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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2012 (01.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/148422 A1

(51) International Patent Classification:
G06F 9/22 (2006.01) *G06F 9/06* (2006.01)

(21) International Application Number:
PCT/US2011/034578

(22) International Filing Date:
29 April 2011 (29.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JEANSONNE, Jeff** [US/US]; 11445 Compaq Center Drive W, Houston, Texas 77070 (US). **JABORI, Monji G** [US/US]; 11445 Compaq Center Drive W, Houston, Texas 77070 (US). **ALI, Vali** [US/US]; 11445 Compaq Center Drive W, Houston, Texas 77070 (US).

(74) Agents: **HABLINSKI, Reed** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: EMBEDDED CONTROLLER TO VERIFY CRTM

(57) Abstract: In one embodiment a computing system includes an embedded controller to verify the provider of the core root of trust for measurement (CRTM).

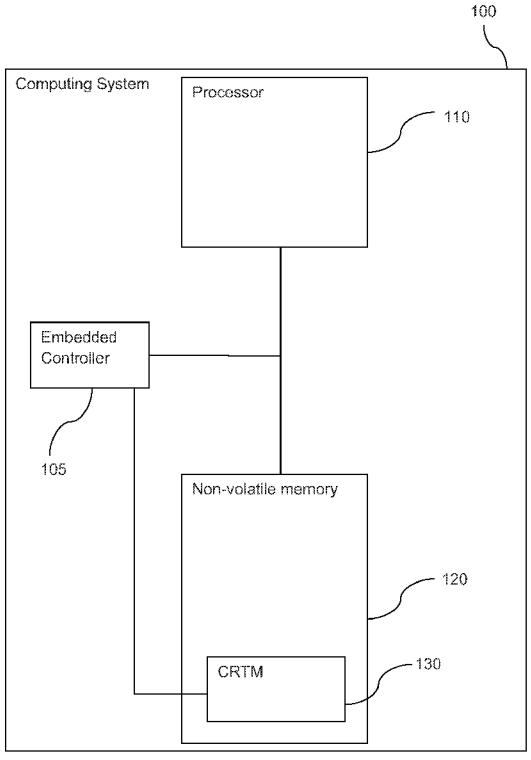

FIG 1

WO 2012/148422 A1

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, 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 the identity of the inventor (Rule 4.17(i))*

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

Published:

— *with international search report (Art. 21(3))*

Embedded Controller to verify CRTM

Background

[0001] Computing systems have basic input/output system (BIOS). The BIOS is a set of software routines that test hardware at startup, starts the operating system and supports the transfer of data among hardware devices. The BIOS routines can be stored on a non-volatile storage such as a read only memory, a programmable read only memory, erasable programmable read only memory, flash memory or another non-volatile memory.

Brief Description Of The Drawings

[0002] Some embodiments of the invention are described with respect to the following figures:

Fig. 1 is a block diagram of a computing system including an embedded controller according to an example embodiment;

Fig. 2 is a block diagram of a computing system including an embedded controller according to an example embodiment;

Fig. 3 is a flow diagram of a method to secure the core root of trust for measurement (CRTM) according to an example embodiment;

Fig. 4 is a flow diagram of a method to secure the core root of trust for measurement (CRTM) according to an example embodiment; and

Fig. 5 is block diagram of a computing system including a computer readable media according to an example embodiment.

Detailed Description

[0003] A computing system can include a computer readable media that stores the BIOS routines. The computer readable media can include a core root of trust for measurement (CRTM). The CRTM can be stored on an immutable part of computer readable media. The immutable part of the computer readable media cannot be erased or written by the components in the computing system such as the processor. A chain of trust can be created by the CRTM.

[0004] The CRTM is boot block code. This piece of code is considered trustworthy. The CRTM is used to measure integrity value of other entities, and should stay unchanged during the lifetime of the platform. CRTM is an extension of normal BIOS, which will be run first to measure other parts of the BIOS block before passing control. The BIOS then measures hardware, and the boot loader and passes control to the boot loader. The boot loader measures an operating system (OS) kernel and passes control to the OS.

[0005] The computer readable media that stores the BIOS and CRTM has an immutable portion created by preventing the host processor or other components from erasing or writing to the portion of the computer readable media. For example the immutable portion of the computer readable media may be in an address range that the host processor is prevented from writing to. However if the computer readable media is removed from the computing system, the computer readable media does not contain protections that prevent the immutable portion of the computer readable media from being rewritten by a memory programmer. The computer readable media could also be replaced by another computer readable media with a different code on the immutable address section. If the CRTM is compromised by removing the computer readable media and replacing it the chain of trust is broken and any further measurements of the integrity of the system are not trustworthy.

