(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 2006/071610 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2005/045998

(22) International Filing Date:
19 December 2005 (19.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/025,751 29 December 2004 (29.12.2004) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **FISH, Andrew, J.** [US/US]; 9630 Bee Dee Drive NE, Olympia, WA 98516 (US).

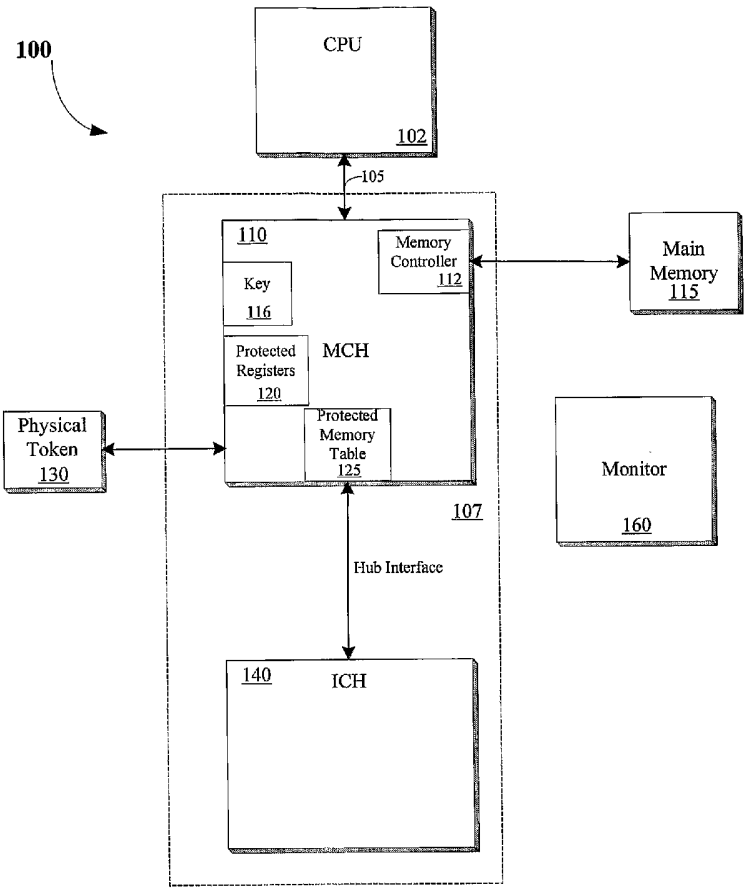
(74) Agents: **VINCENT, Leste, J.** et al.; BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

(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),

[Continued on next page]

(54) Title: MECHANISM TO DETERMINE TRUST OF OUT-OF BAND MANAGEMENT AGENTS



(57) Abstract: According to one embodiment, computer system is disclosed. The computer system includes a central processing unit (CPU) to simultaneously operate a trusted environment and an untrusted environemt and a chipset coupled to the CPU. The chipset includes an interface to couple to a management agent, and protected registers having a bit to indicate if the management agent is provided access to resources within the trusted environment.

WO 2006/071610 A1

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).

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*

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.

MECHANISM TO DETERMINE TRUST OF OUT-OF-BAND MANAGEMENT AGENTS

COPYRIGHT NOTICE

FIELD OF THE INVENTION

[0002] The present invention relates to computer systems; more particularly, the present invention relates to computer systems that may operate in a trusted or secured environment.

BACKGROUND

[0003] The increasing number of financial and personal transactions being performed on local or remote microcomputers has given impetus for the establishment of "trusted" or "secured" microprocessor environments. The problem these environments try to solve is that of loss of privacy, or data being corrupted or abused. Users do not want their private data made public. They also do not want their data altered or used in inappropriate transactions.

Examples of these include unintentional release of medical records or electronic theft of funds from an on-line bank or other depository. Similarly, content providers seek to protect digital content (for example, music, other audio, video, or other types of data in general) from being copied without authorization.

