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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 May 2005 (26.05.2005)

PCT

(10) International Publication Number
WO 2005/048022 A3

(51) International Patent Classification[7]: G06F 11/00, 11/22, 11/30, 11/32, 11/34, 11/36, 12/14, 12/16, 15/18, G08B 23/00

(21) International Application Number: PCT/US2004/033311

(22) International Filing Date: 8 October 2004 (08.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/701,653 5 November 2003 (05.11.2003) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WILEY, Kevin, L.** [US/US]; 518 Arbors Circle, Elgin, TX 78621 (US). **HALL, Michael, L.** [US/US]; 9822 Mandeville Circle, Austin, TX 78750 (US). **LATHEM, Gerald, S.** [US/US]; 508 Arbors Circle, Elgin, TX 78621 (US). **GLEICHAUF, Robert, E.** [US/US]; 326 Arcadia Place, San Antonio, TX 78209 (US).

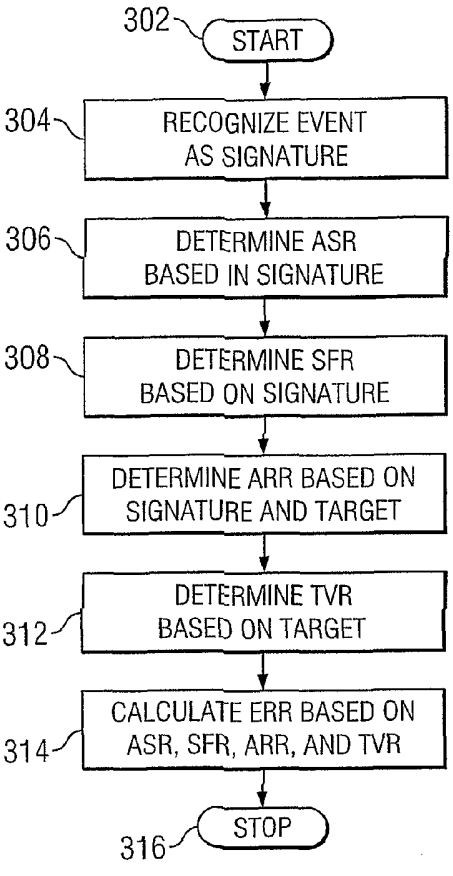
(74) Agent: **SHOWALTER, Barton, E.**; Baker Botts L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR ADDRESSING INTRUSION ATTACKS ON A COMPUTER SYSTEM



(57) Abstract: According to one embodiment of the invention, a computerized method for addressing intrusion detection attacks directed at a computer includes receiving a data stream corresponding to a potential attack on the computer [304] and calculating an event risk rating for the data stream [314]. Calculating the event risk rating includes determining at least one component of the risk rating. In one embodiment, the component risk ratings are: a signature fidelity rating indicative of the likelihood the potential attack will affect the computer in the absence of knowledge regarding the computer [308], an attack relevance rating indicative of the relevance of the potential attack to the computer [310], and a target value rating indicative of the perceived value of the computer [312]. The method also includes responding to the potential attack based on the calculated risk rating.

WO 2005/048022 A3

FR, GB, GR, HU, IE, IT, LU, 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).

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*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
27 April 2006

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/33311

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/00, 11/22, 11/30, 11/32, 11/34, 11/36, 12/14, 12/16, 15/18; G08B 23/00
US CL : 726/23
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)
U.S. : 726/23

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,T	US 6,895,383 B2 (HEINRICH) 17 May 2005 (17.05.2005), column 2, lines 41-59.	1-25
X	US 2003/0093514 A1 (VALDES et al.) 15 May 2003 (15.05.2003), paragraph [0006]-[0007].	1-25
A	US 2002/0147803 A1 (DODD et al.) 10 October 2002 (10.10.2002), paragraphs [0008]-[0011].	1-25

☐ 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 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
24 February 2006 (24.02.2006)

Date of mailing of the international search report
14 MAR 2006

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
Ayaz Sheikh
James R. Matthews
Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/33311

Continuation of B. FIELDS SEARCHED Item 3:
EAST, IEEE, ACM
search terms: intrusion detection system