



- (51) **International Patent Classification:**
G06F 21/22 (2006.01) *G06F 9/30* (2006.01)
- (21) **International Application Number:**
PCT/US201 1/067838
- (22) **International Filing Date:**
29 December 2011 (29.12.2011)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant (for all designated States except US):** **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, M/S: RNB-4-150, Santa Clara, California 95052 (US).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** **VAN DE VEN, Adriaan** [NL/US]; 2411 SW 17th Avenue, Portland, Oregon 97201 (US). **PATEL, Baiju, V.** [US/US]; 10552 NW La Cassel Crest Lane, Portland, Oregon 97229 (US). **MALLICK, Asit, K.** [US/US]; 12067 Ingrid Court, Saratoga, California 95070 (US). **NEIGER, Gilbert** [US/US]; 2111 NE 25th Avenue, Intel Corporation, JF2-65, Hillsboro, Oregon 97124-5961 (US). **COKE, James, S.** [US/US]; 4453 Barnett Ranch Road, Shingle Springs, California 95682 (US). **DIXON, Martin, G.** [US/US]; 4005 NE Hazelfern Place, Portland, Oregon 97232 (US). **BRANDT, Jason, W.** [US/US]; 1106 Maufrains Street, Austin, Texas 78703 (US).

(74) **Agents:** **VINCENT, Lester, J.** et al; Blakely, Sokoloff, Taylor & Zafman LLP, 1279 Oakmead Parkway, Sunnyvale, California 94085-4040 (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, 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.

(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, 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, 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))

(54) **Title:** SUPERVISOR MODE EXECUTION PROTECTION

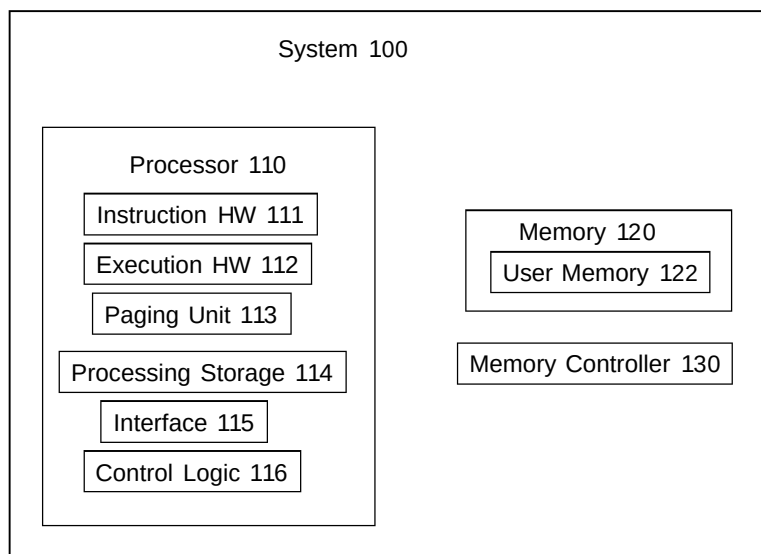


FIGURE 1

(57) **Abstract:** Apparatuses and methods for supervisor mode execution protection are disclosed. In one embodiment, a processor includes an interface to access a memory, execution hardware, and control logic. A region in the memory is user memory. The execution hardware is to execute an instruction. The control logic is to prevent the execution hardware from executing the instruction when the instruction is stored in user memory and the processor is in supervisor mode.



SUPERVISOR MODE EXECUTION PROTECTION

BACKGROUND

1. Field

5 The present disclosure pertains to the field of information processing, and, more specifically, to the field of information processing system security.

2. Description of Related Art

10 Memory based attacks are a significant threat to the security of information processing systems. Some such attacks involve storing malicious code, such as a virus or a worm, or malicious data in the memory of a computer system, then exploiting bugs and/or buffer overflows while running legitimate programs to transfer control to the malicious code or use the malicious data. A commonly used attack, known as a privilege escalation attack, involves storing attack code in application memory, then exploiting a vulnerability in kernel code to jump to the attack
15 code.

Brief Description of the Figures

20 The present invention is illustrated by way of example and not limitation in the accompanying figures.

 Figure 1 illustrates a system and a processor in which an embodiment of the present invention may be present and/or operate.