[0006] Verifying the CRTM by a portion of the computing system that does not change is important for establishing a chain of trust. While the host processor may be able to verify the CRTM, the processor firmware is in the BIOS that can't be verified until the CRTM is used to verify the rest of the BIOS routines.

[0007] In one embodiment, a computing system can include a non-volatile memory. The non-volatile memory can include a portion that is a core root of trust for measurement (CRTM). An embedded controller in the computing system can verify the provider of the CRTM. The host processor in the computing system can execute the CRTM upon verification of the authenticity to measure other parts of the BIOS code.

[0008] In one embodiment, a method of securing the core root of trust for measurement (CRTM) includes reading the CRTM with an embedded controller. The method can hash the CRTM to create a hash value with the embedded controller and decrypt the hash value included with the CRTM using a public key with the embedded controller. It can be determined if the two hashes match in which case, the CRTM is verified to come from a known source that has the associated private key. The loading of the embedded controller code can be stopped if the decrypted hash is an unexpected value.

[0009] With reference to the figures, Fig. 1 is a block diagram of a computing system including an embedded controller according to an example embodiment. The computing system 100 can include a non-volatile memory 120 including a portion that is a core root of trust for measurement (CRTM) 130. The CRTM is a boot block code that is considered trustworthy. The CRTM 130 is used to measure integrity value of other entities. The CRTM 130 should stay unchanged during the lifetime of the computing system. The CRTM 130 is the first piece of code that executes on a platform at boot. The CRTM 130 should be trusted to properly report to a trusted platform module or another component what is the first software/firmware that executes after the CRTM 130.

[0010] An embedded controller 105 can verify the provider of the CRTM 130. The embedded controller 105 may include a keyboard controller to receive key stroke information from a keyboard or cursor movement information from a mouse, a thermal controller to measure temperature or control fans, or combinations for example. The provider of the CRTM may be for example, the manufacturer of the computing system. Verifying the provider of the CRTM may be by a digital signature, CRC, check sum or another verification method for example. A digital signature may be used to identify who produced a file or document or to detect and track any changes that have been made to the document. A digital signature may use a hash function and cryptographic keys. By determining with the embedded controller if the CRTM was from a specific provider a third party may not be able to remove the non-volatile memory 120 from the computing system 100 and replace or reprogram the

memory with a CRTM code that was not signed by the provider and then boot the computing system with the replacement or reprogrammed memory.

[0011] The computing system includes a processor 110 to execute the CRTM upon verification of the authenticity. The execution of the CRTM measures other parts of the BIOS code. The CRTM can hand off the boot process to the BIOS code after the BIOS has been measured. The BIOS can measure the boot loader of the operating system (OS) and the boot loader can measure the OS. A boot loader is code that begins the booting process for a component or system and may include or be firmware. The OS may be the end of the chain that started with the embedded controller verifying the CRTM.

[0012] The CRTM 130 can be an immutable boot block. An immutable boot block cannot be written or erased by an application outside of the immutable boot block of the computing system 100. For example the processor and the embedded controller are able to write to the CRTM if what is being written to the CRTM is a result of the execution of code that is part of the CRTM already so that unknown code does not write to the CRTM.

[0013] Fig. 2 is a block diagram of a computing system including an embedded controller according to an example embodiment. The computing system 200 may include a hash function 235 executed by the embedded controller to determine a hashed value from the CRTM. The embedded controller 205 may access the CRTM and read data based on the hash function 235.

[0014] The embedded controller may include a read only memory 245. The read only memory 245 may include a boot loader 250 for the embedded controller. The embedded controller 205 may provide digital signature verification of the CRTM. The read only memory may also include the hash function 235. The read only memory 245 may be on board the embedded controller. The embedded controller may not be altered such as by reprogramming. For example the read only memory 245 may be in the same package, on the same substrate, or connected to the embedded controller. The embedded controller may include a cryptographic key in the read only memory 245. The cryptographic key can be for decryption of

asymmetric data or symmetric data. The decryption key may be a public key on the embedded controller 205 to decrypt the encrypted hash value 237 from the CRTM 130. The decrypted data can be compared to data generated by the embedded controller from the hash function 235 applied to the CTRM 130 of the basic input output system (BIOS) 225. The comparison can result in the CRTM 130 being verified that it is from the provider or it is not from the provider. If the CRTM is from the provider then the boot process continues and the CRTM measures the BIOS. The processor 110 may access the BIOS 225 after the provider of the CRTM is verified and through the controller hub 215.

