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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 July 2006 (06.07.2006)

PCT

(10) International Publication Number
WO 2006/071630 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2005/046091

(22) International Filing Date:
20 December 2005 (20.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/021,021 23 December 2004 (23.12.2004) US

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

(72) Inventors: **FRANK, Alexander**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **ENGLAND, Paul**; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: **RYDBERG, Sharon**; Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 (US).

(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, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, 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, HU, IE, IS, IT, LT, LU, LV, 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).

Declarations under Rule 4.17:

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

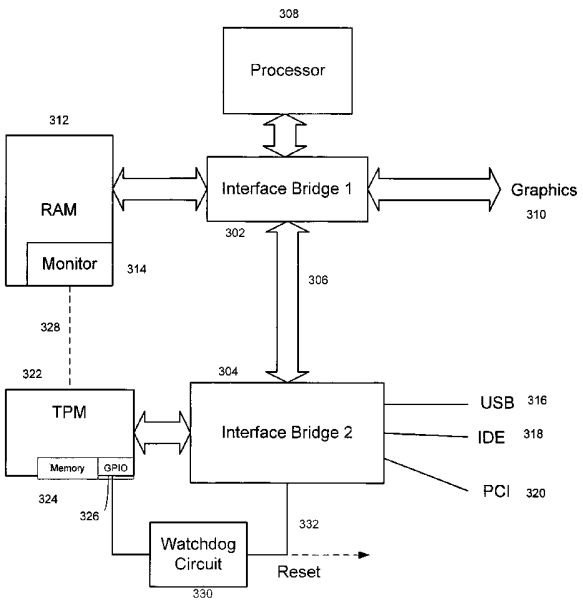
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD TO LOCK TPM ALWAYS 'ON' USING A MONITOR



(57) Abstract: A computer may be secured from attack by including a trusted environment used to verify a known monitor. The monitor may be used to determine a state of the computer for compliance to a set of conditions. The conditions may relate to terms of use, such as credits available for pay-per-use, or that the computer is running certain software, such as virus protection, or that unauthorized peripherals are not attached, or that a required token is present. The monitor may send a signal directly or through the trusted environment to a watchdog circuit. The watchdog circuit disrupts the use of the computer when the signal is not received in a given timeout period.

WO 2006/071630 A2

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.

SYSTEM AND METHOD TO LOCK TPM ALWAYS 'ON' USING A MONITOR

BACKGROUND

[0001] A trusted platform module (TPM) for use in computing devices such as personal computers is known. The purpose of a TPM is to provide computer identity and secure services related to transactions, licensing of application and media, protecting user data, and special functions.

[0002] Trusted platform modules are commercially available, for example, a TPM is available from STM Microelectronics, the ST19WP18 module. The TPM stores keys and subsequently uses those keys to authenticate application programs, BIOS information, or identities. However, use of the TPM is voluntary and according to current and anticipated standards and implementations cannot be used to mandate a condition on the computing device. Some business models assume the computer is out of the direct control of the computer owner/supplier, for example, a pay-per-use business model. In such an instance, circumvention of TPM services may be possible, and if circumvention occurs, may have an undesirable negative impact on the business.

SUMMARY

[0003] A trusted platform module (TPM) may be used to authenticate a monitor program that enforces conditions on a computing device. Owner keys injected or written to the TPM may be used to require that a monitor approved by the owner is operational. In turn, the approved monitor has access to resources of the TPM by way of monitor's authenticated status. Such a secure resource of the TPM may be, for example, a general purpose input/output (GPIO) port. A simple watchdog timer may be configured to reset the computer on a timed interval unless the watchdog timer is restarted within the interval period by a signal received using the GPIO.

[0004] By configuring the computer in this manner, the TPM may be used to help ensure a known monitor is running, and the watchdog timer may be used to help ensure that neither the monitor nor the TPM are disabled or tampered.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Fig. 1 is a block diagram of a network interconnecting a plurality of computing resources;

[0006] Fig. 2 is a simplified and representative block diagram representative of a computer in accordance with an embodiment of the current disclosure;

[0007] Fig. 3 is a simplified and representative block diagram showing a hierarchical representation of functional layers within the computer of Fig. 2;

[0008] Fig. 4 is a simplified and representative block diagram of a computer architecture of the computer of Fig. 2;

[0009] Fig. 5 is a simplified and representative block diagram of an alternate computer architecture of the computer of Fig. 2;

[0010] Fig. 6 is simplified and representative block diagram of the TPM; and

[0011] Fig. 7 is a flow chart depicting a method of locking-on a TPM using a monitor.

DETAILED DESCRIPTION

[0012] 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.

[0013] 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.

[0014] 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.

[0015] Fig. 1 illustrates a network 10 that may be used to implement a dynamic software provisioning system. The network 10 may be the Internet, a virtual private network (VPN), or any other network that allows one or more computers, communication devices, databases, etc., to be communicatively

connected to each other. The network 10 may be connected to a personal computer 12 and a computer terminal 14 via an Ethernet connection 16, a router 18, and a landline 20. On the other hand, the network 10 may be wirelessly connected to a laptop computer 22 and a personal digital assistant 24 via a wireless communication station 26 and a wireless link 28. Similarly, a server 30 may be connected to the network 10 using a communication link 32 and a mainframe 34 may be connected to the network 10 using another communication link 36.

[0016] Fig. 2 illustrates a computing device in the form of a computer 110. Components of the computer 110 may include, but are not limited to a processing unit 120, a system memory 130, and a system bus 121 that couples various system components including the system memory to the processing unit 120. The system bus 121 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

[0017] 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 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, radio frequency, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0018] 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. A basic input/output system 133 (BIOS), containing the basic routines that help to transfer information between elements within computer 110, such as during start-up, is typically stored in ROM 131. RAM 132 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 120. By way of example, and not limitation, Figure 1 illustrates operating system 134, application programs 135, other program modules 136, and program data 137.

[0019] The computer 110 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, Figure 1 illustrates a hard disk drive 141 that reads from or writes to non-removable, nonvolatile magnetic media, a magnetic disk drive 151 that reads from or writes to a removable, nonvolatile magnetic disk 152, and an optical disk drive 155 that reads from or writes to a removable, nonvolatile optical disk 156 such as a CD ROM or other optical media. 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. The hard disk drive 141 is typically connected to the system bus 121 through a non-removable memory interface such as interface 140, and magnetic disk drive 151 and optical disk drive 155 are typically connected to the system bus 121 by a removable memory interface, such as interface 150.

[0020] The drives and their associated computer storage media discussed above and illustrated in Figure 2, provide storage of computer readable instructions, data structures, program modules and other data for the computer 110. In Figure 1, for example, hard disk drive 141 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 keyboard 162 and pointing device 161, commonly referred to as a mouse, trackball or touch pad. 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 a user input interface 160 that is coupled to the system bus, but may be connected by other interface and bus structures, such as a parallel port, game port or a universal serial bus (USB). A cathode ray tube 191 or other type of display device is also connected to the system bus 121 via an interface, such as a video interface 190. In addition to the monitor, computers may also include other peripheral output devices such as speakers 197 and printer 196, which may be connected through an output peripheral interface 190.