[0004] Out-of-band management agents, such as intelligent platform management interface (IPMI) controllers, may need to access resources within a computer system. However, access to the system by out-of-band management agent access could be used to facilitate a security attack.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

[0006] **Figure 1** is a block diagram of one embodiment of a computer system;

[0007] **Figure 2** illustrates one embodiment of a central processing unit;

[0008] **Figure 3** is a diagram of one embodiment of a trusted or secured software environment; and

[0009] **Figure 4** is a flow diagram of one embodiment of providing access to trusted resources.

DETAILED DESCRIPTION

[0010] A mechanism to provide an out-of-band management agent access to a secured computer system is described. According to one embodiment, a trusted port in the computer system is implemented to transmit encryption keys to a USB peripheral without using a USB stack.

[0011] In the following detailed description of the present invention numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form, rather than in detail, in order to avoid obscuring the present invention.

[0012] Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

[0013] **Figure 1** is a block diagram of one embodiment of a computer system 100. Computer system 100 includes a central processing unit (CPU) 102

coupled to bus 105. In one embodiment, CPU 102 is a processor in the Pentium® family of processors including the Pentium® II processor family, Pentium® III processors, and Pentium® IV processors available from Intel Corporation of Santa Clara, California. Alternatively, other CPUs may be used.

[0014] According to one embodiment, CPU 102 includes circuits or logic elements to support secure or trusted operations. For example, CPU 102 may include secure enter (SENTER) logic, not shown, to support the execution of special SENTER instructions that may initiate trusted operations, which may curtail the ability of potentially hostile untrusted code to access secure resources within computer system 100.

[0015] Additionally, CPU 102 may include secure memory to support secure operations. **Figure 2** is a block diagram illustrating one embodiment of CPU 102. CPU 102 includes cache memory (cache) 220, embedded key 230, and page table (PT) registers 240. All or part of cache 220 may include, or be convertible to, private memory (PM) 225. According to one embodiment, private memory 225 is a memory with sufficient protections to prevent access to it by any unauthorized device (e.g., any device other than the associated CPU 102) while activated as a private memory.

[0016] In the illustrated embodiment, cache 220 may have various features to permit its selective isolation as a private memory. In another embodiment not

shown, private memory 225 may be external to and separate from cache memory 220, but still associated with CPU 102. Key 230 may be an embedded key to be used for encryption, decryption, and/or validation of various blocks of data and/or code. PT registers 240 may be a table in the form of registers to identify memory pages that are to be accessible only by protected code, and which memory pages are not to be protected.

[0017] Referring back to **Figure 1**, a chipset 107 is also coupled to bus 105. Chipset 107 includes a memory control hub (MCH) 110. MCH 110 may include a memory controller 112 that is coupled to a main system memory 115. Main system memory 115 stores data and sequences of instructions that are executed by CPU 102 or any other device included in system 100. In one embodiment, main system memory 115 includes dynamic random access memory (DRAM); however, main system memory 115 may be implemented using other memory types. Additional devices may also be coupled to bus 105, such as multiple CPUs and/or multiple system memories.

[0018] Memory 115 may include a protected memory table to define which memory blocks (where a memory block is a range of contiguously addressable memory locations) in memory 115 are to be inaccessible to direct memory access (DMA) transfers. Since all accesses to memory 115 go through MCH 110, MCH 110 may check the protected memory table before permitting

any DMA transfer to take place. In a particular embodiment, MCH 110 may use caching techniques to reduce the number of necessary accesses to protected memory table 320.

[0019] According to one embodiment, MCH 110 includes key 116 to be used in various encryption, decryption and/or validation processes, protected registers 120 and protected memory table 125. In one embodiment, the protected memory table 125 is implemented in MCH 110 as protected memory table 125 and the protected memory table in memory 115 may be eliminated.

[0020] In another embodiment, protected memory table 125 is implemented as the protected memory table in memory 115 as previously described and protected memory table 125 may be eliminated. The protected memory table may also be implemented in other ways not shown. Regardless of physical location, the purpose and basic operation of the protected memory table may be substantially as described.

