

*[Continued on next page]*



NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17:**

— of inventorship (Rule 4.17(iv))

**Published:**

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

**(84) Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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,

## HARDWARE AUTHENTICATION SYSTEM

### Field of Invention

The invention relates to authentication of hardware devices, and more specifically,  
5 but not limited to, Trusted Platform Module (TPM) systems.

### Background

In some situations it is desirable to check the integrity of computer hardware and/or software, for example to ensure that the system has an approved configuration and is  
10 secure. Thus a computer system may be provided which includes a Trusted Platform Module (TPM) chip, containing a unique and secret RSA key, which can be used to authenticate hardware devices.

Current TPM systems contain Platform Configuration Registers (PCRs) which detail  
15 the expected hardware (and/or software) of a system, such that when the system boots via the Basic Input Output System (BIOS), the hardware found during Power On Self Test (POST) can be checked against those listed by the TPM, wherein on finding a match the system is considered to be trusted.

20 However, if the hardware is modified, such as by adding an external device, the system is no longer trusted by TPM as the respective hardware lists are no longer

identical. This may occur even if the change is minor such as a software or firmware update.

As a consequence the system may not be able to load software which relies on the platform being trusted, as may be the case with high-security applications. This is  
5 undesirable when the changes are insignificant with respect to the security of the platform.

The problem is therefore how to allow a user to update their hardware (and/or  
10 software) without contravening the trust provided by TPM.

### **Summary of Invention**

In an aspect of the invention, there is provided an authentication system for a  
15 computer system on which an operating system may be loaded,

said computer system including a Basic Input Output System which runs a Power On Self Test when power is applied to the computer system;

characterised in that if an external device is found during the Power On Self Test, said external device is checked for validity to determine if it is trusted or not.

20

In one embodiment the validity of the external device is checked before an operating system is loaded.

Thus external devices can be added to the computer system before the operating system loads, such that the root of trust is extended (at a low level) to the external device. Advantageously, as the trust is extended before the operating system loads, the security risk of malignant software creating false trust is reduced.

5

In one embodiment the user is responsible for validating the external device, and is prompted to select if the external device is trusted or not. In a further embodiment the validity of the external device is determined by a policy. In a yet further embodiment the validity of the external device is determined by a remote server.

10

In one embodiment the authentication system is integrated into the BIOS. Typically a BIOS can be updated or modified to include the authentication system.

In one embodiment the computer system includes a Trusted Platform Module (TPM) for determining if devices are trusted or not. Typically the TPM contains one or more Platform Configuration Registers (PCRs) that defines which devices the root of trust may be extended to.

In one embodiment the root of trust is extended to devices considered to be trusted by the authentication system. This has the advantage over the TPM alone which cannot extend the root of trust to external devices, as the PCRs defined by the TPM are static.

20

In one embodiment the devices considered to be trusted can be checked for validity with a remote server.

In one embodiment the computer system is virtual. Thus the authentication system  
5 can be used to verify devices on an isolated guest operating system, within a normal host operating system, before the guest operating system is loaded.

In a further aspect of the invention, there is provided a method of authenticating devices in a computer system comprising the steps of:

10 running a Power On Self Test from a Basic Input Output System when power is applied to the computer system;

characterised in that if an external device is found during the Power On Self Test, said external device is checked for validity to determine if it is trusted or not.

15 In one embodiment a Trusted Platform Module (TPM) extends root of trust to devices indicated as being trusted by Platform Configuration Registers (PCRs).

In one embodiment, if the external device is considered to be trusted by a policy, or by a user in response to a prompt, the root of trust is extended to the external device.

20

Typically the root of trust is extended prior to an operating system being loaded.

#### **Brief Description of Drawings**

It will be convenient to further describe the present invention with respect to the accompanying drawings that illustrate possible arrangements of the invention. Other arrangements of the invention are possible, and consequently the particularity of the accompanying drawings is not to be understood as superseding the generality of the preceding description of the invention.

Figure 1 is a schematic view of an authentication system according to an embodiment of the invention.

