United States Patent [19]

Blackledge, Jr. et al.

[54] **TRUSTED PERSONAL COMPUTER SYSTEM WITH IDENTIFICATION**

[75] Inventors: John W. Blackledge, Jr.; Richard A. Dayan; Dennis L. Moeller; Palmer E. Newman; Kenneth J. P. Zubay, all of Boca Raton, Fla.

[73] Assignee: **International Business Machines Corp.**, Armonk, N.Y.

[21] Appl. No.: **947,014**

[22] Filed: **Sep. 17, 1992**

[51] Int. Cl.⁵ H04L 9/00
[52] U.S. Cl. 380/4; 380/49; 380/50; 380/52
[58] Field of Search 380/3, 4, 23, 25, 49, 380/50, 52; 340/825.31, 825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,783,801 11/1988 Kaule 380/3
4,860,351 8/1989 Weingart 380/3
5,163,096 11/1992 Clark et al. 380/4

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Daniel E. McConnell

[57] **ABSTRACT**

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. This invention contemplates protecting a personal computer system which has the capability of becoming a secure system from being placed into that condition by an attack on an unsecured machine. Additionally, in a network environment, it is important to maintaining network security that any given particular system be uniquely identified to the network, in order to guard against the substitution of an insecure "alternate" which would open the network to attack through an insecure system. This invention contemplates provision for such identification in a secure manner.

