7600010-4
IBOS COPY

PERSONAL COMPUTER SYSTEM WITH SECURITY FEATURES AND METHOD

Technical Field

This invention relates to personal computer systems and, more particularly, to such a system having security features enabling control over access to data retained in such a system.

Background to the Invention

Personal computer systems in general and IBM personal computers in particular have attained widespread use for providing computer power to many segments of today's modern society. Personal computer systems can usually be defined as a desk top, floor standing, or portable microcomputer that consists of a system unit having a single system processor and associated volatile and non-volatile memory, a display monitor, a keyboard, one or more diskette drives, a fixed disk storage, and an optional printer. One of the distinguishing characteristics of these systems is the use of a motherboard or system planar to electrically connect these components together. These systems are designed primarily to give independent computing power to a single user and are inexpensively priced for purchase by individuals or small businesses. Examples of such personal computer systems are IBM's PERSONAL COMPUTER AT and IBM's PERSONAL SYSTEM/2 Models 25, 30, 35, 40, L40SX, 50, 55, 57, 65, 70, 80, 90 and 95.

These systems can be classified into two general families. The first family, usually referred to as Family I Models, use a bus architecture exemplified by the IBM PERSONAL COMPUTER AT and other "IBM compatible" machines. The second family, referred to as Family II Models, use IBM's MICRO CHANNEL bus architecture exemplified by IBM's PERSONAL SYSTEM/2 Models 50 through 95. Early Family I models typically used the popular INTEL 8088 or 8086 microprocessor as the system processor. Certain later Family I and the Family II models typically use the high speed INTEL 80286, 80386, and 80486 microprocessors which can operate in a real mode to emulate the slower speed INTEL 8086 microprocessor or a protected mode which extends the addressing range from 1 megabyte to 4 Gigabytes for some models. In essence, the real mode feature of the 80286, 80386, and 80486 processors provides hardware -

compatibility with software written for the 8086 and 8088 microprocessors.

With the phenomenal growth and use of personal computers in the world in recent years, more and more data or information is being collected and retained or stored in such systems. A lot of this data is sensitive in nature. In the wrong hands, data could become embarrassing to individuals, a company could lose a competitive edge, or sensitive data could be used to force payment for silence or lead to physical violence against individuals. As more users recognize the sensitive nature of data and its value, the more it becomes desirable to protect against such misuse. To protect themselves and the persons associated with the stored data, users are requiring incorporation of security and integrity features into the personal computers that they purchase. Users are not the only people to recognize the sensitivity of the data being collected and stored. Governments are also enacting laws to enforce protection of sensitive data. One such government is that of the United States. It has recognized and responded to the gravity of the situation. The United States federal government has defined security levels and the associated requirements it takes to meet those levels, and provides a certification agency for personal computer manufacturers to submit their personal computers in order to see if the systems meet the security level claimed by the manufacturer. The source for the Federal Requirements is the Department of Defense, Trusted Computer System Evaluation Criteria, DOD 5200.28 STD, 12/85, generally referred to as The Orange Book. The government has legislated that by January 1, 1992 all data related to the government must only be processed and stored on personal computers with a minimum security level of C-2. As regards computer system hardware, the essence of the requirements is contained in the Assurance section, Requirement 6: "trusted mechanisms must be continuously protected against tampering and/or unauthorized changes... "

Beginning with the earliest personal computer system of the Family I models, such as the IBM Personal Computer, it was recognized that software compatibility would be of utmost importance. In order to achieve this goal, an insulation layer of system resident code, also known as "firmware", was established between the hardware and software. This firmware provided an operational interface between a user's application program/operating system and the device to relieve the user of the concern about the characteristics of hardware devices. Eventually,

the code developed into a Basic Input/Output System (BIOS), for allowing new devices to be added to the system, while insulating the application program from the peculiarities of the hardware. The importance of BIOS was immediately evident because it freed a device driver from depending on specific device hardware characteristics while providing the device driver with an intermediate interface to the device. Since BIOS was an integral part of the system and controlled the movement of data in and out of the system processor, it was resident on the system planar and was shipped to the user in a read only memory (ROM). For example, BIOS in the original IBM Personal Computer occupied 8K of ROM resident on the planar board.

As new models of the personal computer family were introduced, BIOS had to be updated and expanded to include new hardware and I/O devices. As could be expected, BIOS started to increase in memory size. For example, with the introduction of the IBM PERSONAL COMPUTER AT, BIOS grew to require 32K bytes of ROM.

