# PCSE: A Design Implementation for PC Security



**Editor's Note: This paper was awarded Second Prize in the Computer Security category of the 1988 CISI Essay Contest.**

***A prototype device called a Personal Computer Security Enhancement (PCSE) has been developed by the Secure Applications and Components group of the National Computer Security Center. A much needed security device for the widely used IBM PC, PCSE offers an inexpensive means to provide user authentication and access control. The PCSE device will provide increased security at a cost-effective price. This paper describes the security features of the PCSE project, how they were implemented, and the benefits of equipping PCs with them.***

## INTRODUCTION

Widespread and prolific personal computer usage has heightened concern over data loss through these usually unprotected machines. In response to this concern, the National Computer Security Center (NCSC) has assigned a research group the task of investigating solutions for PC security. Called the Secure Applications and Components Branch, its current focus for research is one of the most popular and widely used PCs, IBM PCs and compatibles, in developing methods to bolster PC security. Called PC Enhancements (PCE), the objective of the research is to address security needs in PC processing environments while retaining the features that have made PCs popular.

The first by-product of the research is an engineering solution for PC security called a Personal Computer Enhancement (PCSE). Designed to improve security, yet be affordable (costing between $150 and $200), the device is intended to help meet current and future needs in PC security.

## VULNERABILITIES

The greatest vulnerabilities that PCs present are usually architecturally based in the computer design. For example, the IBM PC/XT architecture will allow

- User applications to read and write anywhere in memory, including operating system object code.
- User written programs and user utilities to read and write the boot track, directory, file allocations table, and files marked with system or hidden attributes.
- The entire operating system to be replaced trivially.[1]

1. "Threats and Vulnerabilities." Briefing by Mr. Thomas Lunzer, Personal Computer Information Security Conference, Arlington, Virginia, 9–10 May 1988.

Due to the incapabilities of microprocessors, most PCs lack architectural features to implement security mechanisms commonly available in larger computer systems. PCs cannot support adequate password protection, access control, or user authentication. Lack of separation between an operating system, user application programs, and use of files makes computer handled data vulnerable to possible compromise (i.e., unauthorized access, Trojan Horses, Trap Doors, etc.). There are a number of commercial retrofit security products available for PCs; however, few take into fundamental consideration the architectural weakness of a machine like the IBM PC/XT.

## APPROACHING A SOLUTION

In reviewing the basic requirements to implement PC computer security, creating a secure logon procedure was a primary PCSE design consideration. The ensuring of logon access after power up was considered mandatory before progressing to other enhancements. There was a clear need to ensure that only authorized persons could use a given PC.

Access to data stored on PCs is restricted through the turn of a power switch. Once a PC is powered up, any user (authorized or not) is capable of accessing any resident files on the hard disk of a PC. In terms of the Trusted Computer System Evaluation Criteria (TCSEC), the PCE team sought a method to implement user identification and authentication for PCs. Identification and authentication ensures that only authorized users are granted access to a computer and the data residing in it. Therefore, PC user identification and authentication means ensuring that only authorized users can access a PC and PC-resident data.

In researching logon methods, the PCE team reviewed existing commercial products for consideration in implementing a secure PC logon procedure. It was discovered that many commercially available products only add programming code to the autoexec.bat file, must depend upon an operating system, or rely upon software files resident on hard disk. For application in the PCSE design, most commercially available PC security products are considered unsatisfactory because they can be

- *Bypassed.* PCs first "look" for an operating system in drive A before the hard disk (drive C). "Surrogate" copies of an operating system could be used from drive A to bypass a drive C resident operating system and an autoexec.bat file.
- *Replaced.* The hard disk resident autoexec.bat file could be replaced by another one which would allow unauthorized access.
- *Modified.* The existing hard disk resident autoexec.bat file could be modified to include other routines inserted by a perpetrator.
- *Spoofed.* Spoofing, a major concern, is the process of inserting a program that mimics a logon procedure. A spoofing program would prompt users for their password and then record it for later retrieval by its originator.

The PCE team approached PC security by requiring that a logon procedure be executed before an operating system could be loaded. A thorough understanding, therefore, of how the IBM PC powers up, initializes itself, and turns control over to an operating system was needed before the team could proceed.