5 Claims, 7 Drawing Sheets

FIG. 1

15

16

20

19   69

22

FIG. 2

FIG.3

CPU 32

MCPU 39

SCSI 40

ROM 41

RAM 42

SCSI

BIC 35

SIMMS 36

BIOS ROM 38

34

I/O 58

AUDIO 55

EEPROM 59

RTC 68

DSP 51

INST. RAM 52

DATA RAM 54

A/C 56

VSP 46

GRAPHIC VRAM 48

IMAGE VRAM 49

DAC 50

44

45

FLOPPY
PRINTER
KEYBOARD
MOUSE
SERIAL

HEADPHONE
MICROPHONE
LINE IN
LINE OUT
SPEAKER
MIDI
CABLE

NATURAL IMAGE

VFB
MONITOR

61

65a

66a

62

Power
Supply

64

65b

68

66b

RTC

GND
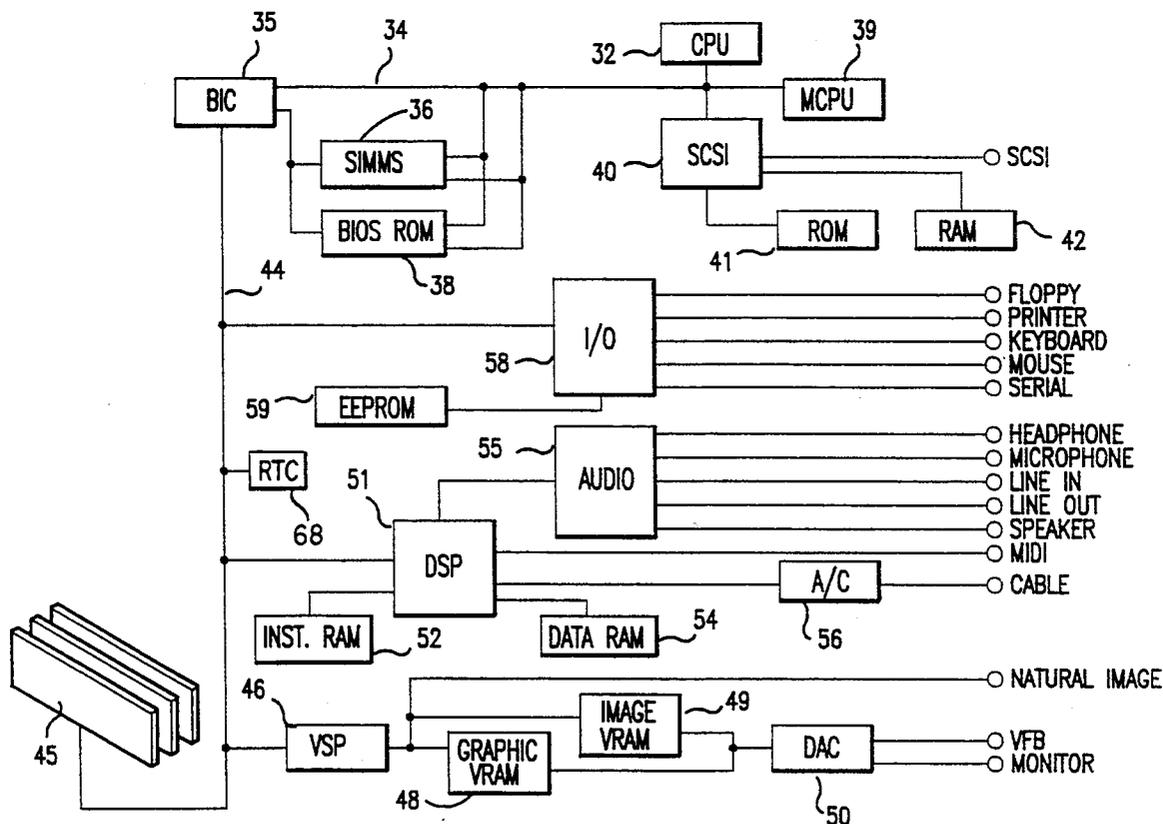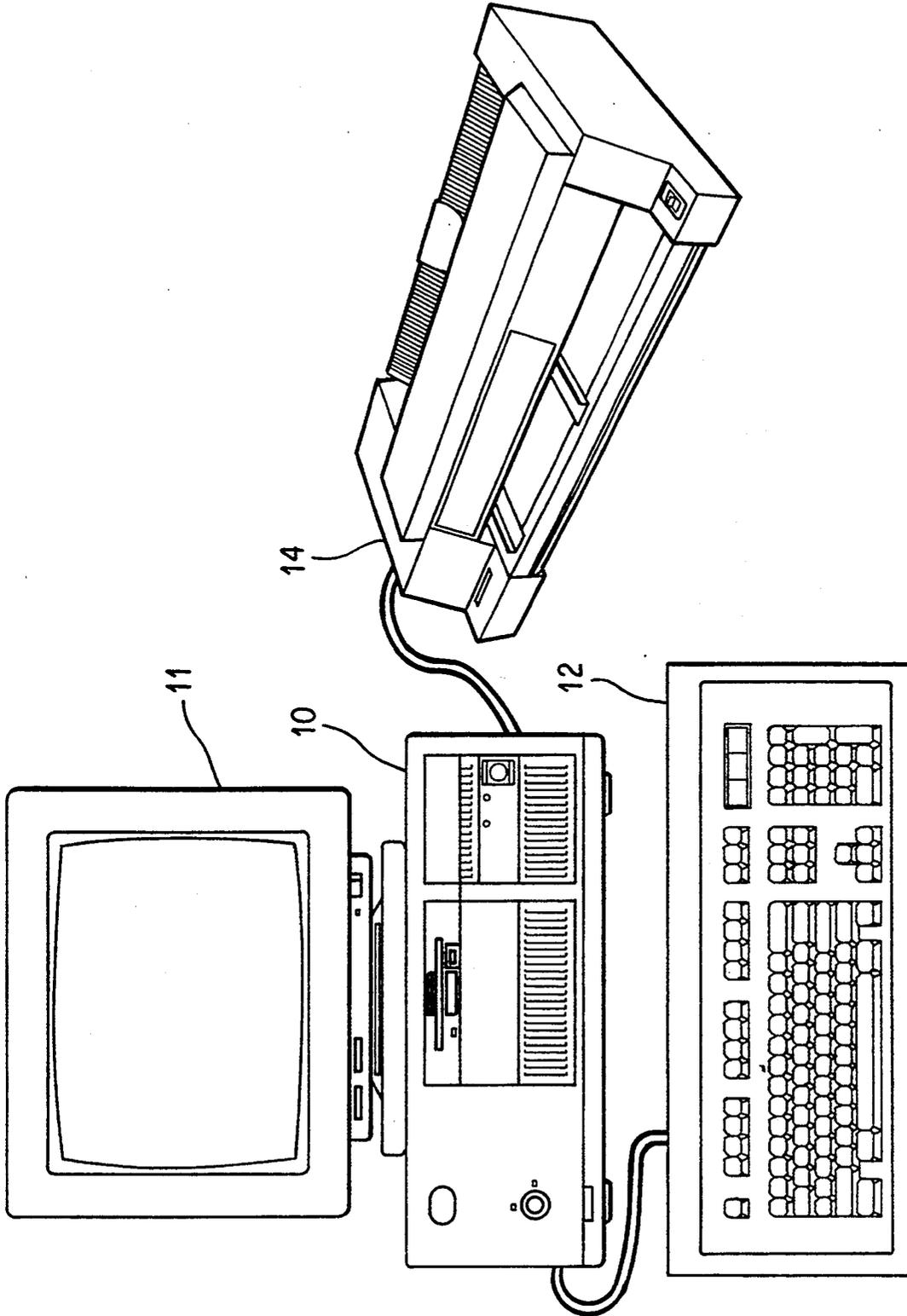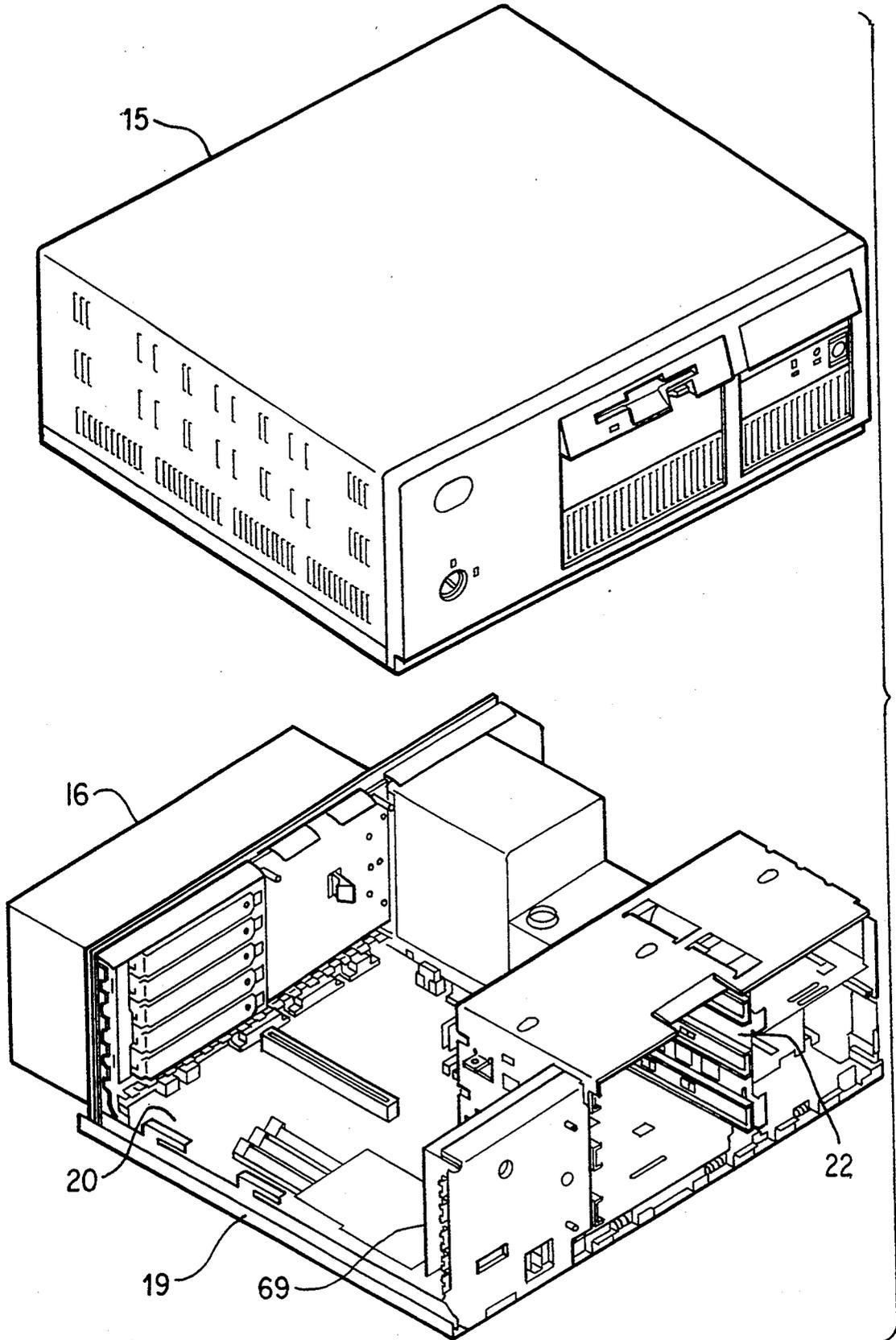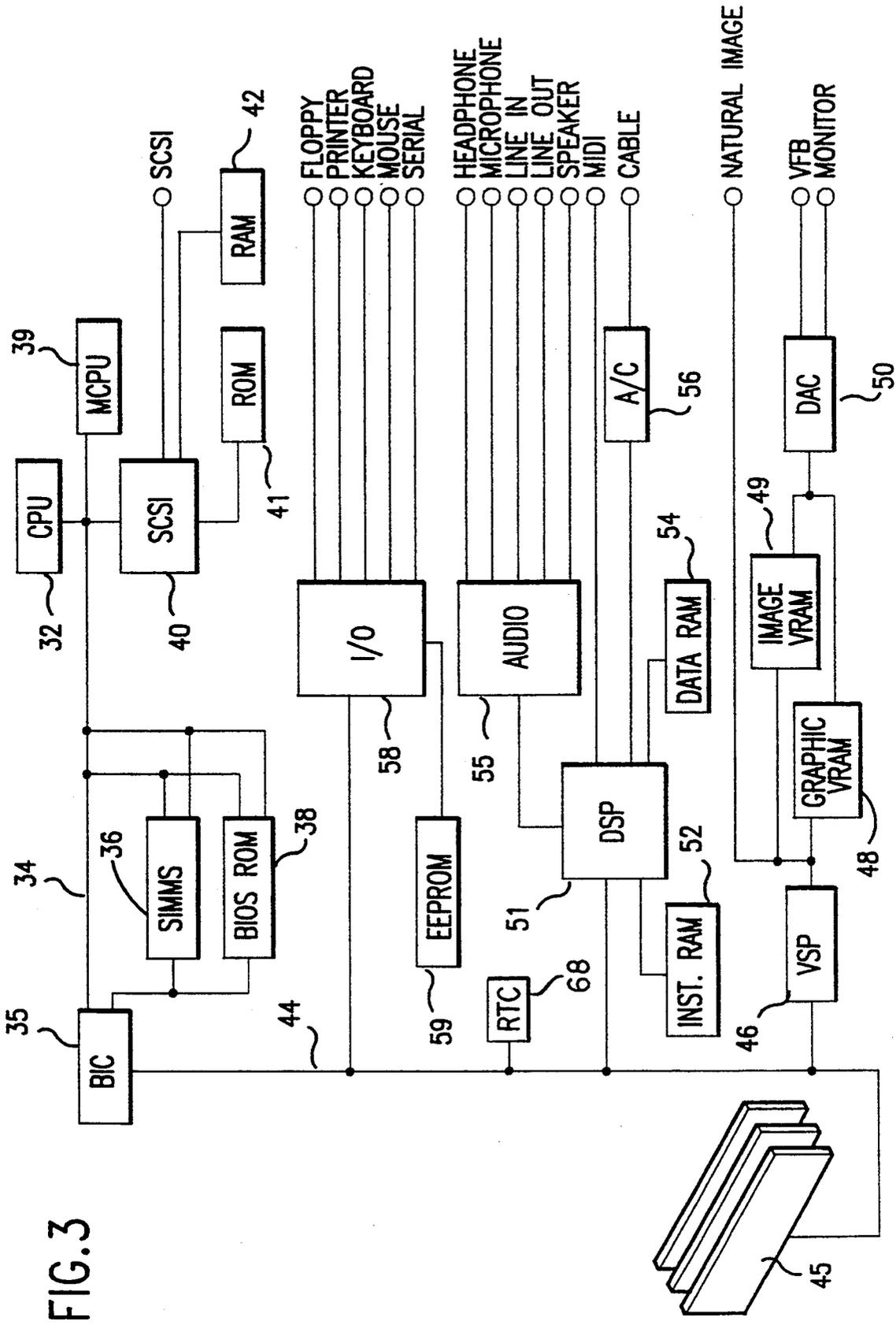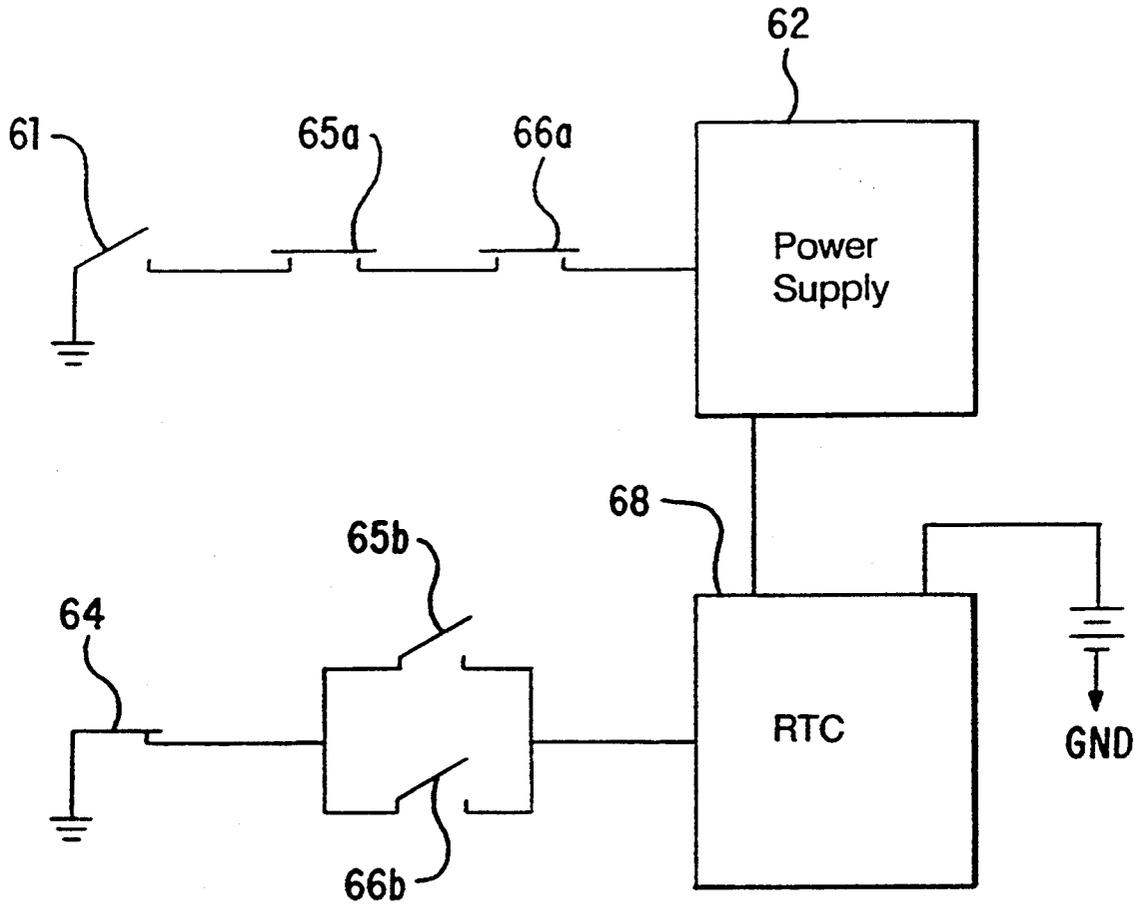