Today, with the development of new technology, personal computer systems of the Family II models are growing even more sophisticated and are being made available to consumers more frequently. Since the technology is rapidly changing and new I/O devices are being added to the personal computer systems, modification to the BIOS has become a significant problem in the development cycle of the personal computer system.

For instance, with the introduction of the IBM Personal System/2 with Micro Channel architecture, a significantly new BIOS, known as advanced BIOS, or ABIOS, was developed. However, to maintain software compatibility, BIOS from the Family I models had to be included in the Family II models. The Family I BIOS became known as Compatibility BIOS or CBIOS. However, as previously explained with respect to the IBM PERSONAL COMPUTER AT, only 32K bytes of ROM were resident on the planar board. Fortunately, the system could be expanded to 96K bytes of ROM. Unfortunately, because of system constraints, this turned out to be the maximum capacity available for BIOS. Luckily, even with the addition of ABIOS, ABIOS and CBIOS could still squeeze into 96K of ROM. However, only a small percentage of the 96K ROM area remained available for expansion. It has been believed that, with the addition of future I/O devices, CBIOS and ABIOS will eventually run out of ROM space. Thus, new

I/O technology will not be able to be easily integrated within CBIOS and ABIOS.

Due to these problems, plus the desire to make modifications in Family II BIOS as late as possible in the development cycle, it became necessary to offload portions of BIOS from the ROM. This was accomplished by storing portions of BIOS on a mass storage device such as a fixed disk, preferably in a defined portion of such a disk known as a system partition. Since a disk provides writing as well as reading capabilities, it became feasible to modify the actual BIOS code on the disk. The disk, while providing a fast and efficient way to store BIOS code, nevertheless greatly increased the probability of the BIOS code being corrupted. Since BIOS is an integral part of the operating system, a corrupt BIOS could lead to devastating results and in many cases to complete failure and non-operation of the system. Thus, it became quite apparent that a means for preventing unauthorized modification of the BIOS code on the fixed disk was highly desirable. This was the subject matter of U.S. Patent Application Ser. No. 07/398,820, filed 08/25/89, and now United States Patent 5,022,077 issued 4 June 1991. The interested reader is referred to that patent for additional information possibly helpful in understanding of the invention here disclosed, and the disclosure of that patent is hereby incorporated by reference into this specification to any extent necessary to a full understanding of the inventions here disclosed.

With the introduction of IBM's PS/2 Micro Channel Systems came the removal of switches and jumpers from I/O adapter cards and planar. The Micro Channel Architecture provided for programmable registers to replace them. Utilities to configure these programmable registers or programmable option select (POS) registers were required. These, and other utilities to improve system usability characteristics along with system diagnostics, were shipped with each system on a system reference diskette.

Prior to initial use, each Micro Channel System requires that its POS registers be initialized. For example, if the system is booted with a new I/O card, or a slot change for an I/O card, a configuration error is generated and the system boot up procedure halts. The user is then prompted to load the system reference diskette and press the F1 key. A "Set Configuration Utility" can then be booted from the system reference

diskette to configure the system. The Set Configuration Utility will prompt the user for the desired action. If the appropriate I/O card's descriptor files are loaded on the system reference diskette, the Set Configuration Utility will generate the correct POS or configuration data in non-volatile storage. The descriptor file contains configuration information to interface the card to the system.

Brief Description of the Invention

With the foregoing in mind, the present invention contemplates that a personal computer of the type described have provided therein and in its operation means for limiting access to certain critical data to only those users have a proper privilege to access such data. In realizing this purpose of the invention, a specialized memory element is provided for receiving and storing a Privileged Access Password (sometimes hereinafter called a "PAP") and for coordinating the access granted to various functions and data to the activation and usage of the PAP.

The invention further contemplates that a user may have choices to activate or inactivate the security provisions made available, so that the system can be adapted to varying needs or desires for securing the usage of the system. In realizing this purpose of the invention, a system configured as contemplated by this invention may be adapted to the security requirements of governmental standards if desired and yet also used in an essentially unsecured manner should the circumstances of use so permit. Thus users of such systems are given great flexibility in application of the systems.

