53 53 20 44 45 4E 49
0003B0  45 44 20 2D 2D 2D 20 49 4D 50 52 4F 50 45 52 20
0003C0  53 59 53 54 45 4D 20 43 4F 4E 46 49 47 55 52 41
0003D0  54 49 4F 4E 00 43 4F 4E 46 49 47 20 20 53 59 53
0003E0  53 45 43 55 52 49 54 59 42 49 4E 44 45 56 49 43
0003F0  45 3D 53 45 43 55 52 49 54 59 2E 42 49 4E 0D 0A
000400  50 38 32 58 5A 5A 43 56 80 FC 00 75 25 80 FA 00
000410  75 20 50 52 1E 57 BA 00 00 8E DA BF 04 02 8A 05
000420  3C 01 74 03 EB 08 90 5F 1F 5A 58 EB 0A 90 5F 1F
000430  5A 58 EA FF 01 00 00 50 53 51 52 1E 06 57 56 55
000440  FB B4 0F CD 10 24 7F B4 00 CD 10 B4 02 B7 00 BA
000450  00 02 CD 10 BF 8C 04 8C CA 8E DA 8A 05 0A C0 74
000460  0C 57 B4 0E BB 00 01 CD 10 5F 47 EB EA 5D 5E 5F
000470  07 1F 5A 59 5B 58 57 83 C4 06 8B FC 36 8B 05 0D
000480  01 00 36 89 05 83 EC 06 5F B4 80 CF 44 72 69 76
000490  65 20 41 20 41 63 63 65 73 73 20 44 65 6E 69 65
0004A0  64 20 0D 0A 0A 00 1E 52 57 50 BA 00 00 8E DA BF
0004B0  04 02 8A 05 0A C0 74 09 BF 17 04 8A 05 24 F3 88
0004C0  05 58 5F 5A 1F EA 0F 02 00 00 FF FF FF FF FF FF
0004D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0004E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0004F0  9B FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000500  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  . . .
  . . .   The rest of the EPROM consists of FF's
  . . .
001FF0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

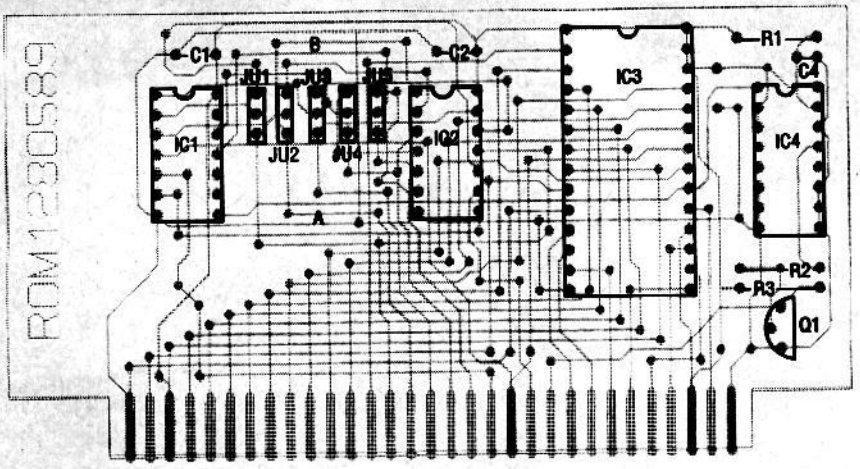



***Fig. 2.*** *PARTS AND JUMPER LOCATIONS. Mount all components as shown here. Table 1 shows how to configure the jumpers for various addresses.*

If all has gone well, any floppy disk in drive A will be ignored and you will be prompted for a password. The default master password is SECURITY. You can change the master password and the user passwords with LOCK.COM, and individual passwords with CHANGE.COM.

To uninstall the security system, delete the DEVICE = SECURITY.BIN line from CONFIG.SYS, park the hard drive, turn the computer off, and remove the card.

## Software

What follows are brief descriptions of the PC Access utility programs. LOCK.COM and CHANGE.COM are provided to establish the passwords and user ID's. A user can alter his or her own password using CHANGE; the system administrator can use LOCK to change the master password, any user ID, and any user password. You can optionally require users to type in both the user ID and the password each time the system boots. But even if you don't require the user ID to be typed in, the audit trail will log it.

HOLD.COM allows a user to suspend computer access until the correct password is entered. HOTKEY establishes what key combination triggers the hold function. HOLDOFF.COM removes HOLD.COM from memory.