FIG. 4
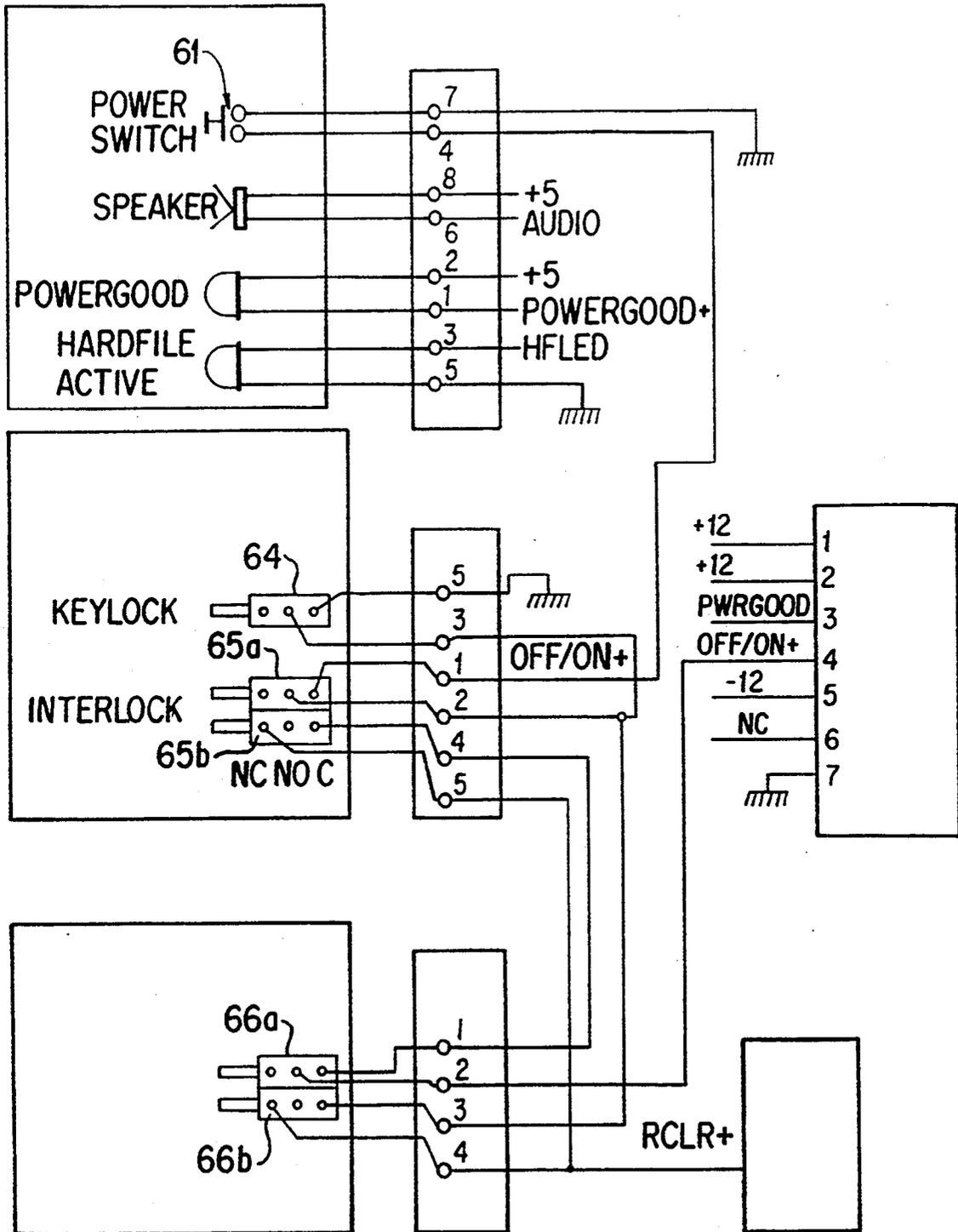
FIG. 5
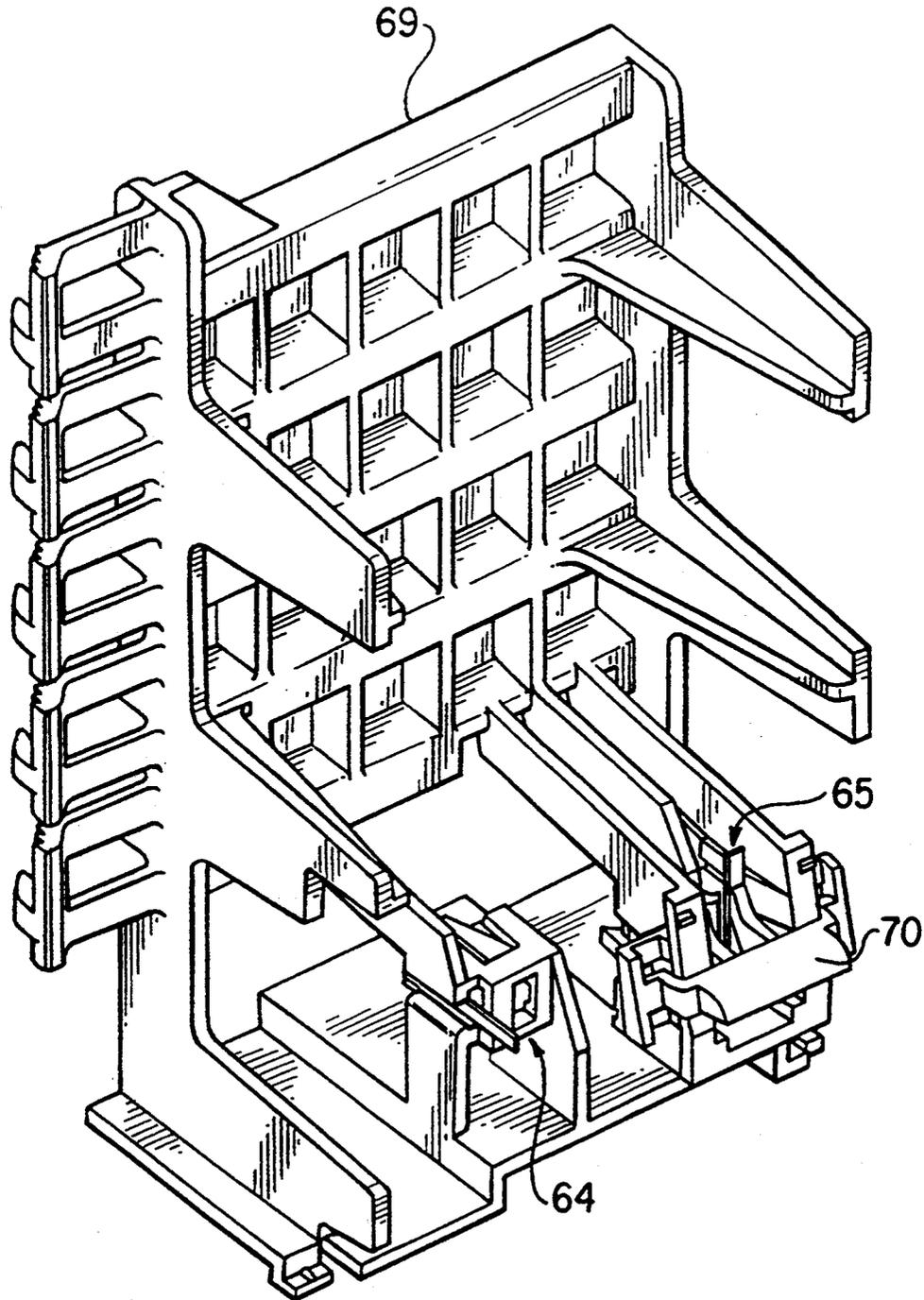
FIG. 6
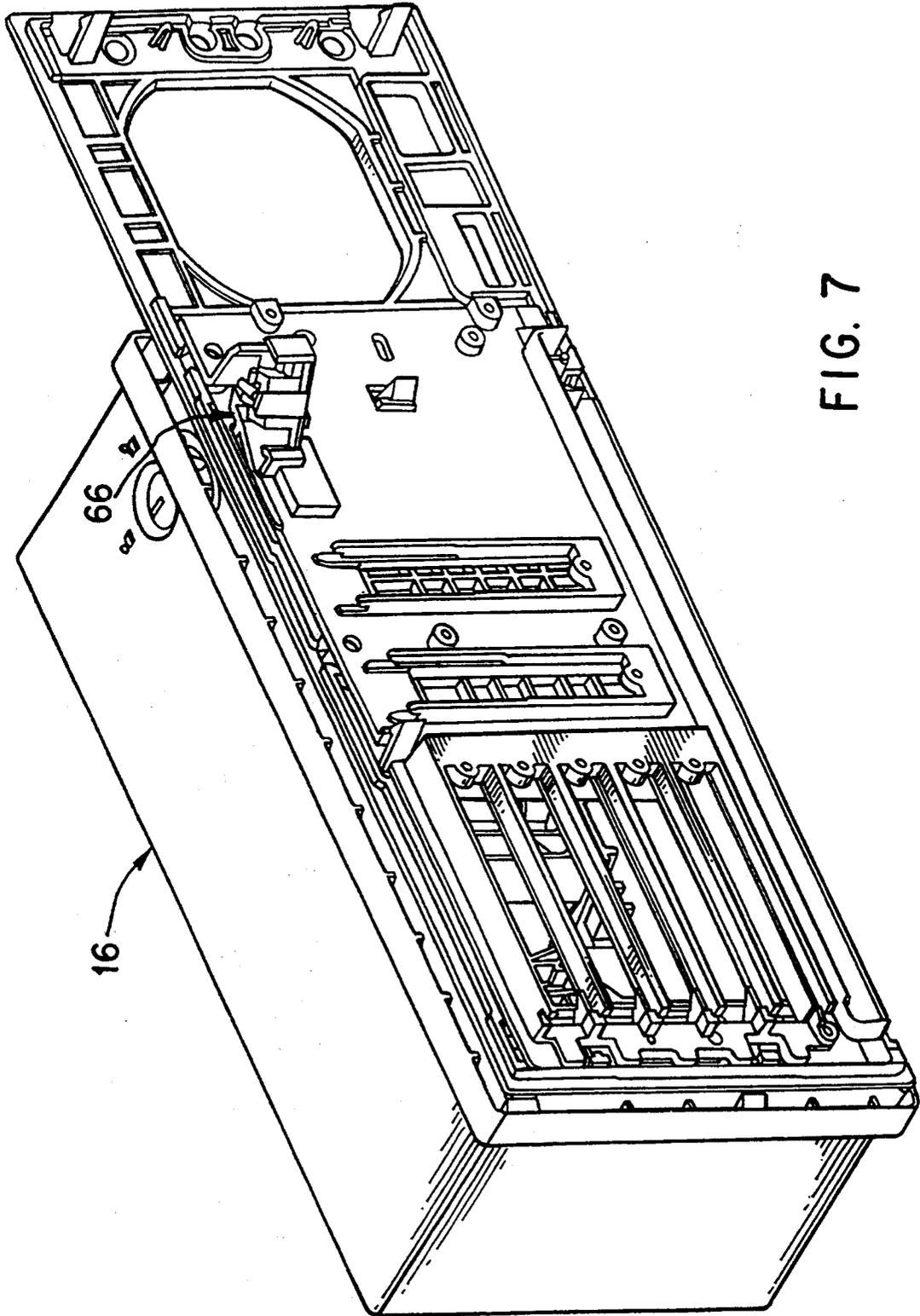
FIG. 7