[0021] In one embodiment, protected registers 120 are registers that are writable by commands that may only be initiated by trusted microcode in CPU 102. Protected microcode is microcode whose execution may be initiated by authorized instruction(s) and/or by hardware that is not controllable by unauthorized devices.

[0022] In one embodiment, protected registers 120 include a register to

enable or disable the use of the protected memory table. Protected registers 120 may also include a writable register identifying the location of the protected memory table so that the location does not have to be hardwired into MCH 110. In a further embodiment, protected registers 120 may include a mode bit to determine the level of access for an out-of-band management agent, as will be discussed below in greater detail.

[0023] MCH 110 is coupled to an input/output control hub (ICH) 140 via a hub interface. ICH 140 provides an interface to input/output (I/O) devices within computer system 100. ICH 140 may support standard I/O operations on I/O busses such as peripheral component interconnect (PCI), accelerated graphics port (AGP), universal serial bus (USB), low pin count (LPC) bus, or any other kind of I/O bus (not shown). An interface may be used to connect chipset 107 with token 130. Physical token 130 may be a circuit to protect data related to creating and maintaining a protected operating environment.

[0024] In a particular embodiment, physical token 130 includes a key (not shown), which may be an embedded key to be used for specific encryption, decryption and/or validation processes. Physical token 130 may also include storage space to be used to hold a digest value and other information to be used in the protected operating environment. In one embodiment the storage space in physical token 130 may include non-volatile memory (e.g., flash memory) to

retain its contents in the event of power loss to the physical token.

[0025] A secure Virtual Machine Monitor 130 module may be stored on a system disk or other mass storage, and moved or copied to other locations as necessary. In one embodiment, prior to beginning a secure launch process monitor 160 may be moved or copied to one or more memory pages in memory 115. Following a secure enter process, a virtual machine environment may be created in which monitor 160 may operate as the most privileged code within the system, and may be used to permit or deny direct access to certain system resources by the operating system or applications within the created virtual machines.

[0026] Once execution control is transferred to monitor 160, computer system 100 enters a trusted or secured software environment (or platform). **Figure 3** illustrates one embodiment of a trusted or secured platform 300. In the **Figure 3** embodiment, trusted and untrusted software may be loaded simultaneously and may execute simultaneously on a single computer system. Monitor 160 selectively permits or prevents direct access to hardware resources 390 from one or more untrusted operating systems 340 and untrusted applications 310.

[0027] In this context, "untrusted" does not necessarily mean that the operating system or applications are deliberately misbehaving, but that the size

and variety of interacting code makes it impractical to reliably assert that the software is behaving as desired, and that there are no viruses or other foreign code interfering with its execution. In a typical embodiment, the untrusted code might include the normal operating system and applications found on today's personal computers.

[0028] Monitor 160 also selectively permits or prevents direct access to hardware resources 380 from one or more trusted or secure kernels 360 and one or more trusted applications 370. Such a trusted or secure kernel 360 and trusted applications 370 may be limited in size and functionality to aid in the ability to perform trust analysis upon it. The trusted application 370 may be any software code, program, routine, or set of routines which is executable in a secure environment. Thus, the trusted application 370 may be a variety of applications, or code sequences, or may be a relatively small application such as a Java applet.

[0029] Instructions or operations normally performed by operating system 340 or kernel 360 that could alter system resource protections or privileges may be trapped by monitor 160, and selectively permitted, partially permitted, or rejected. As an example, in a typical embodiment, instructions that change the CPU 102 page table that would normally be performed by operating system 340 or kernel 360 would instead be trapped by monitor 160, which would ensure that the request was not attempting to change page privileges outside the domain of

its virtual machine.

[0030] Also shown in **Figure 3**, is an out-of-band management agent 390. In one embodiment, out-of-band management agent 390 is an entity that operates software separate from computer system 100. Out-of-band management agent 390 may be implemented as an intelligent platform management interface (IPMI) controller, or other types of service processors. In one embodiment, out-of-band management agent 390 is a virtual machine or a partition of a larger system, such as another computer system or network system.