[0015] The embedded controller may refuse to load the embedded controller code. The embedded controller may operate based on a boot loader in a read only memory. A boot loader can be firmware that determines the operation of the embedded controller. Providing the read only boot loader prevents the embedded controller firmware from being changed allowing the embedded controller to reliably determine the provider of the CRTM.

[0016] Fig. 3 is a flow diagram of a method to secure the core root of trust for measurement (CRTM) according to an example embodiment. The method 300 of securing the core root of trust for measurement (CRTM) includes reading the CRTM with an embedded controller at 305. The embedded controller can verify the digital signature of the CRTM at 315. In one embodiment, verifying the digital signature can include calculating a hash value by applying a hash function to data read from the CRTM.

[0017] An encrypted hash value for the CRTM can be read from the CRTM and be decrypted with the embedded controller. The encrypted stored hash value can be decrypted by applying a key to decrypt the hash value. The key may be a key for symmetric encryption or an asymmetric encryption such as a public and private key encryption technique.

[0018] The embedded controller can determine if the decrypted hash value matches the calculated hash value. If the decrypted hash value is an expected hash value then the CRTM was from a known provider. The expected hash value can be

determined by comparing the decrypted hash value to a value of the hash of the CRTM as calculated by the embedded controller. A match implies that the CRTM was provided by the known provider.

[0019] If the decrypted hash value is not an expected value then the provider of the CRTM cannot be authenticated and the root of the chain of trust can therefore not be established as trustworthy. This may occur if the non-volatile memory storing the CRTM is removed and replaced or reprogrammed outside of the computing system or if the non-volatile memory is damaged causing a corruption of the data on the non-volatile memory. If the decrypted hash value is not an expected value then the embedded controller stops loading the firmware code for the embedded controller at 325. If the firmware for the embedded controller does not load then the computing system does not does not measure the BIOS with the CRTM and control is not passed to the BIOS preventing the computing system from completely booting the operating system.

[0020] Fig. 4 is a flow diagram of a method to secure the core root of trust for measurement (CRTM) according to an example embodiment. The method 400 of includes reading the CRTM with the embedded controller at 405. The embedded controller can hash the CRTM to create a calculated hash value at 410. The encrypted hash value can be decrypted at 415. A determination can be made at 420 to determine if the calculated hash value is an expected value such as the decrypted hash value.

[0021] If the hash value is an expected value then the BIOS is measured with the CRTM at 435 to continue the chain of trust. The CRTM may be executed by the processor to determine if the BIOS is trustworthy. In one embodiment the measurement of the BIOS by the CRTM uses a trusted platform module to store measurements and can optionally store secrets (keys) that will only be released by the TPM upon subsequent boot if the measurements are identical. These keys could be used for sealed storage for example.

[0022] If the hash is not an expected value the embedded controller stops loading firmware code at 425. The CRTM can be prevented from executing on the

host processor at 430 if it is determined that the hash value is an unexpected value. If the CRTM cannot be used to establish that the BIOS is trustworthy then the system will not continue booting.

[0023] Fig. 5 is block diagram of a computing system 500 including a computer readable medium 515 or 516 according to an example embodiment. The computer readable medium 515 or 516 can include code that if executed causes an embedded controller to read the CRTM of a BIOS on a storage. The code can cause the embedded controller to hash the CRTM and to decrypt an encrypted stored hash in the CRTM. The code can cause the embedded controller from continuing to load code from the boot loader ROM of the embedded controller.

[0024] The computer readable medium 515 or 516 may include code that if executed causes an embedded controller to prevent a processor from measuring a BIOS code with the CRTM.

[0025] The techniques described above may be embodied in a computer-readable medium for configuring a computing system to execute the method. The computer readable media may include, for example and without limitation, any number of the following: magnetic storage media including disk and tape storage media; optical storage media such as compact disk media (e.g., CD-ROM, CD-R, etc.) and digital video disk storage media; holographic memory; nonvolatile memory storage media including semiconductor-based memory units such as FLASH memory, EEPROM, EPROM, ROM; ferromagnetic digital memories; volatile storage media including registers, buffers or caches, main memory, RAM, etc.; and the Internet, just to name a few. Other new and various types of computer-readable media may be used to store and/or transmit the software modules discussed herein. Computing systems may be found in many forms including but not limited to mainframes, minicomputers, servers, workstations, personal computers, notepads, personal digital assistants, various wireless devices and embedded systems, just to name a few.

[0026] In the foregoing description, numerous details are set forth to provide an understanding of the present invention. However, it will be understood by those

skilled in the art that the present invention may be practiced without these details. While the invention has been disclosed with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover such modifications and variations as fall within the true spirit and scope of the invention.

