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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2003 (16.10.2003)

PCT

(10) International Publication Number
WO 2003/085497 A3

(51) International Patent Classification:
G06F 12/14 (2006.01) ***G06F 9/455*** (2006.01)

(21) International Application Number:
PCT/US2003/008762

(22) International Filing Date:
20 March 2003 (20.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/112,169 29 March 2002 (29.03.2002) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: **SUTTON, James, II**; 20205 NW Paulina Drive, Portland, OR 97229 (US). **GRAWROCK, David**; 8285 Southwest 184th Avenue, Aloha, OR 97007 (US).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely Sokoloff Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE (patent), AG (patent), AL (patent), AM (patent), AT (patent), AU (patent), AZ (patent), BA (patent), BB (patent), BG (patent), BR (patent), BY (patent), BZ (patent), CA (patent), CH (patent), CN (patent), CO (patent), CR (patent), CU (patent), CZ (patent), DE (patent), DK (patent), DM (patent), DZ (patent), EC (patent), EE (patent), ES (patent), FI (patent), GB (patent), GD (patent), GE (patent), GH (patent), GM (patent), HR (patent), HU (patent), ID (patent), IL (patent), IN (patent), IS (patent), JP (patent), KE (patent), KG (patent), KP (patent), KR (patent), KZ (patent), LC (patent), LK (patent), LR (patent), LS (patent), LT (patent), LU (patent), LV (patent), MA (patent), MD (patent), MG (patent), MK (patent), MN (patent), MW (patent), MX (patent), MZ (patent), NO (patent), NZ (patent), OM (patent), PH (patent), PL (patent), PT (patent), RO (patent), RU (patent), SC, SD (patent), SE (patent), SG (patent), SK (patent), SL (patent), TJ (patent), TM (patent), TN (patent), TR (patent), TT (patent), TZ (patent), UA (patent), UG (patent), UZ (patent), VC, VN (patent), YU (patent), ZA (patent), ZM (patent), ZW (patent).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR EXECUTION OF A SECURED ENVIRONMENT INITIALIZATION INSTRUCTION

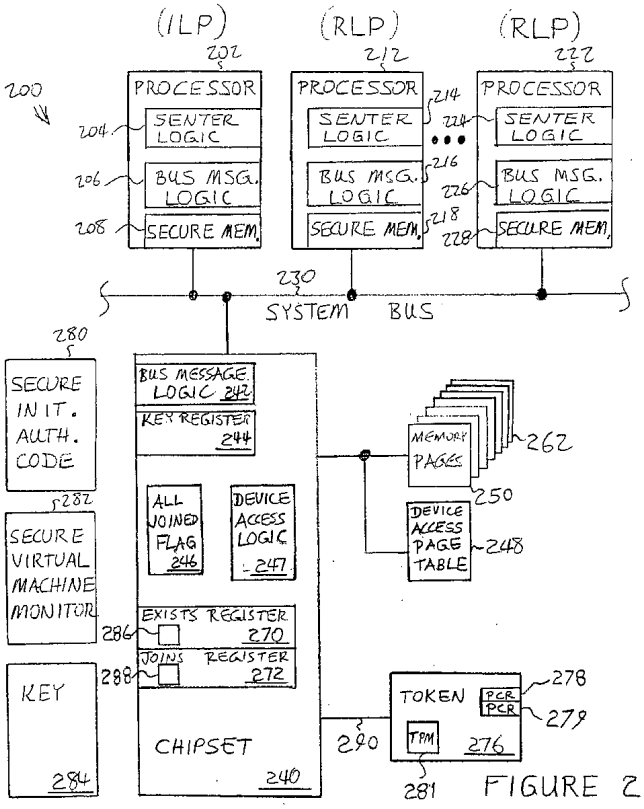

FIGURE 2

(57) Abstract: A method and apparatus for initiating secure operations in a microprocessor system is described. In one embodiment, one initiating logical processor initiates the process by halting the execution of the other logical processors, and then loading initialization and secure virtual machine monitor software into memory. The initiating processor then loads the initialization software into secure memory for authentication and execution. The initialization software then authenticates and registers the secure virtual machine monitor software prior to secure system operations.

WO 2003/085497 A3

(84) **Designated States** *(regional)*: ARIPO (GH, GM, KE, LS, MW, MZ, 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, IT, LU, MC, NL, 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 (Art. 21(3))*

(88) **Date of publication of the international search report**:
11 September 2009

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/08762

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F12/14 G06F9/455

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)
IPC 7 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, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 75565 A (THAKKAR SHREEKANT S ;LIN DERRICK C (US); RENERIS KEN (US); ELLISON) 11 October 2001 (2001-10-11) page 3 -page 11 figure 1C abstract --- -/--	1,3-5, 10, 14-16, 18,20,21

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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
17 July 2003	12. 08. 2003

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	JENNY FORSS/MN

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/08762

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ROBIN J S ET AL: "Analysis of the Intel Pentium's ability to support a secure virtual machine monitor" PROCEEDINGS OF THE NINTH USENIX SECURITY SYMPOSIUM, PROCEEDINGS OF 9TH USENIX SECURITY SYMPOSIUM, DENVER, CO, USA, 14-17 AUG. 2000, pages 129-144, XP002248053 2000, Berkeley, CA, USA, USENIX Assoc, USA ISBN: 1-880446-18-9 the whole document ---	1-49

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 03/08762

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0175565 A	11-10-2001	US 6507904 B1	14-01-2003
		AU 4939501 A	15-10-2001
		CN 1423765 T	11-06-2003
		DE 10196005 T0	13-03-2003
		GB 2377795 A	22-01-2003
		WO 0175565 A2	11-10-2001