(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 October 2004 (21.10.2004)

PCT

(10) International Publication Number
WO 2004/090701 A2

(51) International Patent Classification[7]: G06F 1/26

(21) International Application Number:
PCT/GB2004/001531

(22) International Filing Date: 8 April 2004 (08.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/411,408	10 April 2003 (10.04.2003)	US
10/411,454	10 April 2003 (10.04.2003)	US
10/411,415	10 April 2003 (10.04.2003)	US

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CATHERMAN, Ryan, Charles** [US/US]; 600 Harvest Lane, Raleigh, NC 27606 (US). **GOODMAN, Steven, Dale** [US/US]; 5153 Jeffries Road, Raleigh, NC 27606 (US). **HOFF, James, Patrick** [US/US]; 2901 Alder Ridge Lane, Raleigh, NC 27603 (US). **SPRINGFIELD, Randall, Scott** [US/US]; 107 Garden Gate Drive, Chapel Hill, NC 27516 (US). **WARD, James, Peter** [US/US]; 107 Hemingway Forest Place, Raleigh, NC 27607 (US).

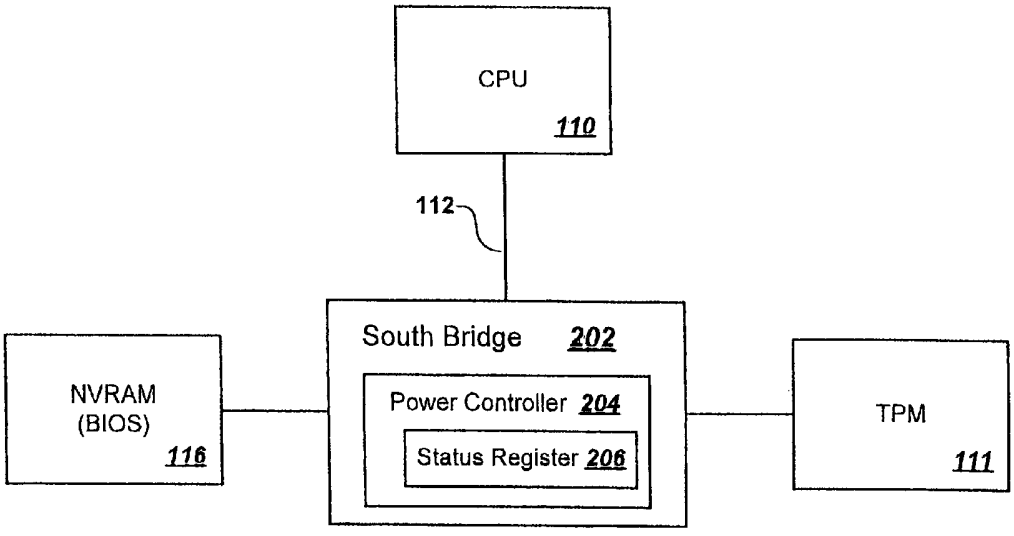
(74) Agent: **WATSON, Justine, Nicola**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: PHYSICAL PRESENCE DETERMINATION IN A TRUSTED PLATFORM



(57) Abstract: A computer system (and a motherboard for a computer system) is presented which provides a trusted platform by which operations can be performed with an increased level trust and confidence. The basis of trust for the computer system (or motherboard) is established by an encryption coprocessor and by code which interfaces with the encryption coprocessor and establishes root of trust metrics for the platform. The encryption coprocessor is built such that certain critical operations are allowed only if physical presence of an operator has been detected. Physical presence is determined by inference based upon the status of registers in the core chipset (e.g. on the motherboard).

WO 2004/090701 A2

Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PHYSICAL PRESENCE DETERMINATION IN A TRUSTED PLATFORM

BACKGROUND OF THE INVENTION

This invention pertains to computer systems and other information handling systems and, more particularly, to a computer system which is built on a trusted platform such as the TCPA industry standard platform.

There is a need in the computer industry to raise the level of confidence with which users run applications and perform network transactions. This is particularly true for electronic commerce transactions where users key in credit card and other sensitive information. Several solutions have emerged in the industry. One solution, the Smart Card, has emerged as a standard for raising the level of confidence by providing hardware which establishes a trusted user. In the Smart Card solution, the computer system is not the trusted entity. Rather, it is the smart card hardware which is the trusted entity and which is associated with a particular user. Another solution, the Trusted Computing Platform, has emerged as a standard for raising the level of confidence by providing hardware which establishes a trusted platform. With the trusted platform the user is not the trusted entity. Rather, it is the platform which is trusted.

Modern computer systems provide remote power-on capability. For example, the computer can be powered on when the RING signal from an incoming FAX is detected at the computer's modem. The computer can then power-on, boot, and receive the incoming fax. Likewise, the computer can be powered on when local area network activity is detected at its LAN card; it can then boot and respond to any local area network requests. Computers with this capability, however, are particularly at risk while unattended because they are vulnerable to attacks even if they are powered off.

SUMMARY OF THE INVENTION

According to one aspect, there is provided a method comprising the steps of: determining whether power was applied to a computer system by the activation of a power-on switch by reading a power-on status register which indicates the occurrence of such activation; and affecting the operation of a trusted platform module (TPM) included in the computer system as a function of said determination.

In one embodiment the power-on status register is settable only in hardware.

In one embodiment, the determining and affecting steps occur subsequent to a reset event and prior to an OS load event which loads the operating system. The OS load event may be a first instance of an INT 19h following the reset event. The reset event may be an event selected from the group consisting of a hardware initiated reset and a software initiated reset. The affecting step preferably further comprises the step of setting a physical presence flag in the TPM. The affecting step further preferably comprises the step of setting a physical presence lock flag in the TPM.

In one embodiment, the determining and affecting steps occur subsequent to a reset event and prior to the availability of a computer system I/O device. Preferably the computer system I/O device is a device selected from the group consisting of a keyboard device, a video device, and a pointing device. The resent event may be an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

In one embodiment the affecting step is one which limits the operation of the TPM in response to a determination in said determining step that the power-on switch was not activated.

In one embodiment the affecting step is one which allows a predetermined trusted operation to execute in the TPM in response to an application of power by the activation of the power-on switch as determined in said determining step.

According to another aspect, the invention provides a method comprising the steps of: determining whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware; configuring a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate lack of physical presence in response to a determination in said determining step that the power-on switch was not activated; wherein said determining and configuring steps occur after a system reset event and before an OS load event, and limiting the operation of the TPM as a function of said configuring step.

In one embodiment the method further comprises the steps of: locking the physical presence flag in the TPM by setting a physical presence lock flag in the TPM; wherein said locking step occurs after the system reset event and before the OS load event. The os load event is preferably an event which loads the operating system and the system reset event is preferably an event selected from the group consisting of a hardware initiated reset and a software initiated reset. The event which loads the operating system may be a first instance of an INT 19h following the system reset event.