The PCE research team initially proposed modification of the ROM-BIOS routines to ensure that a logon procedure would indeed be secure. If a logon procedure could be invoked before transfer of control to an operating system or user, the procedure would inherently be more secure.

Rewriting the existing PC ROM-BIOS was considered impractical. The PCE team proposed, therefore, that a ROM-BIOS extension be included in an expansion board to fit into one of the eight expansion slots standardly available in IBM PCs (see fig. 2).

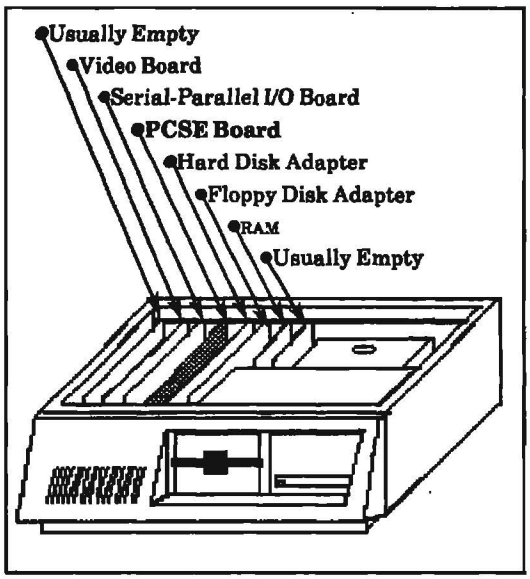


**Fig. 2. PC hardware expansion board arrangement**

The extension could then be supported by additional memory to provide an area to retain necessary security data. As research proceeded, a design intent emerged to make the PCSE device an affordable ($150 to $200) PC security feature that would not cause degradation of PC performance or affect basic compatibility, flexibility, and functionality of existing PCs.

PCE engineers conducted a study of the existing PC BIOS routines. Available BIOS documentation was thoroughly reviewed before initial attempts were made to write a PCSE ROM-BIOS extension code. The intensive programming task was then split into modular sections and sequentially completed.

## IMPLEMENTATION

During 1988, the PCE team began to prototype their expansion board design. The PCSE ROM-BIOS extension resides on the expansion board and interacts with a Random Access Memory (RAM) chip containing access tables referenced by the BIOS extension. The PCSE device design capitalizes on the basic operations of the BIOS. When the PCSE BIOS extension is encountered, control is passed from the PC BIOS to it. The first routines run by the extension implement the PCSE logon.

## THE BIOS

IBM PC architecture was considered revolutionary at the time of its release. IBM did not develop their own operating system software but chose to use the Microsoft Corporation Disk Operating System (MS DOS) instead. PC machine development required only that IBM create a set of support program routines (written in assembly language) known as the Basic Input Output System (BIOS) to be stored in Read Only Memory (ROM) hardware. The BIOS is one of the reasons that the IBM PC is flexible and has become so popular. It has allowed system upgrades without requiring IBM to develop an entirely new machine.

When an IBM PC power switch is turned on, the machine begins operating in hardware. One of the first operations conducted by the PC after power up is the execution of the BIOS stored in the PC ROM area. The PC BIOS routines do a power on self-test, a PC memory check, and an attached equipment check before searching for an operating system on drive A. If a diskette or operating system is not present in drive A, the routines check the hard disk. Once found and retrieved by the BIOS, control is given to the operating system and the user (see fig. 1).