[0021] The computer 110 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer

180. 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, although only a memory storage device 181 has been illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 171 and a wide area network (WAN) 173, but may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0022] When used in a LAN networking environment, the computer 110 is connected to the LAN 171 through a network interface or adapter 170. When used in a WAN networking environment, the computer 110 typically includes a modem 172 or other means for establishing communications over the WAN 173, such as the Internet. The modem 172, which may be internal or external, may be connected to the system bus 121 via the user input interface 160, or other appropriate mechanism. In a networked environment, program modules depicted relative to the computer 110, or portions thereof, may be stored in the remote memory storage device. By way of example, and not limitation, Figure 1 illustrates remote application programs 185 as residing on memory device 181.

[0023] The communications connections 170 172 allow the device to communicate with other devices. The communications connection 170 172 are an example of communication media. The 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. A "modulated data signal" may be 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. Computer readable media may include both storage media and communication media.

[0024] The trusted platform module 125 or other trusted environment, discussed in more detail below, may store data, and keys and verify executable code and data. The trusted platform module specification states in section 4.5.2.1, "As part of system initialization, measurements of platform components and configurations will be taken. Taking measurements will not detect unsafe configurations nor will it take action to prevent continuation of the initialization process. This responsibility rests with a suitable reference monitor such as an operating system." Because the TPM is not defined as an enforcement tool the further enhancements described below supplement the common TPM.

[0025] A watchdog circuit 126 may be configured to measure a period of time and when the time expires trigger a signal 127 that disrupts the operation of the computer 110. The disruption may be a system reset that causes the computer 110 to reboot. The disruption may interrupt data on the system bus 121 or a peripheral bus. To prevent the watchdog 126 from disrupting the operation of the computer 110, a signal over communication connection 128 may be required to reset the period of time and start the timing process again. As shown in Fig. 2, the watchdog timer reset signal may be carried over communication connection 128. As discussed more below, the TPM 125 may initiate the watchdog timer reset responsive to a signal from a monitor program. The steps described in the following may be used to help ensure that a specific, desired, monitor is present and operating by using the combination of the TPM 125 and watchdog circuit 126.

[0026] Fig. 3, a simplified block diagram showing a hierarchical representation of functional layers within a representative computer such as that of Fig. 2, is discussed and described. A trusted platform module 202 may be hardware that resides below the basic input/output structure (BIOS) 204. The TPM 202 may act as a resource to the computer and higher level operations, such as the BIOS 204. The BIOS may activate a monitor 206. The monitor 206 resides below the operating system 208 at the monitor level 210. The monitor 206 may access and use resources of the TPM 202 to carry out policies associated with the operation

of higher level entities. The operating system 208 supports the major functions of the computer 110 and may be responsible (after initial bootstrap processes hand over control) for communication, user input/output, disk and other memory access, application launch, etc. The operating system may also directly access and use the TPM 202. As shown, first and second applications 212 214 may run on the operating system 208. In some cases, the monitor may enforce policies related to both the operating system 208 and the applications 212 214. For example, before application 214 may be launched from disk 216, the operating system may check licensing status, depicted by line 218, to determine if the application 214 meets a given criteria for launching. The criteria for launch and subsequent metering of applications using a monitor function are discussed in more detail in US patent application "Method for Pay-As-You-Go Computer and Dynamic Differential Pricing" filed on Dec. 8, 2004 as attorney docket number 30835/40476. Briefly, the monitor 206 may be used to measure and meter application programs, utilities and computer resources, for example, in a pay-per-use or pre-paid scenario.

[0027] Referring briefly to Fig. 6, the TPM 202 is discussed in more detail. The TPM 202 may have an internal memory 502 comprising both volatile and non-volatile memory, at least part of which may be secure from tampering or unauthorized write operations. The memory may store an owner key 504 for use in validating entities that claim affiliation with the owner for the purpose of configuring the TPM 202 and for establishing trust with an outside entity. The memory may also include, among other things, a platform configuration register (PCR) 506. The PCR 506 may be used to store a hash or other strong identifier associated with the monitor 206. The TPM 202 may also include a clock 508 and cryptographic services 510. Both may be used in the authentication and authorization processes as will be discussed below in more detail. The TPM 202 may also include a bus 512, sometimes referred to as a Single-pin Bus or general purpose input/output (GPIO). In one embodiment, the GPIO 512 may be coupled to the watchdog circuit, as described elsewhere.

[0028] The TPM 202 may also be coupled to a general purpose bus 514 for data communication within the computer, for example, a process running the monitor 206. Using the bus 514, or in some cases another mechanism 516, the TPM 202 may be able to measure the monitor. The measurement of the monitor may include checking a cryptographic hash of the monitor, that is, checking a hash of the memory range occupied by the monitor. The PCR may be used to store the measurement data 506. The owner key 504 may be affiliated with the hash of the monitor 506, for example, by a digitally signed hash of the monitor that requires the owner key 504 for confirmation. The owner key 504 may be written or injected into the TPM 202 at the time of manufacture, or later, for example, at the time of delivery to a customer. The owner key 504, then, is used to authenticate the monitor 206.

[0029] In an exemplary embodiment, the monitor 206 is measured by a trusted module preceding it in the boot sequence, for example, by the BIOS 204. The monitor measurement, such as a hash computed by the BIOS 204, may be stored in the TPM PCR 506 via the bus 514. When the TPM 202 validates the measurement (hash), the TPM 202 may then allow access to the monitor 206 unique keys and/or other secrets allocated to the monitor 206 and stored in the TPM 202. The TPM 202 will allocate to any monitor corresponding keys and secrets to whatever measurement the monitor's measurement matches.

[0030] The TPM may be programmed with an owner key 504 and a corresponding monitor metric 506, i.e. a hash of a known monitor 206. The owner key is used to program or update the monitor metric 506, such that only the entity in possession of the owner key 504 may set the PCR register 506 for the known monitor 206. The standard TPM 202 has a characteristic that only a monitor 206 verified against a given measurement 506 may have control of the GPIO 512. When the GPIO 512 is connected in a tamper-resistant manner to the watchdog circuit 126, a chain of trust may be completed. That is, only a verified monitor 206 may control the GPIO 512 and only the GPIO 512 may be used to restart the watchdog circuit 126. Therefore, while the monitor 206 may be

replaced or altered, only the monitor 206 verified by PCR 506 set by the owner key 506 may be used to restart the timer of the watchdog circuit 126. Thus only the authorized monitor may be used to prevent the watchdog from disrupting the computer 110 by, for example, resetting, the computer 110. The timer of the watchdog circuit 126 may be set to a period selected to allow restoration of a corrupted or tampered computer 110, but short enough to prevent significant useful work to be done on the computer 110. For example, the watchdog may be set to disrupt the computer 110 every 10-20 minutes, unless restarted by the validated monitor 206.

[0031] The owner secret 504 and the monitor measurement 506 may be programmed in a secure manufacturing environment, or may be field programmed using transport keys known to the entity programming the owner key 504. Once the owner key 504 is known, the programming entity, for example, a service provider, may set the measurement of the monitor that will determine what monitor is given access to the GPIO bus. The owner key 504 may be required to re-program the owner key. The use of derived keys may facilitate key distribution, scaling and protection from widespread loss should a local owner key 504 be compromised. Key management techniques are known in the data security arts.