According to another aspect, there is provided a method comprising the steps of: determining whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware; configuring a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate physical presence in response to an application of power by the activation of the power-on switch as determined in said determining step; wherein said determining and configuring steps occur after a system reset event and before an OS load event, and allowing a predetermined trusted operation to execute in the TPM as a function of said configuring step.

Preferably it is possible to lock the physical presence flag in the TPM by setting a physical presence lock flag in the TPM and preferably this is done after the system reset event and before the OS load event. Preferably the os load event is an event which loads the operating system and the system reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset. Preferably the event which loads the operating system is a first instance of an INT 19h following the system reset event.

According to another aspect, there is provided a program product comprising: a computer usable medium having computer readable program code embodied therein, the computer readable program code in said program product being effective when executing to: determine whether power was applied to a computer system by the activation of a power-on switch by reading a power-on status register which indicates the occurrence of such activation; and affect the operation of a trusted platform module (TPM) included in the computer system as a function of said determination.

According to another aspect, there is provided a program product comprising: a computer usable medium having computer readable program code embodied therein, the computer readable program code in said program product being effective when executing to: determine whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware; configure a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate lack of physical presence in response to said determination indicating that the power-on switch was not activated; wherein said determination and configuration occur after a system reset event and before an OS load event, and limit the operation of the TPM as a function of said configuration.

According to another aspect, there is provided a program product comprising: a computer usable medium having computer readable program code embodied therein, the computer readable program code in said program product being effective when executing to: determine whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware; configure a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate physical presence in response to an application of power by the activation of the power-on switch in accordance to said determination; wherein said determination and configuration occur after a system reset event and before an OS load event, and allow a predetermined trusted operation to execute in the TPM as a function of said configuration.

According to another aspect, there is provided an apparatus comprising: a trusted platform module (TPM); a nonvolatile memory having computer readable program code stored therein; and a circuit board which couples said TPM and said nonvolatile memory and which includes a processor which executes the code stored in said nonvolatile memory and further includes a status register which assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated; wherein the processor, when executing the code stored in said nonvolatile memory, is effective to: read the power-on status state of the status register; determine whether the application of power to said circuit board was last previously initiated by the

activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and issue a command which affects the operation of said TPM as a function of the determined power-on state.

In one embodiment, the status register is settable only in hardware.

In one embodiment the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which is stored in other than said nonvolatile memory.

In one embodiment the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which loads the operating system. The code which loads the operating system may be a first instance of an INT 19h following the reset event.

In one embodiment, the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

In one embodiment the code stored in said nonvolatile memory is further effective when executing to: set a physical presence flag in said TPM. The code stored in the nonvolatile memory is preferably further effective when executing to: set a physical presence lock flag in said TPM.

In one embodiment, the code which is effective to read, determine, and issue is executed subsequent to a reset event and prior to any execution of code which accesses a computer system I/O device and the computer system I/O device is preferably a device selected from the group consisting of a keyboard device, a video device, and a pointing device.

In one embodiment the issued command limits the operation of said TPM in response to a determination that the power-on switch was not activated in the last previously initiated application of power based on the power-on status state as read from the status register.

In one embodiment the issued command allows a predetermined trusted operation to execute in said TPM in response to a determination that the power- on switch was activated in the last previously initiated application of power based on the power-on status state as read from the status register.

According to another aspect, there is provided an apparatus comprising: a trusted platform module (TPM); a nonvolatile memory having computer readable program code stored therein; and a circuit board which couples said TPM and said nonvolatile memory and having a processor and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated; wherein the processor and said nonvolatile memory are configured on said circuit board so as to execute code stored therein as the initial code executed by the processor in response to a reset event, the code being effective when executing to: read the power-on status state of the status register; determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and configure a physical presence flag in said TPM to indicate lack of physical presence in response to a determination that the power-on switch was not activated; wherein the code which is effective to read, determine, and configure executes before an OS load event, and wherein operation of said TPM is limited as a function of the configured physical presence flag.

In one embodiment the code stored in said nonvolatile memory is further effective when executing to: lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM; wherein the code locks the physical presence flag before the OS load event. Preferably the os load event is an event which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset. Preferably the event which loads the operating system is a first instance of an INT 19h following the reset event.

According to another aspect, there is provided an apparatus comprising: a trusted platform module (TPM); a nonvolatile memory having computer readable program code stored therein; and a circuit board which couples said TPM and said nonvolatile memory and having a processor and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated; wherein the processor and said nonvolatile memory are configured on said circuit board so as to execute code stored therein as the initial code executed by the processor in response to a reset event, the code being effective when executing to: read the power-on status state of the status register; determine whether

the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and configure a physical presence flag in said TPM to indicate physical presence in response to a determination that the power-on switch was activated; wherein the code which is effective to read, determine, and configure executes before an OS load event, and wherein a predetermined trusted operation is allowed to execute in said TPM as a function of the configured physical presence flag.

In one embodiment the code stored in said nonvolatile memory is further effective when executing to: lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM; wherein the code locks the physical presence flag before the OS load event. Preferably the os load event is an event which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset. Preferably the event which loads the operating system is a first instance of an INT 19h following the reset event.

According to another aspect, there is provided a motherboard comprising: a circuit board having an unpopulated processor socket and a status register which assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated; a trusted platform module (TPM) mounted on said circuit board; and a nonvolatile memory mounted on said circuit board and coupled thereby to said TPM and having computer readable program code stored therein; the code stored in said nonvolatile memory being effective when executing to: read the power-on status state of the status register; determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and issue a command which affects the operation of said TPM as a function of the determined power-on state.

In one embodiment the status register which indicates that power was applied by activation of the power-on switch is settable only in hardware.

In one embodiment the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which is stored in other than said nonvolatile memory.

In one embodiment the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which loads the operating system. Preferably the code which loads the operating system is a first instance of an INT 19h following the reset event.

In one embodiment the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

In one embodiment the code stored in said nonvolatile memory is effective when executing to: set a physical presence flag in said TPM. Preferably the code stored in said nonvolatile memory is further effective when executing to: set a physical presence lock flag in said TPM.

In one embodiment the code which is effective to read, determine, and issue is executed subsequent to a reset event and prior to any execution of code which accesses a computer system I/O device, and the computer system I/O device is a device selected from the group consisting of a keyboard device, a video device, and a pointing device.

In one embodiment, the issued command limits the operation of said TPM in response to a determination that the power-on switch was not activated in the last previously initiated application of power based on the power-on status state as read from the status register.