Brief Description of the Drawings

Some of the objects of the invention having been stated, other objects will appear as the description proceeds, when taken in connection with the accompanying drawings, in which:

Figure 1 is a perspective view of a personal computer embodying this invention;

Figure 2 is an exploded perspective view of certain elements of the personal computer of Figure 1 including a chassis, a cover, and a planar board and illustrating certain relationships among those elements;

Figure 3 is a schematic view of certain components of the personal computer of Figures 1 and 2;

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

Figures 4 and 5 are schematic representations of certain components of the personal computer of Figures 1 and 2 which are related to the security features of the present invention;

Figure 6 is an enlarged scale perspective view of certain components illustrated in Figures 4 and 5;

Figure 7 is a view similar to Figure 6 of certain optional components of the personal computer of Figures 1, 2, 4 and 5 which are related to the security features of the present invention; and

Figures 8, 9a and 9b are schematic flow charts of certain functions involved in the security options available in accordance with the present invention.

Detailed Description of Invention

While the present invention will be described more fully hereinafter with reference to the accompanying drawings, in which a preferred embodiment of the present invention is shown, it is to be understood at the outset of the description which follows that persons of skill in the appropriate arts may modify the invention here described while still achieving the favorable results of this invention. Accordingly, the description which follows is to be understood as being a broad, teaching disclosure directed to persons of skill in the appropriate arts, and not as limiting upon the present invention.

Certain defined terms may be used herein, as follows:

TRUSTED COMPUTING BASE (TCB): The totality of protection mechanisms within a computer system -- including hardware, firmware and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g. a user's clearance) related to the security policy.

TRUSTED SOFTWARE: The software portion of a Trusted Computing Base.

REFERENCE MONITOR CONCEPT: An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

SECURITY KERNEL: The hardware, firmware and software elements of a Trusted Computing Base that implement the reference monitor concept. It

must mediate all accesses, be protected from modification and be verifiable as correct.

TRUSTED COMPUTER SYSTEM: A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

SYSTEM OWNER: The system owner is the user who is responsible for configuring and placing a system in secure mode initially. The system owner will control configuration both initially and whenever an update needs to be made. This person will control the Privileged Access Password and be responsible for maintaining its integrity. The system owner will also maintain physical security of the tamper evident cover keylock key. The system owner will be responsible for maintaining security logs on all systems. The system owner will also have to record all attempted security breaches. The system owner may own more than one system. The system owner is considered an authorized user and can also be a normal user.

SECURE MODE: When a system owner has successfully installed the Privileged Access Password on a personal computer system to invoke security protection provided by the security and integrity elements.

AUTHORIZED USER: Any user who is given permission to use the Privileged Access Password. This person may or may not be the system owner. This person may also have a key for a particular system or a set of systems. If this person is involved in recovering a system from a security breach, they are responsible for reporting it to the system owner. An authorized user may also be a normal user.

NORMAL USER: Any user of the systems authorized to use the systems facilities. In order to change a systems configuration or fix a problem, this user requires the assistance of either the system owner or an authorized user. The normal user does not have the Privileged Access Password or the cover key unless they belong to either the authorized user or system owner category.

UNAUTHORIZED USER: Any one not defined as a system owner, authorized user or normal user. Any use of a secured personal computer system by an unauthorized user is considered a security breach, other than an unsuccessful power on, and an audit trail must exist showing such breaches.

EEPROM: Electrically Erasable Programmable Read Only Memory. This memory technology provides for non-volatile storage of data that can be changed under control of hardware logic. Contents of storage is not lost when power is absent. Contents may be altered only when the

appropriate controls signals on the module are activated in the predefined sequence.

PASSWORD DESCRIPTION: The system has the potential to be protected by two passwords: 1. Privileged Access Password (PAP) and 2. Power On Password (POP). These passwords are intended to be used independently of one another. The PAP is designed to provide protection for the system owner by protecting the Initial Program Load (IPL) device boot list, access to the password utility, and access to the System Reference Diskette or System Partition. The System Partition will only be booted in response to a POST error if there is no PAP installed or the PAP was entered initially during the power on sequence. Initial BIOS Load (IBL) from a diskette will be secured in the same manner as booting the System Reference Diskette. The existence of the PAP will be transparent to a normal user using the POP. The PAP will be installed, changed,or deleted by a utility on the System Reference Diskette or in the System Partition. The PAP, when set and entered correctly, will give the owner access to the entire system, overriding the POP. The POP, working as on all current PS/2 systems, is used to prevent any unauthorized access to the Operating System on the DASD or the facilities of the system.