[0032] Fig. 4 is a block diagram of a representative architecture of a computer 300, the same or similar to computer 110. The computer may have a first and second interface bridges 302 304. The interface bridges 302 304 may be connected by a high speed bus 306. The first interface bridge 302 may be connected to a processor 308, graphics controller 310 and memory 312. The memory 312 may host a monitor program 314, as well as other general purpose memory uses.

[0033] The second interface bridge 304 may be connected to peripheral buses and components, for example, universal serial bus (USB) 316, Integrated Drive Electronics (IDE) 318, or Peripheral Component Interconnect (PCI) 320, used to connect disk drives, printers, scanners, etc. The second interface bridge may also

be connected to a TPM 322. As discussed above, the TPM 322 may have secure memory 324 for key and hash data, and a general purpose input/output (GPIO) 326. The TPM 322 may be physically or logically coupled to the monitor by connection 328. As discussed, the BIOS 204 may measure the monitor 206 and store the measurement in the TPM 322, which allocates to the monitor 314 keys and secrets corresponding to the provided measurement. The monitor 314 is therefore given access to the resources and data locked with these keys and secrets. The connection 328 may also be used by the monitor to control the GPIO 326 for the purpose of sending a signal to the watchdog circuit 330. The signal may cause the watchdog to reset. When the signal is not received by the watchdog circuit 330 in a time period proscribed by a setting in the watchdog circuit 330, a reset, or other disruptive signal may be sent over connection 332. To discourage tampering, the connection between the GPIO 326 and the watchdog circuit 330 may be protected, for example, by potting or routing between circuit board layers to prevent manual restarting of the watchdog circuit 330. The computer reset signal connection 332 may be similarly protected from tampering, or at least a portion of the reset signal connection 332 between the watchdog circuit 330 and the main processor computer reset point (not depicted).

[0034] Fig. 5 is a representative block diagram of an alternate architecture of the computer of Fig. 2. Comparing to the description of Fig. 4, like numbered components are the same. The watchdog circuit 330 has been moved into the second interface bridge 304 showing a representative illustration of how the watchdog circuit 330 may be combined into another circuit to improve tamper resistance. The integration of the watchdog circuit 330 to the second interface bridge chip 304, while itself appropriate, is only illustrative. Since the second interface bridge 304 is a major component of the computer architecture, the desired level of disruption may be carried forth from within the second interface bridge 304. Therefore, a connection from a watchdog circuit external to the second interface bridge 304, such as connection 332, may not be required.

[0035] In this alternate architecture, the GPIO 326 may not be used to signal the reset to the watchdog circuit 330. Instead, a message may be sent over logical connection 334 directly from the monitor 314 to the watchdog circuit 330.

[0036] Because a sufficient level of trust may not exist between the two entities (314 330) the message may be signed using keys held in the TPM 322. For example, these keys may be associated with the monitor 314 during first boot (e.g. on the manufacturing line – for the sake of trustworthiness). Keys may be assigned arbitrarily, or, as mentioned above, keys may be hierarchically derived from a master key and known data such as a root certificate, serial number or manufacturing sequence number, etc. The watchdog timer 330 may be configured to respect only messages signed using these keys, for example, during the first boot of the computer 110 on the assembly line. In addition, the monitor locks these keys into the TPM 322, such that only a monitor 314 identically measured has access to these keys. A variant of this architecture is that the monitor relies on the TPM 322 to allocate it these keys uniquely and respectively to its measurement.

[0037] During normal operation the monitor 314 may request the TPM 322 to sign on its behalf the message to be sent to the watchdog timer 330. The TPM 322 signs the message with the keys that correspond to the monitor 314 (per its measurement that was stored into the TPM 322 by the BIOS during each boot). The monitor 314 may receive the signed message from the TPM 322 over logical connection, for example, connection 328 and then provide it to the watchdog circuit 330 over logical connection 334.

[0038] When the watchdog circuit 330 receives the message, the watchdog circuit 330 may use the keys (set during manufacturing) to authenticate the message. Alternately, it may request verification using key or secret in the TPM 322 using logical connection 336. If another monitor is running, it will measure differently, resulting in different keys & secrets being allocated by the TPM. Therefore, the alternate monitor will not be able to sign the message properly such that it will be authenticated by the watchdog circuit 330. Consequently, the

watchdog circuit 330 will initiate a sanction, such as firing a reset of the computer 110 after the expiration of its timing interval. The use of signed or encrypted messages may reduce the opportunity for attacks on the logical connections 328 and 334.

[0039] Fig. 7, a flowchart illustrating a method to lock a trusted platform module (TPM) always "on" using monitor, is discussed and described. A typical TPM, for example, TPM 125 may be optionally enabled by the user. As described below, the method will help ensure that both the TPM 125 remains enabled, and that a monitor 206 selected by the owner of the business will be executed, at the risk of sanctions such as disabling the computer 110.

[0040] . Starting with application of power at the start 402, the computer 110 may initiate the various hardware components through normal boot mechanisms. This applies to the TPM 322 as well. The boot sequence may follow a Trusted Computing Platform Alliance (TCPA) methodology. The Core Root of Trust for Measurements(CRTM) (not depicted) measures the BIOS 133 and stores 403 its measurement into the TPM 322. Then the CRTM loads and executes the BIOS 133. (The CRTM may ideally be stored in a trustworthy location in the computer 110 which is very difficult to attack).

[0041] The BIOS 133 may execute in a conventional fashion, initiating and enumerating various computer components, with one exception – it may measure each software module before loading and executing it. Also, it may store these measurements into the TPM 322 . Particularly, it may measure the monitor 314 and store 405 the monitor measurement into the TPM 322.

[0042] The TPM 322 allocates 408 keys and secrets uniquely and respectively to the monitor measurement. The essence is that the TPM 322 consistently allocates 408 unique keys & secrets that correspond to a given measurement. Consequently, the secrets available to a monitor 314 are unique, consistent and respective. As a result any monitor may lock resources such that will be

exclusively available only to that particular monitor. For example, this enables the linking of the genuine monitor 314 to the watchdog circuit 330 by programming the GPIO 326 connected to the watchdog circuit 330 to respect only the measurement associated with the genuine monitor 314. The GPIO 326 is then available only to a monitor that measures identically to the genuine monitor 314.

[0043] Regardless of whether the loaded monitor is genuine or not, the boot sequence loads and executes 410 the monitor. The normal boot process may continue 411 and assuming a successful boot, normal operation 412 of the computer 110 follows.

[0044] As soon as the monitor 314 is loaded and executed at 410 it starts its loop (413 - 419). First, the monitor 314 sends 413 a message to the watchdog circuit 330 via the TPM GPIO 326. The message may signal the TPM 322 to use the GPIO 326 to signal the watchdog circuit 330 to restart its timer (not depicted).

[0045] After sending the message to the TPM 322, the monitor returns to the testing state 414. The monitor may test 414 that the state of the computer 110 complies with a current policy. The current policy may involve the specific presence or absence of known programs, utilities or peripherals. The test may also be related to metering or other pay-per-use metrics. For example, the test may check for available provisioning packets for consumption vs. specific application program operation. In another embodiment, the test may be related to operation during a specific time period, such as calendar month.