TRUSTED PERSONAL COMPUTER SYSTEM WITH IDENTIFICATION

RELATED APPLICATIONS

This invention is related to inventions described in co-pending applications Ser. Nos. 889,324 and 889,325 filed May 27, 1992 and owned in common with the invention here described.

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 (also known as and occasionally mentioned herein as a system board, system planar or 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, 56, 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 57 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.

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. The system partition also stores an image of a system reference diskette, which includes certain utility programs used in establishing system configuration and the like. 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 cor-

rupt 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 Aug. 25, 1989, and now U.S. Pat. No. 5,022,077 issued Jun. 4, 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.

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 products in order to see if the products 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 Jan. 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. For 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 . . . ."

BRIEF DESCRIPTION OF THE INVENTION

Having in mind the discussion given above, this invention contemplates protecting a personal computer system which has the capability of becoming a secure system from being placed into that condition by an attack on an unsecured machine. Such an attack, if successful, would bar a system owner from access to data properly stored in the system while the system was in a desired, insecure, state.

Certain approaches to securing a personal computer system may involve the use of components added to the system as it becomes a secure system. The present invention contemplates provision for such additional security components and their adaptation into the BIOS organization described hereinabove.

One environment of use in which it may be desirable to accommodate security provisions made in a personal computer system is a network in which a plurality of such systems are connected together one to another and possibly to a central file server system. In such a network it is important to maintaining network security that any given particular system be identified to the network, in order to guard against the substitution of an insecure "alternate" which would open the network to attack through an insecure system. This invention contemplates provision for such identification.

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:

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

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

FIG. 3 is a schematic view of certain components of the personal computer of FIGS. 1 and 2;

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

FIG. 6 is an enlarged scale perspective view of certain components illustrated in FIGS. 4 and 5; and

FIG. 7 is a view similar to FIG. 6 of certain optional components of the personal computer of FIGS. 1, 2, 4 and 5 which are related to the security features of 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 total- 5 ity 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 uni- 10 fied 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 15 clearance) related to the security policy.

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

TRUSTED PROGRAM: A program included in Trusted Software. 20

OPEN PROGRAM: A program operable on a Trusted Computing Base and which is other than a Trusted Program.

REFERENCE MONITOR CONCEPT: An access control concept that refers to an abstract machine 25 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 30 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 informa- 35 tion.

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 when- 40 ever 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 45 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 50 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 55 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 60 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. 65

NORMAL USER: Any user of a system authorized to use the system facilities. In order to change a system 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 tamper evident cover keylock 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 correctly 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 (FIG. 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 FIG. 2. In the form illustrated in FIG. 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 (also described herein as a motherboard or system board) 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 (FIG. 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 FIG. 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 the BIOS 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 battery backed nonvolatile memory (conventionally CMOS RAM) for receiving and retaining data regarding the system configuration and a real time clock (RTC) 68 (FIG. 3).

While the present invention is described hereinafter with particular reference to the system block diagram of FIG. 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 FIG. 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 (MCPU) 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 internal or 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.

As will be appreciated, a system 10 as described to this point may be used in applications where security provisions are unnecessary and indeed unwanted as well as in applications where security provisions are not only wanted but required. A system manufacturer, knowing that any given system may be used in either or both of such environments must prepare a system for use in either such environment. The focus of the invention here described is on rendering such a system adaptable to both such environments of use.