Referring now more particularly to the accompanying drawings, a microcomputer embodying the present invention is there shown and generally indicated at 10 (Figure 1). As mentioned hereinabove, the computer 10 may have an associated monitor 11, keyboard 12 and printer or plotter 14. The computer 10 has a cover 15 which cooperates with a chassis 19 in defining an enclosed, shielded volume for receiving electrically powered data processing and storage components for processing and storing digital data, as shown in Figure 2. In the form illustrated in Figure 2, the computer 10 also has an optional I/O cable connection cover 16 which extends over and protects the connection points of I/O cables with the computer system. At least certain of the system components are mounted on a multilayer planar 20 or motherboard which is mounted on the chassis 19 and provides a means for electrically interconnecting the components of the computer 10 including those identified above and such other associated elements as floppy disk drives, various forms of direct access storage devices, accessory cards or boards, and the like.

The chassis 19 has a base and a rear panel (Figure 2, and which may be covered externally by the cable connection cover 16) and defines at

least one open bay for receiving a data storage device such as a disk drive for magnetic or optical disks, a tape backup drive, or the like. In the illustrated form, an upper bay 22 is adapted to receive peripheral drives of a first size (such as those known as 3.5 inch drives). A floppy disk drive, a removable media direct access storage device capable of receiving a diskette inserted thereinto and using the diskette to receive, store and deliver data as is generally known, may be provided in the upper bay 22.

Prior to relating the above structure to the present invention, a summary of the operation in general of the personal computer system 10 may merit review. Referring to Figure 3, there is shown a block diagram of a personal computer system illustrating the various components of the computer system such as the system 10 in accordance with the present invention, including components mounted on the planar 20 and the connection of the planar to the I/O slots and other hardware of the personal computer system. Connected to the planar is the system processor 32. While any appropriate microprocessor can be used as the CPU 32, one suitable microprocessor is the 80386 which is sold by INTEL. The CPU 32 is connected by a high speed CPU local bus 34 to a bus interface control unit 35, to volatile random access memory (RAM) 36 here shown as Single Inline Memory Modules (SIMMs) and to BIOS ROM 38 in which is stored instructions for basic input/output operations to the CPU 32. The BIOS ROM 38 includes the BIOS that is used to interface between the I/O devices and the operating system of the microprocessor 32. Instructions stored in ROM 38 can be copied into RAM 36 to decrease the execution time of BIOS. The system also has, as has become conventional, a circuit component which has CMOS ROM for receiving and retaining data regarding the system configuration and a real time clock (RTC).

While the present invention is described hereinafter with particular reference to the system block diagram of Figure 3, it is to be understood at the outset of the description which follows that it is contemplated that the apparatus and methods in accordance with the present invention may be used with other hardware configurations of the planar board. For example, the system processor could be an Intel 80286 or 80486 microprocessor.

Returning now to Figure 3, the CPU local bus 34 (comprising data, address and control components) also provides for the connection of the

microprocessor 32 with a math coprocessor 39 and a Small Computer Systems Interface (SCSI) controller 40. The SCSI controller 40 may, as is known to persons skilled in the arts of computer design and operation, be connected or connectable with Read Only Memory (ROM) 41, RAM 42, and suitable external devices of a variety of types as facilitated by the I/O connection indicated to the right in the Figure. The SCSI controller 40 functions as a storage controller in controlling storage memory devices such as fixed or removable media electromagnetic storage devices (also known as hard and floppy disk drives), electro-optical, tape and other storage devices.

The bus interface controller (BIC) 35 couples the CPU local bus 34 with an I/O bus 44. By means of the bus 44, the BIC 35 is coupled with an optional feature bus such as a MICRO CHANNEL bus having a plurality of I/O slots for receiving MICRO CHANNEL adapter cards 45 which may be further connected to an I/O device or memory (not shown). The I/O bus 44 includes address, data, and control components.

Coupled along the I/O bus 44 are a variety of I/O components such as a video signal processor 46 which is associated with video RAM (VRAM) for storing graphic information (indicated at 48) and for storing image information (indicated at 49). Video signals exchanged with the processor 46 may be passed through a Digital to Analog Converter (DAC) 50 to a monitor or other display device. Provision is also made for connecting the VSP 46 directly with what is here referred to as a natural image input/output, which may take the form of a video recorder/player, camera, etc. The I/O bus 44 is also coupled with a Digital Signal Processor (DSP) 51 which has associated instruction RAM 52 and data RAM 54 available to store software instructions for the processing of signals by the DSP 51 and data involved in such processing. The DSP 51 provides for processing of audio inputs and outputs by the provision of an audio controller 55, and for handling of other signals by provision of an analog interface controller 56. Lastly, the I/O bus 44 is coupled with a input/output controller 58 with an associated Electrical Erasable Programmable Read Only Memory (EEPROM) 59 by which inputs and outputs are exchanged with conventional peripherals including floppy disk drives, a printer or plotter 14, keyboard 12, a mouse or pointing device (not shown), and by means of a serial port. The EEPROM plays a part in the security provisions described hereinafter.

