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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 August 2003 (14.08.2003)

PCT

(10) International Publication Number
WO 03/067847 A2

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US03/02185

(22) International Filing Date: 24 January 2003 (24.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/066,140 1 February 2002 (01.02.2002) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor: **YADAV, Satyendra**; 9523 NW Maring Drive, Portland, OR 97229 (US).

(74) Agent: **HARRIS, Scott, C.**; Fish & Richardson, P.C., 4350 La Jolla Village Drive, Suite 500, San Diego, CA 92122 (US).

(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, 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, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(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, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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.

WO 03/067847 A2

(54) Title: INTEGRATED NETWORK INTRUSION DETECTION

(57) Abstract: Intrusion preludes may be detected (including detection using fabricated responses to blocked network requests), and particular sources of network communications may be singled out for greater scrutiny, by performing intrusion analysis on packets blocked by a firewall. An integrated intrusion detection system uses an end-node firewall that is dynamically controlled using invoked-application information and a network policy. The system may use various alert levels to trigger heightened monitoring states, alerts sent to a security operation center, and/or logging of network activity for later forensic analysis. The system may monitor network traffic to block traffic that violates the network policy, monitor blocked traffic to detect an intrusion prelude, and monitor traffic from a potential intruder when an intrusion prelude is detected. The system also may track behavior of applications using the network policy to identify abnormal application behavior, and monitor traffic from an abnormally behaving application to identify an intrusion.