[0046] When the test 414 fails, the No branch may be followed 416, where the monitor acts in accordance with the policy. The action may be just a warning code sent to the operating system or a warning message presented to user. The action may be some sanction imposed on the operating system and user, e.g. limiting or eliminating a certain function of the computer. This may apply to hardware and/or software functions. For instance, the computer may be slowed down, certain software may be disabled, or certain devices may be disabled, e.g. a

webcam. More severe sanctions may be to limit the amount of RAM available to the OS, or to reduce the Instruction-Set-Architecture available to the operating system. In an exemplary embodiment, one course of action available to the monitor 314 when a non-compliant condition is found may be to not take action to restart the timer of the watchdog circuit 330 and let the watchdog circuit 330 impose a sanction.

[0047] When the test succeeds, the Yes branch from 414 may be followed. In either case, execution waits 419 for an interval before returning to step 413. The wait interval avoids exhausting the computer's resources by repeatedly running the monitor 314. Obviously, this wait interval 419 should be some fraction of the watchdog timer counting period. The determination of a usable fraction may be the likelihood that normal operation of the computer would delay execution completion of the loop. Then the loop returns to step 413 discussed above. The period for repeating the loop may be set to any time less than the watchdog circuit timeout period, otherwise an unwarranted disruption may take place.

[0048] When the TPM 322 receives 420 the message, the TPM 322 acts according to the monitor measurement. If the measurement is deemed non-genuine 420 fails, the No branch may be taken to box 422, which takes no action, i.e. the signal to the watchdog circuit 330 is not sent. No further action may be needed by the TPM 322 because the watchdog circuit 330 will disrupt the computer 110 unless steps are taken to stop it. Optionally, the TPM 322 may, at 422, generate an error for logging generate a warning/error code, notify the operating system and may display a message to the user.

[0049] When the TPM 322 verifies that the monitor measurement is genuine, the GPIO 326 may be activated to signal 424 the watchdog circuit 330 to restart its timer. As discussed above, restarting the watchdog circuit timer prevents the watchdog circuit 330 from initiating a disruptive action, such as a reset of the computer 110. The watchdog circuit 330 may then restart 426 the timer at its initial value. The timer will then count 428 and test 430 for expiration of a pre-determined time. The timer period may be settable. Timer implementation is

known and whether the timer counts up to a given number, down to zero, counts to a set clock time, or other mechanism, is a design choice.

[0050] If the timer has not expired, the no branch from 430 may be taken back to 428, which will take another count from the timer. When time has expired, the yes branch from 430 may be taken and the watchdog may enforce a sanction by disrupting 432 the computer. The disruption may be a system reset, causing a re-boot, disabling of peripherals, etc. The period for the watchdog circuit timer to count down to a disruption 432 may be enough to allow a user to correct a non-compliant condition on the computer 110, but should be frequent enough to restrict reliable or useful activity on the computer 110.

[0051] The link from 432 to 426 may be conceptual. If the disruption is implemented by a reset of the whole computer, this link is moot. In the event of a more subtle disruption, e.g. slowing the computer down, this link is used to restart the count down and may result in a more disabling disruption, for example, cause a reset.

[0052] It can be seen that two purposes of the owner of a business associated with supplying computers on a pay-per-use or other underwriter may be accomplished by the above method. First, if the TPM 322 is disabled because the user opted out of using the TPM 322 or hacked the computer to disable the TPM 322, messages to the watchdog circuit 330 will not be generated and the computer 110 will be disrupted.

[0053] Similarly, if the TPM 322 is enabled and operational, but the monitor is altered or replaced, possibly to alter or ignore the policies in effect (e.g. usage policies), the TPM will not honor the monitor requests. Practically, an altered monitor measurement is different than the measurement of the genuine monitor. Consequently, when the monitor measurement is stored into the TPM 322, it will allocate a set of keys and secrets respective and unique to the altered monitor, and different from those needed for operation of the GPIO 326. As a result any message from the altered monitor to the TPM to signal the GPIO 326 will not be

honored. Therefore, the watchdog circuit 330 will not receive restart signals and the computer 110 will be disrupted.

[0054] In both cases, the TPM 322 must be enabled and the genuine monitor 314 must be in place and operational for correct operation of the computer 110.

[0055] Other uses for the above method and apparatus may be envisioned. For example, part of the boot process may require presentation of credentials by an authorized user. If correct credentials are not presented, the boot process may not load the genuine monitor, which will ultimately result in the disabling of the computer 110.

Claims:

1. A computer implementing a trusted computing base for enforcing operation of a monitor, the computer comprising:

a processor for executing the monitor;

a trusted environment coupled to the processor for ensuring execution of the monitor, the trusted environment adapted to receive a message from the monitor;

a watchdog circuit coupled to the trusted environment, the watchdog circuit disrupting the computer after a period, unless the trusted environment receives the message within the period.

2. The computer of claim 1, wherein the trusted environment cryptographically identifies the monitor.

3. The computer of claim 2, wherein the trusted environment further comprises a general purpose input/output port and the monitor is given access to the general purpose input/output port after being cryptographically identified.

4. The computer of claim 1, wherein the watchdog circuit further comprises a timer for determining the period and wherein the watchdog circuit receives a signed restart signal to restart the timer, when the signed restart signal is verified.

5. The computer of claim 1, wherein the trusted environment is coupled to the watchdog circuit via a dedicated communication line.

6. The computer of claim 1, wherein the watchdog circuit causes the computer to reboot when disrupting the computer.

7. The computer of claim 6, wherein a signal causing the computer to reboot is carried on a conductor, the conductor adapted for resistance to tampering.

8. The computer of claim 1, wherein the monitor verifies a token at least once in conjunction with sending the message.

9. The computer of claim 9, wherein the token comprises a version number for use by the monitor in determining whether the monitor is the current version.

10. A method of encouraging a known operating state in a computer comprising:

executing a known monitor;

sending a signal from the known monitor to a watchdog circuit; and

preventing the watchdog circuit from disrupting an operation of the computer responsive to the signal.

11. The method of claim 10, further comprising verifying an authenticity of the known monitor.

12. The method of claim 10, wherein sending the signal from the monitor further comprises sending the signal from the monitor to a trusted environment before sending the signal to the watchdog circuit.

13. The method of claim 10, further comprising:

signing the signal =, and the watchdog verifying anauthenticity of the signal.

14. The method of claim 10, further comprising:

disrupting the operation of the computer when the signal is not received in a pre-determined time.

15. A watchdog circuit for use in computer comprising:

a timer for determining a period of time;

an input for receiving a signal to restart the timer; and

an output for disrupting an operation of the computer when the signal is not received during the period of time.

16. The watchdog circuit of claim 15, further comprising a cryptographic capability wherein the signal is digitally signed and the cryptographic circuit determines an authenticity of the signal.

17. The watchdog circuit of claim 15, wherein the input is coupled to a trusted environment.

18. The watchdog circuit of claim 17, wherein the trusted environment regulates the signal to the watchdog circuit.

19. The watchdog circuit of claim 15, wherein the output is coupled to one of a reset circuit and a bus driver circuit.

20. The watchdog circuit of claim 15, wherein the watchdog circuit is disposed in the computer in a manner to limit access to one of the timer, the input and the output.