One particular example is that a non-secured system must be guarded against undesirably becoming a secured system. One result, should such a conversion occur, would be that data stored in a non-secured system may become unavailable should the system be covertly converted to a secured system, as could occur where the system has security provisions which a system owner may elect not to effectuate.

In achieving certain objectives of securing a personal computer system as described herein, 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 (or PAP) when in the active state. The erasable memory element preferably is at least one field or portion of the electrically erasable programmable read only memory device or EEPROM 59 (FIG. 3) described above. The system also has an option or security switch mounted within the enclosure and operatively connected with the erasable memory element 59 for setting the used field or portion of that memory element to the active and inactive states. The option switch (also called security switch) 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 (also mentioned herein as the write enable or unlocked state), the EEPROM 59 is set to be active and to store a PAP. In the write enable state, the PAP may be written to the EEPROM, changed or removed. In the other or inactive state (also mentioned herein as the write disabled or locked state), the PAP storage capability of the EEPROM is set to be inactive.

In accordance with certain features of the invention here described, the EEPROM also contains a system unique identifier installed by the manufacturer and accessible to a network server when the system 10 is connected into a secure network and the security features here described are activated.

As mentioned above, the system 10 also has a second component having erasable memory capabilities, namely battery supported, non-volatile CMOS RAM and an associated real time clock (RTC), indicated at 68. The CMOS RAM stores data indicative of the system configuration including, in accordance with this invention, data regarding the successful entry of the PAP on power up of the system 10. At least one tamper detection switch is provided, mounted within the enclosure and operatively connected with the CMOS RAM for detecting opening of the enclosure and for clearing or setting certain data stored in that memory element in response to any switching of the tamper detection switch on an unauthorized opening of the enclosure.

The 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.

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. The POP and at least certain bits indicative of the validity of the PAP (if installed) are stored in the CMOS RTC. Changes in data retained in the CMOS RTC and in the EEPROM are independent one from the other.

FIG. 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 (FIGS. 4, 5 and 6) responsive to removal of the main cover 15 and a switch 66 (FIGS. 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 (FIG. 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 setting a segment of that memory to a distinctive state (such as all "1"s) 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, setting that segment to a distinctive state 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. This setting of a memory segment to a distinctive state requires the previously stored password for purposes of booting an operating system; that is, booting an operating system requires entry of a valid PAP as otherwise disclosed in this description.

The keylock switch 64 and main enclosure cover switch 65 are preferably mounted on a front card guide member 69 (FIGS. 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 in such a position that an actuating lever 70 for the cover switch 65 protrudes through an opening in an 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.

In accordance with this invention, the default state of the system 10 as manufactured puts the system into unsecured mode on power-up. In order for the system to become a secure system, the system owner must open the locked covers and intentionally change the state of the security switch provided on the system planar 20, thereby enabling the activation of a security password to render the system a secure system. Thus the presence of the security features described to this point guards against the initially unsecured system becoming a se-

11

cured system without the knowledge of the system owner or other authorized user.

As mentioned briefly hereinabove, the present invention contemplates that provision be made for the use of additional security components. More particularly, various manufacturers offer option cards which may be mounted as one of the cards **45** connected into the system via the I/O option bus **44**. Certain such commercially available option cards offer connections to encryption "keys" which may be in the form of signature recognition pens, magnetic stripe cards, or ROM containing tokens. When such option cards are added to a system such as the system **10** when set in a secure state, an additional level of protection may be provided. Further, when so added, the system owner becomes the only authorized person having access to the option card and to the Set Configuration utility program stored in the image of the reference diskette maintained in the system partition of the system DASD.

This invention also contemplates that a system unique identifier be stored in the EEPROM **59**. The identification stored in the EEPROM is accessible by software running on a network server or the like with which the system **10** is connected. Thus the network can verify that the system located at a particular location in the network is and continues to be the secure system for which controlled access is allowed. The identification stored in the EEPROM is protected by the fact that the EEPROM is a read-only device, requiring special hardware to effect any change in the identification stored in the memory.

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.

What is claimed is:

1. A personal computer system for receiving and retaining data and for enabling data retained within the system to be secured against unauthorized access, the system comprising:

12

a normally closed enclosure,

an enclosure lock for normally maintaining said enclosure in a securely locked condition denying access to the interior of the enclosure apart form possession of a key for said enclosure lock,

an erasable memory element mounted within said enclosure for selective activation to one of an active state and an inactive state,

an option switch mounted and accessible solely from within said enclosure and connected with said erasable memory element for setting said erasable memory element to a selected one of the active and inactive states, and

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

2. A personal computer system in accordance with claim **1** 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 respective active and inactive states of said memory element.

3. A personal computer system in accordance with claim **2** wherein said option switch is manually operated and positioned within said enclosure for manual access only after opening of said enclosure.

4. A personal computer system in accordance with claim **1** wherein said erasable memory element is an electrically erasable programmable read only memory element.

5. A personal computer system in accordance with claim **4** wherein said electrically erasable programmable read only memory device contains a system unique identifier enabling software running on a network server with which the system is connected to verify that the system located at a particular location in the network is and continues to be a secure system for which controlled access is allowed.

* * * * *

45

50

55

60

65