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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2003 (04.12.2003)

PCT

(10) International Publication Number
WO 03/100617 A1

(51) International Patent Classification[7]: G06F 11/30

(21) International Application Number: PCT/US03/16119

(22) International Filing Date: 22 May 2003 (22.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/357,957 22 May 2002 (22.05.2002) US

(71) Applicant: LUCID SECURITY CORPORATION [US/US]; Lee Park Corporate Center, Suite 6100, 555 North Lane, Conshohocken, PA 19428 (US).

(72) Inventors: PHATAK, Vikram; 1438 Evans Road, Lower Gwynedd, PA 19002 (US). SCIPIONI, Robert; 3797 Mill Road, Collegeville, PA 19426 (US). SHAH, Paraji; Suite 6100, 555 North Lane, Conshohocken, PA 19428 (US).

(74) Agents: KLUGER, Joan, T. et al.; Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103 (US).

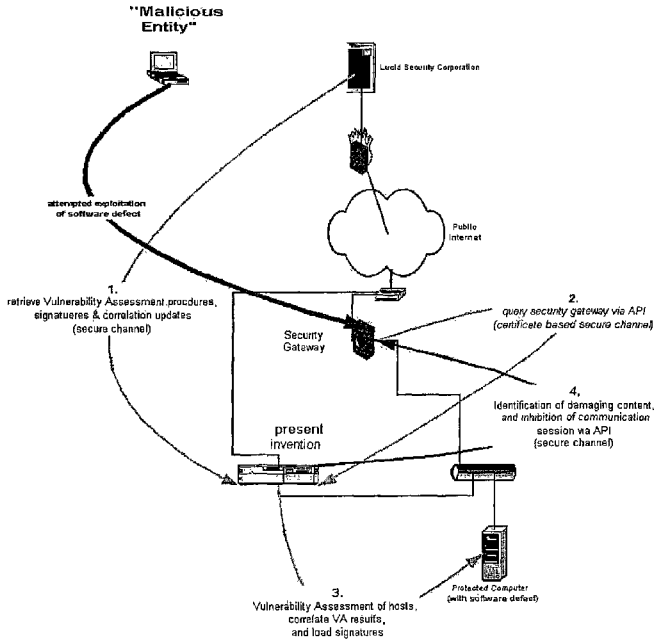
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, 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, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: ADAPTIVE INTRUSION DETECTION SYSTEM



(57) Abstract: An intrusion detection method wherein a vulnerability determination or vulnerability assessment (3) of one or more computers or hosts is performed to determine whether and what vulnerability exist on the computers or hosts, accomplished by using existing vulnerability determination or vulnerability assessment (3) information that can be continually updated (1). Attack signatures, which can also be continually adapted (1), are identified and correlated with the specific vulnerabilities identified. One or more designated IP sessions associated with attempted vulnerability exploitation are then inhibited (4) or disconnected.

WO 03/100617 A1

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.