What is claimed is:

1. A computing system comprising:
a non-volatile memory including a portion that is a core root of trust for measurement (CRTM);
an embedded controller to verify the provider of the CRTM; and
a host processor to execute the CRTM upon verification of the authenticity to measure other parts of the BIOS code.

2. The system of claim 1, wherein the CRTM is an immutable boot block.

3. The system of claim 1, further comprising a read only memory for boot code on board the embedded controller executed by the embedded controller during boot.

4. The system of claim 1, wherein the embedded controller is not a programmable.

5. The system of claim 1, further comprising a hash function executed by the embedded controller to determine a hashed value from the CRTM.

6. The system of claim 5, further comprising a public key stored on the embedded controller to decrypt the hashed value.

7. The system of claim 6, wherein the embedded controller refuses to load the embedded controller code.

8. There system of claim 7, further comprising an embedded controller boot loader in read only memory.

9. A method of securing the core root of trust for measurement (CRTM) on a computing system comprising:
reading the CRTM with an embedded controller;
verifying a digital signature of the CRTM with the embedded controller; and

stopping the loading of the embedded controller code if the decrypted hash does not match the calculated hash

10. The method of claim 9, further comprising preventing the CRTM from executing on a processor if the digital signature verification of the CRTM fails.

11. The method of claim 9, further comprising measuring a portion of the BIOS with the CRTM if the digital signature of the CRTM is verified.

12. A computer readable medium comprising code that if executed causes an embedded controller to:

read the CRTM of a BIOS on a storage;

calculate the hash of the CRTM;

decrypt the encrypted hash of the CRTM included with that CRTM;

compared the decrypted hash as the calculated hash; and

stop loading code from the boot loader ROM of the embedded controller if the hashes are not equal.

13. The computer readable medium of claim 12 further comprising code that if executed causes an embedded controller to:

prevent a processor from measuring a BIOS code with the CRTM.

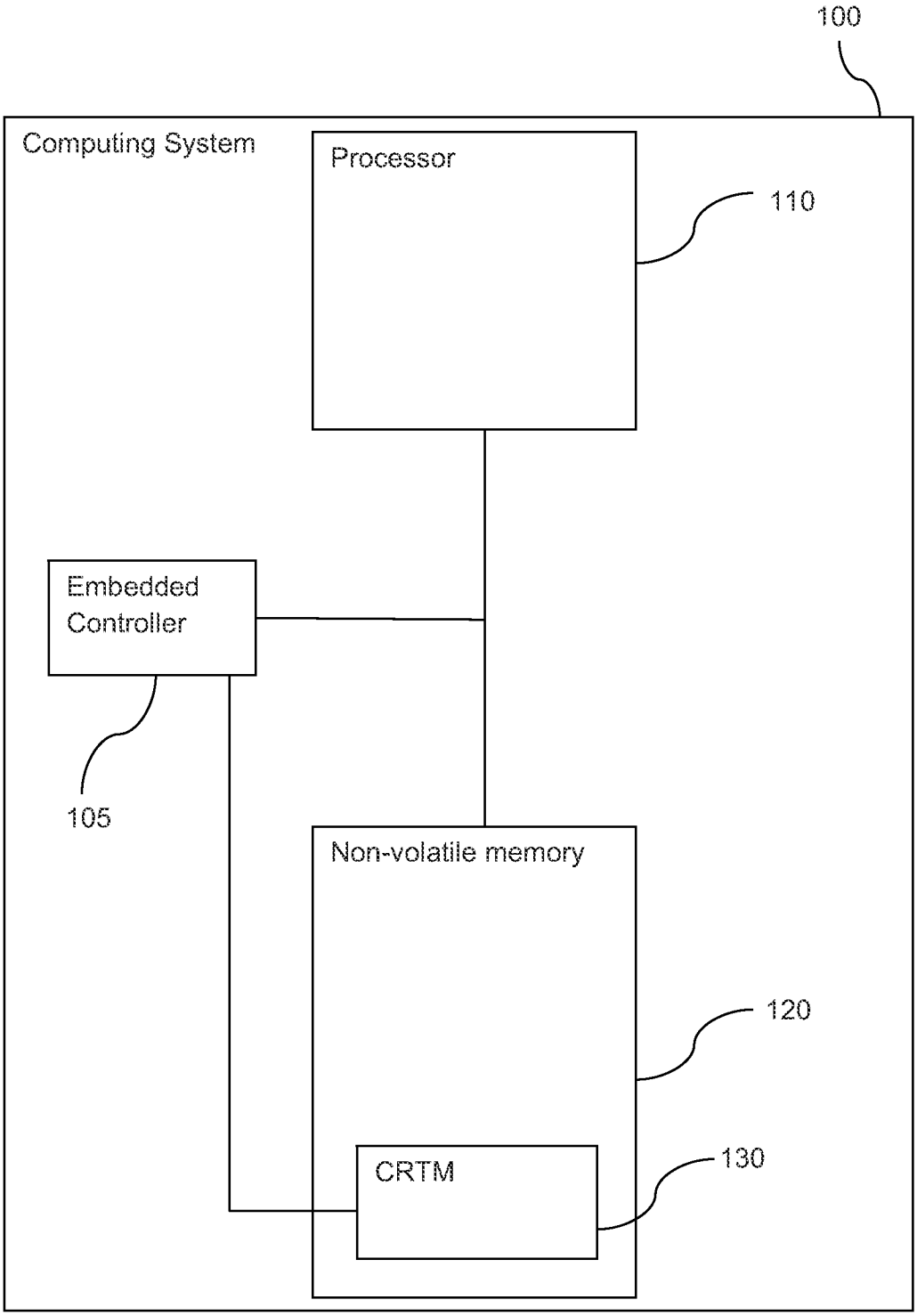
100
Computing System
Processor
110
Embedded
Controller
105
Non-volatile memory
120
CRTM
130