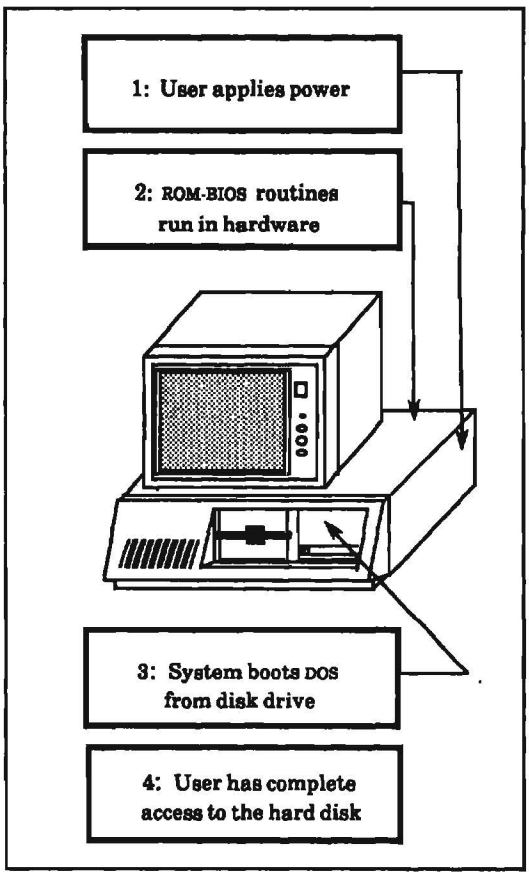


**Fig. 1. Standard PC logon procedure**

The PCSE ROM-BIOS logon routines determine if a user logon attempt is valid by referencing an access table in a secure memory area on the PCSE board (see figs. 2 and 3). If valid, the PCSE ROM-BIOS extension disables access to the secure memory area, then returns control back to the standard BIOS routines that run normally. If a login attempt is invalid, a set number of attempts are allowed (set by a security administrator) before a restart of the PC is required.

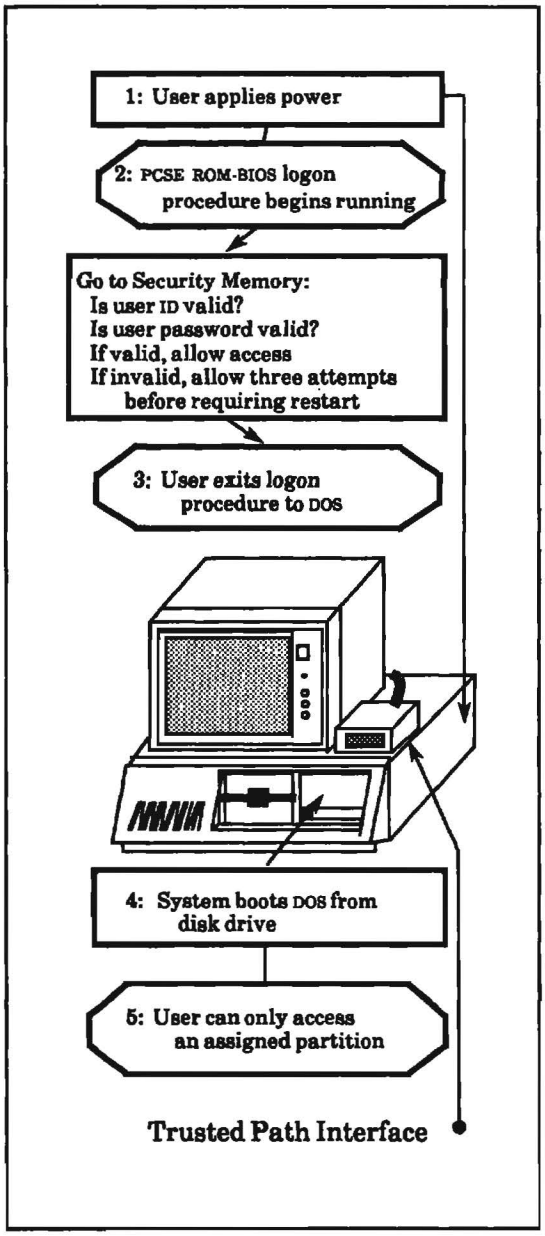


**Fig. 3. PCSE logon procedure**

## TRUSTED PATH INTERFACE

The PCSE design includes a Trusted Path Interface that is connected directly to the PCSE expansion board. The Trusted Path Interface, an external box hardwired to the PCSE expansion board DB-25 connector, offers insurance against user spoofing. The box houses two 8-character alphanumeric displays. PCSE uses this display to directly show what PCSE mode of operation is being used (see fig. 4). The Trusted Path Interface is locked-up before PCSE returns control to the BIOS routines. The display, therefore, cannot be overwritten by malicious software attempting to spoof the PCSE login. If a spoof attempt occurs, the display would show that the interface is not operating in normal mode, indicating to the user that something is wrong.