[0031] According to one embodiment, the mode bit within protected registers 120 enables out-of-band agent 390 to access or modify trusted or secure resources within platform 300. In such an embodiment, out-of-band agent 390 is treated as a trusted component if the mode bit is enabled. Thus, platform 300 can attest to the ability to trust out-of-band agent 390. However, out-of-band agent 390 is to be trusted in order for platform 300 to be trusted.

[0032] In one embodiment, third party review is conducted of all the code in out-of-band agent 390 to certify that agent 390 is secure. In further embodiments, the third party review may also certify that agent 390 is to maintain secrets, perform cryptographic strength encryption and attestation. Once agent 390 is certified, the mode bit may be enabled.

[0033] If out-of-band agent 390 is not certified the mode bit is disabled,

indicating that agent 390 is not to be trusted. As a result, out-of-band agent 390 is not permitted to affect the trust of platform 300, and platform 300 can be trusted without attesting to the trust of out-of-band agent 390.

[0034] **Figure 4** is a flow diagram of one embodiment for providing access of platform 300to an out-of-band agent 390. At processing block 410, a request is received from out-of-band agent 390 to access the resources of computer system 100, particularly platform 300. It processing block 420, the mode bit within register 120 is checked to determine the security status of out-of-band agent 390.

[0035] At decision block 430, it is determined whether the mode bit is enabled. If the mode bit is enabled, out-of-band agent 390 is trusted and is permitted to access trusted resources, processing block 440. Trusted code on platform 300 can attest to if the system 100 hardware (e.g., hardware 380) is in a mode that requires trusting out-of-band agent 390. If the mode bit is disabled, out-of-band agent 390 is untrusted, resulting in hardware 390 preventing access to any trusted resource in computer system 100.

[0036] The above-described mechanism enables a single chipset to be used with both trusted and untrusted out-of-band agents, as well as to be able to attest to the need to trust the out-of-band agent.

[0037] Whereas many alterations and modifications of the present invention will no doubt become apparent to a person of ordinary skill in the art

after having read the foregoing description, it is to be understood that any particular embodiment shown and described by way of illustration is in no way intended to be considered limiting. Therefore, references to details of various embodiments are not intended to limit the scope of the claims, which in themselves recite only those features regarded as essential to the invention.

CLAIMS

What is claimed is:

1. A computer system comprising:

a central processing unit (CPU) to simultaneously operate a trusted environment and an untrusted environment; and

a chipset, coupled to the CPU, including:

an interface to couple to a management agent; and

protected registers having a bit to indicate if the management agent is provided access to resources within the trusted environment.

2. The computer system of claim 1 wherein the management agent is permitted to access the resources within the trusted environment if the bit is enabled.

3. The computer system of claim 2 wherein the management agent is permitted to modify the resources within the trusted environment if the bit is enabled.

4. The computer system of claim 1 wherein the management agent is not permitted to access the resources within the trusted environment if the bit is disabled.

5. The computer system of claim 4 wherein the management agent is permitted to access resources within the untrusted environment if the bit is disabled.

6. A method comprising:

receiving a request from a management agent to access a computer system simultaneously operating a trusted environment and an untrusted environment; and

determining if a bit within a protected register is enabled; and

permitting the management agent to access resources within the trusted environment if the bit is enabled.

7. The method of claim 6 further comprising permitting the management agent to modify the resources within the trusted environment if the bit is enabled.

8. The method of claim 6 further comprising preventing the management agent from accessing the resources within the trusted environment if the bit is disabled.

9. The method of claim 6 further comprising permitting the management agent to access resources within the untrusted environment if the bit is disabled.

10. A system comprising:

an out-of-band management agent; and

a computer system platform to simultaneously host a trusted environment and an untrusted environment, the computer system platform including an integrated circuit (IC) having:

an interface to couple to the out-of-band management agent; and

protected registers having a bit to indicate if the management agent is provided access to resources within the trusted environment.

11. The system of claim 10 wherein the management agent is permitted to access the resources within the trusted environment if the bit is enabled.