In achieving certain objectives of the present invention as described more fully hereinafter, the personal computer system 10 has an erasable memory element mounted within the system enclosure for selective activation to active and inactive states and for receiving and storing a privileged access password (defined more fully hereinafter) when in the active state. The erasable memory element preferably is the electrically erasable programmable read only memory device or EEPROM 59 (Figure 3). The system also has an option or security switch mounted within the enclosure and operatively connected with the erasable memory element 59 for setting that memory element to the active and inactive states and at least one tamper detection switch 60 (Figures 4, 5 and 6) mounted within the enclosure and operatively connected with the erasable memory element for detecting opening of the enclosure and for clearing any stored privileged access password from that memory element in response to any switching of the tamper switch. The option switch (also called security switch in this disclosure) may be, for example, a jumper mounted on the system planar 20 and manually settable to two different states by a person having access to the planar. In one state, the EEPROM 59 is set to be active and to store a PAP as described herein. In the other, the PAP storage capability of the EEPROM is set to be inactive.

The system processor 32, in accordance with this invention, is operatively connected with the EEPROM 59 and functions in part for controlling access to at least certain levels of data stored within the system by distinguishing between the active and inactive states of the PAP storage capability of the memory element and between entry and non-entry of any stored privileged access password (PAP). By manipulating the option switch, an operator (or more specifically the person charged with supervising and maintaining the security) of the system may select between secured operation of the system and unsecured operation of the system by selecting respective active and inactive states of the EEPROM.

Referring now to the schematic views of Figures 4 through 7, certain of the hardware features contributing to this invention will now be more particularly described.

Figure 4 illustrates certain relationships among the conventional power control or "on/off" switch 61, the conventional power supply 62, switches which change conductive state in response to opening or removal of enclosure covers such as the main cover 15 and the cable connection

cover 16, and a keylock switch 64. The switches which change state on opening or removal of enclosure covers are, in the illustrated form of this invention, two in number; namely a switch 65 (Figures 4, 5 and 6) responsive to removal of the main cover 15 and a switch 66 (Figures 4, 5 and 7) responsive to removal of the cable connection cover 16. Each switch has two components, one normally open (65a and 66a, respectively) and one normally closed (65b and 66b, respectively). The second switch 66 is optional, as is the cable connection cover 16. However, as will be clear from a thoughtful consideration of the disclosure here made, the presence of the optional cover and switch assures more complete security control over the system.

The normally open contact sets of the cover switches 65 and 66 are connected in series with the main power switch 61 and to the power supply 62 (Figure 4). As a consequence, if an attempt is made to "power up" the system 10 with the covers removed, the contact sets 65a and 66a will be open and prevent system operation. With the covers in place, the contact sets are held closed and normal system operation may be initiated.

The normally closed contact sets of the cover switches 65 and 66 are connected in series with the keylock switch 64 and to the RTC and CMOS memory 68. The normally closed contact sets 65b and 66b are held open by the presence of the covers 15, 16 and will close on the removal of those covers. The keylock switch 64 is normally held closed on locking of the enclosure lock which is conventionally supplied on the computer system 10. These three contact sets provide an alternate path to ground for current otherwise energizing portions of the RTC and CMOS memory, and have the effect of clearing a segment of that memory if energization is lost, as upon unauthorized removal of a cover while the system is in an enclosure locked state. As that memory is checked by POST, clearing of that segment will result in a configuration error signal being generated which will alert a system owner that an attempt (successful or otherwise) has been made to breach system security.

The keylock switch 64 and main enclosure cover switch 65 are preferably mounted on a front card guide member 69 (Figures 2 and 6) so as to be appropriately positioned relative to the lock provided in the main enclosure cover 15. The front card guide member is mounted in the computer system frame is such a position that an actuating lever 70 for the cover switch 65 protrudes through an opening in the upright front

frame member, to be actuated by the cover 15 when present and positioned to close the system enclosure.