 Figure 2 illustrates a method for supervisor mode execution protection according to an embodiment of the present invention.

Detailed Description

25 The following description describes embodiments of techniques for supervisor mode execution protection. In the following description, specific details such as processor and system configurations may be set forth in order to provide a more thorough understanding of the present invention. It will be appreciated, however, by one skilled in the art that the invention may be practiced without such specific details. Additionally, some well known structures, circuits, and the like have not been shown in detail, to avoid unnecessarily obscuring the present invention.

 Embodiments of the present invention provide for using an attribute assigned to memory

pages to provide supervisor mode execution protection. Techniques according to embodiments of the present invention may be implemented within any approach to memory management, including page-based memory management data structures, nested page-based memory management data structures used by virtualization technologies, and parallel access data structures.

Figure 1 illustrates system 100, an information processing system in which an embodiment of the present invention may be present and/or operate. System 100 may represent any type of information processing system, such as a server, a desktop computer, a portable computer, a set-top box, a hand-held device, or an embedded control system. System 100 includes processor 110, memory 120, and memory controller 130. Systems embodying the present invention may include any other components or other elements, including any number of additional processors and/or memories. Any or all of the components or other elements in any system embodiment may be connected, coupled, or otherwise in communication with each other through any number of buses, point-to-point, or other wired or wireless connections.

Processor 110 may represent any type of processor, including a general purpose microprocessor, such as a processor in the Core® Processor Family, or other processor family from Intel Corporation, or another processor from another company, or any other processor for processing information according to an embodiment of the present invention. Processor 110 may include any number of execution cores and/or support any number of execution threads, and therefore may represent any number of physical or logical processors, and/or may represent a multi-processor component or unit.

Processor 110 supports execution of software at different privilege levels, according to any known approach. For example, processor 110 may recognize four privilege levels, which may be labeled zero to four, where the higher number means less privilege. The four privilege levels may be pictured as rings of protection, with privilege level zero, in the center, is intended for executing operating system ("OS") kernel level code, levels one and two are intended for executing OS services code, and level four, the outermost ring, is intended for executing application code.

Memory 120 may represent any static or dynamic random access memory, semiconductor-based read only or flash memory, magnetic or optical disk memory, any other type of medium readable by processor 110 and/or other elements of system 100, or any combination of such mediums. Memory controller 130 may represent a controller for controlling access to memory 120 and maintaining its contents. In an embodiment, memory controller 130 may be integrated onto the same integrated circuit as processor 110.

According to embodiments of the present invention, memory 120 may include user memory 122, which may be locations and/or regions referred to as application or user memory, which is intended to store instructions and data for used by application software. These locations and/or regions may be labeled as application memory according to any known technique. In an embodiment, each such location may include a bit or field which may store a certain value to indicate that it is user memory. In an embodiment, an entry at a higher level in a paging or other memory hierarchy may include a bit or field which may store a certain value to indicate that all lower level pages or other regions to which it may refer are user memory. For example, pages may be designated as user memory in a page directory entry and/or a translation lookaside buffer ("TLB") entry using a user/supervisor flag bit. In an embodiment, registers, tables, or other data structures may be used to designate a range or ranges of memory 120 designated as user memory.

Processor 110 may include instruction hardware 111, execution hardware 112, paging unit 113, processing storage 114, interface 115, and control logic 116, plus any other desired units or elements.

Instruction hardware 111 may represent any circuitry, structure, or other hardware, such as an instruction decoder, for fetching, receiving, decoding, and/or scheduling instructions. Any instruction format may be used within the scope of the present invention; for example, an instruction may include an opcode and one or more operands, where the opcode may be decoded into one or more micro-instructions or micro-operations for execution by execution hardware 112. In an embodiment, one of the instructions types may be an identification instruction, to which processor 110 is designed to respond with information to identify processor 110 or anything about processor 110. For example, the identification instruction may be the CPUID instruction in the instruction set architecture of the Intel® Core® Processor Family. In response to this instruction, processor 110 may return information that includes an indication that processor 110 supports supervisor mode execution protection according to an embodiment of the present invention.

