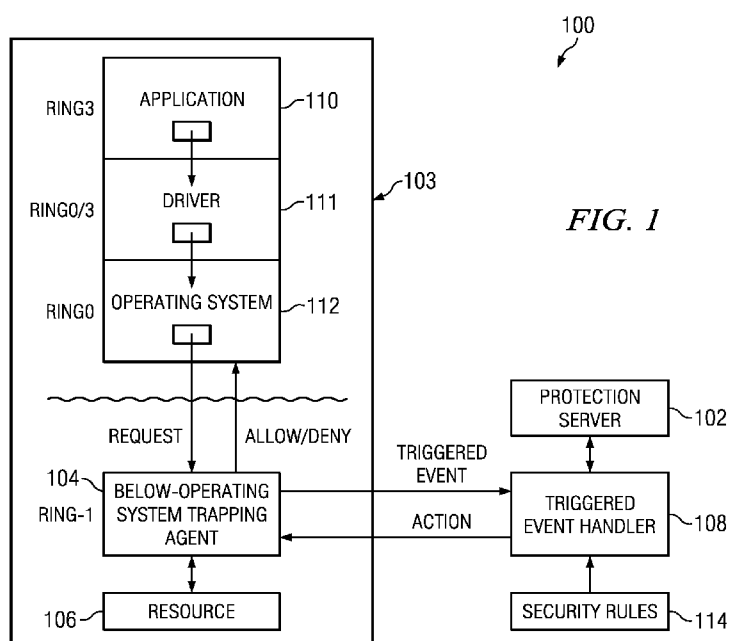




- (51) International Patent Classification:
- | | | | | |
|-----------------------------|-----------------------------|------------|----------------------------|----|
| <i>G06F 21/20</i> (2006.01) | <i>G06F 21/22</i> (2006.01) | 13/077,227 | 31 March 2011 (31.03.2011) | US |
| <i>G06F 11/30</i> (2006.01) | <i>G06F 13/14</i> (2006.01) | 13/076,512 | 31 March 2011 (31.03.2011) | US |
| | | 13/076,480 | 31 March 2011 (31.03.2011) | US |
| | | 13/076,473 | 31 March 2011 (31.03.2011) | US |
| | | 13/076,493 | 31 March 2011 (31.03.2011) | US |
- (21) International Application Number: PCT/US2012/030702
- (22) International Filing Date: 27 March 2012 (27.03.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
- | | | |
|------------|----------------------------|----|
| 13/073,810 | 28 March 2011 (28.03.2011) | US |
| 13/073,791 | 28 March 2011 (28.03.2011) | US |
| 13/073,842 | 28 March 2011 (28.03.2011) | US |
| 13/073,853 | 28 March 2011 (28.03.2011) | US |
| 13/073,864 | 28 March 2011 (28.03.2011) | US |
| 13/074,741 | 29 March 2011 (29.03.2011) | US |
| 13/074,925 | 29 March 2011 (29.03.2011) | US |
| 13/074,947 | 29 March 2011 (29.03.2011) | US |
| 13/075,049 | 29 March 2011 (29.03.2011) | US |
| 13/075,072 | 29 March 2011 (29.03.2011) | US |
| 13/074,831 | 29 March 2011 (29.03.2011) | US |
| 13/075,101 | 29 March 2011 (29.03.2011) | US |
| 13/077,270 | 31 March 2011 (31.03.2011) | US |
| 13/076,537 | 31 March 2011 (31.03.2011) | US |
| 13/077,305 | 31 March 2011 (31.03.2011) | US |
- (71) Applicant (for all designated States except US): **MCAFEE, INC.** [US/US]; 3965 Freedom Circle, Santa Clara, California 95054 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **SALLAM, Ahmed Said** [EG/US]; 10171 Vicksburg Drive, Cupertino, California 95014 (US).
- (74) Agent: **SUVA II, Jerry F.**; Baker Botts L.L.P., 98 San Jacinto Blvd., Suite 1500, Austin, Texas 78701 (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.

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR VIRTUAL MACHINE MONITOR BASED ANTI-MALWARE SECURITY



(57) Abstract: A system for securing an electronic device includes a memory, a processor, one or more operating systems residing in the memory for execution by the processor, a resource of the electronic device communicatively coupled to the operating system, a virtual machine monitor configured to execute on the electronic device at a level below all of the operating systems of the electronic device accessing the resource, and a security agent configured to execute on the electronic device at a level below all operating systems of the electronic device accessing the resource. The virtual machine monitor is configured to intercept a request of the resource made from a level above the virtual machine monitor and inform the security agent of the request. The security agent is configured to determine whether the request is indicative of malware.



(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:

— *as to the identity of the inventor (Rule 4.17(i))*

Published:

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

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

28 February 2013

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/20(2006.01)i, G06F 11/30(2006.01)i, G06F 21/22(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)

IPC: G06F; G06Q; G06K; H04N; H04L

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: virtual network, virtual machine, operating system, security, malware

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009-0165133 A1 (JOO-YOUNG HWANG et al.) 25 June 2009 See abstract, paragraphs [0023, 0024, 0029, 0030, 0036, 0037, 0042, 0043, 0047, 0051, 0052, 0055, 0068, 0069, 0072], claims 1, 2, 10, 11, 19 and figure 1.	1-145
A	US 7239709 B1 (Masazumi Yamada et al.) 03 July 2007 See abstract claims 1, 36, 45, 46, 54, 55 and figure 1.	1-145
A	US 06049289 A (DENNIS W. WAGGAMON et al.) 11 April 2000 See abstract; claim 1 and figure 2.	1-145
A	US 6693965 B1 (HISASHI INOUE et al.) 17 February 2004 See abstract; claims 1-6 and figure 1.	1-145



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

17 OCTOBER 2012 (17.10.2012)

Date of mailing of the international search report

18 OCTOBER 2012 (18.10.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Park Jin A

Telephone No. 82-42-481-8536



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/030702

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0165133 A1	25.06.2009	KR 10-2009-0068833 A	29.06.2009
US 7239709 B1	03.07.2007	EP 0989557 A1	29.03.2000
		EP 0989557 A4	23.12.2009
		JP 11-232776 A	27.08.1999
		JP 3429660 B2	22.07.2003
		KR 10-0611867 B1	11.08.2006
		WO 99-38164 A1	29.07.1999
US 06049289 A	11.04.2000	US 2004-0085185 A1	06.05.2004
		US 6667684 B1	23.12.2003
US 6693965 B1	17.02.2004	EP 1022895 A2	26.07.2000
		EP 1022895 A3	04.04.2001
		JP 2000-216980 A	04.08.2000
		JP 2000-332988 A	30.11.2000