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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 May 2008 (02.05.2008)

PCT

(10) International Publication Number
WO 2008/052135 A2

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2007/082562

(22) International Filing Date: 25 October 2007 (25.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/862,930 25 October 2006 (25.10.2006) US
11/923,513 24 October 2007 (24.10.2007) US

(71) Applicant *(for all designated States except US)*: **ARCSIGHT, INC.** [US/US]; 5 Results Way, Cupertino, CA 95014 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LAHOTI, Ankur** [IN/IN]; C/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US). **HUANG, Hui** [US/US]; C/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US). **BEEDGEN, Christian, F.** [DE/US]; C/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US).

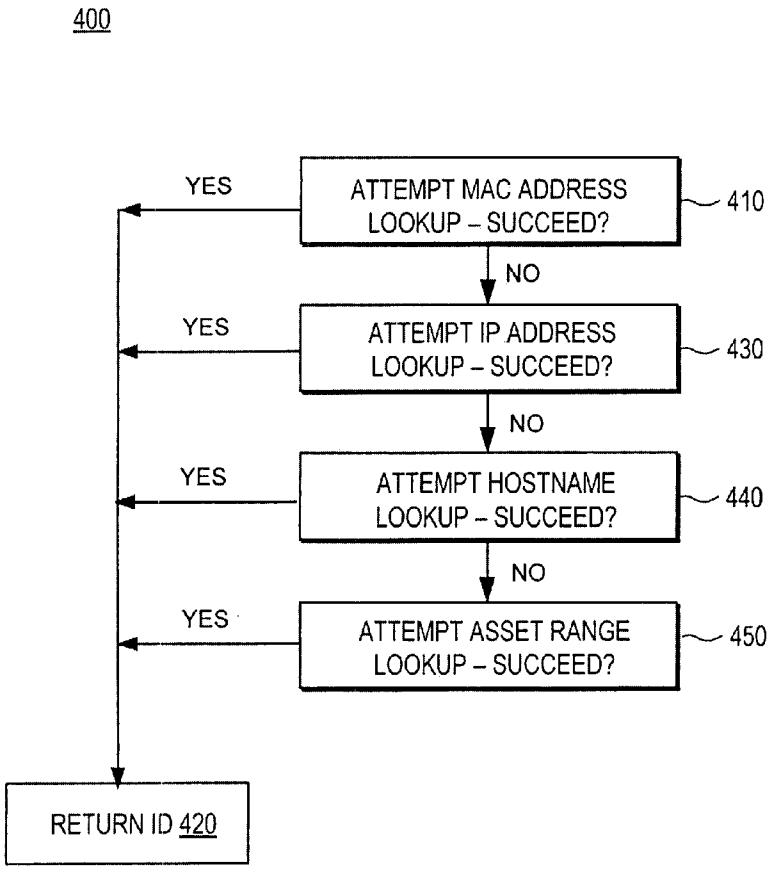
(74) Agents: **TRUESDALE, Sabra-Anne** et al.; Fenwick & West LLP, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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),

[Continued on next page]

(54) Title: REAL-TIME IDENTIFICATION OF AN ASSET MODEL AND CATEGORIZATION OF AN ASSET TO ASSIST IN COMPUTER NETWORK SECURITY



(57) Abstract: A unique identifier is assigned to a network node and is used to obtain an "asset model" corresponding to the node and to determine whether the node is a member of a particular category. An asset model is a set of information about a node (e.g., the node's role within the enterprise, software installed on the node, and known vulnerabilities/weaknesses of the node). An identifier lookup module determines a node's identifier based on characteristics of the node (such as IP address., host name, network zone, and/or MAC address), which are used as keys into lookup data structures. A category lookup module determines whether a particular node is a member of (i.e., within) a particular category using a transitive closure to model the categories (properties) that can be attached to an asset model. A transitive closure for a particular asset category is stored as a bitmap, similar to bitmap indexing.

WO 2008/052135 A2

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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:

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