Execution hardware 112 may include any circuitry, structure, or other hardware, such as an arithmetic unit, logic unit, floating point unit, shifter, etc., for processing data and executing instructions, micro-instructions, and/or micro-operations.

Paging unit 113 may represent any circuitry, structure, or other hardware, such as a TLB for translating addresses with which processor 110 accesses memory 120. Paging unit 113 may perform address translations, for example the translation of a logical or linear address to a physical address, according to any known memory management technique. To perform address translations, paging unit 113 refers to one or more data structures stored in processor 110,

memory 120, any other storage location in system 100 not shown in Figure 1, and/or any combination of these components and locations. The data structures may include page directories and page tables according to the architecture of the Core® Processor Family, as modified according to embodiments of the present invention, and/or a table stored in a TLB.

5 In one embodiment, paging unit 113 receives a linear address provided by an instruction to be executed and/or of data to be fetched by processor 110. Paging unit 113 uses portions of the linear address as indices into hierarchical tables, including page tables. The page tables contain entries, each including a field for a base address of a page in memory 120. Any page size (e.g., 4 kilobytes) may be used within the scope of the present invention. Therefore, the linear address
10 used by a program to access memory 120 may be translated to a physical address used by processor 110 to access memory 120.

Processing storage 114 may represent any type of storage usable for any purpose within processor 110, for example, it may include any number of data registers, instruction registers, status registers, other programmable or hard-coded registers or register files, or any other storage
15 structures. In an embodiment, processing storage 114 may include a control register according to the architecture of the Core® Processor Family (e.g., CR4), which may include a programmable bit location or another size field to be used to enable supervisor mode execution protection according to embodiments of the present invention. For example, operating system software or other system software may perform a write to CR4 to set (e.g., write to a value of T) a
20 supervisor mode execution protection enable bit in CR4 to enable the feature. In one embodiment, software executing instructions at a more privileged privilege level (e.g., rings 0, 1, or 2) may be referred to as running in supervisor mode and software executing at a less privileged privilege level (e.g., ring 4) may be referred to as running in user mode.

Interface unit 115 may represent any circuitry, structure, or other hardware, such as a bus
25 unit or any other unit, port, or interface, to allow processor 110 to communicate with memory 120 through any type of bus, point to point, or other connection, directly or through any other component, such as a chipset or memory controller.

Control logic 116 may represent microcode, programmable logic, hard-coded logic, or any other type of logic to control the operation of the units and other elements of processor 110 and
30 the transfer of data within processor 110. Control logic 116 may cause processor 110 to perform or participate in the performance of method embodiments of the present invention, such as the method embodiments described below, for example, by causing processor 110 to execute instructions received by instruction hardware 111 and micro-instructions or micro-operations derived from instructions received by instruction hardware 111.

According to embodiments of the present invention, processor 100 may execute instructions from user memory when operating in user mode, but processor 100 cannot execute instructions from user memory when operating in supervisor mode. This feature may be implemented with control logic that causes a fault when instruction unit 111 attempts to fetch an instruction from user memory when processor 100 is executing code in supervisor mode.

Figure 2 illustrates an embodiment of the present invention in a method, method 200, for supervisor mode execution protection. The description of Figure 2 may refer to elements of Figure 1, but method 200 and other method embodiments of the present invention are not intended to be limited by these references.

In block 210, OS software running on processor 110 may execute a CPUTD instruction to determine that processor 110 supports a supervisor mode execution protection feature according to an embodiment of the present invention. In box 212, the OS software may execute a write to CR4 to enable the supervisor mode execution protection feature.

In box 220, the OS software may transfer control to an application program. In box 222, the application program may begin execution in user mode. In box 224, the application may attempt to fetch an instruction from user memory. In box 226, the application is allowed to fetch the instruction from user memory. In box 228, the instruction is executed.

In box 230, control is transferred from the application program to the OS software. In box 232, the OS software continues running in supervisor mode. In box 234, the OS software attempts to fetch an instruction from user memory. In box 236, the attempt to fetch an instruction from user memory while in supervisor mode causes a fault, so the instruction cannot be fetched or executed.

Within the scope of the present invention, method 200 may be performed in a different order than that shown in Figure 2, with illustrated boxes omitted, with additional boxes added, or with a combination of reordered, omitted, or additional boxes.

