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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2006 (20.07.2006)

PCT

(10) International Publication Number
WO 2006/076307 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/000715

(22) International Filing Date: 10 January 2006 (10.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/642,649 10 January 2005 (10.01.2005) US

(71) Applicant *(for all designated States except US)*: **REGENTS OF THE UNIVERSITY OF MINNESOTA** [US/US]; 450 Mcnamara Alumni Center, 200 Oak Street Southeast, Minneapolis, MN 55455 (US).

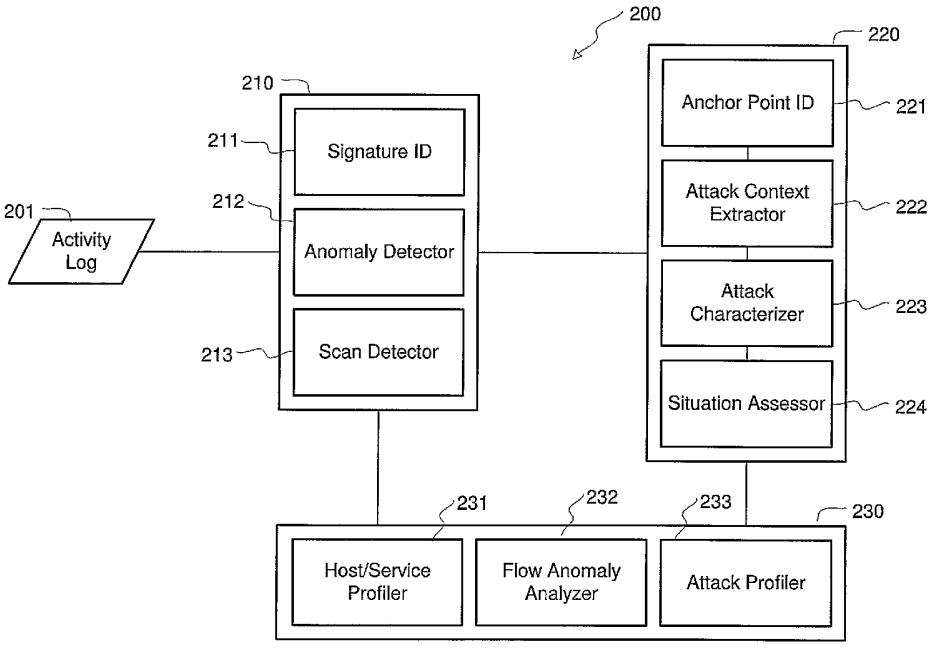
(71) Applicants and
(72) Inventors: **CHANDOLA, Varun** [IN/US]; 1900 Como Avenue Se, Minneapolis, MN 55414 (US). **EILERTSON, Eric** [US/US]; 3081 Avon Street N., Roseville, MN 55113 (US). **LIU, Haiyang** [CN/US]; 100 Old York Road, Apt. 1019, Jenkintown, Pennsylvania 19046 (US). **SHANECK, Mark** [US/US]; 1209 Gibbs Avenue, St. Paul, MN 55108 (US). **CHOI, Changho** [KR/US]; 1301 Gibbs Avenue, St. Paul, MN 55108 (US). **SIMON, Gyorgy** [HU/US]; 3506 Minikahda Court #21, St. Louis Park, MN 55416 (US). **KIM, Yongdae** [KR/US]; 5110 Holly Lane No. #1, Plymouth, MN 55446 (US). **KUMAR, Vipin** [IN/US]; 17430 45th Avenue North, Plymouth, MN 55446 (US). **SRIVASTAVA, Jaideep** [US/US]; 17805 45th Avenue North, Plymouth, MN 55446 (US). **ZHANG, Zhi-li** [CN/US]; 3009 Lake Shore Drive, Minneapolis, MN 55416 (US).

(74) Agents: **STEFFEY, Charles E.** et al.; Schwegman, Lundberg, Woessner & Kluth, PA, P.o. Box 2938, Minneapolis, MN 55402 (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,

[Continued on next page]

(54) Title: DETECTION OF MULTI-STEP COMPUTER PROCESSES SUCH AS NETWORK INTRUSIONS



(57) Abstract: Multi-step processes such as intrusions into computer networks are detected from individual activities or events such as communications by identifying anchor points (Fig 2, 220) that are likely to be part of the process, proceeding from the anchor points to extract other activitiesas a context of the anchor points, and characterizing the process from the activities in the context. The process may be characterized as sets of context activities.

WO 2006/076307 A3

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, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, 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).

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:
21 September 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/US06/00715

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00**(2006.01)

USPC: 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20020133721 A1 (Adjaoute) 19 September 2002 (19.09.2002), page 9, paragraphs 0119-0119.	1-23

☐ 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
29 May 2006 (29.05.2006)

Date of mailing of the international search report
14 JUL 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
Beemnet W Dada

Telephone No. (571) 272-3847

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