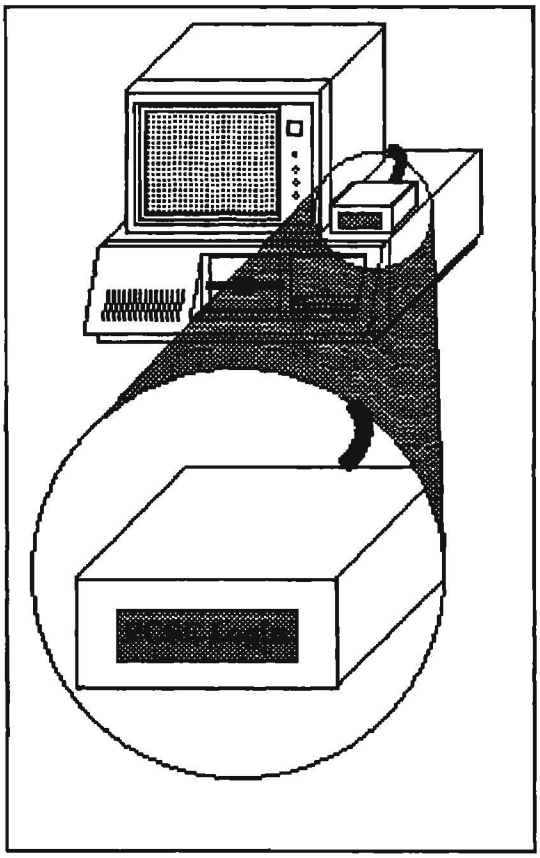

**Fig. 4. PCSE trusted path interface**

During login, the Trusted Path Interface will display "PCSE login." Using this interface feature, users can visually verify whether they are being spoofed, or identify what user mode they are in. The use of this interface, along with the PCSE ROM-BIOS logon procedure, adequately addresses the absence of user identification and authentication in standard PCs.

## SECURITY MEMORY

The PCE development team recognized that storage and protection of memory access information is an implicit problem for ensuring authorized user logon. Access control schemes using access information stored in readable files can be subject to possible circumvention, replacement, or alteration. Several utility programs (Debug, Norton Utilities, etc.) allow the perusal of storage space (disk or ROM areas) by users. In the design phase of the PCSE device, therefore, it was determined that the ROM-BIOS extension needed an area from where access information could be securely retrieved. The information stored in this area would be used for comparison against user login and in defining user profiles. Additionally, the needed memory area would also require protection from utility program perusal.

Assignment of a separate memory chip to contain security relevant data was the PCE solution for protecting access control information. Consisting of a battery-backed RAM chip, security memory contains security relevant information such as user profiles (user machine and recording media access rights) defined by a system security administrator.

When the PCSE logon procedure is running, the Security Memory chip is enabled for use by the ROM-BIOS extension routines and then disabled before control is given to an operating system. Disabling PCSE security memory RAM through hardware, therefore, protects the security memory area from utility program perusal.

## OBJECT REUSE

Memory space on a standard IBM PC/XT or AT hard disk is assigned using record pointers. Record pointers indicate ("point" to) the location on recording media of the beginning of a file. When PC files are erased only the record pointer is removed, not the data starting at the pointer location on the media. After pointer erasure, the pointer location and the recording area following it can be used to place a new pointer and data (the saving of a new file). If the space is not reused, however, then the data still remaining on the recording media (disk) following the erased pointer can be recovered by specialized utility programs. Utility programs with file recovery options (Norton Utilities, for example) can recover files with erased record pointers. Files with erased record pointers are recoverable if subsequent new files have not been saved over the storage area to be recovered.

Though many available recovery programs were designed for the retrieval of accidentally erased files, they can be used for the recovery of remnant data left by other users. Known as object reuse or magnetic remanence, the problem has become a concern in the sharing of different types of magnetic media, including the IBM PC hard disk.

## PC DISK PARTITIONING

Coupled with the problems of object reuse, separation of data between more than one user of a machine is a problem of growing importance. Ensuring separation of data between users was an important design consideration for the PCE team.

