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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number
WO 2004/082195 A3

(51) International Patent Classification[7]: H04L 9/00, 9/32, G06F 11/30

(21) International Application Number: PCT/US2004/007347

(22) International Filing Date: 9 March 2004 (09.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/385,229 10 March 2003 (10.03.2003) US

(71) Applicant: **WORLDCOM, INC.** [US/US]; 1133 19th Street, N.W., Washington, 20036 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HOEFELMEYER, Ralph, Samuel** [US/US]; 17650 Woodhaven Drive, Colorado springs, CO 80908-1348 (US). **PHILLIPS, Theresa, Eileen** [US/US]; 12535 Sweet Leaf Terrace, Fairfax, Virginia 22033 (US). **WIERDERIN, Shawn, Edward** [US/US]; 508 Westridge Dr. S.W., Cedar Rapids, Iowa 52404 (US).

(74) Agent: **GROLZ, Edward, W.**; Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11530 (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, 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, 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)) for the following designations 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, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

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: 6 January 2005

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.

(54) Title: SECURE SELF-ORGANIZING AND SELF-PROVISIONING ANOMALOUS EVENT DETECTION SYSTEMS

(57) Abstract: An approach for providing managed security services is disclosed. A database, within a server or a pre-existing anomalous event detection system, stores a rule set specifiying a security policy for a network associated with a customer. An anomalous detection event module is deployed with a premise of the customer. The anomalous detection event module monitors a sub-network of the network based on the rule sets. The anomalous event detection module is further configured to self-organize by examining components of the network and to monitor for anomalous events according to the examined components, and to self-provision by selectively creating another instance of the anomalous detection event module to monitor another sub-network of the network.

WO 2004/082195 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/07347

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00, 9/32; G06F 11/30
US CL : 713/157, 201, 168
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. : 713/157, 201, 168

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 --- Y	US 5,557,742 A (SMAHA et al) 17 September 1996 (17.09.1996), column 4, lines 42-60, column 5 lines 1-67, column 8 lines 29-59, column 9 lines 1-48, column 11 lines 24-33.	1,3,5-10,12-14,16,18,20-23,25,27-29 --- 2,4,11,15,17,19,24,26
Y	US 6,158,010 A (MORICONI et al) 5 December 2000 (05.12.2000), column 4, lines 1-18.	2,15,17,24
Y	US 6,178,505 B1 (SCHNEIDER et al) 23 January 2001 (23.01.2001), column 8, lines 15-59, column 20, lines 1-50.	4,11,19,26

☐ 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
14 October 2004 (14.10.2004)

Date of mailing of the international search report
15 NOV 2004

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. (703) 305-3230

Authorized officer
Ayaz Sheikh
Telephone No. 703-305-9648

Form PCT/ISA/210 (second sheet) (January 2004)