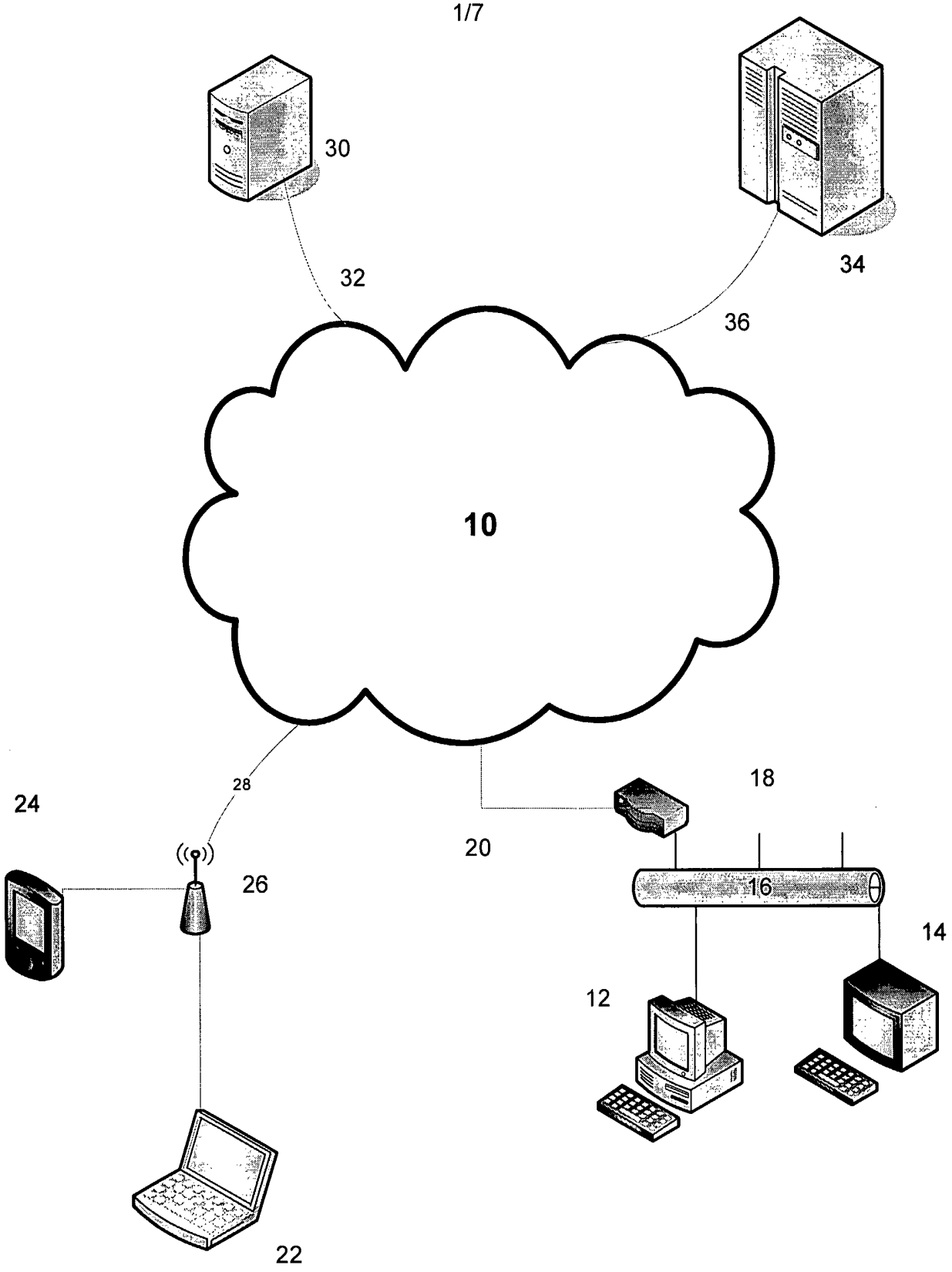


FIG. 1

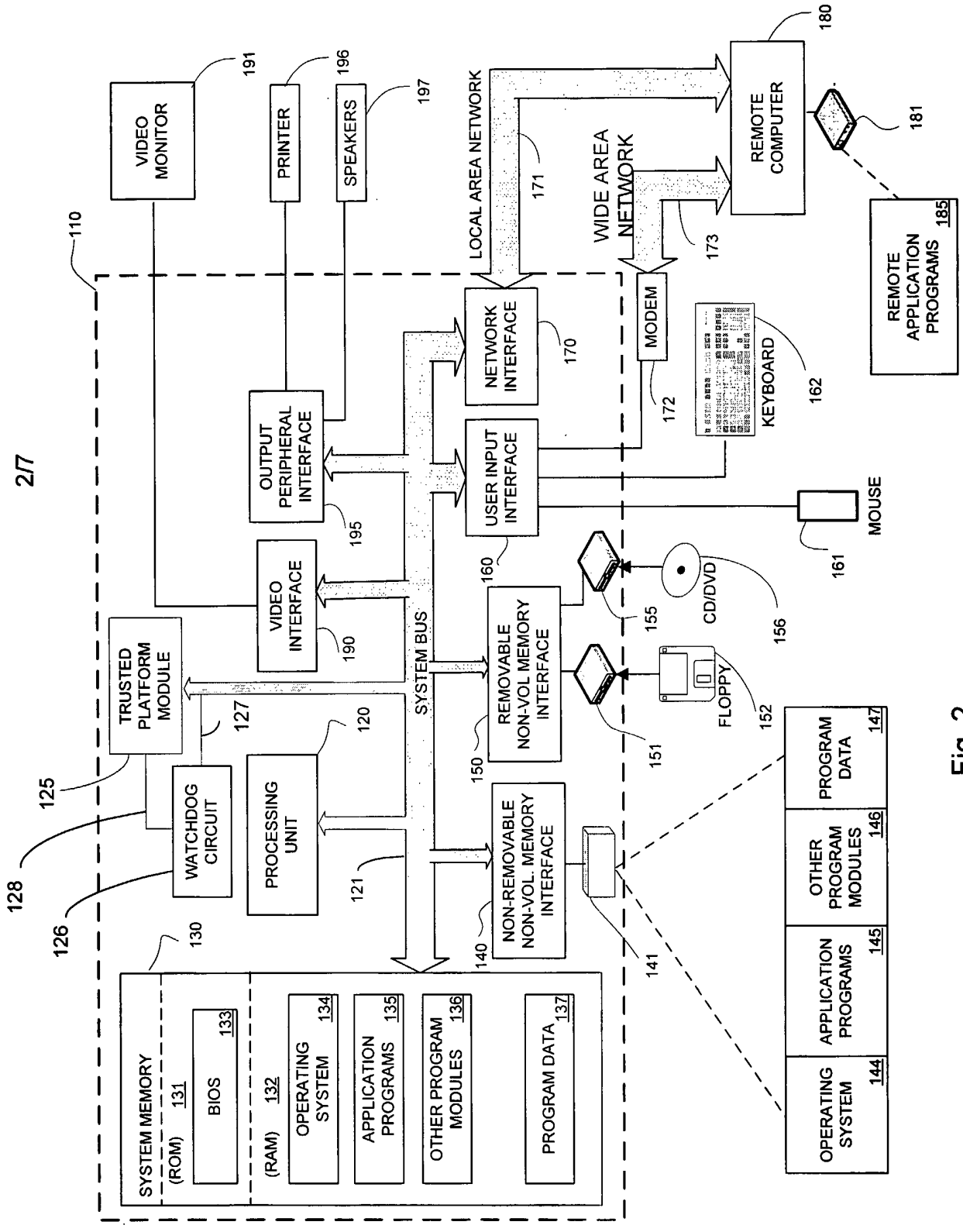

VIDEO MONITOR
191
PRINTER
196
SPEAKERS
197
LOCAL AREA NETWORK
171
WIDE AREA NETWORK
REMOTE COMPUTER
180
181
110
OUTPUT PERIPHERAL INTERFACE
195
NETWORK INTERFACE
170
MODEM
172
173
REMOTE APPLICATION PROGRAMS
185
KEYBOARD
162
USER INPUT INTERFACE
160
MOUSE
161
VIDEO INTERFACE
190
SYSTEM BUS
CD/DVD
155
156
TRUSTED PLATFORM MODULE
125
127
REMOVABLE NON-VOL MEMORY INTERFACE
150
FLOPPY
151
152
WATCHDOG CIRCUIT