> There are no provisions for data labeling (in PCs). Controlled sharing of data is very difficult: none of the software is trusted and object reuse problems make it impossible to know exactly what data is being shared.[2]

One way of separating data often used in large systems is called partitioning. Partitioning of magnetic media is a method of ensuring that a user (or user group) can only use an assigned area of storage memory. In mainframe computers, data separation is commonly enforced by an operating system or security kernel that allocates memory for use by one or a defined set of users. In PCs, the Disk Operating System (DOS) and the 8088/8086 microprocessor used in the design architecture will not securely support mechanisms that separate data and protect memory areas containing information such as access tables. Analysis of the architectural weaknesses of the IBM PC prompted a PCE design proposal to include hard disk partitioning through the PCSE BIOS extension. Data labeling was not proposed because the PC design architecture is considered incapable of supporting a security kernel that is necessary for data labeling.

PC disk partitioning has been implemented recently in the PCSE prototype. The PCSE expansion board ROM-resident partitioning mechanism restricts unauthorized access, modification, and copying of information stored on the hard disk between authorized users. PCSE security administrators define the access rights per user (user profile) in PCSE security memory access tables. The PCSE ROM-BIOS extension uses these tables to set user privileges after login. PCSE partitioning is also transparent at the user level. After logon, users will be able to choose from and use only what has been previously allocated for their use (see fig. 5).

Including partitioning in the PCSE design has provided the following security attributes:

- Confinement of PC object reuse to defined areas of storage memory between a defined set of users. PCSE object reuse can occur only between user partitions with similar read and write access as defined by a security administrator in PCSE security memory.
- Confinement of malicious code (Trojan Horses, Viruses, etc.) to defined and manageable areas of storage memory.
- Separation of user files and access rights between several users of a single PC.
- The ability to separate access rights between several machines in a multiple PC processing environment.

## DESIGN SUMMATION

Like the machine that it has been built to secure, the PCSE prototype is designed to be upward compatible. In its present phase of development, the prototype is currently fieldable as a PC logon and partitioning device that will operate with the IBM PC, IBM PC/XT, or the IBM PC/AT. Current developments in the design include allowing data transfers between partitions that will allow read and write access to files in more than one partition. Proposals for future PCSE design developments include disk encryption and use of the advanced features available in IBM PC upward compatible machines. PCSE additions could capitalize on features such as protected mode (making it possible to introduce security kernels), trusted application loaders, data encryption, or smart cards for user authentication.

2. "In-House Research and Development Work Plan for PC Security Enhancements." Investigative report by [redacted] PCSE Team Chief, 2 December 1986.

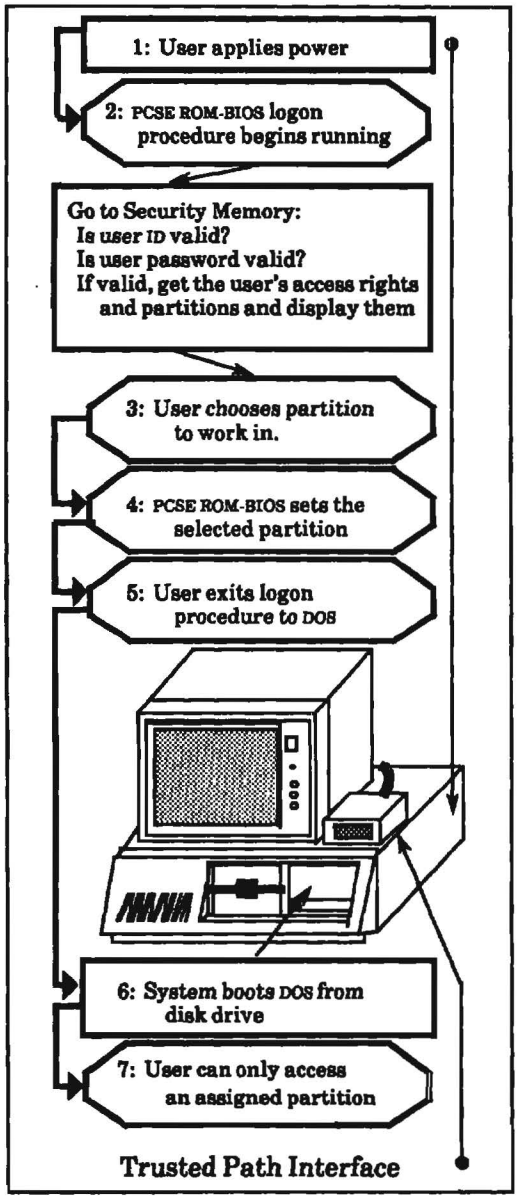


**Fig. 5. Partitioned PC system**

## CONCLUSION

Concentrating on the many vulnerabilities present in processing environments of today, the focus of the NCSC Secure Applications and Component Branch has been to create an affordable means of providing PC security.