10

### **Detailed Description**

In general the system comprises the following steps, as indicated by the dashed lines in Figure 1:

15

When the user starts up the machine, the Basic Input Output System (BIOS) runs a Power On Self Test (POST), and then measures, loads and runs a Hardware and Firmware Authentication System, hereinafter referred to as a Substantiation System.

20 The Substantiation System collects all platform evidence of the machine (hardware properties such as manufacture date, serial number, version, test functionality of the device etc).

The Substantiation System then verifies 102 collected platform evidences with the local core evidence storage.

If validation is required in order to boot the platform, Substantiation System sends  
5 103 collected platform evidences to server for validation process.

The Substantiation System then executes 104 server's instruction(s) for the next stage of booting the machine.

10 Figure 1 can be explained in more detail as follows;

The trusted BIOS loads up and runs 200 POST, which checks 201 if the next boot device is either an external device or an internal device. If it is an internal device, trusted BIOS measures 202 internal memory/storage and extend the measurement to  
15 PCR to define which devices are trusted. The trusted BIOS loads 203 Substantiation System into main memory and calls 204 Substantiation System. The Substantiation System measures 205 Root of Trust for Measurement (RTM) from the Internal Core Evidence Storage i.e. a secure storage device or database and also extends these measurements to PCR 240, then loads and calls 206 RTM.

20

The Substantiation system checks 207 if it is the first time run or not. If it is not first time run, it will collect 214 hardware evidence by executing functional tests on the hardware. The collected evidence is measured 215 and the stored evidence is

measured 216. The Result of measurement for new evidence and stored evidence are compared 217, and any differences are checked 218.

- If it is the first time run, the location of the initial core evidence is checked 208. If it
- 5 is local core evidence storage, hardware evidence is collected by executing 210 functional tests on the hardware on the machine. If the core evidence is not local, local core evidence storage is created 209 based on configuration or properties policy. The collected evidence is measured 211 and the measurement is extended to the PCR 240. The evidence is stored 212 inside the Internal Core Evidence Storage.
- 10 The need to update the server is checked 213. If an update to the server is not needed, it will proceed to the next booting stage and the process ends 226.

If the integrity of the system is valid, the client and server are informed 219 about the changes on the platform, and the server makes security related decisions 220.

15

If the POST determines that there is an external device, such as an external drive, the trusted BIOS measures and loads the external Master Boot Record (MBR) and extends 222 it to PCR 240.

- 20 The MBR measures 223 the external storage and extends it to PCR 240. The trusted BIOS executes 224 the Substantiation system to determine if the external storage is trusted – a user prompt may be generated asking the user if the device is trusted or not. The Substantiation system may also check 225 whether validation with server is

needed or not. If validation with the server is needed, secure communication is established 227, and the client sends 228 evidence to the server. The server compares 229 the evidence sent with core evidence stored inside the server and checks 230 if the compared evidences is valid or not. The server informs the client machine that  
5 the machine is trusted 232 or not trusted 231 accordingly, and then the Substantiation System executes 221 server instructions. If the external device is not trusted it is halted or the process of concern is stopped.

It will be appreciated by persons skilled in the art that the present invention may also  
10 include further additional modifications made to the device which does not affect the overall functioning of the device.

**Claims**

1. An authentication system for a computer system on which an operating system may be loaded,  
5           said computer system including a Basic Input Output System which runs (200) a Power On Self Test when power is applied to the computer system;  
              characterised in that if an external device is found during the Power On Self Test, said external device is checked for validity (224) to determine if it is trusted or not.  
10
2. An authentication system according to claim 1 wherein the validity of the external device is checked (224) before an operating system is loaded.
3. An authentication system according to claim 1 or 2 wherein the user is  
15           prompted to select if the external device is trusted or not.
4. An authentication system according to any preceding claim wherein the authentication system is integrated into the Basic Input Output System.
- 20   5. An authentication system according to any preceding claim wherein the computer system includes a Trusted Platform Module for determining if devices are trusted or not.