128
126
PROCESSING UNIT
120
121
NON-REMOVABLE NON-VOL. MEMORY INTERFACE
140
141
PROGRAM DATA
147
OTHER PROGRAM MODULES
146
APPLICATION PROGRAMS
145
OPERATING SYSTEM
144
SYSTEM MEMORY
130
(ROM) 131
BIOS 133
(RAM) 132
OPERATING SYSTEM 134
APPLICATION PROGRAMS 135
OTHER PROGRAM MODULES 136
PROGRAM DATA 137

Fig. 2

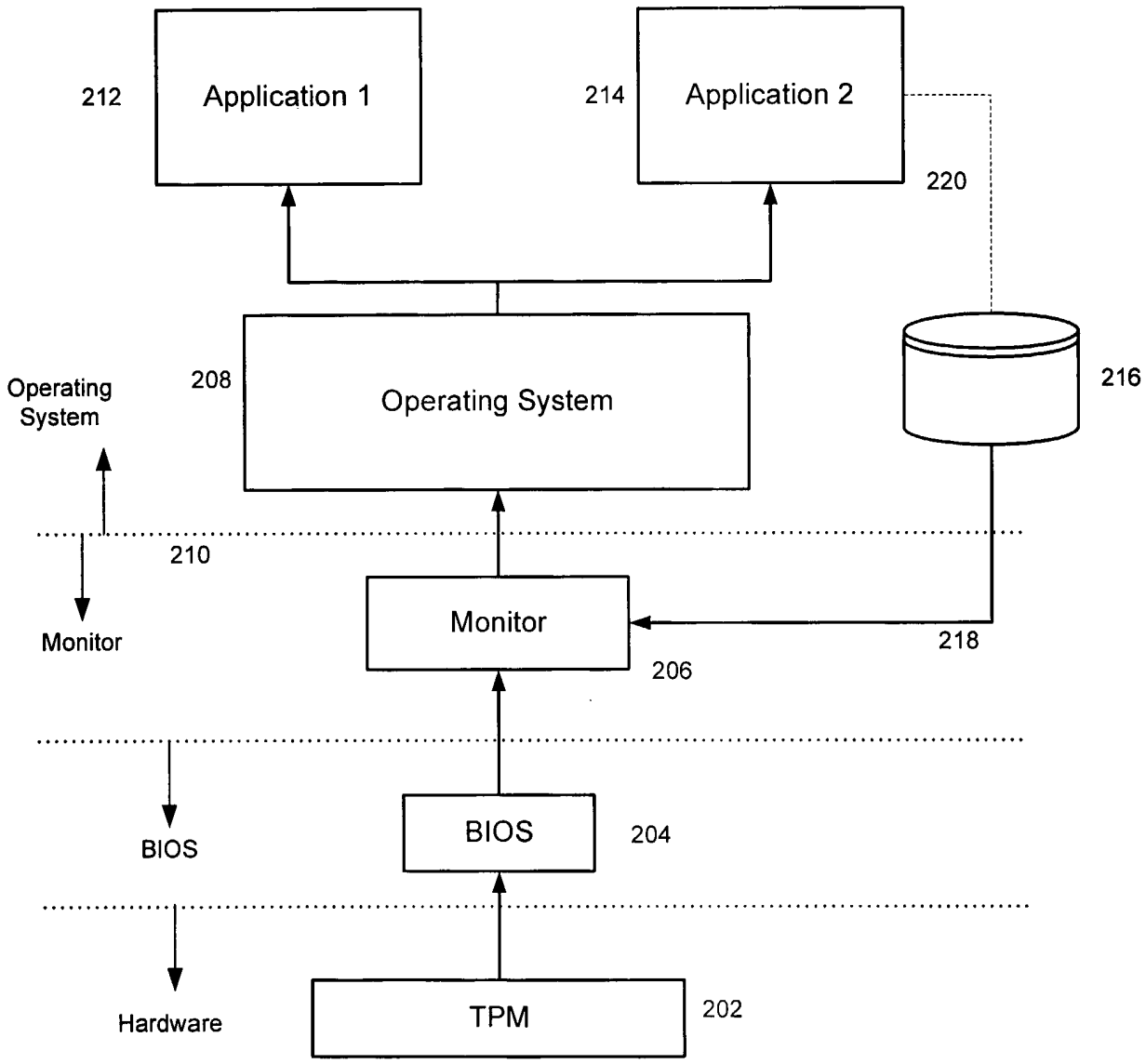

212
Application 1
214
Application 2
220
208
Operating System
216
Operating System
210
Monitor
Monitor
218
206
BIOS
BIOS
204
Hardware
TPM
202

