

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
5 April 2007 (05.04.2007)

PCT

(10) International Publication Number
WO 2007/038245 A3

(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:

PCT/US2006/036934

(22) International Filing Date:

21 September 2006 (21.09.2006)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

60/720,255 23 September 2005 (23.09.2005) US

11/532,855 18 September 2006 (18.09.2006) US

(71) Applicant (for all designated States except US):
WIDEVINE TECHNOLOGIES, INC. [US/US]; 900
FOURTH AVENUE, Suite 3400, Seattle, WA 98164 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KOELLE, Katharina, Veronika** [DE/US]; 601 Catherine Street, Ann Arbor, MI 48104 (US). **MIDWINTER, Wendy** [CA/CA]; 77 Finch Avenue East, Toronto, ON M2N 6H8 (CA).

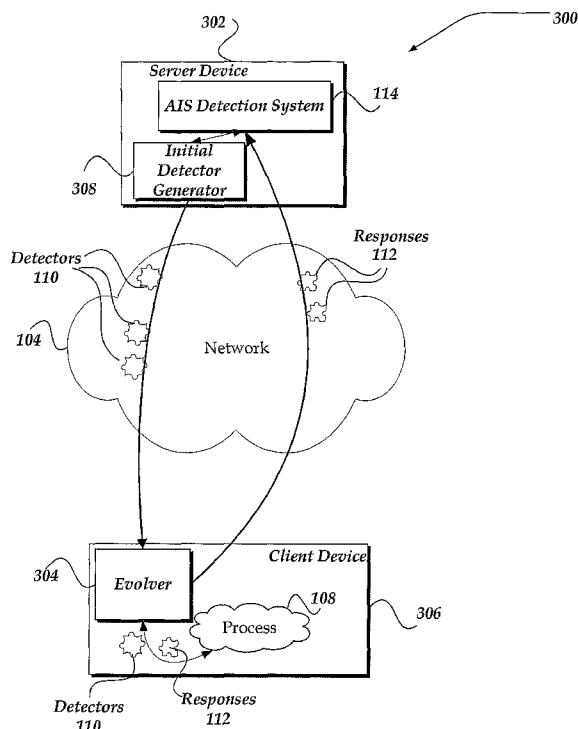
(74) Agent: **BRANCH, John, W.**; Darby & Darby P.C., P.O. Box 770, Church Street Station, New York, NY 10008-0770 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, 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, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR EVOLVING DETECTORS TO DETECT MALIGN BEHAVIOR IN AN ARTIFICIAL IMMUNE SYSTEM



(57) Abstract: A system, apparatus, and method are directed to evolving detectors in an Artificial Immune System for use in detecting unauthorized computing activities. In one embodiment, a population of detectors is generated with a matching value and expectation value of zero. The detectors are then compared to logged fragments of system calls within a computing device to modify the matching value. When the matching value for a given detector is equal to or greater than an expectation value, the detector's expectation value may be set to the matching value. The detectors may then evolve and/or generate other detectors using mutation, and/or recombination, or the like. Detectors continue to generate and/or to evolve until a detector's matching value reaches a determined value, in which case, the detector may be evaluated to determine if an unauthorized activity is detected. If an unauthorized activity is detected, a detection response may be performed.



Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

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

15 November 2007

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 06/36934

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 11/00 (2007.01)

USPC - 726/22

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)

USPC: 726/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC: 713/187; 713/188

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PubWEST(USPT,PGPB,EPAB,JPAB); DialogPRO(Engineering); Google Scholar

Search Terms: artificial, immune, detector, compar, matching value, expectation value

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0164023 A1 (KOELLE et al.) 07 November 2002 (07.11.2002), FIG. 1, 4, para [0036]-[0037], [0046]-[0062], [0119]-[0122]	1-20
Y	US 2005/0038818 A1 (HOOKS) 17 February 2005 (17.02.2005), Abstract, FIGs 2-4, 7; para [0044]-[0051], [0055]-[0061], [0068]-[0074], [0077], [0107]-[0109].	1-20

☐ Further documents are listed in the continuation of Box C.

* 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 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

18 May 2007 (18.05.2007)

Date of mailing of the international search report

20 SEP 2007

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774