FIG 1

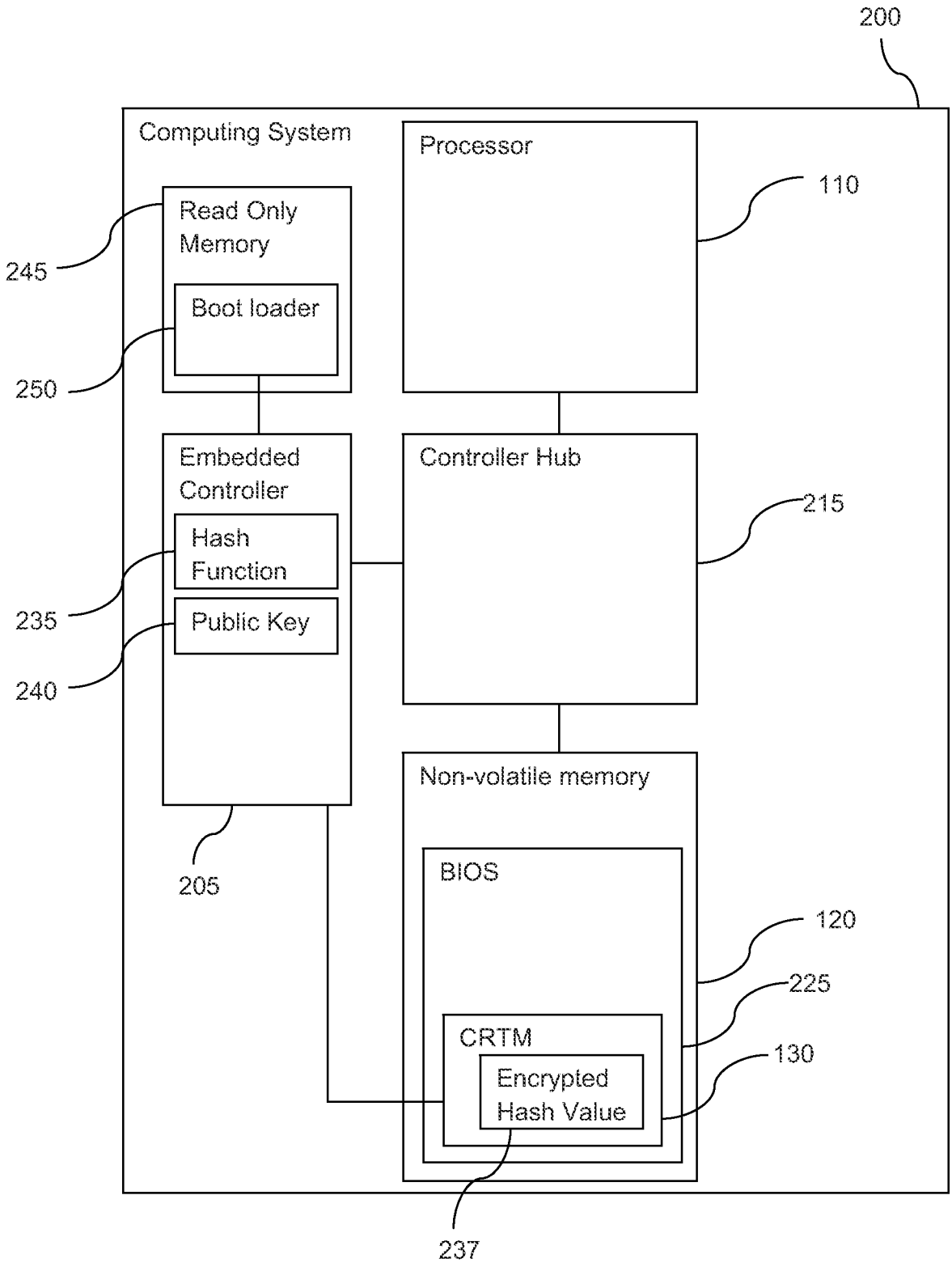
200
Computing System
Processor
110
Read Only Memory
245
Boot loader
250
Embedded Controller
Hash Function
235
Public Key
240
Controller Hub
215
Non-volatile memory
205
BIOS
120
225
CRTM
130
Encrypted Hash Value
237