Fig. 3

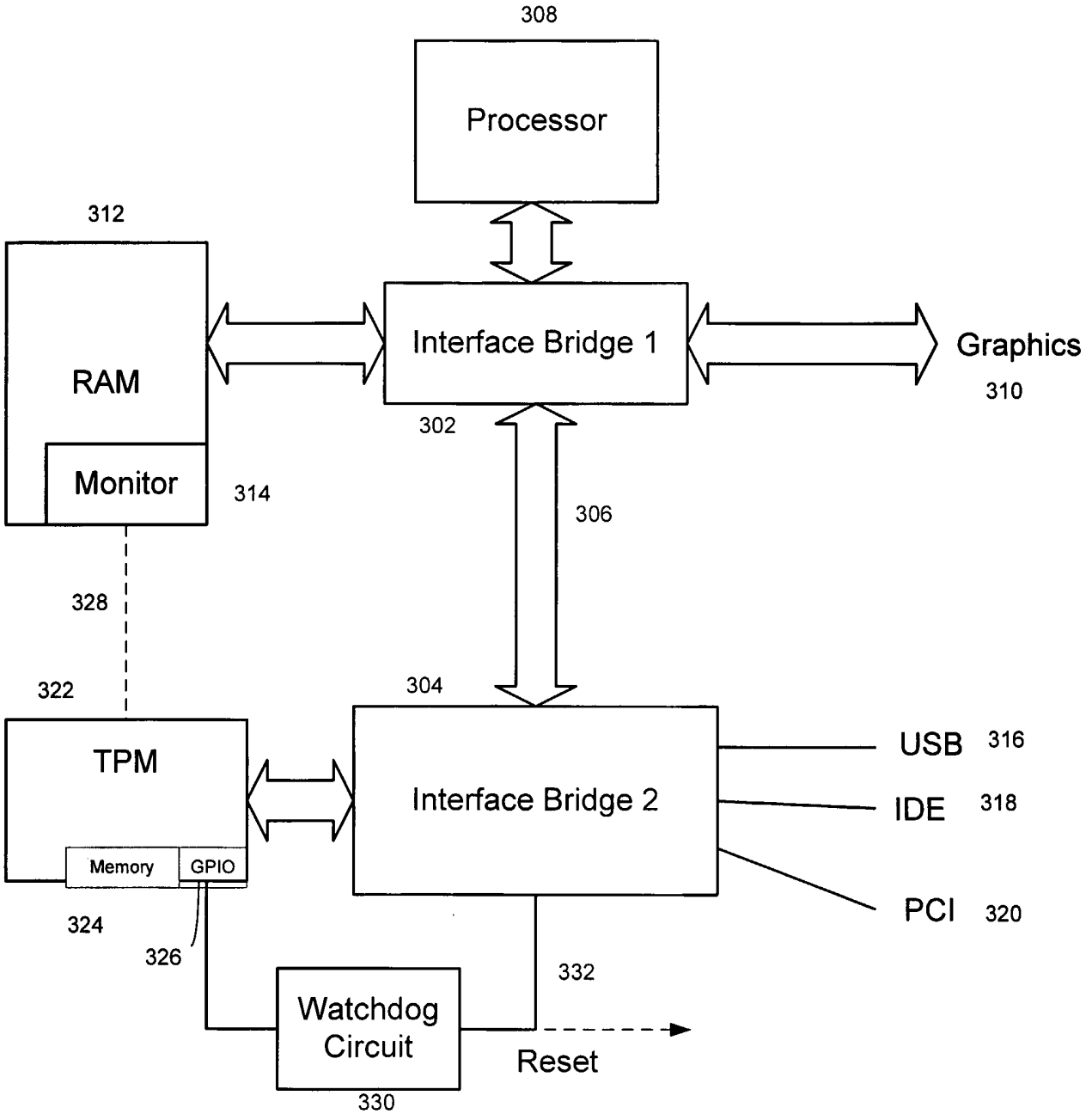

308
Processor
312
RAM
Monitor
314
Interface Bridge 1
302
Graphics
310
306
328
322
304
TPM
Memory
GPIO
324
326
Interface Bridge 2
USB
316
IDE
318
PCI
320
332
Watchdog Circuit
330
Reset

Fig. 4

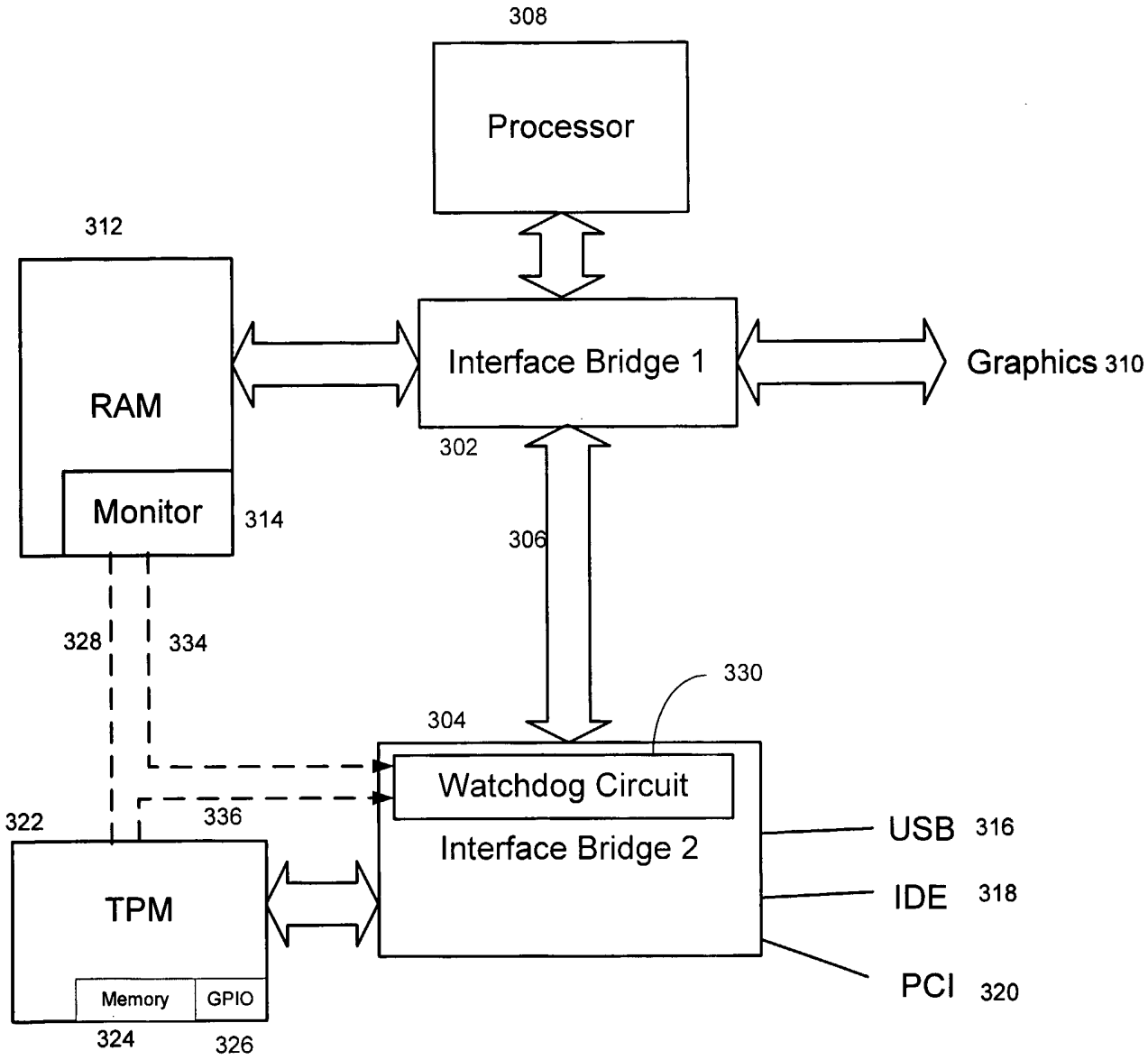

308
Processor
312
RAM
Monitor
314
Interface Bridge 1
302
Graphics 310
306
328
334
330
304
Watchdog Circuit
Interface Bridge 2
322
336
TPM
Memory
GPIO
324
326
USB 316
IDE 318
PCI 320