Thus, techniques for supervisor mode execution protection are disclosed. While certain embodiments have been described, and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art upon studying this disclosure. In an area of technology such as this, where growth is fast and further advancements are not easily foreseen, the disclosed embodiments may be readily modifiable in arrangement and detail as facilitated by enabling technological advancements without departing from the principles of the present disclosure or the scope of the accompanying

claims.

Claim

What is claimed is:

1. A processor comprising:

5 an interface to access a memory, wherein a region in the memory is user memory;
execution hardware to execute an instruction; and
control logic to prevent the execution hardware from executing the instruction when the
instruction is stored in user memory and the processor is in supervisor mode.

10 2. The processor of claim 1, further comprising instruction hardware to fetch the
instruction, wherein the control logic is to prevent the execution hardware from executing the
instruction by preventing the instruction hardware from fetching the instruction from user
memory when the processor is in supervisor mode.

15 3. The processor of claim 1, wherein the processor is in supervisor mode when executing
software in a privilege level higher than a lowest privilege level.

4. The processor of claim 1, further comprising a paging unit, wherein the paging unit is to
translate a linear address to a physical address using a page table hierarchy, and the region may
20 be designated as user memory by a flag at any level in the page table hierarchy.

5. The processor of claim 1, wherein the execution unit is also to execute a processor
identification instruction by returning an indication that the processor includes control logic to
prevent the processor from executing from user memory when the processor is in supervisor
25 mode.

6. The processor of claim 1, further comprising processing storage including a
programmable storage location to enable the control logic to prevent the processor from
executing from user memory when the processor is in supervisor mode.

30 7. A method comprising:
attempting, by software running on a processor in supervisor mode, to execute an
instruction; and
preventing the processor from executing the instruction when the instruction is stored in

user memory.

8. The method of claim 7, wherein attempting includes attempting to fetch the instruction from memory, and preventing includes preventing fetching the instruction from user memory.

5

9. The method of claim 7, wherein preventing includes causing a fault.

10. The method of claim 7, further comprising executing a processor identification instruction to determine that the processor supports preventing execution from user memory when in supervisor mode.

10

11. The method of claim 7, further comprising writing to a control register to enable prevention of execution from user mode when the processor is in supervisor mode.

12. The method of claim 7, further comprising attempting, by the processor running in user mode, to execute the instruction.

15

13. The method of claim 12, further comprising allowing the processor running in user mode to execute the instruction.

20

14. The method of claim 12, wherein attempting, by the processor running in user mode, to execute the instruction includes attempting, by the processor running in user mode, to fetch the instruction.

15. The method of claim 13, wherein allowing the processor running in user mode to execute the instruction includes allowing the processor running in user mode to fetch the instruction.

25

16. A system comprising:

a memory, including a region of user memory; and

a processor coupled to the memory, including

execution hardware to execute an instruction, and

control logic to prevent the execution hardware from executing the instruction when the instruction is stored in user memory and the processor is in supervisor mode.

30

17. The system of claim 16, wherein the processor also includes instruction hardware to fetch the instruction, wherein the control logic is to prevent the execution hardware from executing the instruction by preventing the instruction hardware from fetching the instruction from user memory when the processor is in supervisor mode.

5

18. The system of claim 16, wherein the processor is in supervisor mode when executing software in a privilege level higher than a lowest privilege level.

19. The system of claim 16, wherein the memory is accessible as a plurality of pages, and
10 user memory includes a subset of the plurality of pages.

20. The system of claim 19, further comprising a paging unit, wherein the paging unit is to translate a linear address to a physical address using a page table hierarchy, and the region may be designated as user memory by a flag at any level in the page table hierarchy.

