



- (51) International Patent Classification:
G06F 21/52 (2013.01) G06F 15/78 (2006.01)
G06F 12/08 (2006.01) G06F 11/10 (2006.01)
- (21) International Application Number:
PCT/US2016/015438
- (22) International Filing Date:
28 January 2016 (28.01.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
14/612,067 2 February 2015 (02.02.2015) US
- (71) Applicant: QUALCOMM INCORPORATED [US/US];
ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

- (72) Inventors: KRISHNASWAMY, Arvind; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). ACAR, Can; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). TURNER, Robert; 5775 Morehouse Drive, San Diego, California 92121-1714 (US).
- (74) Agents: HUNTER, Shane et al.; HUNTER CLARK PLLC, 900 Cummings Center, Suite 213-T, Beverly, Massachusetts 01915 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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,

[Continued on next page]

(54) Title: AUTHENTICATED CONTROL STACKS

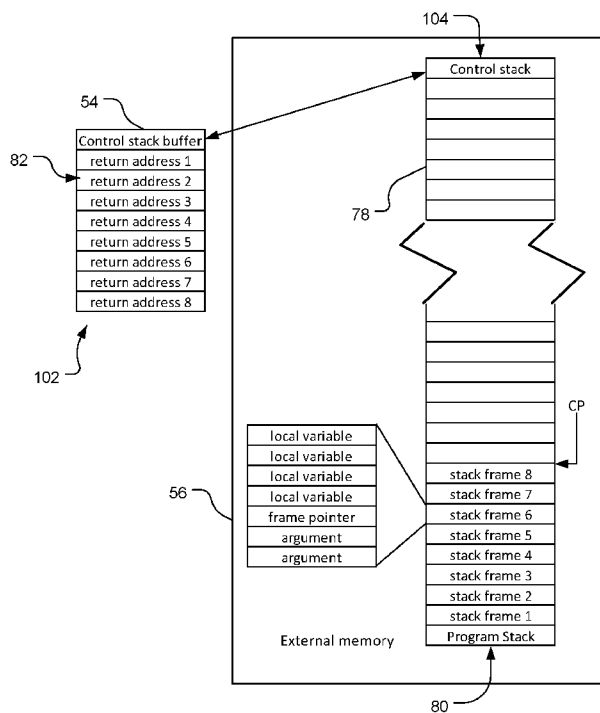


FIG. 4

(57) Abstract: A method of producing a control stack includes: writing a plurality of control information entries into a control stack buffer that is internal to a processor in response to one or more function calls; and in response to the control stack buffer being full and receiving a further function call, writing: the plurality of control information entries to an external memory that is external to the processor; and a further control information entry, corresponding to the further function call, to the control stack buffer.



GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

(88) Date of publication of the international search report:
29 September 2016

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/015438

A. CLASSIFICATION OF SUBJECT MATTER
 INV. G06F21/52 G06F12/08 G06F15/78 G06F11/10
 ADD.
 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 practicable, 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	GB 2 343 031 A (SUN MICROSYSTEMS INC [US]) 26 April 2000 (2000-04-26)	1,9,16, 23
Y	page 1 - page 2; figure 3a page 7 - page 10	2-8, 10-15, 17-22, 24-29
	----- -/--	

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"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)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"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</p> <p>"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</p> <p>"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</p> <p>"&" document member of the same patent family</p>
---	---

Date of the actual completion of the international search 28 July 2016	Date of mailing of the international search report 05/08/2016
---	--

Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Rey, Salvador
--	---

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/015438

Box No. 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 No. 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 fees, this Authority did not invite payment of additional fees.

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.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2016/015438

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	LEE R B ET AL: "Architecture for Protecting Critical Secrets in Microprocessors", COMPUTER ARCHITECTURE, 2005. ISCA '05. PROCEEDINGS. 32ND INTERNATIONAL SYMPOSIUM ON MADISON, WI, USA 04-08 JUNE 2005, PISCATAWAY, NJ, USA, IEEE, 4 June 2005 (2005-06-04), pages 2-13, XP010807890, DOI: 10.1109/ISCA.2005.14 ISBN: 978-0-7695-2270-8 sections 4.1 , 4.4 - 4.4.2, 4.5, 7; figure 6	2-5, 10-13, 17-20, 24-27
Y	----- US 2006/161773 A1 (OKAZAKI ATSUYA [JP] ET AL) 20 July 2006 (2006-07-20) paragraph [0077] - paragraph [0090]; figures 4a-4c,9	2-5, 10-13, 17-20, 24-27
X	----- US 2007/277021 A1 (O'CONNOR JAMES M [US] ET AL) 29 November 2007 (2007-11-29)	1,6,9, 14,16, 21,23,28
Y	paragraph [0033] - paragraph [0034]; figures 1a-1b,4a-4c paragraph [0063] paragraph [0083] - paragraph [0106] paragraph [0218] - paragraph [0226] paragraph [0282] - paragraph [0292]	7,8
Y	----- RUBYB LEE ET AL: "Enlisting Hardware Architecture to Thwart Malicious Code Injection", 27 January 2004 (2004-01-27), SECURITY IN PERVASIVE COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER-VERLAG, BERLIN/HEIDELBERG, PAGE(S) 237 - 252, XP019002202, ISBN: 978-3-540-20887-7 sections 5 and 5.1	6-8,14, 15,21, 22,28,29
Y	----- CHIUEH T-C ET AL: "RAD: a compile-time solution to buffer overflow attacks", PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, IEEE COMPUTER SOCIETY, US, 16 April 2001 (2001-04-16), pages 409-417, XP002292775, ISSN: 1063-6927 ISBN: 978-1-4577-0295-2 sections 3, 3.1 and 3.2 -----	6-8,14, 15,21, 22,28,29

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/015438

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
GB 2343031	A	26-04-2000	CA 2277638 A1	24-01-2000
			DE 19934067 A1	04-05-2000
			GB 2343031 A	26-04-2000
			US 6108767 A	22-08-2000
			US 6167504 A	26-12-2000

US 2006161773	A1	20-07-2006	JP 2006203564 A	03-08-2006
			US 2006161773 A1	20-07-2006

US 2007277021	A1	29-11-2007	EP 0976034 A1	02-02-2000
			JP 3634379 B2	30-03-2005
			JP 2000513464 A	10-10-2000
			KR 20050052529 A	02-06-2005
			US 6532531 B1	11-03-2003
			US 2003115238 A1	19-06-2003
			US 2003200351 A1	23-10-2003
			US 2005267996 A1	01-12-2005
			US 2007277021 A1	29-11-2007
			WO 9727539 A1	31-07-1997

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

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

1. claims: 1-5, 9-13, 16-20, 23-27

Writing a plurality control information entries of function calls in a control stack buffer into external memory when buffer full and receiving a further function call, and determining an authentication tag using at least two entries of said plurality.

2. claims: 6-8, 14, 21, 28

Writing a plurality control information entries of function calls in a control stack buffer into external memory when buffer full and receiving a further function call, said control information entries being stored in a first area of external memory which is physically displaced from a second area of said memory containing program data corresponding to the control information entries.

3. claims: 15, 22, 29

Writing a plurality control information entries of function calls in a control stack buffer into external memory when buffer full and receiving a further function call by forming a shadow stack, with at least primary portions of the control information entries being duplicates of primary portions of stack frame control information entries written in stack frames, said stack frames being stored in external memory.