FIG 2

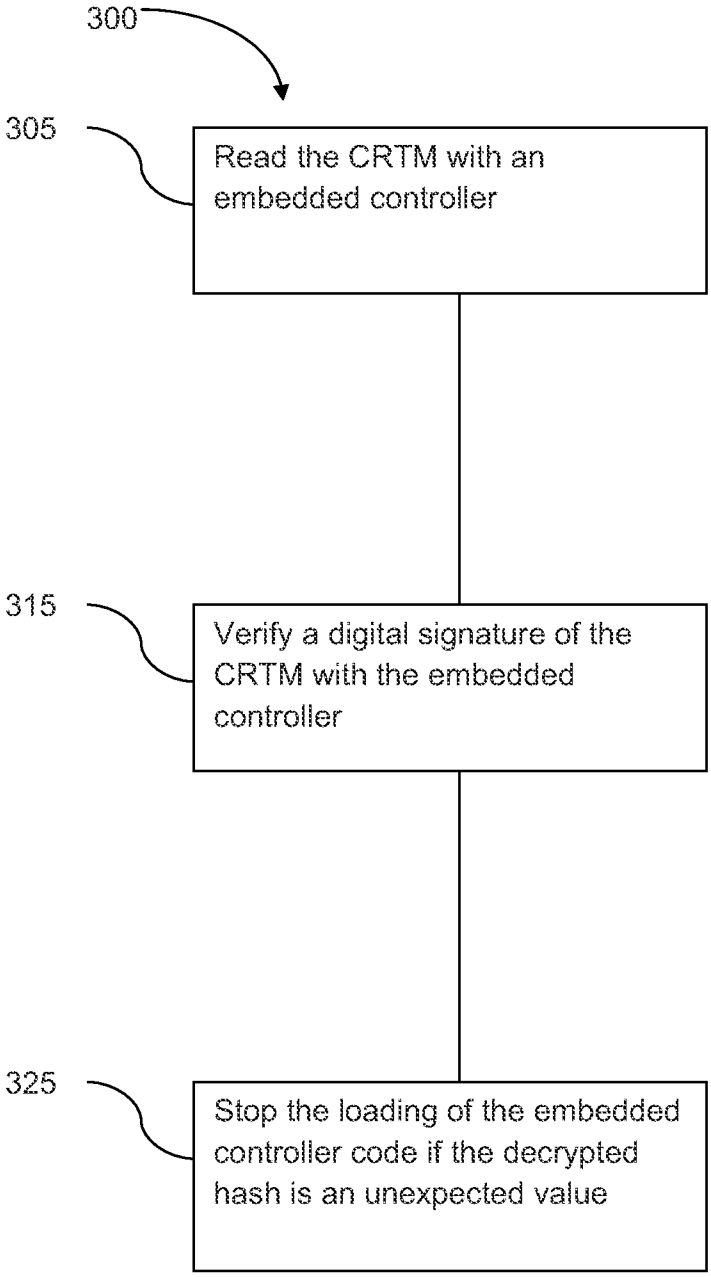
300
305
Read the CRTM with an embedded controller
315
Verify a digital signature of the CRTM with the embedded controller
325
Stop the loading of the embedded controller code if the decrypted hash is an unexpected value

