

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/028121 A3

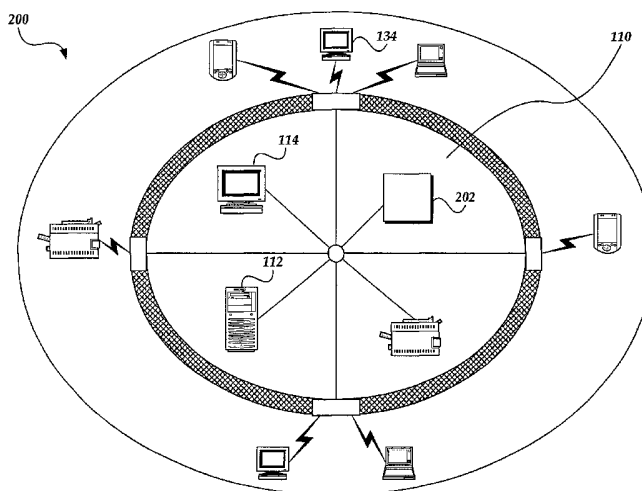
- (51) International Patent Classification⁷: H04L 9/00, 9/32, G06F 11/30, 12/14, 15/16
- (74) Agent: POWELL, Tracy, S.; Christensen O'Connor Johnson Kindness PLLC, 1420 Fifth Avenue, Suite 2800, Seattle, WA 98101 (US).
- (21) International Application Number: PCT/US2003/030839
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, 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, 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.
- (22) International Filing Date: 23 September 2003 (23.09.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 60/412,965 23 September 2002 (23.09.2002) US
- (84) Designated States (regional): ARIPO patent (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, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (for all designated States except US): WIMETRICS CORPORATION [US/US]; Meadowcreek Professional Center, 22525 SE 64th Place, Suite 241, Issaquah, WA 98027 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): ROSENBERGER, Joel [US/US]; 2438 278th Ct. SE, Fall City, WA 98024 (US).

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR WIRELESS LOCAL AREA NETWORK MONITORING AND INTRUSION DETECTION



(57) Abstract: The present invention provides a system and method for providing real-time wireless network (200) monitoring and intrusion detection (202). The present invention profiles wireless devices (134) and maintains a database of known/authorized wireless device profiles (134). Wireless devices (134) are analyzed to determine the threat level they pose to the network (110), and if the threat level exceeds a predetermined threshold, the invention refuses to bridge the network traffic from the wireless devices (134) to the wired network (110). The present invention provides reporting of the wireless activity, the known and unknown wireless devices (134), and the threat levels posed by the wireless devices (134). If an unknown wireless device is determined to be, or may be, a wireless access point, an alert is generated, such as notifying a system administrator to take appropriate action.

WO 2004/028121 A3



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

13 May 2004

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/US03/30839

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00, 9/32; G06F 11/30, 12/14, 15/16
 US CL : 380/270; 713/200, 201, 202; 709/223, 224; 370/912, 913

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. : 380/270; 713/200, 201, 202; 709/223, 224; 370/912, 913

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.
X,E	US 2003/0217289 A1 (AMMON et al) 20 November 2003, see Abstract, paragraphs 12,25,73,117,118, and 136	1-66
X,E	US 2003/0217283 A1 (HRASTAR et al) 20 November 2003, see paragraphs 19,48,139,158,159, and 163	1-66

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

27 February 2004 (27.02.2004)

Date of mailing of the international search report

11 MAR 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 *Michelle R. Revak*
 Christopher Revak
 Telephone No. 703-305-3900

INTERNATIONAL SEARCH REPORT

PCT/US03/30839

Continuation of B. FIELDS SEARCHED Item 3:

BRS (files: USPAT, DERWENT, EPO, JPO, IBM TDBs, USPGPUB)

search terms: intrusion, intruder, attack, attacked, attacker, attacking, hostile, detect, detected, detecting, detection, monitor, monitoring, monitored, audit, audited, auditing, analyze, analyzing, analyzed, analysis, unknown, unrecognized, unrecognize, device, location, component, pda, node, cellular, phone, laptop, wireless, portable, authorize, authorization, authorizing, authorized, authenticate, authentication, authenticated, authenticating, verify, verification, verifying, verified