The FINDROMS program helps locate a free segment in high memory. It searches for the 55AA pattern that signifies a BIOS extension, and reports on any that it finds.

TRAIL.COM can be executed by AUTOEXEC.BAT to record user ID, access date, and access time. TRAIL should be one of the first programs in AUTOEXEC.BAT (after running any programs needed to update time and date from a real-time clock).

The audit file (a hidden system file) can be decoded by use of AUDIT.COM, as follows:

AUDIT Filename

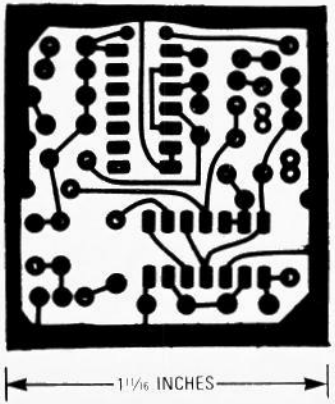
After you hit the RETURN key, AUDIT will prompt the user for the master password. After the password is entered correctly, AUDIT will decode audit trial entries from the encoded file and append them to the specified file. If no file exists with the given filename, a new file will be created. The audit trail will then be cleared of entries. This function works even if user ID's are not required for system access.

## Conclusion

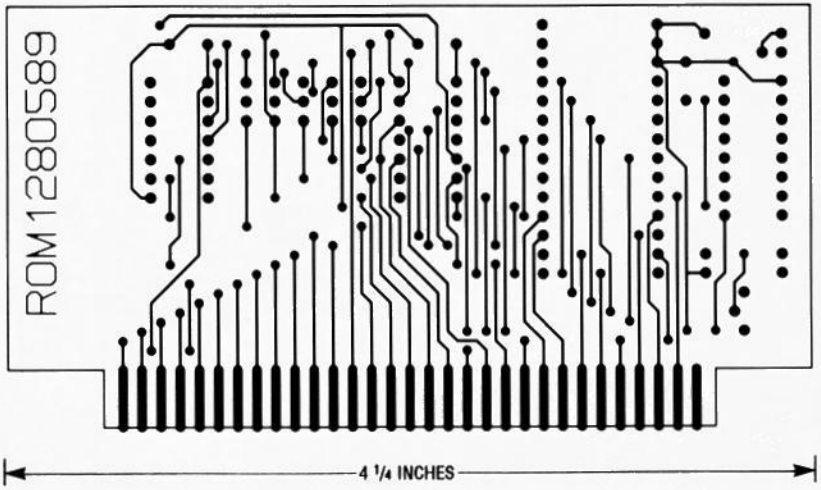
PC Access is inexpensive, easy to build and install, yet nonetheless provides a significant deterrent to unauthorized access to your hard drive.

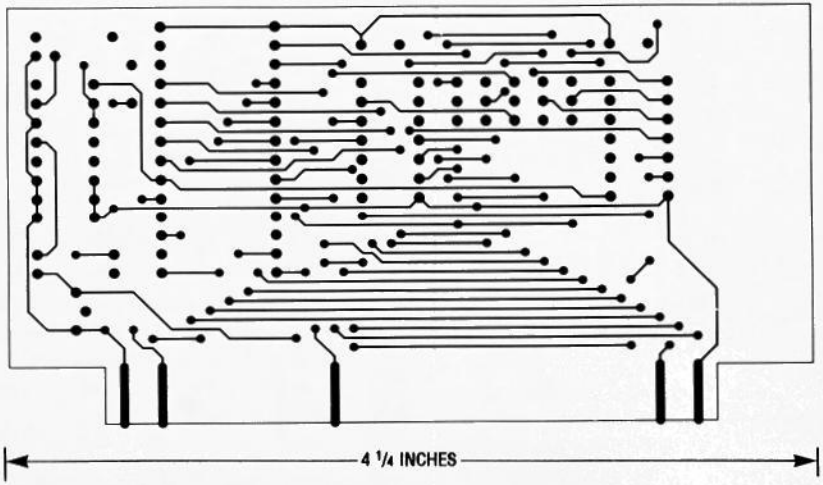
Additionally, the PC Access circuit board can be used to develop other ROM extensions. Not only does the PC Access give you an inexpensive way to protect your computer, it also provides an excellent flat form that allows you to learn more about how your computer works.◆CD◆

# PC SERVICE




**FOIL PATTERN** for the windshield-wiper delay unit.




**ABOVE RIGHT** is the component side of the PC Access. At right is the solder side.