The cable cover switch 66 is preferably mounted on the rear panel of the system frame, positioned to be actuated by a latch member mounted on the cable cover 16 and rotatable under the control of a manually operable keylock similar to that provided on the enclosure cover 15. When the optional cable cover 16 is used (as will be the case where full security of the system is desired or required), latching or locking of the cover to the rear panel causes the latch member to close the associated normally open contact set 66a and open the normally closed contact set 66b.

The new security and integrity features described above and hereinafter work independently of a previously offered personal computer security feature, the Power on Password (POP). These additional security and integrity features provide a secure platform for operating system certification under applicable regulations such as the Orange Book. An additional password is required to place the system in secure mode. The new password is here referred to as the Privileged Access Password (PAP). To maintain compatibility with previous personal computer systems, the POP is still supported. This disclosure deals with the new security and integrity features as they relate to POST and the password utility executing on a personal computer system with an EEPROM, option switch, and tamper evident covers.

Password Security is implemented by system hardware features; an EEPROM, a security switch and a tamper evident cover switch, firmware, POST and the system software password utility. Once the PAP has been installed, the system is in secure mode. The PAP is saved in the EEPROM. A backup copy of the PAP is also maintained in the EEPROM. This is done to prevent accidental loss of the PAP when a power failure occurs during the installation, change, or removal of the PAP.

Two bits in the EEPROM are used as a state machine that lets POST know exactly where the power outage occurred in the update sequence and if possible recover from a system board replacement situation. The password utility maintains the update indicator field, a two bit state machine used during any access to the PAP. If a power outage occurred during the password modification, when power is restored POST checks the

state machine (POST actually checks the state machine on all power ups.) If the PAP is updated successfully (a '00' state), POST proceeds in the normal manner. If the update has started before power is lost (a '01' state), POST will check for the presence of a valid backup PAP. If valid, the user must enter the backup or old PAP to boot the system reference diskette or system partition. If not valid, POST will hang and the system owner will have to intervene to remedy the situation, which might require replacing the system board. If the primary PAP has been updated successfully (a '10' state), POST will use the primary PAP (the new PAP) to validate any attempts to use the system reference diskette or boot the system partition. POST will assume the backup PAP is invalid. POST will copy the primary PAP to the backup PAP in this case.

If the option or security switch is not in the unlocked position an error will be displayed. The system owner will have to intervene by unlocking the covers and changing the position of the security switch. If the backup PAP has been updated successfully (a '11' state), both the primary and backup PAP are considered valid and POST will verify the validity of the Primary PAP, prior to confirming the entry of the PAP by the user.

The POP is maintained in CMOS. Two bits will be maintained in CMOS for use as a password indicators for the PAP. One indicator is used to signify that the system is in secure mode (PAP installed). The second indicator is to signify that the PAP was entered during the initial power on, cold boot. These two indicators will be initialized and set at the cold boot only. Prior to IPL, the indicators will be write protected unless the system reference diskette or system partition is booted.

To prevent any unauthorized access to the passwords, the IPL device boot list, the EEPROM CRC, and all the indicators will be locked prior to Initial Program Load (IPL) booting an operating system. To lock out these areas, POST will set special hardware latches that cannot be reset unless the system is powered off. At the beginning of POST Stage I, initial power on, POST will check to see if the EEPROM is locked. If it is locked, POST will display an error and halt the system because the hardware is not functional. The system owner will need to intervene to remedy the situation which might require that the system board be replaced. When the system has been tampered with, the first 14 bytes of RAM storage in CMOS associated with the RTC and control registers are

unaffected. The next 50 bytes of CMOS are set to all "one's" (binary value 1) as briefly described above. Upon detecting this condition, POST will halt and display an appropriate error. The system owner/authorized user will need to intervene to remedy the situation which might require that the system board be re-configured.

If the system owner forgets the PAP, the system board(s) affected will need to be replaced.

If the POP is forgotten, the system owner can toggle the tamper evident cover switch to destroy the contents of CMOS as described above, and then enter the PAP (if installed) to boot the System Reference Diskette or the System Partition to run the password utility, to reinstall the POP.

When a system has been powered on with neither password installed, POST will not prompt for a password. However, if the System Reference Diskette is not present or the System Partition boot is not requested or present, POST will lock the POP, the PAP, the backup PAP, the IPL device boot list, the EEPROM CRC, and all the indicators. This is done to prevent any accidental or malicious access to these areas. If the System Reference Diskette is present or the System Partition boot is requested, these locations are left unlocked to allow the system owner to invoke secure mode.