PCSE research began with a thorough study of PC operations and vulnerabilities. Prototype development began by concentrating on implementing user identification and authentication before an operating system could be loaded. Through an expansion board, PCE engineers created a logon procedure that operates as an extension of the existing PC ROM-BIOS. Executing before an operating system is loaded, this procedure helps control access to PCs and is operating system independent. The PCSE design team used the ROM-BIOS extension and logon procedure as an initial step in creating a foundation on which to build other security enhancements.

Currently fieldable as a retrofit security device for PC security, the current PCSE prototype includes the following:

- *Logon Procedure.* An assembly language routine implemented through a PCSE ROM-BIOS extension. Implemented through ROM, the procedure offers an operating system independent method of providing user identification and authentication.
- *Security Memory.* A storage area in a battery-backed RAM chip. The area stores information for user access and privilege (user profiles) as defined by PCSE security administrators. The chip is enabled for use by the PCSE ROM extension and then disabled before an operating system is loaded.
- *Trusted Path Interface.* Designed to prevent spoofing, it is an external box with an alphanumeric display mounted externally to a PC. Connected directly to the PCSE expansion board, this display verifies to the user what PCSE function or operation is being enforced.
- *Device/Function Access Control.* Access to computer functions and peripheral devices can be defined by PCSE security administrators on a per user basis.
- *Hard Disk Partitioning.* A method of separating memory storage areas between authorized users on a PC hard disk.

The PCSE design provides PC protection at a reasonable cost. Development of the prototype expansion board has shown that there is a functional method of implementing authentication and identification in PCs through the use of ROM-BIOS extension.

## EPILOGUE

Since September 1988, the PCSE development team has completed the initial prototype phase of the project. An optional Trusted Path Interface was developed as a cost effective replacement for the alphanumeric display version. It consists of a single LED display. Nine prototype printed wiring boards were manufactured by R9 and reviewed for design reproduction, T2 reconfigured the expansion board circuit layout for production of 100 prototype boards, and C1 will be evaluating the device against the subsystem criteria of the Trusted Computer Security Evaluation Criteria (TCSEC) before the prototypes are released for operational testing and evaluation.

This phase of the PCSE design effort represents a consolidation of research and development by C3 over a brief period of time. The Secure Applications and Components Branch is pursuing further research and development of PCSE through testing the device against known PC computer viruses. This will help determine the PCSE device feasibility in restricting or containing the propagation of computer viruses. PCE engineers are also currently interfacing a smart card reader into the PCSE device. Authorized users will be required to insert a smart card and enter a personal identification number (PIN) before they can use a PCSE equipped PC.

STATUTORILY EXEMPT

*Acknowledgments*

I would like to thank the members of the Secure Applications and Components PC Enhancements engineering team: [redacted] for their critiques and advice in preparing this paper on PCSE.

[redacted]

STATUTORILY EXEMPT

BIBLIOGRAPHY

[redacted] "In-House Research and Development Work Plan for PC Security Enhancements." Investigative report for the Office of Research and Development, National Computer Security Center, 2 December 1986. P.L. 86-36

[redacted] "A First Step Towards Personal Computer Security." Office of Research and Development, National Computer Security Center.

Lunzer, Thomas. "Threats and Vulnerabilities." A briefing presented to the Personal Computer Information Security Conference, Arlington, Virginia, 9–10 May 1988.

[redacted] "Personal Computers Products Listing." Office of Research and Development, National Computer Security Center database of commercially produced products, 29 June 1988.

[redacted] "Personal Computers and Security." Office of Research and Development, National Computer Security Center, 22 June 1988.