Fig. 5

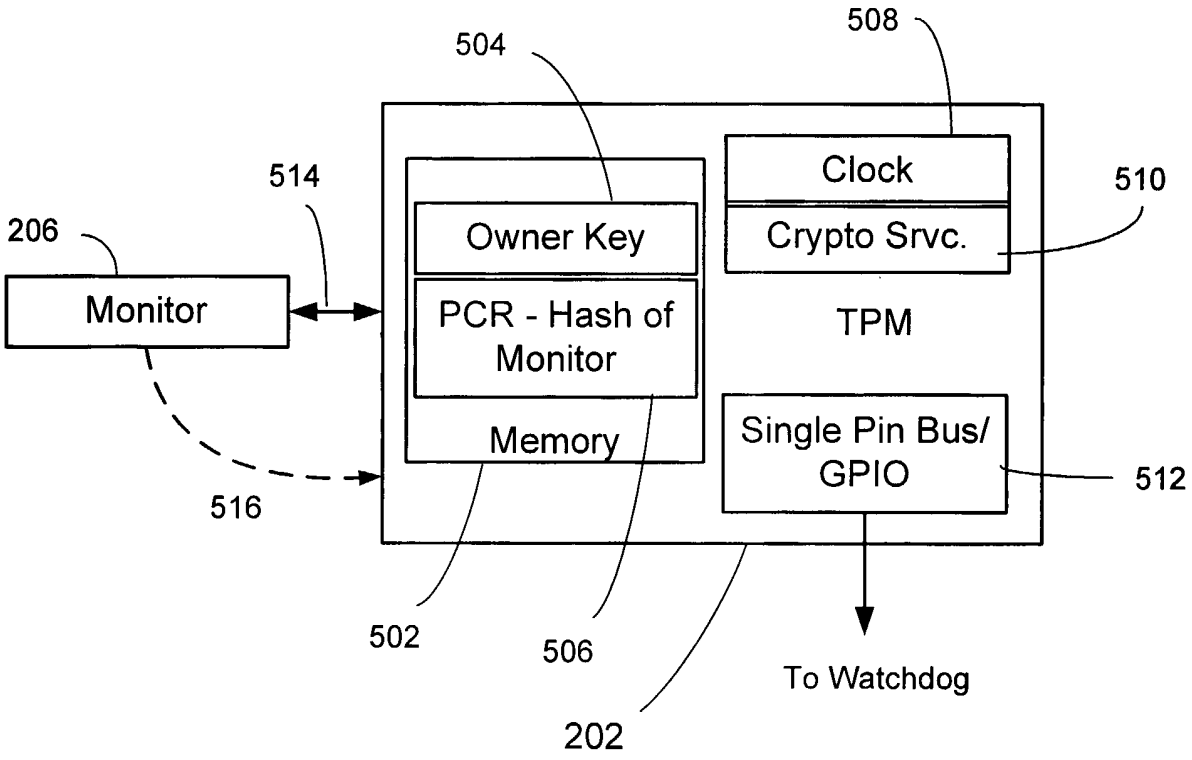

504
508
514
Clock
510
206
Owner Key
Crypto Srvc.
Monitor
PCR - Hash of Monitor
TPM
Memory
Single Pin Bus/ GPIO
512
516
502
506
To Watchdog
202

Fig. 6

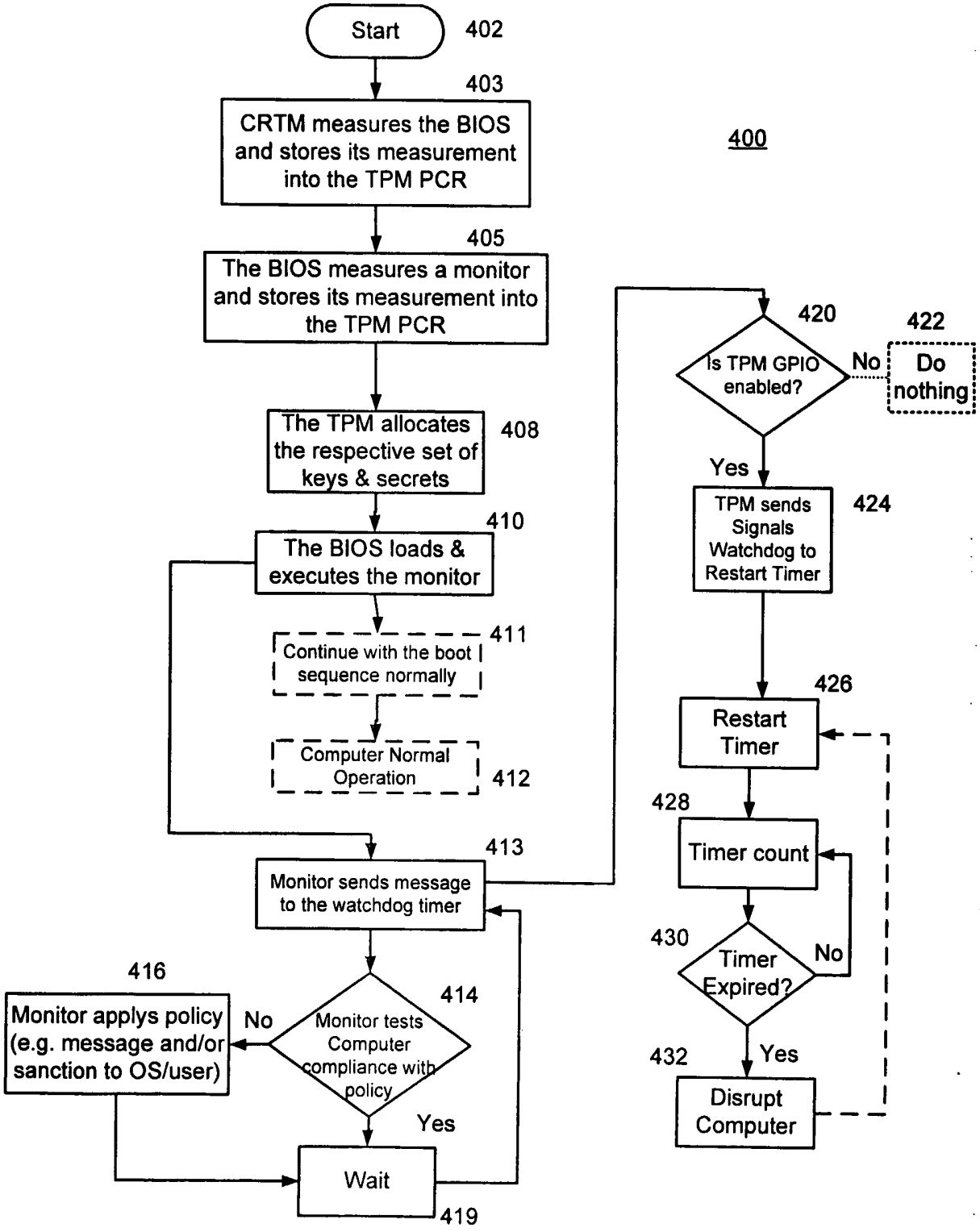

400
Start
402
403
CRTM measures the BIOS and stores its measurement into the TPM PCR
405
The BIOS measures a monitor and stores its measurement into the TPM PCR
The TPM allocates the respective set of keys & secrets
408
410
The BIOS loads & executes the monitor
411
Continue with the boot sequence normally
Computer Normal Operation
412
413
Monitor sends message to the watchdog timer
414
Monitor tests Computer compliance with policy
No
416
Monitor applys policy (e.g. message and/or sanction to OS/user)
Yes
Wait
419
420
Is TPM GPIO enabled?
No
422
Do nothing
Yes
TPM sends Signals Watchdog to Restart Timer
424
426
Restart Timer
428
Timer count
430
Timer Expired?
No
Yes
432
Disrupt Computer

Fig. 7