In one embodiment the issued command allows a predetermined trusted operation to execute in said TPM in response to a determination that the power-on switch was activated in the last previously initiated application of power based on the power-on status state as read from the status register.

According to another aspect, there is provided a motherboard comprising: a trusted platform module (TPM); a nonvolatile memory having computer readable program code stored therein; and a circuit board which couples said TPM and said nonvolatile memory and having an unpopulated processor socket and a status register which is settable

only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated; wherein said nonvolatile memory is configured on said circuit board so as to execute code stored therein as the initial code executed in response to a reset event, the code being effective when executing to: read the power-on status state of the status register; determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and configure a physical presence flag in said TPM to indicate lack of physical presence in response to a determination that the power-on switch was not activated; wherein the code which is effective to read, determine, and configure executes before the execution of code which is stored in other than said nonvolatile memory, and wherein operation of said TPM is limited as a function of the configured physical presence flag.

In one embodiment the code stored in said nonvolatile memory is further effective when executing to: lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM; wherein the code locks the physical presence flag before the execution of code which is stored in other than said nonvolatile memory. Preferably the execution of code which is stored in other than the nonvolatile memory is code which loads the operating system and the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset. Preferably the code which loads the operating system is a first instance of an INT 19h following the reset event.

According to another aspect, there is provided a motherboard comprising: a trusted platform module (TPM); a nonvolatile memory having computer readable program code stored therein; and a circuit board which couples said TPM and said nonvolatile memory and having an unpopulated processor socket and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated; wherein said nonvolatile memory is configured on said circuit board so as to execute code stored therein as the initial code executed in response to a reset event, the code being effective when executing to: read the power-on status state of the status register; determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch

coupled to said circuit board based on the power-on status state as read from the status register; and configure a physical presence flag in said TPM to indicate physical presence in response to a determination that the power-on switch was activated; wherein the code which is effective to read, determine, and configure executes before the execution of code which is stored in other than said nonvolatile memory, and wherein a predetermined trusted operation is allowed to execute in said TPM as a function of the configured physical presence flag.

In one embodiment the code stored in said nonvolatile memory is further effective when executing to: lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM; wherein the code locks the physical presence flag before the execution of code which is stored in other than said nonvolatile memory. Preferably the execution of code which is stored in other than said nonvolatile memory is code which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset. Preferably the code which loads the operating system is a first instance of an INT 19h following the reset event.

According to one embodiment, there is provided a computer system having a trusted platform module (TPM), a nonvolatile memory which stores program code, and a circuit board on which the TPM and the nonvolatile memory are supported. The circuit board preferably also includes a processor for executing the code. The circuit board preferably also includes a status register which assumes a power-on status state indicating how power was last previously applied. The code, while executing, is preferably effective to read the power-on status state of the status register. The code then preferably determines if the last application of power was previously initiated by the activation of a power-on switch. The determination is preferably based on the power-on status state as read from the status register. Preferably, depending on the result, a command is issued which affects the operation of the TPM.

According to one embodiment, there is provided a motherboard article of manufacture for use in the fabrication of computer systems. The motherboard preferably supports and provides electrical interconnection between a trusted platform module (TPM) and a nonvolatile memory which stores program code. The motherboard also preferably includes an unpopulated processor socket which provides

connection for a processor. The socket is preferably so arranged that, when the motherboard is used to manufacture a computer system, the provided processor executes the code in the nonvolatile memory. The motherboard preferably also includes a status register which assumes a power-on status state indicating how power was last previously applied. The code preferably, when executed, is effective to read the power-on status state of the status register. The code preferably then determines if the last application of power was previously initiated by the activation of a power-on switch. The determination is preferably based on the power-on status state as read from the status register. Preferably depending on the result, a command is codified to issue which affects the operation of the TPM.

Preferably according to one embodiment, there is provided a method of providing a trusted platform in a computer system. A determination is preferably made as to whether power was applied to the computer system by the activation of a power-on switch. In making the determination, a power-on status register is preferably read which indicates the occurrence of such activation. Preferably, depending on the outcome of the determination, the operation of a trusted platform module included in the computer system is affected.

In another embodiment, a program product is provided on a computer readable medium having program code stored therein for providing a trusted platform in a computer system. The code is preferably effective when executing to determine whether power was applied to the computer system by the activation of a power-on switch. In making the determination, a power-on status register is preferably read which indicates the occurrence of such activation. Preferably depending on the outcome of the determination, the operation of a trusted platform module included in the computer system is affected.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention will now be described, by way of example only, and with reference to the following drawings:

Fig. 1 illustrates a computer system configured in accordance with an embodiment of the present invention.

Fig. 2 is a detailed block diagram of the security components of an embodiment of the present invention.

Fig. 3 is a perspective view of the motherboard which supports and provides electrical interconnection for the security components of one embodiment of the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

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.

Referring now to the accompanying drawings, and first to Figure 3, there is illustrated a perspective view of a motherboard 301 or circuit board configured in accordance with an embodiment of the present invention. Motherboard 301 provides mechanical support and electrical interconnection between the TPM 111, the NVRAM 116, a core Southbridge chipset 202, and an unpopulated processor socket. This circuit arrangement provides the basis for the manufacture of a trusted system platform which presents and receives information to and from the user. The platform, when manufactured, is composed of the circuit arrangement shown in Figure 3, a processor or CPU provided at the socket 310, and primary peripheral devices (not shown) attached to the circuit board 301. Primary peripheral devices are considered to be those devices which directly attach to and directly interact with the motherboard 301. Examples are PCI cards, LPC components, USB Host controllers and root hubs, attached serial and parallel ports, etc. However, USB and IEEE 1394 devices are not considered primary peripheral devices.

Figure 1 illustrates an exemplary computer system 113 configured in accordance with a preferred embodiment of the present invention (e.g. a computer system which utilizes the motherboard configured in accordance with an embodiment of the present invention). System 113 has a central processing unit (CPU) 110, which is coupled to various other components by system bus 112. The system bus 112 may be a straight bus, or it can be a

hierarchal system of buses. A flash nonvolatile random access memory ("NVRAM") 116 is coupled to the system bus 112 and includes a basic input/output system ("BIOS") that controls certain basic functions of the computer system 113. The function performed by NVRAM 116 of storing the basic input output system is the same as that traditionally performed by a ROM device. The flash device of the present embodiment has the advantage of being field upgradable. Random access memory ("RAM") 114, I/O adapter 118, and communications adapter 134 are also coupled to the system bus 112. I/O adapter 118 may be a small computer system interface ("SCSI") adapter that communicates with a disk storage device 120. Communications adapter 134 interconnects bus 112 with an outside network 160 (e.g., the Internet) enabling the computer system to communicate with other such systems. Input/Output devices are also connected to system bus 112 via user interface adapter 122 and display adapter 136. Keyboard 124 and mouse 126 are all interconnected to bus 112 via user interface adapter 122. Display monitor 138 is connected to system bus 112 by display adapter 136. In this manner, a user is capable of inputting to the system 113 through the keyboard 124 or mouse 126 and receiving output from the system via display 138.

Implementations of the invention preferably include implementations as a computer system programmed to execute the method or methods described herein, and as a computer program product. According to the computer system implementation, sets of instructions or program code for executing the method or methods may be resident in the NVRAM 116. In alternative embodiments, the program code need not reside on NVRAM 116, but can reside on other nonvolatile memories. Until required by the computer system (e.g. one fabricated with the motherboard 301), the program code may be stored as a computer program product in another computer memory, for example, in disk drive 120 (which may include a removable memory such as an optical disk or floppy disk for eventual use in the disk drive 120). In one embodiment(s), regardless of its source, the program code executes as the initial code which runs subsequent to any reset event in the computer system. Further, the code can also be stored at another computer and transmitted when desired to the user's workstation by a network or by an external network 160. One skilled in the art would appreciate that the physical storage of the program code physically changes the medium upon which it is stored so that the medium carries computer readable information. The change may be electrical, magnetic, chemical, biological, or some other physical change. While it is convenient to describe the invention in terms of instructions, symbols, characters, or

the like, the reader should remember that all of these and similar terms should be associated with the appropriate physical elements.

Computer system 113 is implemented to provide a user with a trusted platform upon which certain trusted operations can be performed (e.g. the motherboard 301 may be implemented to provide the user with such a trusted platform). The system (in one embodiment, the motherboard 301) is constructed in accordance to the Trusted Computing Platform Alliance (TCPA) specification entitled *TCPA Main Specification Version 1.1b*, which is hereby incorporated by reference herein. In the preferred embodiment, computer system 113 (in one embodiment, the motherboard 301) is implemented as a PC architecture system and is further adherent to the *TCPA PC Specific Implementation Specification Version 1.00* which is also hereby incorporated herein by reference. Trusted platform module (TPM) 111 is a cryptographic processor which provides computer system 113 (in one embodiment, the motherboard 301) with hardware assisted cryptographic capabilities. TPM 111 can be a fully integrated security module designed to be integrated into systems. Any type of cryptographic processor can be utilized. However, in the preferred embodiment, TPM 111 implements version 1.1b of the TCPA specification for Trusted Platform Modules (TPM). The TPM 111 includes an asymmetric encryption co-processor which amongst other things performs key generation, random number generation, digital signature key generation, and hash generation functions. The TPM 111 is capable of computing a RSA signature using CRT and has an Internal EEPROM Storage for storing a predetermined number of RSA Keys. Also included are a set of 20-byte platform configuration registers (PCRs) for establishing the root of trust for the platform. One example of such a TPM device is an Atmel ™ part number AT97SC320.

In addition to storing the BIOS code, NVRAM 116 also stores code which is used to perform power on self test (POST) routines. A portion of this POST code is responsible for establishing the root of trust for the platform. Trust is established in the platform by having the NVRAM 116 and TPM 111 physically and/or logically coupled in the computer system to form a trusted building block.

As will be explained in greater detail hereinafter, NVRAM 116 and TPM 111 are assembled on a circuit board (e.g. motherboard 301), also known as a motherboard, in such a way that trusted code stored in the NVRAM 116 gains control of the computer system upon a system reset. This trusted code is known as the Core Root of Trust for Measurement (CRTM). In order to verify that the POST code being run is the code shipped by

manufacturer, each section --before it is executed-- is first sized by the CRTM itself (in one embodiment, the code is arranged on the motherboard 301 such that each section -- before it is executed -- is first sized by the CRTM itself). Each section of code is checked for length and check sum, and a hash is created which represents the code being run. Each hash is then stored in one of the 20 byte PCRs within the TPM 111. Verification of these hash values can then be performed by comparing the hash values against published hash values which are published by the manufacturer for verification purposes.

Since it is possible to remotely power-on the computer system, for example by wake on LAN or wake on RING, it is possible to remotely power-on the system and attack it. However, such an attack can be prevented by providing a physical presence detect feature (e.g. on motherboard 301) which meets the requirements of the TCPA specification. In order to maintain a secure system, the CRTM code checks for the physical presence of a person upon power-on before certain critical operations can be performed at the computer system. As will be described in further detail as the description of the present embodiment ensues, rather than implementing a physical jumper or switch as directed by the TCPA specification, the system of the present embodiment (in one embodiment, the motherboard 301) checks for physical presence by examining the core chipset registers for indication of how the computer was powered on. Based upon this examination, the computer system of the present embodiment infers the physical presence of a user. When it is inferred that there is no physical presence, the CRTM code interfaces with the TPM 111 in such a way that the TPM 111 from that point on, from that boot on, will refuse certain critical types of TPM transactions. On the other hand, when it is inferred that there is physical presence, certain critical types of TPM transactions are allowed. Avoiding a physical jumper or switch provides the present embodiment with a lower cost of manufacture. Moreover, the lack of a physical jumper or switch allows the components to be made without electrical or mechanical uniqueness. This lack of uniqueness, in turn, allows a greater ability to leverage the components of the present system as components in other systems sharing the same electrical and mechanical design, thereby further lowering overall costs for the manufacturer (e.g. to leverage the motherboard 301 in any system sharing the same electrical and mechanical design).

Referring to Figure 3 and as previously discussed, there is illustrated a perspective view of a circuit board 301 or motherboard configured in accordance with an embodiment of the present invention.

Circuit board 301 preferably provides mechanical support and electrical interconnection between the TPM 111, the NVRAM 116, a core Southbridge chipset 202, the CPU or a processor (e.g. provided at socket 310). This circuit arrangement provides the basis for a trusted system platform which presents and receives information to and from the user. The platform itself is composed of the circuit arrangement shown in Figure 3, a processor or CPU provided at the socket 310, and primary peripheral devices (not shown) attached to the circuit board 301. Primary peripheral devices are considered to be those devices which directly attach to and directly interact with the CPU 110. Examples are PCI cards, LPC components, USB Host controllers and root hubs, attached serial and parallel ports, etc. However, USB and IEEE 1394 devices are not considered primary peripheral devices.

Referring to Figure 2 and Figure 3, The processor 110 executes the CRTM code stored in the NVRAM 116. As stated previously, this CRTM code interacts with the TPM 111 in such way as to provide a trusted platform. The trusted CRTM code stored in NVRAM 116 and the TPM 111 are the basic components of the trusted platform and are the only trusted components of the platform. When the proper binding is established between the CRTM code and the TPM 111, a basis for trust is established in the platform. The binding of NVRAM 116 and TPM 111 can be physical or logical and is considered to be outside the scope of the present invention. Details concerning the binding of the CRTM to the TPM 111 are well known in the trusted computing art and are omitted so as to not obfuscate the present disclosure in unnecessary detail. In the present embodiment, the CRTM is contained within a portion of NVRAM 116. In another embodiment, however, the CRTM code consumes the entirety of NVRAM 116. Since the CRTM and the TPM 111 are the only trusted components of the platform and since indication of physical presence requires a trusted mechanism to be activated by the platform user, the indication of physical presence is contained within the CRTM code of NVRAM 116 and the TPM 111.

The bus 112 of the preferred embodiment is a hierarchical bus having a north bus bridge (hereinafter "Northbridge," not shown) and a south bus bridge 202 (hereinafter "Southbridge"). The Northbridge encompasses buses which are operationally closer to the processor, such as memory and caching buses. The Southbridge 202 encompasses buses which are closer to system I/O, such as X-Bus, IDE, LPC, and other buses. Note, however, that the bus 112 of the preferred embodiment need not be implemented as a hierarchical bus. Instead, a flat bus as schematically shown in Figure 1 can be implemented physically. Alternatively, a hierarchy involving only

a single bridge chip may be used. The Southbridge 202 provides an LPC bus which, amongst other components, couples NVRAM 116. The LPC bus is a low pin count bus based on the IBM® PCAT bus and forms part of the hierarchical bus 112 (IBM is a registered trademark of International Business Machines Corporation in the United States and other countries). The Southbridge 202 also couples the TPM 111. Southbridge 202 also includes a number of low-level system controllers such as an Advanced Configuration and Power Interface (ACPI) compliant power controller 204. ACPI is an industry-standard interface for OS-directed configuration and power management. The ACPI power controller 204 within the Southbridge 202 provides a hardware interface between the operating system and the devices whose power is being controlled. Many of the functions provided by power controller 204 are accessed via registers as either enable or status registers. One such register is status register 206. Status register 206 contains a series of bits each of which gives status as to the power configuration of the machine and as to its current and initial status. In the preferred embodiment, one of the bits, the power switch bit, is reserved to indicate whether power was last applied to the system by the activation of the system power switch housed on the front face of the system. The system power switch can be connected directly to the circuit board 301 (e.g. motherboard) or indirectly through the power supply. The system power switch can also be mounted on the power supply directly although mounting the power switch to the front face is preferred. When the last application of power was applied to the machine (in one embodiment, to the motherboard 301) by the system power switch, the power switch bit is asserted. When the last application of power was applied to the machine by other than the system power switch, the power switch bit is de-asserted. Thus, if the system (in one embodiment, the system manufactured with the motherboard 301) is remotely powered on, via wake on LAN or wake on RING events, for example, the power switch bit is de-asserted. In the preferred embodiment the power switch bit is implemented such that it is settable only in hardware and not by software. This is done in order to prevent spoofing by trojan or virus software attempting to breach the security of the platform. Allowing the power switch bit to be reset (set to a deasserted state) by software is considered an acceptable design choice since the de-assertion of the power switch bit after the operating system loads is ignored, and even if not ignored software de-assertion of the power switch bit would otherwise serve to increase the level of security in the system. In the preferred embodiment, the power switch bit indicates whether the application of power by the system power switch was initiated at the time of the last power-on event. In an alternative embodiment, the power switch bit can be

designed to indicate whether the system power switch has been depressed. In the latter case, the software which makes the determination must run sooner or otherwise take other measures to make a trusted determination.

Preferably, the processor 110 executes the CRTM code stored in NVRAM 116 as the initial code that executes after a system reset. (In one embodiment, motherboard 301 is constructed with a processor such as processor 110 provided at socket 310.) The system (in one embodiment, the motherboard 301) enters the reset state from either a hardware or software reset event. The hardware reset state is entered upon an application of power in the computer system or it can be entered via a dedicated system reset switch. In the preferred embodiment, the CRTM code is given initial control of the computer system in order to establish trust in the platform. Once the CRTM code executes, the CRTM interacts with the TPM 111 in order to establish the root of trust for the platform. As described previously herein, the CRTM code verifies itself through the use of the hashing functions and PCR registers of the TPM 111. In addition and amongst other things, the CRTM code reads the status register 206 for the current state of the power switch bit. The CRTM code then makes an inference as to the presence or absence of a user at the machine and based on this inference issues a command to the TPM 111 to either limit or allow certain critical TPM functions.

When the power switch bit of status register 206 is found to be in an asserted state, an inference is made that a user is present at the machine. In this case, the issued command allows a predetermined set of functions to execute at the TPM 111. In the preferred embodiment, the issued command is a command which sets a physical presence flag in TPM 111. The TPM 111 is then implemented to only allow certain functions when physical presence is indicated as per the physical presence flag. An example of such a command is a command which resets the TPM 111 to its factory default state. Such a command can only be accepted and executed by TPM 111 if physical presence has been determined.

Conversely, when the power switch bit of status register 206 is found to be in an de-asserted state, an inference is made that a user is not present at the machine. In this case, the issued command blocks a predetermined set of functions to execute at the TPM 111. In the preferred embodiment, the issued command is a command which resets the physical presence flag in TPM 111 following the determination indicating lack of physical presence. The TPM 111 is then implemented to limit certain functions when physical presence is not indicated as per the

physical presence flag. Given this set of circumstances, the exemplary command which attempts to reset the TPM 111 to its factory default state would be blocked by TPM 111 since no physical presence is indicated.

For the most part, details concerning which commands are limited and which commands are allowed by the TPM 111 have been omitted in as much as such details are not necessary to obtain a complete understanding of the present invention and are within the skills of persons of ordinary skill in the relevant art. Otherwise, a reader of arbitrary skill who is interested in details concerning the commands is otherwise directed toward the TCPA specifications incorporated by reference which present such details.

In an alternative embodiment, in addition to setting or resetting the physical presence flag in TPM 111, an additional command is issued which sets a physical presence lock flag in TPM 111. TPM 111 is then implemented such that the value of the physical presence flag is not changeable once the physical presence lock flag has been set. The locking of the physical presence flag has a lifetime which extends to the next platform reset.

Regardless of whether the physical presence flag is locked by the mechanism of the lock flag or by some other binding mechanism, once all of the CRTM metrics have been documented in the hash tables of the TPM 111 PCR's and once physical presence or lack thereof has been established at the TPM 111, the platform is thereafter considered to be trusted and secured to the extent determined. After platform trust has been established, control can then be passed to non-secure code.

In one embodiment of the present invention, control is then passed to nonsecure POST code residing within NVRAM 116. In this embodiment, the code which is given control after the platform is secured is code which accesses any computer system I/O device such as a keyboard device, a video device, or a pointing device.

In another embodiment, the CRTM code is considered to be the entirety of code stored within NVRAM 116. In this embodiment, control is then passed to nonsecure code stored in other than the NVRAM 116. Generally, this would be code which loads the operating system. In an IBM PC compatible computer system (in one embodiment, in a motherboard for an IBM PC compatible computer system), the loading of the operating system is typically instantiated by the execution of a software INT 19 executed as

the last instruction stored within the NVRAM 116. However, one of ordinary skill in the art is able to use other methods to load the operating system and any method used would not depart from the spirit and scope of the present invention.

CLAIMS

1. A method comprising the steps of:

determining whether power was applied to a computer system by the activation of a power-on switch by reading a power-on status register which indicates the occurrence of such activation; and

affecting the operation of a trusted platform module (TPM) included in the computer system as a function of said determination.

2. The method of Claim 1 wherein the power-on status register is settable only in hardware.

3. The method of Claim 1 wherein said determining and affecting steps occur subsequent to a reset event and prior to an OS load event which loads the operating system.

4. The method of Claim 3 wherein the OS load event is a first instance of an INT 19h following the reset event.

5. The method of Claim 3 wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

6. The method of Claim 3 wherein said affecting step further comprises the step of:

setting a physical presence flag in the TPM.

7. The method of Claim 6 wherein said affecting step further comprises the step of:

setting a physical presence lock flag in the TPM.

8. The method of Claim 1 wherein said determining and affecting steps occur subsequent to a reset event and prior to the availability of a computer system I/O device, wherein the computer system I/O device is a device selected from the group consisting of a keyboard device, a video device, and a pointing device.

9. The method of Claim 8 wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

10. The method of Claim 1 wherein said affecting step is one which limits the operation of the TPM in response to a determination in said determining step that the power-on switch was not activated.

11. The method of Claim 1 wherein said affecting step is one which allows a predetermined trusted operation to execute in the TPM in response to an application of power by the activation of the power-on switch as determined in said determining step.

12. A method comprising the steps of:

determining whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware;

configuring a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate lack of physical presence in response to a determination in said determining step that the power-on switch was not activated;

wherein said determining and configuring steps occur after a system reset event and before an OS load event, and

limiting the operation of the TPM as a function of said configuring step.

13. The method of Claim 12, further comprising the steps of:

locking the physical presence flag in the TPM by setting a physical presence lock flag in the TPM;

wherein said locking step occurs after the system reset event and before the OS load event.

14. The method of Claim 13 wherein the os load event is an event which loads the operating system and wherein the system reset event is

an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

15. The method of Claim 14 wherein the event which loads the operating system is a first instance of an INT 19h following the system reset event.

16. A method comprising the steps of:

determining whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware;

configuring a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate physical presence in response to an application of power by the activation of the power-on switch as determined in said determining step;

wherein said determining and configuring steps occur after a system reset event and before an OS load event, and

allowing a predetermined trusted operation to execute in the TPM as a function of said configuring step.

17. The method of Claim 16 further comprising the steps of:

locking the physical presence flag in the TPM by setting a physical presence lock flag in the TPM;

wherein said locking step occurs after the system reset event and before the OS load event.

18. The method of Claim 17 wherein the os load event is an event which loads the operating system and wherein the system reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

19. The method of Claim 18 wherein the event which loads the operating system is a first instance of an INT 19h following the system reset event.

20. A program product comprising:

a computer usable medium having computer readable program code embodied therein, the computer readable program code in said program product being effective when executing to:

determine whether power was applied to a computer system by the activation of a power-on switch by reading a power-on status register which indicates the occurrence of such activation; and

affect the operation of a trusted platform module (TPM) included in the computer system as a function of said determination.

21. A program product comprising:

a computer usable medium having computer readable program code embodied therein, the computer readable program code in said program product being effective when executing to:

determine whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware;

configure a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate lack of physical presence in response to said determination indicating that the power-on switch was not activated;

wherein said determination and configuration occur after a system reset event and before an OS load event, and

limit the operation of the TPM as a function of said configuration.

22. A program product comprising:

a computer usable medium having computer readable program code embodied therein, the computer readable program code in said program product being effective when executing to:

determine whether power was applied to a computer system by the activation of a power-on switch coupled to the computer system by reading a power-on status register which indicates the occurrence of such activation, wherein the power-on status register is settable only in hardware;

configure a physical presence flag of a trusted platform module (TPM) included in the computer system to indicate physical presence in response to an application of power by the activation of the power-on switch in accordance to said determination;

wherein said determination and configuration occur after a system reset event and before an OS load event, and

allow a predetermined trusted operation to execute in the TPM as a function of said configuration.

23. Apparatus comprising:

a trusted platform module (TPM);

a nonvolatile memory having computer readable program code stored therein; and

a circuit board which couples said TPM and said nonvolatile memory and which includes a processor which executes the code stored in said nonvolatile memory and further includes a status register which assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated;

wherein the processor, when executing the code stored in said nonvolatile memory, is effective to:

read the power-on status state of the status register;

determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch

coupled to said circuit board based on the power-on status state as read from the status register; and

issue a command which affects the operation of said TPM as a function of the determined power-on state.

24. Apparatus of Claim 23 wherein the status register is settable only in hardware.

25. Apparatus of Claim 23 wherein the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which is stored in other than said nonvolatile memory.

26. Apparatus of Claim 23 wherein the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which loads the operating system.

27. Apparatus of Claim 26 wherein the code which loads the operating system is a first instance of an INT 19h following the reset event.

28. Apparatus of Claim 25 wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

29. Apparatus of Claim 25 wherein the code stored in said nonvolatile memory is further effective when executing to:

set a physical presence flag in said TPM.

30. Apparatus of Claim 29 wherein the code stored in said nonvolatile memory is further effective when executing to:

set a physical presence lock flag in said TPM.

31. Apparatus of Claim 23 wherein the code which is effective to read, determine, and issue is executed subsequent to a reset event and prior to any execution of code which accesses a computer system I/O device, wherein the computer system I/O device is a device selected from the group consisting of a keyboard device, a video device, and a pointing device.

32. Apparatus of Claim 23 wherein the issued command limits the operation of said TPM in response to a determination that the power-on

switch was not activated in the last previously initiated application of power based on the power-on status state as read from the status register.

33. Apparatus of Claim 23 wherein the issued command allows a predetermined trusted operation to execute in said TPM in response to a determination that the power- on switch was activated in the last previously initiated application of power based on the power-on status state as read from the status register.

34. Apparatus comprising:

a trusted platform module (TPM);

a nonvolatile memory having computer readable program code stored therein; and

a circuit board which couples said TPM and said nonvolatile memory and having a processor and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated;

wherein the processor and said nonvolatile memory are configured on said circuit board so as to execute code stored therein as the initial code executed by the processor in response to a reset event, the code being effective when executing to:

read the power-on status state of the status register;

determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and

configure a physical presence flag in said TPM to indicate lack of physical presence in response to a determination that the power-on switch was not activated;

wherein the code which is effective to read, determine, and configure executes before an OS load event, and wherein operation of said TPM is limited as a function of the configured physical presence flag.

35. Apparatus of Claim 34 wherein the code stored in said nonvolatile memory is further effective when executing to:

lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM;

wherein the code locks the physical presence flag before the OS load event.

36. Apparatus of Claim 35 wherein the os load event is an event which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

37. Apparatus of Claim 36 wherein the event which loads the operating system is a first instance of an INT 19h following the reset event.

38. Apparatus comprising:

a trusted platform module (TPM);

a nonvolatile memory having computer readable program code stored therein; and

a circuit board which couples said TPM and said nonvolatile memory and having a processor and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated;

wherein the processor and said nonvolatile memory are configured on said circuit board so as to execute code stored therein as the initial code executed by the processor in response to a reset event, the code being effective when executing to:

read the power-on status state of the status register;

determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and

configure a physical presence flag in said TPM to indicate physical presence in response to a determination that the power-on switch was activated;

wherein the code which is effective to read, determine, and configure executes before an OS load event, and wherein a predetermined trusted operation is allowed to execute in said TPM as a function of the configured physical presence flag.

39. Apparatus of Claim 38 wherein the code stored in said nonvolatile memory is further effective when executing to:

lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM;

wherein the code locks the physical presence flag before the OS load event.

40. Apparatus of Claim 39 wherein the os load event is an event which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

41. Apparatus of Claim 40 wherein the event which loads the operating system is a first instance of an INT 19h following the reset event.

42. A motherboard comprising:

a circuit board having an unpopulated processor socket and a status register which assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated;

a trusted platform module (TPM) mounted on said circuit board; and

a nonvolatile memory mounted on said circuit board and coupled thereby to said TPM and having computer readable program code stored therein;

the code stored in said nonvolatile memory being effective when executing to:

read the power-on status state of the status register;

determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and

issue a command which affects the operation of said TPM as a function of the determined power-on state.

43. The motherboard of Claim 42 wherein the status register which indicates that power was applied by activation of the power-on switch is settable only in hardware.

44. The motherboard of Claim 42 wherein the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which is stored in other than said nonvolatile memory.

45. The motherboard of Claim 42 wherein the code which is effective to read, determine, and issue is executed after a reset event and prior to the execution of code which loads the operating system.

46. The motherboard of Claim 45 wherein the code which loads the operating system is a first instance of an INT 19h following the reset event.

47. The motherboard of Claim 44 wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

48. The motherboard of Claim 44 wherein the code stored in said nonvolatile memory is further effective when executing to:

set a physical presence flag in said TPM.

49. The motherboard of Claim 48 wherein the code stored in said nonvolatile memory is further effective when executing to:

set a physical presence lock flag in said TPM.

50. The motherboard of Claim 42 wherein the code which is effective to read, determine, and issue is executed subsequent to a reset event and prior to any execution of code which accesses a computer system I/O device, wherein the computer system I/O device is a device selected from the group consisting of a keyboard device, a video device, and a pointing device.

51. The motherboard of Claim 42 wherein the issued command limits the operation of said TPM in response to a determination that the power-on switch was not activated in the last previously initiated application of power based on the power-on status state as read from the status register.

52. The motherboard of Claim 42 wherein the issued command allows a predetermined trusted operation to execute in said TPM in response to a determination that the power-on switch was activated in the last previously initiated application of power based on the power-on status state as read from the status register.

53. A motherboard comprising:

a trusted platform module (TPM);

a nonvolatile memory having computer readable program code stored therein; and

a circuit board which couples said TPM and said nonvolatile memory and having an unpopulated processor socket and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated;

wherein said nonvolatile memory is configured on said circuit board so as to execute code stored therein as the initial code executed in response to a reset event, the code being effective when executing to:

read the power-on status state of the status register;

determine whether the application of power to said circuit board was last previously initiated by the activation of a power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and

configure a physical presence flag in said TPM to indicate lack of physical presence in response to a determination that the power-on switch was not activated;

wherein the code which is effective to read, determine, and configure executes before the execution of code which is stored in other than said

nonvolatile memory, and wherein operation of said TPM is limited as a function of the configured physical presence flag.

54. The motherboard of Claim 53 wherein the code stored in said nonvolatile memory is further effective when executing to:

lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM;

wherein the code locks the physical presence flag before the execution of code which is stored in other than said nonvolatile memory.

55. The motherboard of Claim 54 wherein the execution of code which is stored in other than said nonvolatile memory is code which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

56. The motherboard of Claim 55 wherein the code which loads the operating system is a first instance of an INT 19h following the reset event.

57. A motherboard comprising:

a trusted platform module (TPM);

a nonvolatile memory having computer readable program code stored therein; and

a circuit board which couples said TPM and said nonvolatile memory and having an unpopulated processor socket and a status register which is settable only in hardware and assumes a power-on status state which indicates how the application of power to said circuit board was last previously initiated;
wherein said nonvolatile memory is configured on said circuit board so as to execute code stored therein as the initial code executed in response to a reset event, the code being effective when executing to:

read the power-on status state of the status register;

determine whether the application of power to said circuit board was last previously initiated by the activation of a

power-on switch coupled to said circuit board based on the power-on status state as read from the status register; and

configure a physical presence flag in said TPM to indicate physical presence in response to a determination that the power-on switch was activated;

wherein the code which is effective to read, determine, and configure executes before the execution of code which is stored in other than said nonvolatile memory, and wherein a predetermined trusted operation is allowed to execute in said TPM as a function of the configured physical presence flag.

58. The motherboard of Claim 57 Wherein the code stored in said nonvolatile memory is further effective when executing to:

lock the physical presence flag in said TPM by setting a physical presence lock flag in said TPM;

wherein the code locks the physical presence flag before the execution of code which is stored in other than said nonvolatile memory.

59. The motherboard of Claim 58 wherein the execution of code which is stored in other than said nonvolatile memory is code which loads the operating system and wherein the reset event is an event selected from the group consisting of a hardware initiated reset and a software initiated reset.

60. The motherboard of Claim 59 wherein the code which loads the operating system is a first instance of an INT 19h following the reset event.

FIG. 1

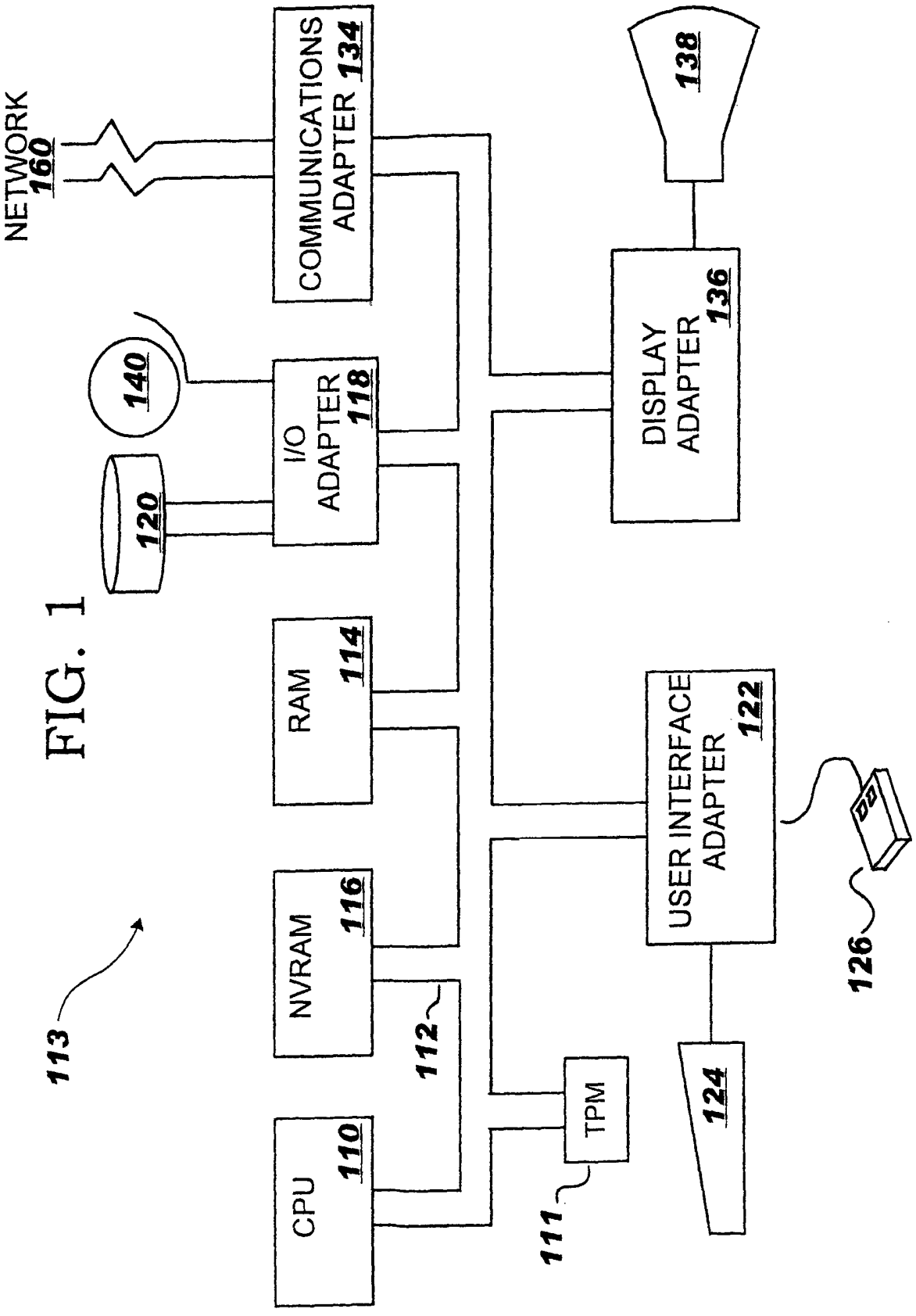

NETWORK
160
COMMUNICATIONS ADAPTER 134
138
DISPLAY ADAPTER 136
140
I/O ADAPTER 118
120
RAM 114
NVRAM 116
112
USER INTERFACE ADAPTER 122
126
113
CPU 110
TPM
111
124

FIG. 2

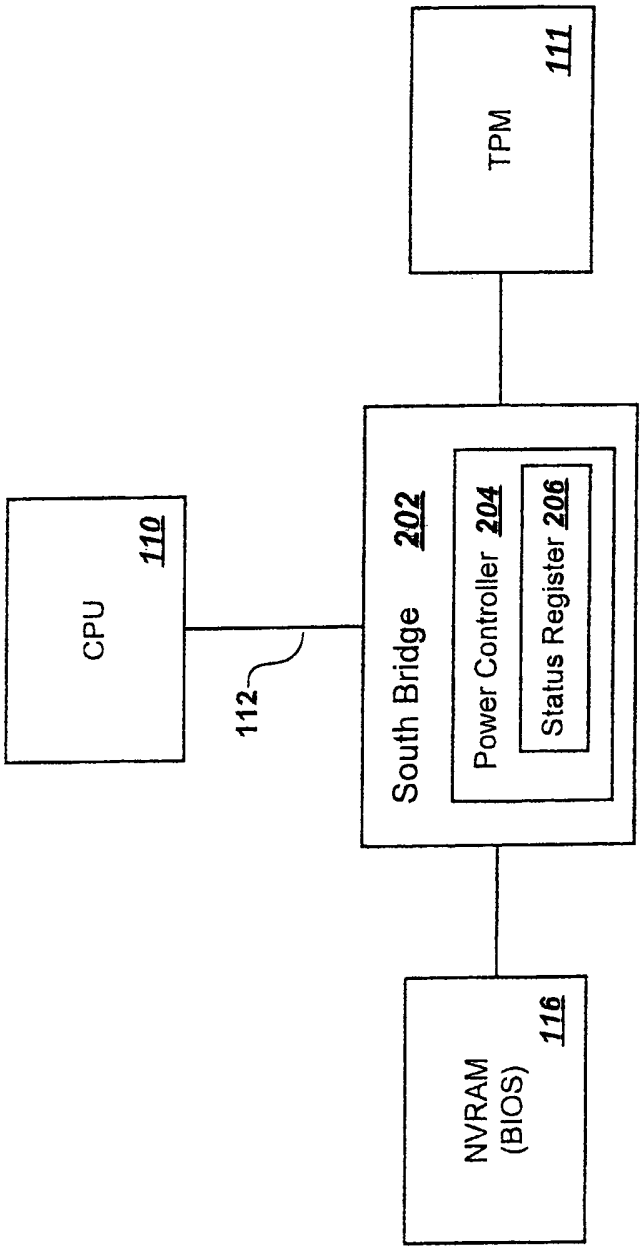

TPM
111
CPU
110
112
South Bridge
202
Power Controller
204
Status Register
206
NVRAM
(BIOS)
116

FIG. 3