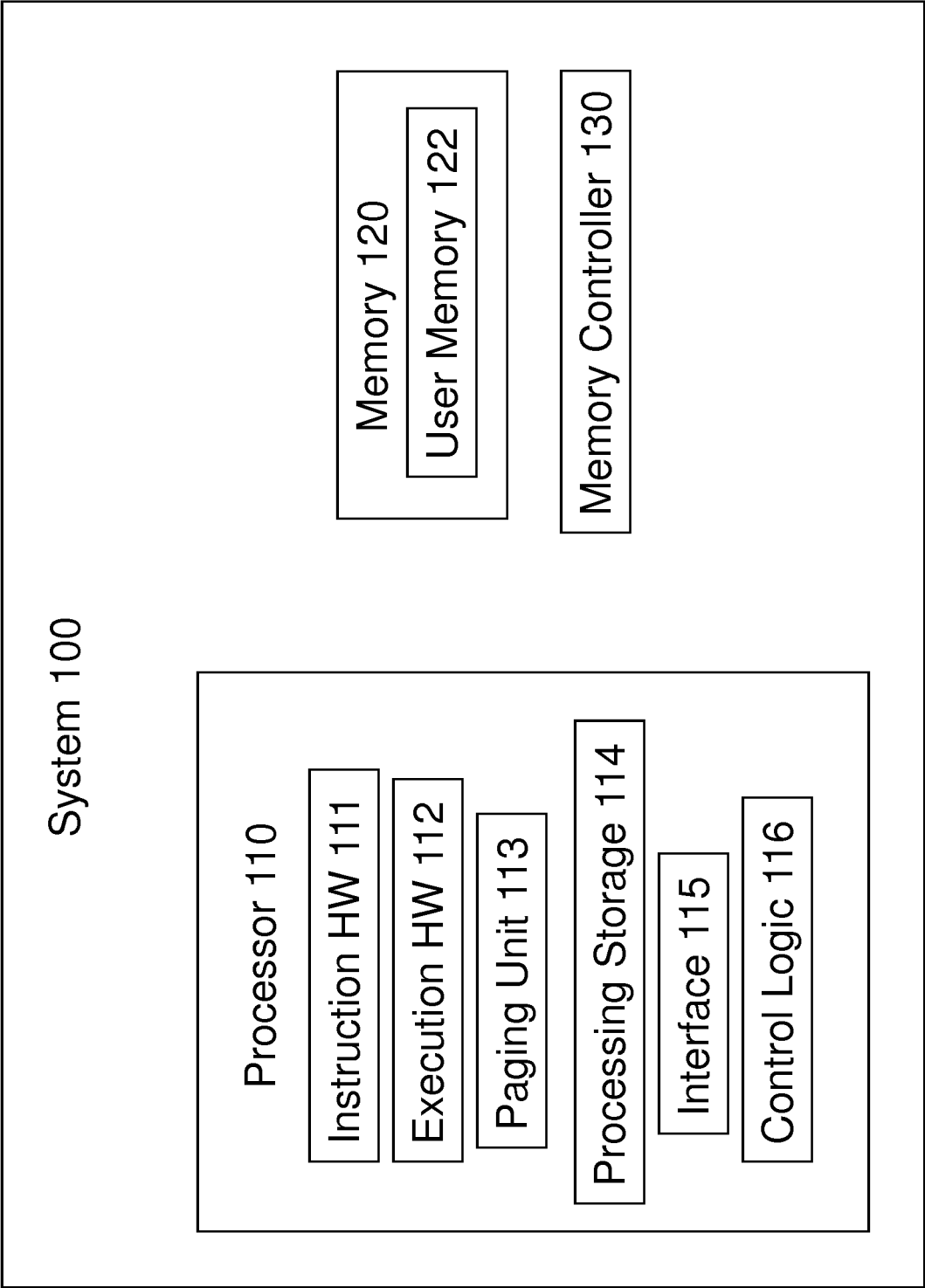


FIGURE 1

Method 200

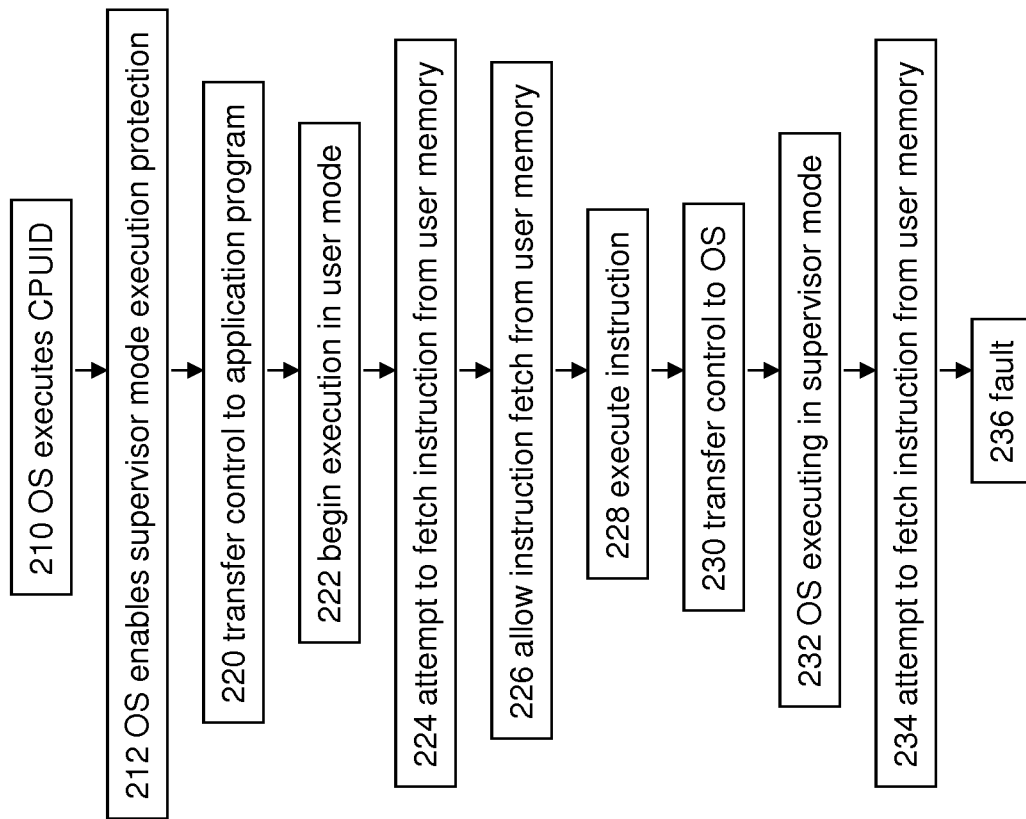


FIGURE 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/067838

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22(2006.01)i, G06F 9/30(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 21/22; G06F 9/44; G06F 12/14; G06F 9/00

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: supervisor, mode, execution, protection, access, user, memory, instruction, fetch, privilege

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010-0169601 A1 (FUNK DAVID WILLIAM et al.) 01 July 2010 See abstract; paragraphs [74] - [81]; figure 2.	1-4, 7-20
A	See the whole document.	5, 6
Y	Intel Developer Forum 2011 (Varghese George et al.) 13 September 2011 See page 9.	1-4, 7-20
A	See the whole document.	5, 6
A	US 2004-0168047 A1 (SHIN-ICHIRO FUKAI et al.) 26 August 2004 See abstract; paragraphs [44] - [57]; figures 2, 7.	1-20
A	US 2002-0087853 A1 (RAVI P. SINGH et al.) 04 July 2002 See abstract; paragraphs [9] - [15]; figure 1.	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

19 SEPTEMBER 2012 (19.09.2012)

Date of mailing of the international search report

19 SEPTEMBER 2012 (19.09.2012)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan
City, 302-70 1, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Shin Sang Gil

Telephone No. 82-42-481-8480



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US201 1/067838

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0 169601 A1	01.07,2010	US 2008-00 10425 A1 US 768 1000 B2 US 7984257 B2	10.01,2008 16.03,2010 19.07,2011
US 2004-0 168047 A1	26.08,2004	CN 1525323 A CN 1525323 CO JP 2004-28080 1 A	01.09,2004 01.09,2004 07.10,2004
US 2002-0087853 A1	04.07,2002	CN 100342327 CO CN 1483 160 A JP 03720807 B2 JP 2004-52 1413 A JP 2004-52 1413 T KR 10-05360 19 B1 TW 23240 1 A TW 23240 1 B US 6763453 B2 Wo 02-054226 A2 Wo 02-054226 A3	10.10,2007 17.03,2004 30.11,2005 15.07,2004 15.07,2004 14.12,2005 11.05,2005 11.05,2005 13.07,2004 11.07,2002 11.07,2002