When a system has been powered on with a POP installed, but no PAP installed, POST will verify the POP password checksum. If the checksum is bad, POST will erase the POP in CMOS and not prompt for a password. Otherwise, POST will prompt for a password. If the System Reference Diskette is not present or the System Partition boot is not requested, the POP, the PAP, the backup PAP, the IPL device boot list, the EEPROM CRC, and all the indicators will be locked to prevent any access.

When a system has been powered on with a valid PAP installed (Secure mode) but no POP installed, POST will verify the PAP checksum. If the checksum is good, POST will prompt the user to enter the PAP if the System Reference Diskette is present or the System Partition boot is requested. Otherwise, POST will not prompt for a password and the POP, the PAP, the backup PAP, the IPL device boot list, the EEPROM CRC, and all the indicators will be locked to prevent any access. If the PAP

checksum is bad, an error is displayed and the system is halted. This is to prevent a condition where POST could accidentally give unprotected access to a user to a system which was previously in secure mode when the EEPROM failed. The system owner will need to intervene to remedy the situation which might require that the system board be replaced.

When the system has been powered on with both a valid PAP and a valid POP installed, POST will prompt the user to enter a password. If the POP is entered, POST will not boot from the System Reference Diskette or the System Partition. The system can only boot using the existing IPL device list. If the PAP is entered at the prompt rather than the POP, the user can boot from the System Reference Diskette, the System Partition, the IBL diskette, or the normal IPL device list. An indicator is set that signifies that the PAP was successfully entered at initial power up time, so that a system reference diskette or system partition boot may occur later on in this power on session. The authorized user must be aware that once the PAP has been successfully entered, the system is available to boot the system reference diskette or system partition after a soft reboot (Ctrl-Alt-Del) as long as power is maintained. POST will not prompt the user for a password after a soft reboot, hence the need for the PAP successfully entered indicator and its protection. Once finished with the system the authorized user must power off the system to prevent this situation from occurring.

In brief, if a user can boot from the System Reference Diskette or the System Partition on a cold start, the POP, the PAP, the backup PAP, the IPL device boot list, the EEPROM CRC, and all the indicators will remain unlocked. This condition gives trusted software (ie. the System Reference Diskette) and an authorized user access to the security parameters for the system. After POST verifies that either password is entered correctly, it will acknowledge the entry by displaying a confirmation icon. POST will skip prompting for the POP as described above when Network Server (Unattended Start) Mode is active.

Flowchart logic for the scenarios just described are depicted in Figures 8 and 9, where links between the steps specifically illustrated in Figures 9a and 9b are indicated by process blocks occupied by single letter designations in order to simplify the charting.

A system that has the Network Server (Unattended Start) Mode installed will complete the booting process all the way through the target operating system boot but the keyboard will be locked using the POP. However, if a system reference diskette is present or the System Partition boot is requested, the password prompt will be displayed to allow the owner to enter the PAP and gain control of the system. If a system is in the secure state and the user wants to boot from the system reference diskette or the system partition after the keyboard is already locked out, the user must power the system down and initiate a cold boot, from a power off state with the system reference diskette in the diskette drive.

In conjunction with the POST changes, the password utility must include support for the PAP. The utility will support installing, changing and removing a PAP, and will interlock these three functions with the position of the option or security switch. The security switch should remain in the locked position until an authorized user wishes to set, change or remove the PAP. At that time, the user should remove the system covers and move the security switch to the unlocked (change) position; then the PAP can be modified (either set, changed or removed). After PAP modification, the security switch should be returned to the locked position, and it should remain in that position until further modification is necessary. This will ensure maximum system security in the interim between PAP modifications. When the security switch is placed in the unlocked position, hardware logic external to the EEPROM allows the storing of the PAP into the EEPROM. When the security switch is placed in the locked position, external hardware logic prevents any changes to the PAP locations in the EEPROM. Appropriate messages will appear if the authorized user attempts to modify the PAP when the security switch is in the locked position. Also, messages will remind the user to return the security switch to the locked position after a modification is complete. An additional safety feature is built into the password utility that prohibits the authorized user from setting the PAP equal to the POP. Checks will be made when setting or changing the PAP to ensure that the new PAP does not equal the current POP of the system. Also, when changing or removing the PAP, the current PAP must be known.