FIG 3

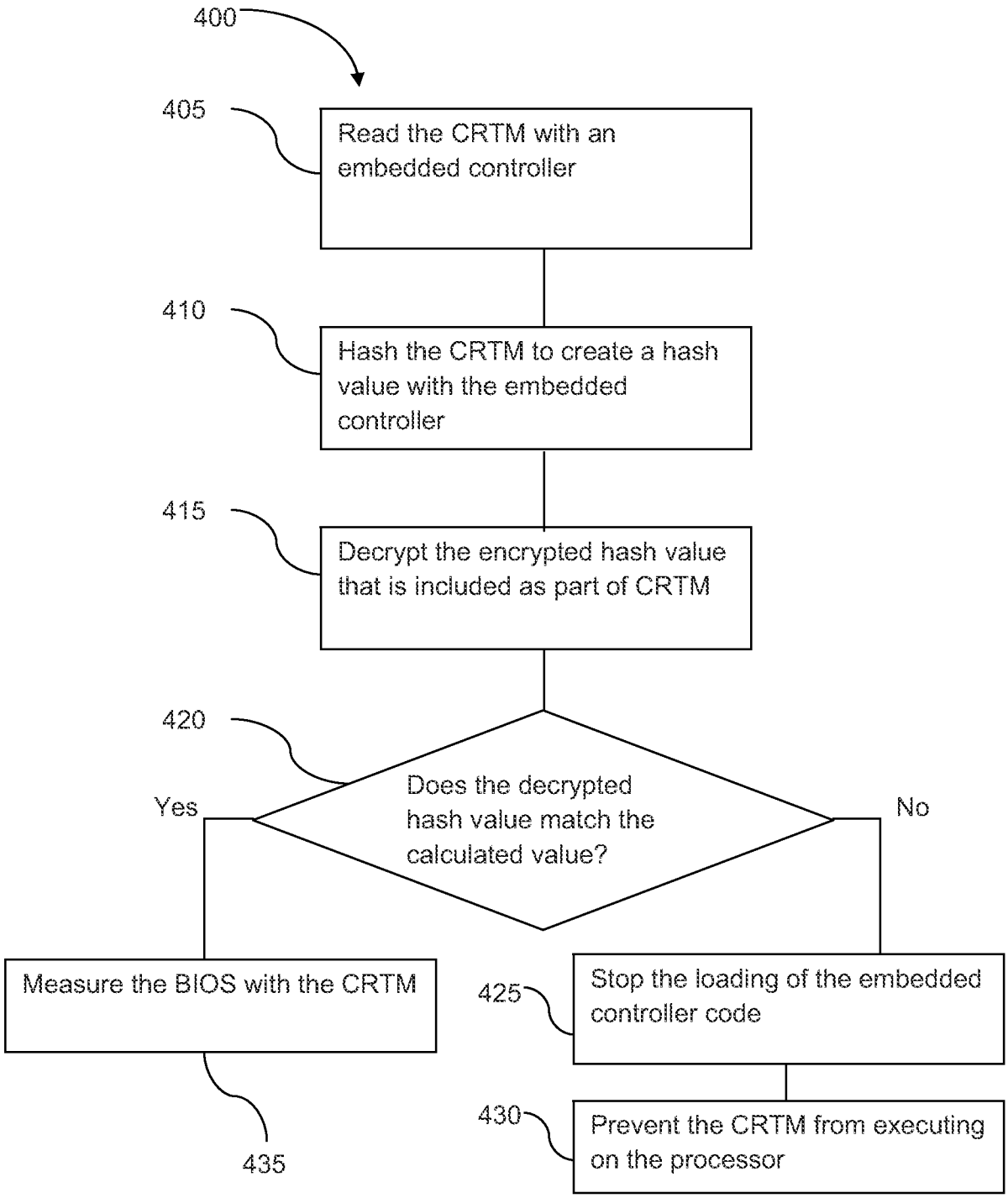
400
405
Read the CRTM with an embedded controller
410
Hash the CRTM to create a hash value with the embedded controller
415
Decrypt the encrypted hash value that is included as part of CRTM
420
Does the decrypted hash value match the calculated value?
Yes
No
Measure the BIOS with the CRTM
435
425
Stop the loading of the embedded controller code
430
Prevent the CRTM from executing on the processor