6. An authentication system according to claim 5 wherein the Trusted Platform Module contains one or more Platform Configuration Registers that define a root of trust indicating trusted devices.

5 7. An authentication system according to claim 6 wherein the root of trust is extended to devices considered to be trusted.

8. An authentication system according to claim 7 wherein the devices considered to be trusted can be checked for validity with a remote server.

10

9. An authentication system according to any preceding claim wherein the computer system is virtual.

10. A method of authenticating devices in a computer system comprising the steps  
15 of:

running (200) a Power On Self Test from a Basic Input Output System when power is applied to the computer system;

characterised in that if an external device is found during the Power On Self Test, said external device is checked for validity (224) to determine if it is  
20 trusted or not.

11. A method according to claim 10 wherein a Trusted Platform Module extends root of trust to devices indicated as being trusted by Platform Configuration Registers.
- 5 12. A method according to claim 11 wherein if the external device is valid, the root of trust is extended thereto, prior to an operating system being loaded.
13. A method according to any of claims 10-12 wherein the check for validity comprises a user's answer in response to a prompt.



# INTERNATIONAL SEARCH REPORT

International application No  
PCT/MY2013/000022

A. CLASSIFICATION OF SUBJECT MATTER  
INV. G06F21/57  
ADD.

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 practicable, search terms used)

EP0-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 2008/226080 A1 (LI BIN [JP])<br>18 September 2008 (2008-09-18)<br>paragraph [0054] - paragraph [0064];<br>figure 6<br>paragraph [0077] - paragraph [0083];<br>figure 15 | 1-13                  |
| X         | -----<br>US 2005/141717 A1 (CROMER DARYL C [US] ET<br>AL CHALLENGER DAVID CARROLL [US] ET AL)<br>30 June 2005 (2005-06-30)<br>paragraph [0004] - paragraph [0030]          | 1-13                  |
| X         | -----<br>US 7 430 668 B1 (CHEN LIQUN [GB] ET AL)<br>30 September 2008 (2008-09-30)<br>column 10 - column 13; figure 6<br>-----<br>-/--                                     | 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 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

31 May 2013

Date of mailing of the international search report

13/06/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040,  
Fax: (+31-70) 340-3016

Authorized officer

Jascau, Adrian

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/MY2013/000022

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                       | Relevant to claim No. |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | US 2003/135727 A1 (CHALLENGER DAVID CARROLL [US] ET AL) 17 July 2003 (2003-07-17) paragraph [0022] - paragraph [0042]<br>-----                                                                                           | 1-13                  |
| X         | US 2005/033987 A1 (YAN ZHENG [FI] ET AL) 10 February 2005 (2005-02-10) paragraph [0072] - paragraph [0073]; figure 5<br>-----                                                                                            | 1-13                  |
| T         | Seth David Schoen: "EOF - Give TCPA an Owner Override",<br><br>1 December 2003 (2003-12-01), XP055064540,<br>Retrieved from the Internet:<br>URL:www.linuxjournal.com/article/7055<br>[retrieved on 2013-05-29]<br>----- |                       |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/MY2013/000022

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s)                                            | Publication<br>date                                  |
|-------------------------------------------|---------------------|-----------------------------------------------------------------------|------------------------------------------------------|
| US 2008226080 A1                          | 18-09-2008          | EP 1970829 A1<br>JP 4994903 B2<br>JP 2008236089 A<br>US 2008226080 A1 | 17-09-2008<br>08-08-2012<br>02-10-2008<br>18-09-2008 |
| US 2005141717 A1                          | 30-06-2005          | NONE                                                                  |                                                      |
| US 7430668 B1                             | 30-09-2008          | US 7430668 B1<br>WO 0048061 A1                                        | 30-09-2008<br>17-08-2000                             |
| US 2003135727 A1                          | 17-07-2003          | US 2003135727 A1<br>US 2006107034 A1                                  | 17-07-2003<br>18-05-2006                             |
| US 2005033987 A1                          | 10-02-2005          | NONE                                                                  |                                                      |