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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 January 2006 (05.01.2006)

PCT

(10) International Publication Number
WO 2006/002368 A3

(51) International Patent Classification:
G06F 1/00 (2006.01)

(21) International Application Number:
PCT/US2005/022468

(22) International Filing Date: 22 June 2005 (22.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/582,206 22 June 2004 (22.06.2004) US
10/934,868 3 September 2004 (03.09.2004) US

(71) Applicant *(for all designated States except US)*: **SUN MICROSYSTEMS, INC.** [US/US]; 4150 Network Circle, Santa Clara, CA 95054 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TAHAN, Thomas, E.** [US/US]; P.O. Box 12086, La Jolla, CA 92039 (US).

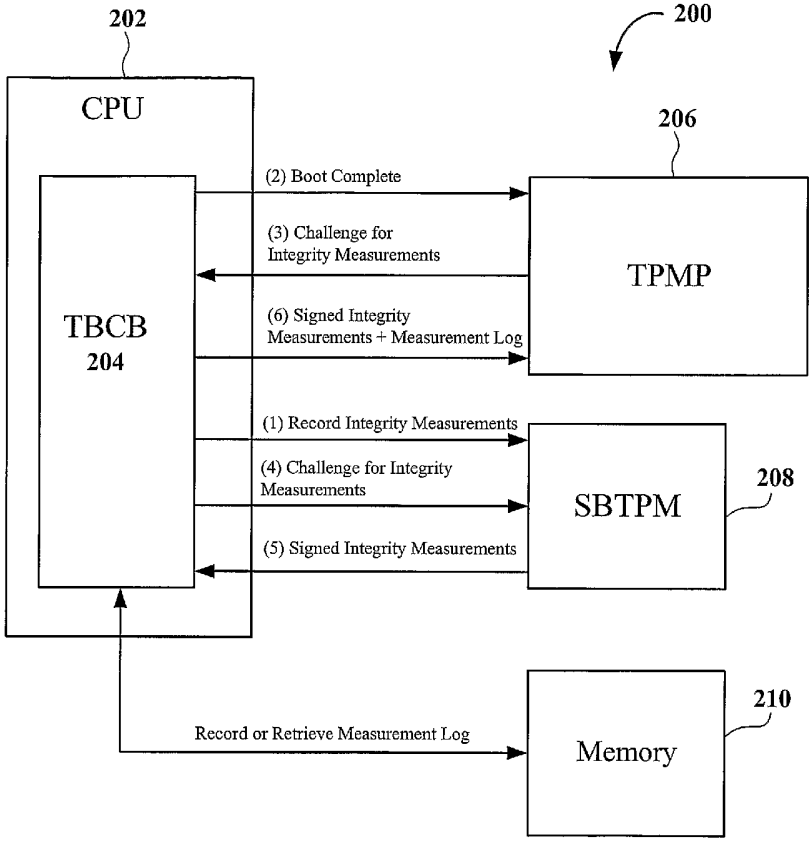
(74) Agent: **HSU, Michael, K.**; Martine Penilla & Gencarella, LLP, 710 Lakeway Drive, Suite 200, Sunnyvale, CA 94085 (US).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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, MC, NL, PL, PT, RO,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR SECURING A COMPUTER BOOT



(57) Abstract: A method for securing a computer boot is provided. In this method, integrity measurements of program code being loaded for execution are taken during the computer boot, and the integrity measurements are stored in a system board trusted platform module (SBTPM). Subsequently, the integrity measurements are transferred from the SBTPM to a trusted platform module peripheral (TPMP) when the TPMP is initialized and accessible. Systems for securing a computer boot are also described.

WO 2006/002368 A3

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

(88) Date of publication of the international search report:
20 April 2006

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.

INTERNATIONAL SEARCH REPORT

Intern I application No
PCT/US2005/022468

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00

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 6 609 199 B1 (DETREVILLE JOHN) 19 August 2003 (2003-08-19) column 2, line 33 - line 61 column 6, line 56 - column 7, line 2 column 7, line 32 - line 47 column 8, line 1 - line 59 column 9, line 22 - line 28 column 9, line 67 - column 10, line 22 figures 4-6	1,2, 10-22
A	US 2003/226031 A1 (PROUDLER GRAEME JOHN ET AL) 4 December 2003 (2003-12-04) paragraph [0007] - paragraph [0009] paragraph [0037] paragraph [0043] paragraph [0060] - paragraph [0064]	1,2, 10-22

-/--

[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
10 October 2005	24 02 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	Sigolo, A

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

INTERNATIONAL SEARCH REPORT

Inter l application No
PCT/US2005/022468

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 2003/084285 A1 (CROMER DARYL CARVIS ET AL) 1 May 2003 (2003-05-01) the whole document	1,2, 10-22
A	WO 2004/003824 A (INTEL CORPORATION) 8 January 2004 (2004-01-08) the whole document	1,2, 10-22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2005/022468

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1, 2, 10-22

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1,2,10-22

   Method for securing a computer boot by means of integrity measurements of program code being loaded for execution.

   ---

2. claims: 3-9,23-25

   Method of implementing secure transactions between devices.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr al application No
PCT/US2005/022468

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6609199 B1	19-08-2003	NONE	
US 2003226031 A1	04-12-2003	DE 10254621 A1	12-06-2003
		GB 2382419 A	28-05-2003
		US 2005223221 A1	06-10-2005
US 2003084285 A1	01-05-2003	NONE	
WO 2004003824 A	08-01-2004	AU 2003280494 A1	19-01-2004
		CN 1678968 A	05-10-2005
		EP 1518158 A1	30-03-2005
		US 2004003288 A1	01-01-2004