It is contemplated that a personal computer system will initially be shipped with the security switch in the locked position and the tamper evident cover locked. This is done to prevent any person other than the system owner from setting the system into secure mode. Unlike the POP,

the PAP cannot be erased through hardware manipulation. If the PAP is forgotten or an unauthorized user places the system into secure mode, the system board must be replaced. The logic represented in the above description can be found in Figure 8.

In the drawings and specifications there has been set forth a preferred embodiment of the invention and, although specific terms are used, the description thus given uses terminology in a generic and descriptive sense only and not for purposes of limitation.

* C L M S *

Claims

1. A personal computer system for receiving and retaining data and capable of securing data retained within the system against unauthorized access, the system comprising:

a normally closed enclosure,

an erasable memory element mounted within said enclosure for selective activation to active and inactive states and for receiving and storing a privileged access password when in the active state,

an option switch mounted within said enclosure and operatively connected with said erasable memory element for setting said erasable memory element to the active and inactive states, and

a system processor mounted within said enclosure and operatively connected with said erasable memory element for controlling access to at least certain levels of data stored within the system by distinguishing between the active and inactive states of said memory element and between entry and non-entry of any stored privileged access password.

2. A personal computer system according to claim 1 further comprisingin accordance with Claim 1 further comprising:

a second erasable memory element mounted within said enclosure for receiving and storing data indicative of the state of the first said erasable memory element and of correct entry of any stored privileged access password, and

a tamper detection switch mounted within said enclosure and operatively connected with said second erasable memory element for detecting unauthorized opening of said enclosure and for invalidating any privileged access password stored in the first said erasable memory element in response to any switching of said tamper switch.

3. A personal computer system in accordance with Claim 1 or 2 wherein said first erasable memory element is an electrically erasable programmable read only memory device.

4. A personal computer system in accordance with Claim 1, 2 or 3 wherein said option switch functions for enabling an operator to select between secured operation of the system and unsecured operation of the system by selecting respecting active and inactive states of said first memory element.

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

5. A personal computer system in accordance with Claim 4 wherein said option switch is manually operable and positioned within said enclosure for manual access only after opening of said enclosure.

6. A personal computer system in accordance with Claim 2 wherein said second erasable memory element is a battery backed CMOS RAM.

7. A method of operating a personal computer system having an enclosure, a system processor mounted within the enclosure, a selectively activable erasable memory element mounted within the enclosure, an option switch mounted within the enclosure for setting the memory element to active and inactive states, and a tamper detection switch mounted within the enclosure for detecting opening of the enclosure, the method comprising the steps of:

selectively setting the memory element into active state;

storing a privileged access password in the active memory element;

controlling access to at least certain levels of data stored within the system by distinguishing between the active and inactive states of the memory element and between entry and non-entry of the privileged access password; and

invalidating the privileged access password stored in the memory element in response to any switching of the tamper switch.

8. A method in accordance with Claim 7 wherein said step of selectively setting the memory element into active state comprises opening the system enclosure and manually changing the setting of the option switch.

9. A method of operating a personal computer system having a system processor and memory elements, the method comprising the steps of:

providing for the reception by and storage in the system of first and second passwords and for the loading into the system of trusted and open programs;

distinguishing among the storage of (a) no passwords, (b) a first password, and (c) a second password;

distinguishing between the loading and requested execution of (d) trusted and (e) open programs;

distinguishing among the entry by a user of (f) no passwords, (g) the first password, and (h) the second password; and

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

controlling access by a user to trusted programs (d) in response to the entry by a user of the second password (h).

10. A method according to Claim 9 wherein said step of distinguishing among storage of passwords comprises distinguishing between the storage of a power on password as the first password and of a privileged access password as the second password.

11. A method according to Claim 9 wherein said step of controlling access comprises recognizing the storage of no passwords (a) and granting access to any program by any user.

12. A method according to Claim 9 wherein said step of controlling access comprises recognizing the storage of a first password (b) and granting access to any program only to a user entering the first password (b).

13. A method according to Claim 9 wherein said step of controlling access comprises recognizing the storage of a second password (c) and granting access to any program only to a user entering the second password (c).

14. A method according to Claim 9 wherein said step of controlling access comprises recognizing the storage of a first password (b) and of a second password (c), granting access to any program only to a user entering the first password (b), and granting access to a trusted program only to a user entering the second password (c).

15. A method according to Claim 14 wherein said step of controlling access further comprises granting access to any program to a user entering the second password (c) absent any need to first enter the first password (b).

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED