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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2008 (02.10.2008)

PCT

(10) International Publication Number
WO 2008/118663 A1

(51) International Patent Classification:
G06F 9/445 (2006.01)

(21) International Application Number:
PCT/US2008/057057

(22) International Filing Date: 14 March 2008 (14.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/692,237 28 March 2007 (28.03.2007) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventor: **CARPENTER, Todd L.**; c/o Microsoft Corporation, International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) Title: DIRECT PERIPHERAL COMMUNICATION FOR RESTRICTED MODE OPERATION

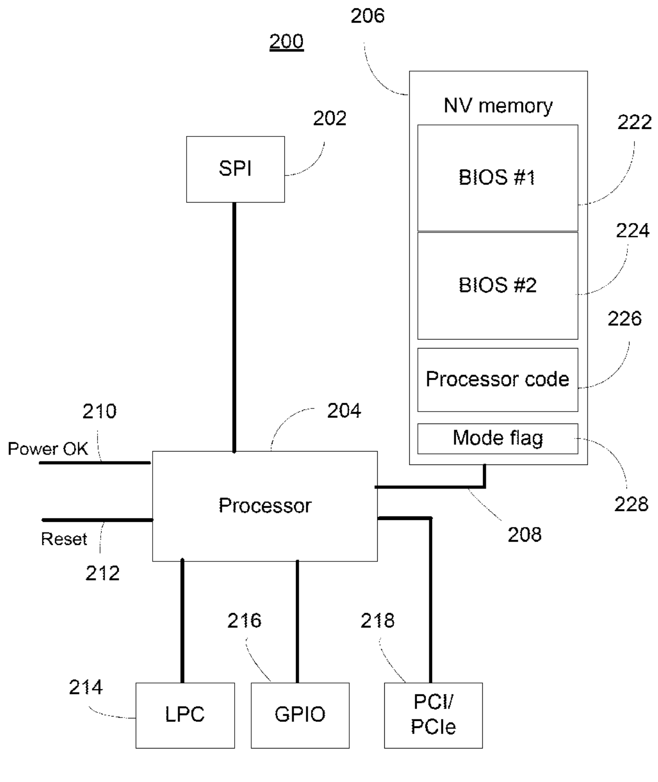

Fig. 2

(57) Abstract: A computer that self-administers operating in restricted and unrestricted operating modes boots from a main processor and operates normally in the unrestricted operating mode and operates from an alternate processor in a security module in the restricted operating mode. The alternate processor may communicate directly with peripheral devices such as a display controller and keyboard. Because the main processor is not used and may not even be started in the restricted operating mode, viruses, shims, and other related attacks are virtually eliminated. In one embodiment, the security module may operate as a PCI bus master when in the restricted operating mode.

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

DIRECT PERIPHERAL COMMUNICATION FOR RESTRICTED MODE OPERATION

BACKGROUND

[0001] In many cases, it is desirable to restrict the operation of a computer to known modes. For example, a parent may wish to restrict gaming time while allowing word processing. In another example, a company may wish to limit the use of an expensive peripheral, such as a 3-D printer, to only authorized users. In another example, a pay-per-use computer may have an unlimited use mode when the terms of an associated contract are satisfied and a restricted use mode that only allows input of additional usage time or points when terms of the associated contract are not met.

[0002] In the latter case, a low, subsidized, initial price of a computer may require a contractual obligation to recoup an underwriters investment. Because contractual terms may have already been intentionally disregarded, a user may be inclined to attempt to defeat or evade the restricted use mode. Doing so may allow the user to enjoy the benefits of the computer without meeting contractual terms, such as payment of monthly subscription fees, to the detriment of the underwriter.

SUMMARY

[0003] A computer may be required to self-administer a restricted-use mode when a user is able to isolate the computer from other means of sanctioning, such as a computer network or Internet Service Provider (ISP). Therefore, the circuitry involved in the restricted use mode can be expected to attract hacking attempts by unscrupulous users. An attack profile for defeating restricted mode operation is directly related to the number of components that are active, particularly those involved in enforcing such operation. The attack profile may be dramatically reduced when a security module used for metering and enforcement acts as a bus master, for example, on a peripheral component interconnect (PCI) bus, to directly communicate with a limited number of required components. For example, a security module may directly control a display interface and keyboard controller to provide a minimal user interface to allow entry of data to restore full services.

[0004] By avoiding use of the computer's main processor, main memory, disk drives, other chipset components, etc., most conventional attacks, such as buffer overflow attacks or memory swapping, are immediately eliminated. Even though the security module may become the focus of attacks, this also allows a design and manufacturing focus on protection of the security module rather than trying to protect every hardware and software aspect of the computer. The security module may be a standalone component or may be integrated into a communication or processing circuit, such as one of the chipset components common in known computer architectures.

[0005] The use of pre-boot direct device communication may be used to in many embodiments. In one embodiment, basic user interface and communication functions may be supported without intervention from a main processor of the computer. In another embodiment, the direct device communication may be used in conjunction with system checks verify the security and health of the computer. Following such checks, the direct device communication may be used to unlock those same components for normal operation supporting a normal boot process with a standard basic input/output system (BIOS).

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Fig. 1 is a simplified and exemplary block diagram of a computer system suitable for use with peer-to-peer communication for secure operation;

[0007] Fig. 2 is a simplified and exemplary block diagram of a security module; and

[0008] Fig. 3 is a flow chart of an exemplary method of executing peer-to-peer communication for secure operation.

DETAILED DESCRIPTION

[0009] Although the following text sets forth a detailed description of numerous different embodiments, it should be understood that the legal scope of the description is defined by the words of the claims set forth at the end of this disclosure. The detailed description is to be construed as exemplary only and does not describe every possible embodiment since describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology developed after the filing date of this patent, which would still fall within the scope of the claims.

[0010] It should also be understood that, unless a term is expressly defined in this patent using the sentence "As used herein, the term '______' is hereby defined to mean..." or a similar sentence, there is no intent to limit the meaning of that term, either expressly or by implication, beyond its plain or ordinary meaning, and such term should not be interpreted to be limited in scope based on any statement made in any section of this patent (other than the language of the claims). To the extent that any term recited in the claims at the end of this patent is referred to in this patent in a manner consistent with a single meaning, that is done for sake of clarity only so as to not confuse the reader, and it is not intended that such claim term by limited, by implication or otherwise, to that single meaning. Finally, unless a claim element is defined by reciting the word "means" and a function without the recital of any structure, it is not intended that the scope of any claim element be interpreted based on the application of 35 U.S.C. § 112, sixth paragraph.

[0011] Much of the inventive functionality and many of the inventive principles are best implemented with or in software programs or instructions and integrated circuits (ICs) such as application specific ICs. It is expected that one of ordinary skill, notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation. Therefore, in the interest of brevity and minimization of any risk of obscuring the principles and concepts in accordance to the present invention, further discussion of such software and ICs, if any, will be limited to the essentials with respect to the principles and concepts of the preferred embodiments.

[0012] With reference to Fig. 1, an exemplary system for implementing the claimed method and apparatus includes a general purpose computing device in the form of a computer 110. Components shown in dashed outline are not technically part of the computer 110, but are used to illustrate the exemplary embodiment of Fig. 1. Components of computer 110 may include, but are not limited to, a main processor 120, a system memory 130, a memory/graphics interface 121, also known as a Northbridge chip, and an I/O interface 122, also known as a Southbridge chip. A memory 130 and a graphics processor 190 may be coupled to the memory/graphics interface 121. A monitor 191 or other graphic output device may be coupled to the graphics processor 190.

[0013] A series of system busses may couple various these system components including a high speed system bus 123 between the main processor 120, the memory/graphics interface 121 and the I/O interface 122, a front-side bus 124 between the memory/graphics interface 121 and the system memory 130, and an advanced graphics processing (AGP) bus 125 between the memory/graphics interface 121 and the graphics processor 190. The system bus 121 may be any of several types of bus structures including, by way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus and Enhanced ISA (EISA) bus. As system architectures evolve, other bus architectures and chip sets may be used but often generally follow this pattern. For example, companies such as Intel and AMD support the Intel Hub Architecture (IHA) and the Hypertransport architecture, respectively.

[0014] Computer 110 typically includes a variety of computer readable media. Computer readable media can be any available media that can be accessed by computer 110 and includes both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes both volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can accessed by computer 110. Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term “modulated data signal” means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0015] The system memory 130 includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) 132. The system ROM 131 may contain permanent system data 143, such as identifying and manufacturing information. In some embodiments, a basic input/output system (BIOS) may also be stored in system ROM 131. RAM 132 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by main processor 120. By way of example, and not limitation, Fig. 1 illustrates operating system 134, application programs 135, other program modules 136, and program data 137.

[0016] The I/O interface 122 may couple the system bus 123 with a number of other busses 126, 127 and 128 that couple a variety of internal and external devices to the computer 110. A serial peripheral interface (SPI) bus 128 may connect to a basic input/output system (BIOS) memory 133 containing the basic routines that help to transfer information between elements within computer 110, such as during start-up.

[0017] A security module 129 may also be coupled to the I/O controller 122 via the SPI bus 126. In other embodiments, the security module 129 may be connected via any of the other busses available in the computer 110. In a pay-per-use business model, the security module 129 may meter usage, support booting from a known BIOS, and monitor compliance to metering-related policies. When tampering or other suspicious behavior is observed that may indicate attempts to circumvent pay-per-use operation, the security module 129 may sanction the computer by forcing operation in a limited function mode.

[0018] A super input/output chip 160 may be used to connect to a number of ‘legacy’ peripherals, such as floppy disk 152, keyboard/mouse 162, and printer 196, as examples. The super I/O chip 122 may be connected to the I/O interface 121 with a low pin count (LPC) bus, in some embodiments. The super I/O chip is widely available in the commercial marketplace.

[0019] In one embodiment, bus 128 may be a Peripheral Component Interconnect (PCI) bus, or a variation thereof, may be used to connect higher speed peripherals to the I/O interface 122. A PCI bus may also be known as a Mezzanine bus. Variations of the PCI bus include the Peripheral Component Interconnect-Express (PCI-E) and the Peripheral Component Interconnect – Extended (PCI-X) busses, the former having a serial interface and the latter being a backward compatible parallel interface. In other embodiments, bus

128 may be an advanced technology attachment (ATA) bus, in the form of a serial ATA bus (SATA) or parallel ATA (PATA).

[0020] The computer 110 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, Fig. 1 illustrates a hard disk drive 140 that reads from or writes to non-removable, nonvolatile magnetic media. Removable media, such as a universal serial bus (USB) memory 152 or CD/DVD drive 156 may be connected to the PCI bus 128 directly or through an interface 150. Other removable/non-removable, volatile/nonvolatile computer storage media that can be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like.

[0021] The drives and their associated computer storage media discussed above and illustrated in Fig. 1, provide storage of computer readable instructions, data structures, program modules and other data for the computer 110. In Fig. 1, for example, hard disk drive 140 is illustrated as storing operating system 144, application programs 145, other program modules 146, and program data 147. Note that these components can either be the same as or different from operating system 134, application programs 135, other program modules 136, and program data 137. Operating system 144, application programs 145, other program modules 146, and program data 147 are given different numbers here to illustrate that, at a minimum, they are different copies. A user may enter commands and information into the computer 20 through input devices such as a mouse/keyboard 162 or other input device combination. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 120 through one of the I/O interface busses, such as the SPI 126, the LPC 127, or the PCI 128, but other busses may be used. In some embodiments, other devices may be coupled to parallel ports, infrared interfaces, game ports, and the like (not depicted), via the super I/O chip 160.

[0022] The computer 110 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 180 via a network interface controller (NIC) 170, . The remote computer 180 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer

110. The logical connection depicted in Fig. 1 may include a local area network (LAN), a wide area network (WAN), or both, but may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0023] In some embodiments, the network interface may use a modem (not depicted) when a broadband connection is not available or is not used. It will be appreciated that the network connection shown is exemplary and other means of establishing a communications link between the computers may be used.

[0024] Fig. 2 depicts a security module 200, similar to the security module 129 of Fig. 1. The exemplary embodiment of the security module 200 is but one example of a security module suitable for use in this application. The security module 200 may be a standalone component. In other embodiments, the security module 200 may be incorporated in another component, for example, a chipset component such as the I/O interface 122. The I/O interface 122 is strategically located on each of the major system busses and allows almost transparent access to most of the major systems and components of a computer as shown in Fig. 1.

[0025] The security module 200 may have several functions. One function may be to represent the interests of an underwriter with a financial stake in the computer by requiring that the underwriter's contractual terms are met. Those terms may include payment for use of the computer in the form of a subscription or metered usage time. The security module 200 may include metering circuitry (not depicted) and a memory for saving stored value. The security module 200 may or may not have integrated BIOS memory.

[0026] The security module 200 may also include circuitry and applications associated with its second function of enforcing a limited function mode of operation when the contractual terms are not met. The goal of the limited, or restricted, mode of operation is to deny the user beneficial use of the computer while supporting enough functionality to restore normal operation by updating the subscription or adding resources to the stored value balance. The use of direct communication for restricted mode operation may be one aspect of this enforcement function. As shown in Fig. 2, a serial peripheral interface (SPI) 202 may be coupled to a processor 204 and a nonvolatile memory 206. The SPI interface 202 may be connected to an SPI master device, such as I/O interface 122 of Fig. 1. In one embodiment, the processor 204 may be coupled to the nonvolatile memory 206 via a bus

208 that may be another serial peripheral interface or another kind of memory bus. In another embodiment, the SPI interface 202 may connect to both the processor and the nonvolatile memory 206.

[0027] The processor 204 may be coupled to other exemplary bus interfaces such as an low pin count (LPC) interface 214, a general purpose input/output (GPIO) interface 216, or a PCI interface 218. In other embodiments, more or fewer busses may be connected to the processor 204. The nonvolatile memory 206 may include partitions for a first BIOS 222, a second BIOS 224, as well as executable processor code 226 used by the processor 204. A mode flag 228 may provide a secure way of persisting the operating state of the computer, that is, restricted or unrestricted, following the next reset.

[0028] A power OK pin 210 may be used to monitor or set a signal indicating that the power supply is stable. As will be discussed, this signal may also be used to selectively disable some circuits. A reset output 212 may be used by the processor 204 to cause an interruption in operation of a computer incorporating the security device 200, such as computer 110 of Fig. 1.

[0029] The processor 204 may be a single-chip processor such as an ARM processor from ARM Ltd of Cambridge, UK, although similar processors from Intel and Freescale Semiconductor are also available. The nonvolatile memory 206 may be a flash technology device widely available in the commercial marketplace.

[0030] In operation, when reset activity is detected, for example, when a Power OK signal 210 transitions from inactive to active, the processor 204 may read the mode flag 228 to determine how to start the computer 110. If the mode flag indicates normal operation, the processor 204 may allow access to a BIOS designated for normal operation, for example, BIOS 222. However, when the mode flag 228 indicates operation is to be in the restricted mode, the processor 204 may block access to the normal boot BIOS and may instead cause the computer 110 to boot from a secondary BIOS 224. The secondary BIOS 224 may not activate all the functions of the computer 110. In one embodiment, the BIOS 224 is code only used by the processor 204 or a link to the processor code 226. In this embodiment, with operation designated in the restricted mode, the processor 204 may take over operation of the computer 110.

[0031] In order to accomplish this, the processor 204, responsive to executable commands in the alternate BIOS 224 or processor code 226, may create a direct link to various peripheral devices needed for minimal functionality. Such minimal functionality may include access to the graphics controller 190 to enable output to the monitor 191 and to the keyboard/mouse 162, either directly or through the Super I/O chip 160. Minimal functionality may also include a direct connection to the network interface 170 for communication with a remote computer 180, or to access a network accessible user input device, such as a terminal (not depicted).

[0032] Direct connection does not necessarily mean without any intervening circuitry, but rather is intended to denote that data is passed without any intervention or activity on part of the main processor 120. Because the main processor 120 is bypassed, the associated peripherals, firmware, and software associated with activating and operating the main processor 120 are also unnecessary and may also be bypassed or not even started. The degree to which the main processor 120 and other devices, such as disk drives, the Northbridge, etc. are not activated is a design decision, but each boot activity from a normal boot that is not performed, contributes to lowering the overall attack profile of the computer 110.

[0033] The smallest possible attack profile may then be provided by only activating the minimal number of components required to conditions for unrestricted operation. In one embodiment, the minimal number of components may be use of enough of the display 191 to support a prompt and enough of an input capability, such as keyboard/mouse 162 to support entry of an unlock code or provisioning packet. Other useful peripherals for entry of provisioning information may be removable media such as floppy disk 152, CD/DVD 156, or USB port 152 to support a flash drive. Connection to remote computer 180 via network interface 170 may also provide access to restoration data such as a provisioning packet.

[0034] Not starting the main processor 120 also implies that any attack targeted at the operating system 134 or applications 135, including viruses, would be not be effective, since the OS 134 and applications 135 are not activated.

[0035] In one embodiment that disables the main processor 120, the processor 204 may have Power OK output 210 connected to a Power OK input (not depicted) on the main processor 120. When the processor 204 determines that operation is to be in the restricted operation mode, the Power OK output 210 may be reset, causing the main processor to not start, or if operating, to cease operation, as if the power were shutting down. Other circuits that respond to the Power OK signal may be similarly disabled when the processor 204 determines operation in the restricted mode. For example, a non-removable non-volatile memory controller 140, such as a disk controller, may be prevented from starting when operation is in the restricted mode by controlling the Power OK signal.

[0036] After determining that the computer 110 is to be operated in the restricted mode, the direct link may be established between the security module 200 and another peripheral or peripheral controller, such as graphics processor 190. The security module 200 may operate as a bus master when communicating over the PCI bus 128. Operation as aPCI bus master allows the security module 200 perform known control functions to select a target component from among connected PCI devices and carry on bidirectional communication with the targeted component. When other busses are used, appropriate controls and protocols may be used. For example, even though the protocol may dictate certain signal levels and timing, the message traffic may follow other standard formats such as XML, to allow standardization and convenience for development, debugging, and maintenance of inter-component messaging.

[0037] Another risk for restricted mode operation may be substitution of components, either to try to circumvent control by the security module 200 or to strip parts from the computer for resale. Both of these threats may be addressed by cryptographic verification that the correct components are present and functional, or at least functional enough to respond to a challenge issued by the security module 200. While in a secure manufacturing environment, or in another trusted setting, components installed in the computer may be given secret keys that can be used for one-way or mutual verification. Such mutual verification between the security module 200 and other components may be performed as part of each boot, only when tampering is suspected, when in the restricted operating mode, or a combination of these.

[0038] Fig. 3, a method of using peer-to-peer communication for secure operation of a computer, is discussed and described. At block 302, when a computer, such as computer 110 of Fig. 1, is started, an early process may activate a security module, such as security module 129 of Fig. 1. Optionally, at block 303, certain components may be designated to start in a locked mode. The locked mode setting of components such as the I/O interface 122, the memory/graphics interface 121, the network interface 170, the processor 120, etc., may further hinder attempts to bypass security measures taken at startup. Components started in the locked mode may support normal operating functions after being unlocked by the security module 129.

[0039] At block 304, the security module 129 may determine whether the computer should be activated in a normal, unrestricted operating mode or a restricted operating mode. This determination may be made by checking the state of a memory location, such as mode flag 228 of Fig. 2. A flag value of zero may indicate normal operation and a flag value of one may indicate restricted operation. As mentioned above, the goal of restricted operation is to limit use of the computer to only those functions required to bring the computer back into compliance with contractual terms of operation, e.g. updating a subscription end date or adding usage time to a stored value balance in the security module 129.

[0040] When, at block 304, the determination is made that operation should be in the unrestricted mode, the "unrestricted" branch from block 304 may be taken to block 305. If the component locking function at block 303 was active, at block 305 an unlock message may be sent to each of those components previously locked. A single message may be broadcast to each component on a single bus or a series of independent messages may be sent to each locked component. In one embodiment, a security module 200 may hold the power OK line 210 to the processor 120 until all components acknowledge being unlocked, at which point the power OK line 120 may be released and the processor 120 can begin a normal boot sequence. At block 306, the security module 129 may allow booting from a standard BIOS and for operation to proceed under normal conditions, that may include usage metering and tamper monitoring. If, during the course of operation, conditions change, such as a metering balance going to zero, the mode flag 228 may be set and a reset forced on the computer 110 to send operation back to block 302.

[0041] When, at block 304, the determination is made that a condition exists that indicates operation in a restricted mode, such as the mode flag 228 being set or a zero stored value balance, the "restricted" branch from block 304 may be taken to block 308. At block 308, the security module 129 may block execution of the normal boot process. In one embodiment, the security module 129 may block access to the normal boot BIOS 222 and instead use the security module’s own internal processor 204 to support the restricted mode operation operating from an alternate BIOS 224 or from executable code 226 used for the security module’s normal execution. If, at block 303, components were started in the locked mode, those components required for restricted operation may be unlocked. For example, the memory/graphics interface 121 and the network interface 170 may be unlocked as needed.

[0042] Part of the restricted mode operation may include verification of one or more peripheral devices through a cryptographic challenge response function. For example, the security module 129 may send an encrypted nonce to a graphics processor 190 and receive back the decrypted nonce and an encrypted device identifier. If, at block 310, the peripheral device verification passes, the past branch from block 310 may be taken to block 312.

[0043] At block 312, the security module 129 may send a message, and some embodiments an encrypted message, to the graphics controller 190 or another device capable of supporting user interface, such as a TDD hearing impaired interface (not depicted). The message may prompt a user to enter an unlock code or token, such as a flash disk, to recover from the condition that caused operation in the restricted mode. In some cases the token may be available via the network interface 170 from a remote device, such as remote computer 180. In such a circumstance the network interface 170 may be activated and controlled directly from the security module 129.

[0044] At block 314, the security module 129 received a requested data and at block 316 determine if the data is sufficient to allow restoration of full operation. If so, the "yes" branch from block 316 may be taken to block 318 where the mode flag 228 may be cleared, or otherwise set to unrestricted, and the computer may be reset, for example by activating the reset output 212 of the security module 129. In another embodiment, components locked at block 303 may be unlocked and operation may continue through a normal boot. If, at block 316 the data does not satisfy the requirements for restoration of operation, the "no" branch from block 316 may be taken to block 312 and the user prompted to reenter the unlock code or other restoration data.

[0045] At block 310, if the peripheral device verification fails, indicating physical tampering with the device or a catastrophic failure, the user may not be allowed to enter an unlock code. There may be little or no reason to allow a user to try to restore normal operation to a computer that is either damaged or intentionally tampered because subsequent operation may not support accurate metering or other security monitoring. Execution may follow the "failed" branch from block 310 to block 320 where the mode flag 228 may be set (or re-set) to the restricted mode of operation and the computer forced into a reset returning execution to block 302.

[0046] By disabling virtually all the major functions of a computer by bypassing a main processor and using a secondary processor to support direct, encrypted communication between the secondary processor and selected peripheral devices, the risk of overriding a restricted operating mode may be significantly reduced. Such a strategy may offer a significant incentive to potential underwriters to support a pay-per-use business model. Because the execution environment for the restricted mode operation is almost completely separate from that of normal operation, the likelihood of an easily propagated attack, such as through scripting, can also be lowered significantly.

[0047] Although the foregoing text sets forth a detailed description of numerous different embodiments of the invention, it should be understood that the scope of the invention is defined by the words of the claims set forth at the end of this patent. The detailed description is to be construed as exemplary only and does not describe every possibly embodiment of the invention because describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology developed after the filing date of this patent, which would still fall within the scope of the claims defining the invention.

[0048] Thus, many modifications and variations may be made in the techniques and structures described and illustrated herein without departing from the spirit and scope of the present invention. Accordingly, it should be understood that the methods and apparatus described herein are illustrative only and are not limiting upon the scope of the invention.

CLAIMS

We claim:

1. An electronic device arranged and adapted for use in an unrestricted mode of operation and a restricted mode of operation comprising:

a first processor (120) coupled to a system bus (121) used to operate the computer (110) during unrestricted operation;

a display controller (190) coupled to the first processor (120);

and

a security module (129) coupled to the display controller (190) and the first processor (120), the security module (129) having a memory (206) and a second processor (204) and being operable to manage direct communication with the display controller (190) without involvement from the first processor (120), the memory (206) storing a mode setting (228) and instructions executable by the second processor (204) for directly displaying a message via the display controller (190) when the mode setting (228) indicates operation in the restricted mode.

2. The electronic device of claim 1, wherein the memory further comprises processor-executable instructions for direct communication with an input device for receiving data at the security module.

3. The electronic device of claim 1, wherein the memory further comprises processor-executable instructions for direct communication with a network interface.

4. The electronic device of claim 1, wherein communication between the security module (129) and the display controller (190) uses XML.

5. The electronic device of claim 1, wherein the security module further comprises a power management output (210) operable to disable operation of the first processor (120).

6. The electronic device of claim 1, wherein the electronic device further comprises a plurality of components, each supporting direct communication with the security module (129), each powering up in a locked mode until a signal from the security

module (129) enables normal operation when the mode setting (228) indicates operation in the unrestricted mode.

7. The electronic device of claim 1, wherein the memory comprises a separate basic input/output system (BIOS) program for the unrestricted (222) and the restricted (224) modes of operation.

8. A method of operating a computer (110) having a limited function mode and full function mode comprising:

performing a reset of the computer;

activating a program in a memory (206) of a security module (200), the program bypassing use of a main processor (120) of the computer (110);

reading a flag (228) in a non-volatile memory (206) indicating that operation is to be in the limited function mode;

sending a message from the security module (129) to a graphics controller (190) causing a prompt to be displayed;

receiving data at the security module (129);

determining when the data satisfies a requirement;

setting the flag (228) in the non-volatile memory (206) to indicate that operation after the next boot is to be in an unrestricted mode of operation when the data satisfies the requirement; and

performing a reset of the computer (110).

9. The method of claim 8, further comprising encrypting the message.

10. The method of claim 8, further comprising exchanging a cryptographic verification from each of a predetermined set of peripheral devices at the security module.

11. The method of claim 10, further comprising resetting the computer (110) when the cryptographic verification of at least one of the predetermined set of peripheral devices fails.

12. The method of claim 8, further comprising:

reading the flag (228) in the non-volatile memory (206) indicating that operation is to be in the full function mode; and sending an unlock message from the security module (129) to at least one computer component prior to a normal boot cycle.

13. The method of claim 8, further comprising sending an unlock message from the security module (129) to at least one computer component (190) when the determining when the data satisfies the requirement is true.

14. The method of claim 8, wherein receiving data comprises receiving data from one of an input device (162), a removable media (152), and a network interface controller (170).

15. The method of claim 8, further comprising executing a normal boot cycle when reading the flag (228) in the non-volatile memory (206) indicates that operation is to be in the unrestricted mode of operation.

16. A computer-readable medium (140) having computer-executable instructions for implementing a method of operating a computer that has a main processor (120) and an alternate processor, the alternate processor (204) operating in a tamper-resistant environment (200), the method comprising:

booting from the alternate processor (204) when a condition exists indicating that the computer (110) operate in a restricted mode;

activating direct communication between the alternate processor (204) and any of a plurality of peripheral devices including a data output device (190);

providing user interface functions comprising display of data via direct communication with the data output device (190).

17. The computer-readable medium of claim 16, wherein the plurality of peripheral devices comprises a user interface input device (162) and the method further comprises directly receiving at the alternate processor (204) data from the user interface input device (162).

18. The computer-readable medium of claim 16, wherein the plurality of peripheral devices comprises a network interface controller (170) and the method further comprises directly communicating with a remote entity (180) via direct communication with the network interface controller (170).

19. The computer-readable medium of claim 16, wherein activating direct communication between the alternate processor (204) and any of the plurality of peripheral devices comprises cryptographically verifying the identity of at least one of the plurality of peripheral devices (190).

20. The computer-readable medium of claim 16, wherein booting from the alternate processor (204) when a condition exists indicating that the computer (110) operate in a restricted mode comprises booting from the main processor (120) when no condition exists requiring the computer (110) to operate in the restricted mode.

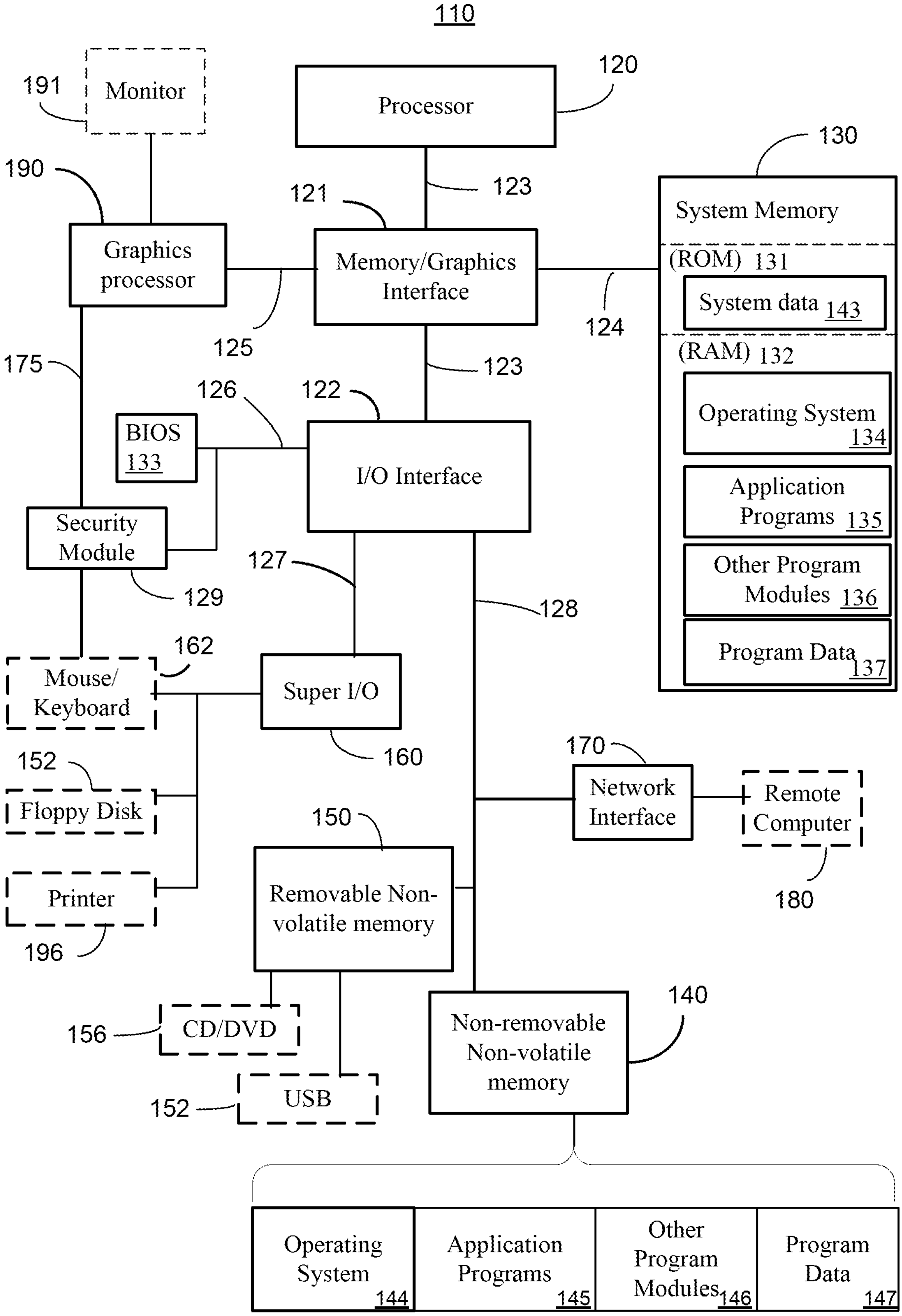
110
Monitor
191
Processor
120
130
System Memory
(ROM) 131
System data 143
(RAM) 132
Operating System 134
Application Programs 135
Other Program Modules 136
Program Data 137
190
Graphics processor
121
Memory/Graphics Interface
123
124
125
175
126
122
123
BIOS 133
I/O Interface
Security Module
127
129
128
162
Mouse/ Keyboard
Super I/O
160
152
Floppy Disk
170
Network Interface
Remote Computer
180
150
Removable Non-volatile memory
Printer
196
140
156
CD/DVD
Non-removable Non-volatile memory
152
USB
Operating System 144
Application Programs 145
Other Program Modules 146
Program Data 147

Fig. 1

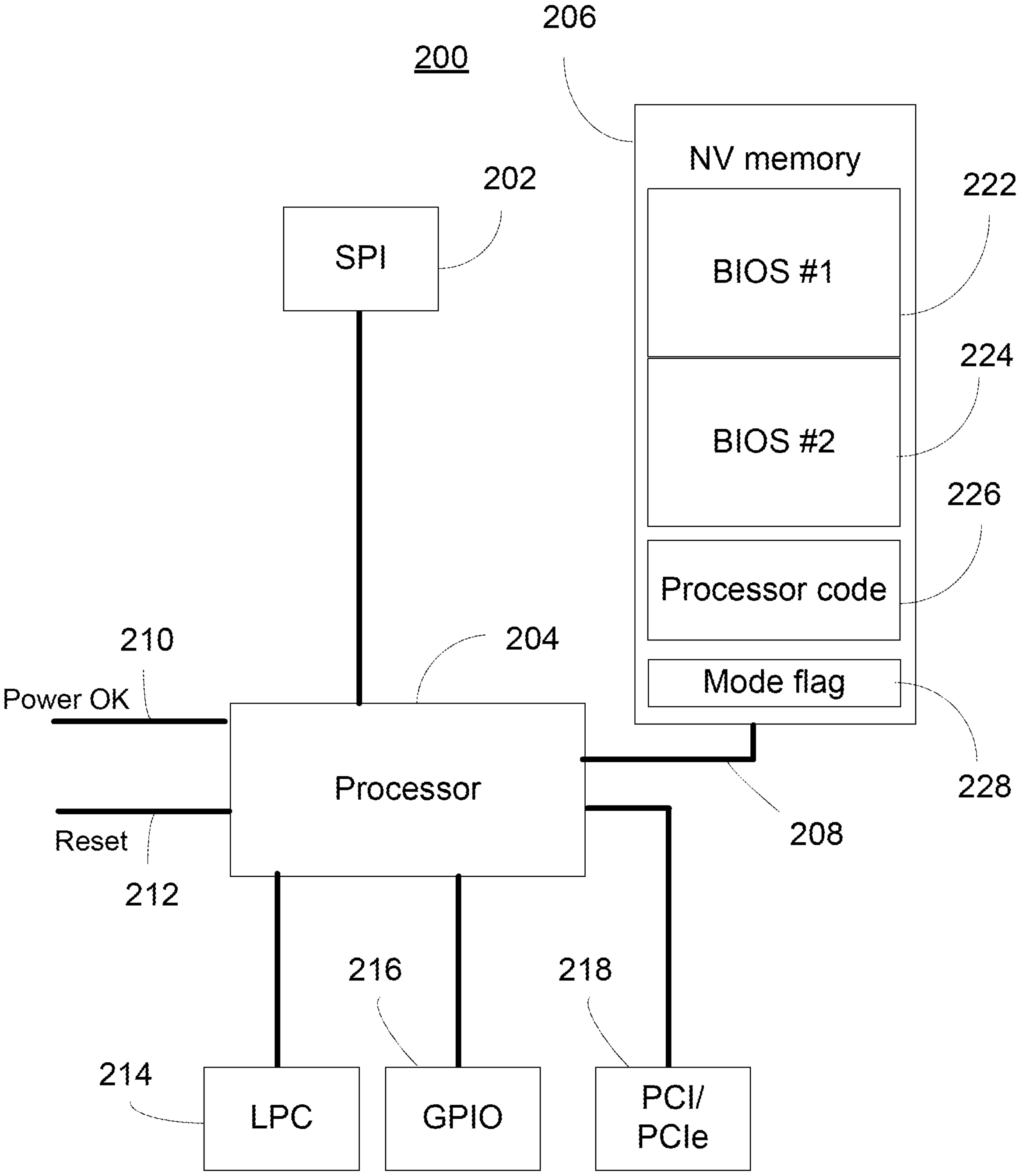
200
206
NV memory
202
SPI
222
BIOS #1
224
BIOS #2
226
Processor code
210
204
Power OK
Mode flag
Processor
228
208
Reset
212
216
218
214
LPC
GPIO
PCI/
PCIe

Fig. 2

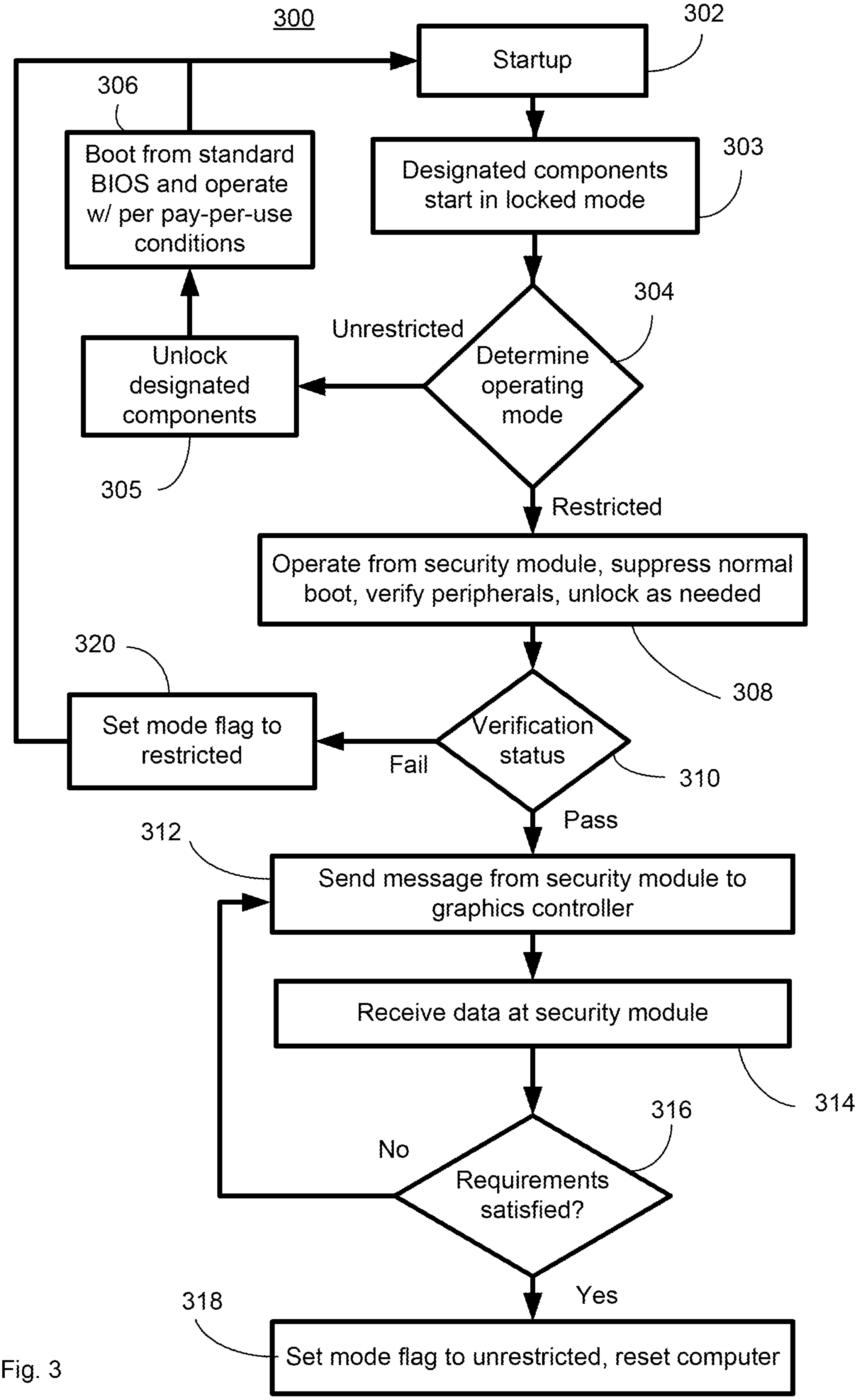
300
Startup
302
Designated components start in locked mode
303
306
Boot from standard BIOS and operate w/ per pay-per-use conditions
Unrestricted
Determine operating mode
304
Unlock designated components
305
Restricted
Operate from security module, suppress normal boot, verify peripherals, unlock as needed
308
320
Set mode flag to restricted
Fail
Verification status
310
Pass
312
Send message from security module to graphics controller
Receive data at security module
314
316
No
Requirements satisfied?
Yes
318
Set mode flag to unrestricted, reset computer

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/057057

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/445(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 8 : G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models since 1975
Japanese utility models and applications for utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(Kipo Internal), Google, YesKisti
keywords: DRN, security, protect*, limit*, restrict*, mode, processor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2006/0090084 A1 (BUER, M.) 27 APRIL 2006 See figures 1,2 and their descriptions.	1-20
A	US2006/0129848 A1 (PAKSOY, E. et al.) 15 JUNE 2006 See figure 1 and its description.	1-20
A	US2004/0153672 A1 (WATT, S.C. et al.) 05 AUGUST 2004 See Summary.	1-20
A	US2005/0033969 A1 (KIIVERI, A. et al.) 10 FEBRUARY 2005 See abstract; claim 1.	1-20
A	US2004/0210906 A1 (BERESNEVICHIENE, Y. et al.) 21 OCTOBER 2004 See Summary; figure 2 and its description.	1-20
PA	US2007/0113266 A1 (ROSS, A.D. et al.) 17 MAY 2007 See abstract; figure 1 and its decription.	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 28 JULY 2008 (28.07.2008)	Date of mailing of the international search report **28 JULY 2008 (28.07.2008)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer YOON, Hye Sook Telephone No. 82-42-481-8370

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/057057

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0090084 A1	27.04.2006	NONE	
US 2006-0129848 A1	15.06.2006	NONE	
US 2004-0153672 A1	05.08.2004	AU 2003-274383 A1 CN 1711524 A DE 60308215 C0 EP 1563375 A1	15.06.2004 21.12.2005 19.10.2006 17.08.2005
US 2005-0033969 A1	10.02.2005	CN 1322385 C	20.06.2007
US 2004-0210906 A1	21.10.2004	GB 2398134 A1	11.08.2004
US 2007-0113266 A1	17.05.2007	WO 2007-058889 A2 CN 101008966 A	24.05.2007 01.08.2007