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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2008 (17.07.2008)

PCT

(10) International Publication Number
WO 2008/085449 A3

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

(21) International Application Number:
PCT/US2007/026279

(22) International Filing Date:
20 December 2007 (20.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/620,689 7 January 2007 (07.01.2007) US

(71) Applicant *(for all designated States except US)*: **APPLE INC.** [US/US]; 1 Infinite Loop, Cupertino, CA 95014 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SMITH, Michael** [AU/US]; 475 E. Mckinley Avenue, Sunnyvale, CA 94086 (US). **DE CESARE, Joshua** [US/US]; 678 Regas Drive, Campbell, CA 95008 (US). **DE ATLEY, Dallas, Blake** [US/US]; 4508 17th Street, #2, San Francisco, CA 94114 (US). **WRIGHT, John, Andrew** [US/US]; 364 Crescent Avenue, San Francisco, CA 94110 (US).

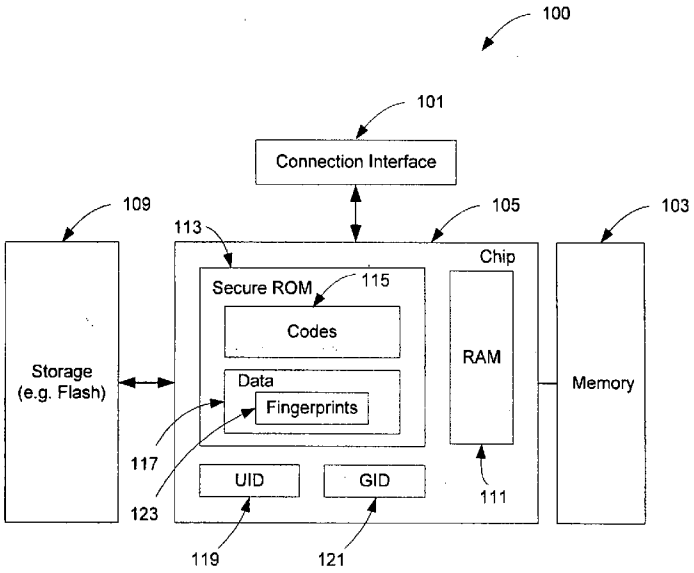
(74) Agents: **SCHELLER, James, C.** et al.; Blakely, Sokoloff, Taylor & Zafman Llp, 1279 Oakmead Parkway, Sunnyvale, CA 94085-4040 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, MT, NL, PL,

[Continued on next page]

(54) Title: SECURE BOOTING A COMPUTING DEVICE



(57) Abstract: A method and an apparatus for executing codes embedded inside a device to verify a code image loaded in a memory of the device are described. A code image may be executed after being verified as a trusted code image. The embedded codes may be stored in a secure ROM (read only memory) chip of the device. In one embodiment, the verification of the code image is based on a key stored within the secure ROM chip. The key may be unique to each device. Access to the key may be controlled by the associated secure ROM chip. The device may complete establishing an operating environment subsequent to executing the verified code image.

WO 2008/085449 A3

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*

(88) Date of publication of the international search report:
16 October 2008

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/026279

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 369 764 A (MICROSOFT CORP [US]) 10 December 2003 (2003-12-10)	1-4, 6-12, 14-30
Y	figures 2B,3,4 paragraphs [0003], [0009], [0011], [0032], [0033]	5,13
X	US 2003/056107 A1 (CAMMACK WILLIAM E [US] ET AL) 20 March 2003 (2003-03-20)	1,9,17
Y	paragraphs [0032] - [0035], [0044], [0045]	5,13

-/--

[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
6 August 2008	18/08/2008

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	Preuss, Norbert

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/026279

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 6 185 678 B1 (ARBAUGH WILLIAM A [US] ET AL) 6 February 2001 (2001-02-06)	1,9, 17-19, 22,25-29
A	figures 1b,1c,2a column 4, lines 33-59 column 8, lines 23-37 column 10, lines 45-67 column 11, lines 26-29	2-8, 10-16, 20,21, 23,24,30
X	US 2005/138409 A1 (SHERIFF TAYIB [US] ET AL) 23 June 2005 (2005-06-23)	1-4, 6-12,14, 30
A	paragraphs [0014], [0017], [0029], [0059]	5,13
X	US 2006/090084 A1 (BUER MARK [US]) 27 April 2006 (2006-04-27)	1,9, 17-19
A	paragraphs [0072], [0137], [0140], [0149], [0153]	5,13
X	US 6 263 431 B1 (LOVELACE JOHN V [US] ET AL) 17 July 2001 (2001-07-17)	1-4, 6-12, 14-30
A	figures 1-3 column 4, lines 7-21 column 5, lines 7-21	5,13
A	US 2004/064457 A1 (ZIMMER VINCENT J [US] ET AL) 1 April 2004 (2004-04-01) figures 1,5,8,9A paragraphs [0019], [0023], [0037], [0044], [0061]	1-30
A	EP 1 659 472 A (RES IN MOTION LTD [CA]) 24 May 2006 (2006-05-24) figures 2,3 paragraphs [0002], [0003], [0007], [0008], [0027]	6,9,21, 27,30
T	US 6 587 947 B1 (O'DONNELL AMY [US] ET AL) 1 July 2003 (2003-07-01) paragraphs [0021], [0022]	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/026279

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1369764 A	10-12-2003	AU 2003204376 A1	08-01-2004
		CN 1469238 A	21-01-2004
		JP 4052978 B2	27-02-2008
		JP 2004013905 A	15-01-2004
		US 2005138270 A1	23-06-2005
		US 2003229777 A1	11-12-2003
US 2003056107 A1	20-03-2003	NONE	
US 6185678 B1	06-02-2001	NONE	
US 2005138409 A1	23-06-2005	NONE	
US 2006090084 A1	27-04-2006	NONE	
US 6263431 B1	17-07-2001	NONE	
US 2004064457 A1	01-04-2004	NONE	
EP 1659472 A	24-05-2006	US 2006112266 A1	25-05-2006
US 6587947 B1	01-07-2003	NONE	