12. The system of claim 11 wherein the management agent is permitted to modify the resources within the trusted environment if the bit is enabled.

13. The system of claim 10 wherein the management agent is not permitted to access the resources within the trusted environment if the bit is disabled.

14. The system of claim 13 wherein the management agent is permitted to access resources within the untrusted environment if the bit is disabled.

15. The system of claim 10 wherein the management agent is a virtual machine of a second computer system platform.

16. An article of manufacture including one or more computer readable media that embody a program of instructions, wherein the program of instructions, when executed by a processing unit, causes the processing unit to:

receive a request from a management agent to access a computer system simultaneously operating a trusted environment and an untrusted environment; and

determine if a bit within a protected register is enabled; and

permit the management agent to access resources within the trusted environment if the bit is enabled.

17. The article of manufacture of claim 16 wherein the program of instructions, when executed by a processing unit, further causes the processing unit to permit the management agent to modify the resources within the trusted environment if the bit is enabled.

18. The article of manufacture of claim 16 wherein the program of instructions, when executed by a processing unit, further causes the processing unit to prevent the management agent from accessing the resources within the trusted environment if the bit is disabled.

19. The article of manufacture of claim 16 wherein the program of instructions, when executed by a processing unit, further causes the processing unit to permit the

management agent to access resources within the untrusted environment if the bit is disabled.

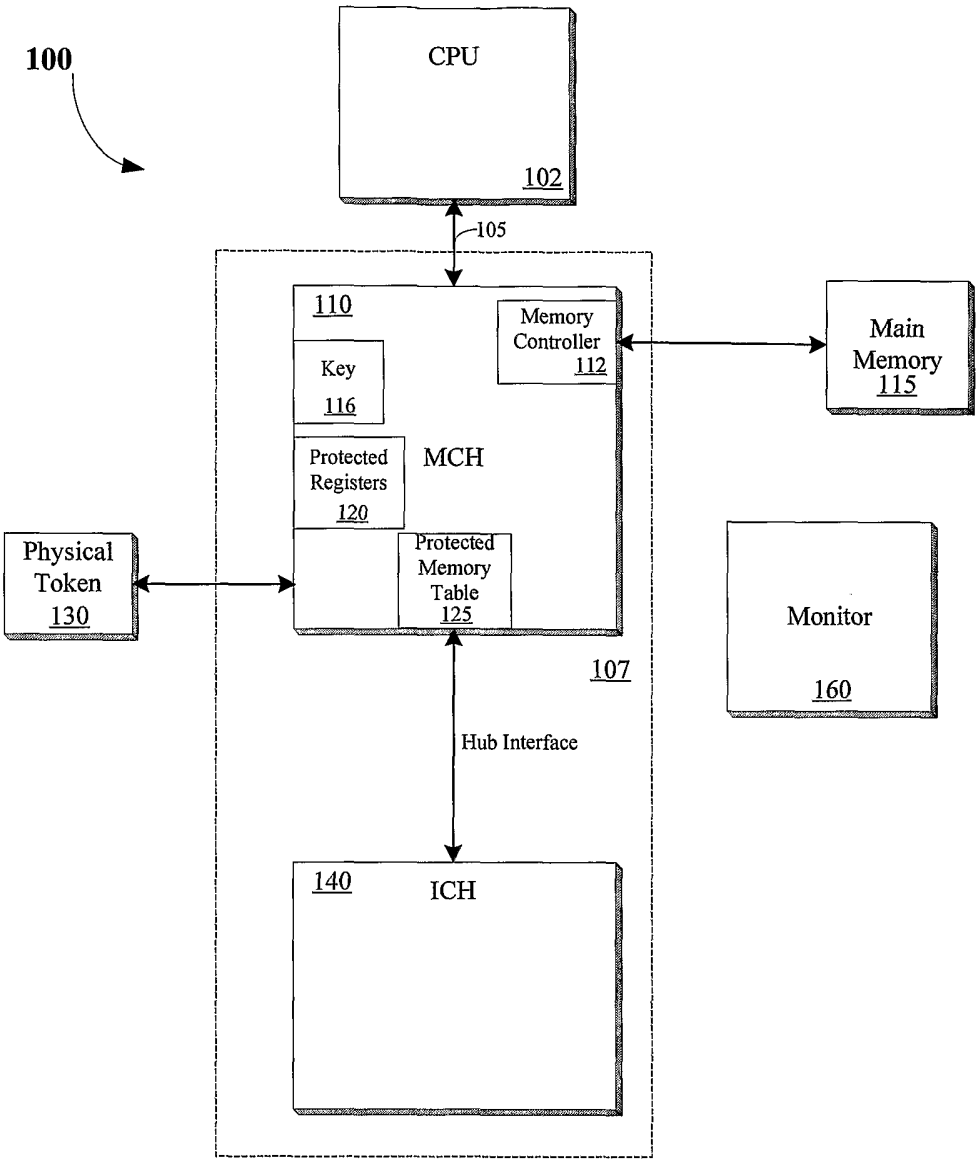
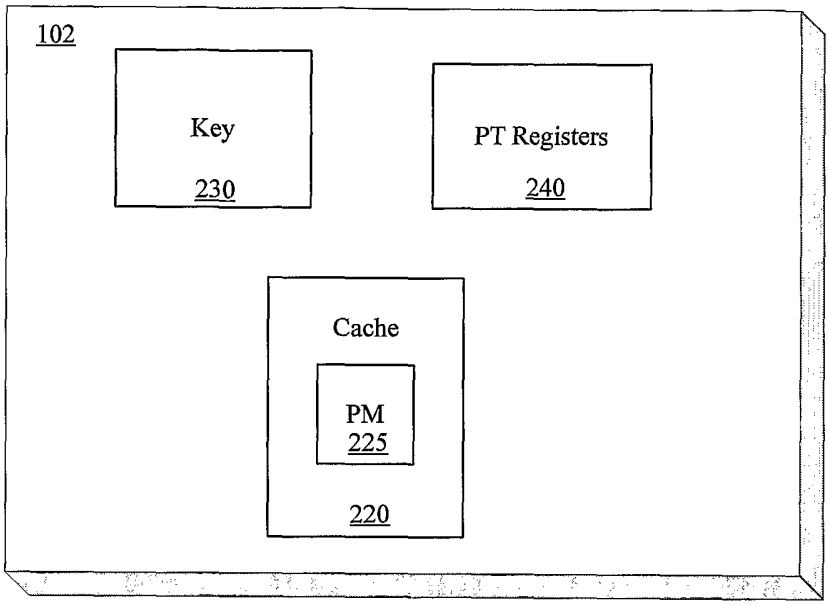

