

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
9 February 2012 (09.02.2012)

(10) International Publication Number
WO 2012/018525 A3

PCT

(51) International Patent Classification:
G06F 12/14 (2006.01) **G06F 13/14** (2006.01)
G06F 9/22 (2006.01)

(21) International Application Number:
PCT/US2011/044621

(22) International Filing Date:
20 July 2011 (20.07.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/852,280 6 August 2010 (06.08.2010) US

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

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SWANSON, Robert C.** [US/US]; 7142 Grayhawk Lane NE, Olympia, Washington 98516 (US). **ZIMMER, Vincent J.** [US/US]; 1937 South 369th Street, Federal Way, Washington 98003 (US). **WEHAGE, Eric R.** [US/US]; 15140 Palmer Lane SE, Tenino, Washington 98589 (US). **BU-**

LUSU, Mallik [IN/US]; 3243 Lady Fern Lp NW, Olympia, Washington 98502 (US).

(74) Agents: **TROP, Timothy N.** et al.; Trop, Pruner & Hu, P.C., 1616 S. Voss Rd., Ste. 750, Houston, Texas 77057-2631 (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.

(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,

[Continued on next page]

(54) Title: SUPPORTING A SECURE READABLE MEMORY REGION FOR PRE-BOOT AND SECURE MODE OPERATIONS

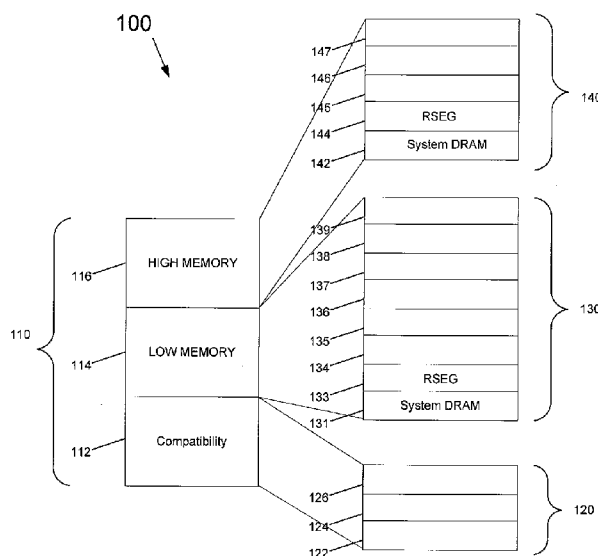


FIG. 1

(57) Abstract: In one embodiment, the present invention includes a method for determining whether an address map of a system includes support for a read only region of system memory, and if so configuring the region and storing protected data in the region. This data, at least some of which can be readable in both trusted and untrusted modes, can be accessed from the read only region during execution of untrusted code. Other embodiments are described and claimed.



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

— *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))*

Published:

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

(88) Date of publication of the international search report:

19 April 2012

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/044621**A. CLASSIFICATION OF SUBJECT MATTER****G06F 12/14(2006.01)i, G06F 9/22(2006.01)i, G06F 13/14(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 12/14; G06F 12/02; G06F 9/445; H04N 7/16; H03M 1/68; G06F 12/08

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: memory, address, map, read only

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007-0220276 A1 (DAREN CROXFORD et al.) 20 September 2007 See [0011] - [0090].	1-20
A	US 2008-0244211 A1 (TAKAFUMI ITO) 02 October 2008 See [0021] - [0139].	1-20
A	US 2004-0268084 A1 (STEVE LONGERBEAM et al.) 30 December 2004 See [0021] - [0067].	1-20
A	US 7117352 B1 (CHRISTOPHER M. GILES et al.) 03 October 2006 See column 2, line 9 - column 15, line 44.	1-20

☐ 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

29 FEBRUARY 2012 (29.02.2012)

Date of mailing of the international search report

29 FEBRUARY 2012 (29.02.2012)

Name and mailing address of the ISA/KR

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

Facsimile No. 82-42-472-7140

Authorized officer

KWON, Oh Seong

Telephone No. 82-42-481-8526



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/044621

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0220276 A1	20.09.2007	GB 0608533 D0 GB 2436378 A GB 2436378 B JP 2007-249933 A	07.06.2006 26.09.2007 27.10.2010 27.09.2007
US 2008-0244211 A1	02.10.2008	JP 2008-090519 A	17.04.2008
US 2004-0268084 A1	30.12.2004	None	
US 7117352 B1	03.10.2006	None	