FIG 4

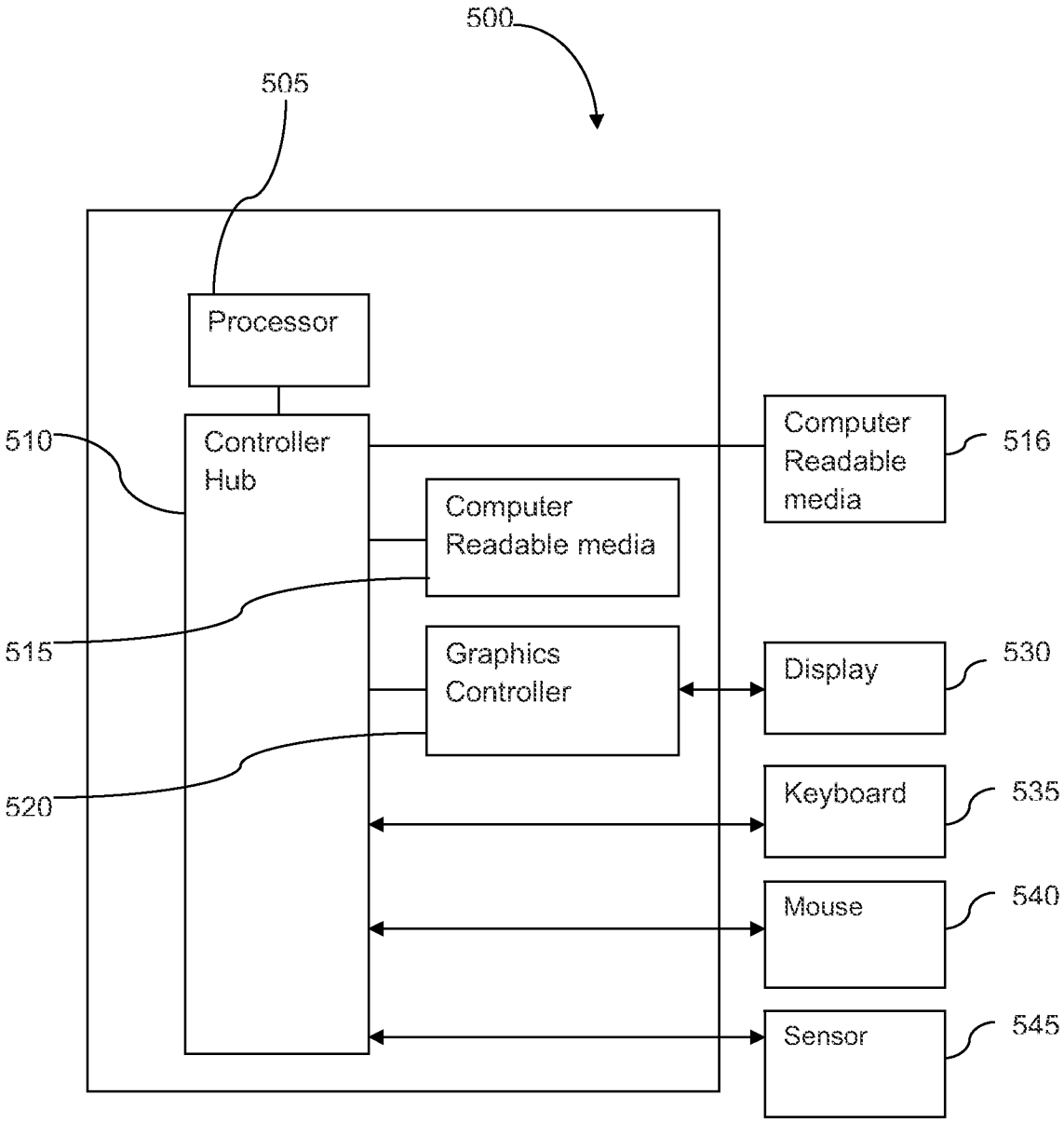
500
505
Processor
510
Controller Hub
Computer Readable media
516
Computer Readable media
515
Graphics Controller
Display
530
520
Keyboard
535
Mouse
540
Sensor
545

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/034578

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/22(2006.01)i, G06F 9/06(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)

G06F 9/22; G06F 9/30; G06F 9/445; G06F 9/24; G06F 12/14; G06F 9/00

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
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: CRTM, verification, BIOS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008-0126779 A1 (NED, S.) 29 May 2008 See abstract, paragraphs [0013]-[0017],[0027],[0033]-[0036],[0039], and figur	1-2,9-11
Y	e 1.	12-13
A		3-8
Y	US 6263431 B1 (LOVELACE, J.V. et al.) 17 July 2001	12-13
A	See abstract, column 5 line 36-line 67, figure 3, and claim 1.	1-11
A	US 2008-0148064 A1 (CARROLL, C.D. et al.) 19 June 2008 See abstract, paragraphs [0036]-[0038],[0042], figure 2, and claim 8.	1-13
A	US 2009-0204822 A1 (WAYNE, F.J. et al.) 13 August 2009 See abstract, paragraph [0028], figure 1, and claim 8.	1-13

☐ 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	Date of mailing of the international search report
30 DECEMBER 2011 (30.12.2011)	**02 JANUARY 2012 (02.01.2012)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Cheongsa-ro,
Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Hwang, Seung Hee

Telephone No. 82-42-481-5749

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/034578

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0126779 A1	29.05.2008	None	
US 6263431 B1	17.07.2001	None	
US 2008-0148064 A1	19.06.2008	None	
US 2009-0204822 A1	13.08.2009	US 2005-0108564 A1 US 7533274 B2 US 7962759 B2	19.05.2005 12.05.2009 14.06.2011