100
CPU
102
105
110
Memory Controller
112
Key
116
Protected Registers
120
MCH
Protected Memory Table
125
Main Memory
115
Physical Token
130
Monitor
160
107
Hub Interface
140
ICH

FIG. 1


102
Key
230
PT Registers
240
Cache
PM
225
220

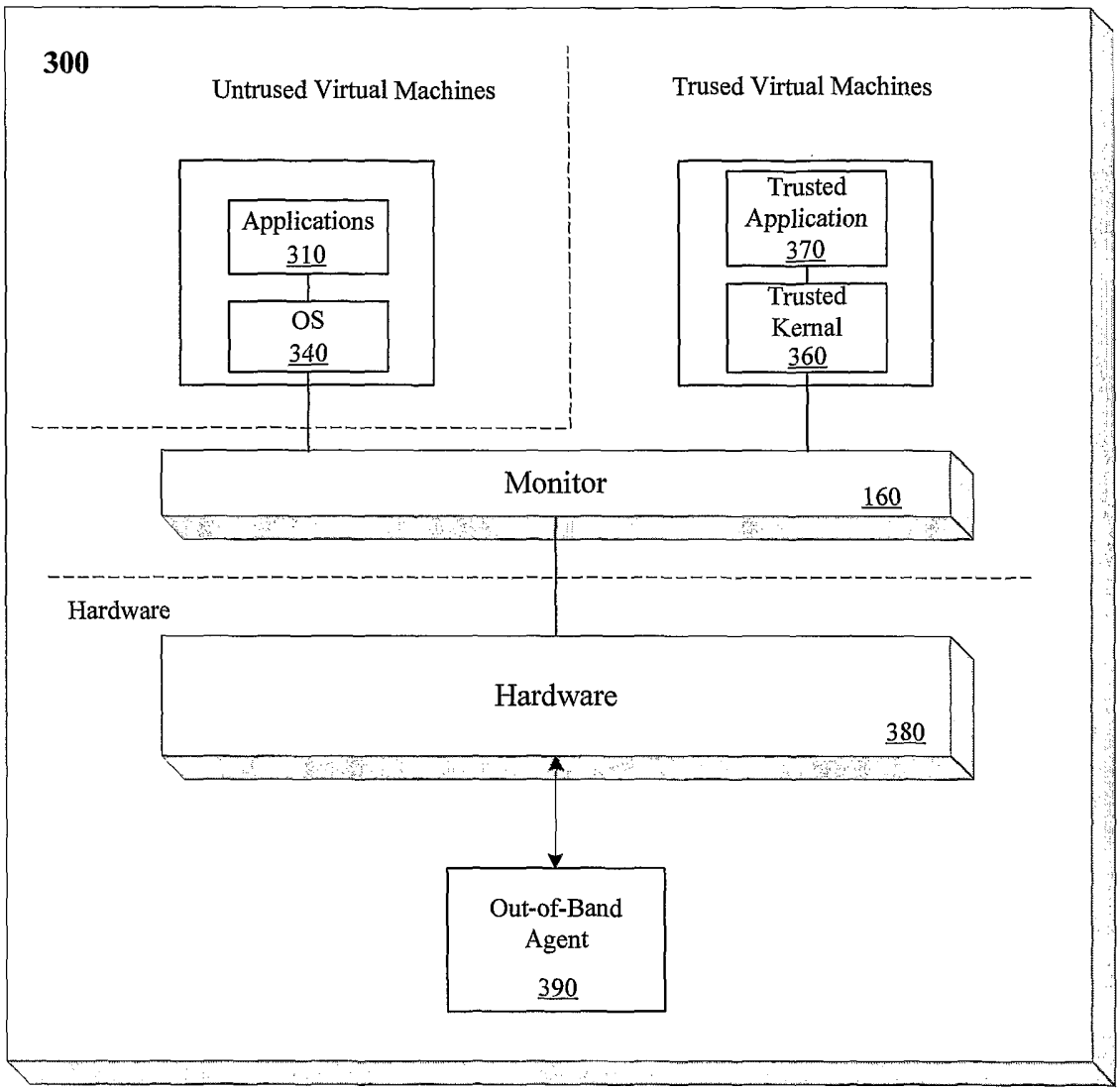

300
Untrused Virtual Machines
Trused Virtual Machines
Applications
310
OS
340
Trusted
Application
370
Trusted
Kernal
360
Monitor
160
Hardware
Hardware
380
Out-of-Band
Agent
390

FIG.
3

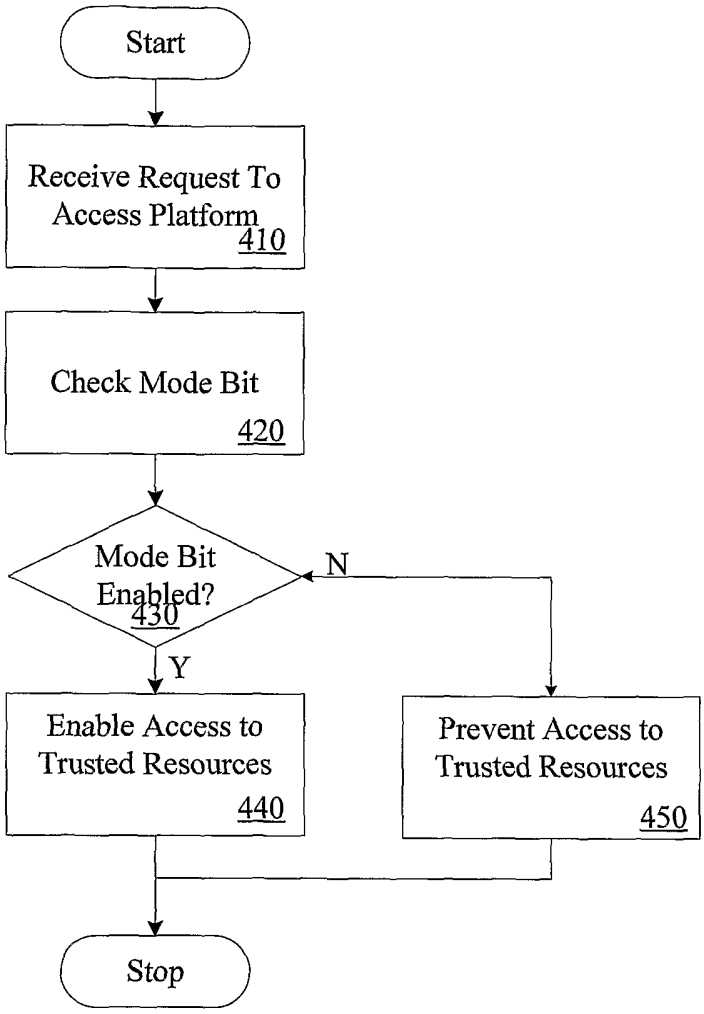

Start
Receive Request To Access Platform
410
Check Mode Bit
420
Mode Bit Enabled?
430
N
Y
Enable Access to Trusted Resources
440
Prevent Access to Trusted Resources
450
Stop

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2005/045998

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD. G06F21/02

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)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/003321 A1 (GLEW ANDREW F ET AL) 1 January 2004 (2004-01-01) page 1, paragraph 11 - page 3, paragraph 26 figure 1	1-19
X	US 2003/204693 A1 (MORAN DOUGLAS R ET AL) 30 October 2003 (2003-10-30) page 2, paragraphs 13,14,17 page 3, paragraph 21 page 5, paragraph 41	1-19
X	EP 0 312 194 A (HITACHI, LTD) 19 April 1989 (1989-04-19) abstract page 3, lines 3-6,38-42 page 6, lines 50,51 figure 1	1-19

-/--

[X] Further documents are listed in the continuation of Box C. [X] 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 document 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 another 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	Date of mailing of the international search report
11 May 2006	18/05/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2005/045998

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/188165 A1 (SUTTON JAMES A ET AL) 2 October 2003 (2003-10-02)	
A	US 2003/226014 A1 (SCHMIDT RODNEY W ET AL) 4 December 2003 (2003-12-04)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
/US2005/045998

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004003321 A1	01-01-2004	NONE	
US 2003204693 A1	30-10-2003	NONE	
EP 0312194 A	19-04-1989	DE 3853759 D1	14-06-1995
		DE 3853759 T2	16-11-1995
		HK 27696 A	23-02-1996
		JP 1096747 A	14-04-1989
		JP 3023425 B2	21-03-2000
		KR 9704513 B1	28-03-1997
		US 5305460 A	19-04-1994
US 2003188165 A1	02-10-2003	AU 2003224737 A1	20-10-2003
		DE 10392470 T5	07-04-2005
		GB 2402788 A	15-12-2004
		GB 2419986 A	10-05-2006
		GB 2419987 A	10-05-2006
		GB 2419988 A	10-05-2006
		GB 2419989 A	10-05-2006
		JP 2005535005 T	17-11-2005
		WO 03085497 A2	16-10-2003
		US 2005182940 A1	18-08-2005
US 2003226014 A1	04-12-2003	AU 2002360617 A1	19-12-2003
		CN 1630849 A	22-06-2005
		EP 1509839 A2	02-03-2005
		GB 2405976 A	16-03-2005
		JP 2005528686 T	22-09-2005
		WO 03102745 A2	11-12-2003