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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 November 2005 (17.11.2005)

PCT

(10) International Publication Number
WO 2005/107424 A3

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 1/00* (2006.01)

(21) International Application Number:
PCT/US2005/015933

(22) International Filing Date: 4 May 2005 (04.05.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/839,613 4 May 2004 (04.05.2004) US

(71) Applicant *(for all designated States except US)*: **ARCSIGHT, INC.** [US/US]; 1309 S. Mary Avenue, Sunnyvale, California 94087 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SAURABH, Kumar** [IN/US]; 2016 Klamath Avenue, Apt. 1, Santa Clara, California 95051 (US). **TIDWELL, Kenny** [US/US]; 914 S. Springer Road, Los Altos, California 94924 (US).

(74) Agent: **FURST, Adam**; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 (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, KM, 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, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

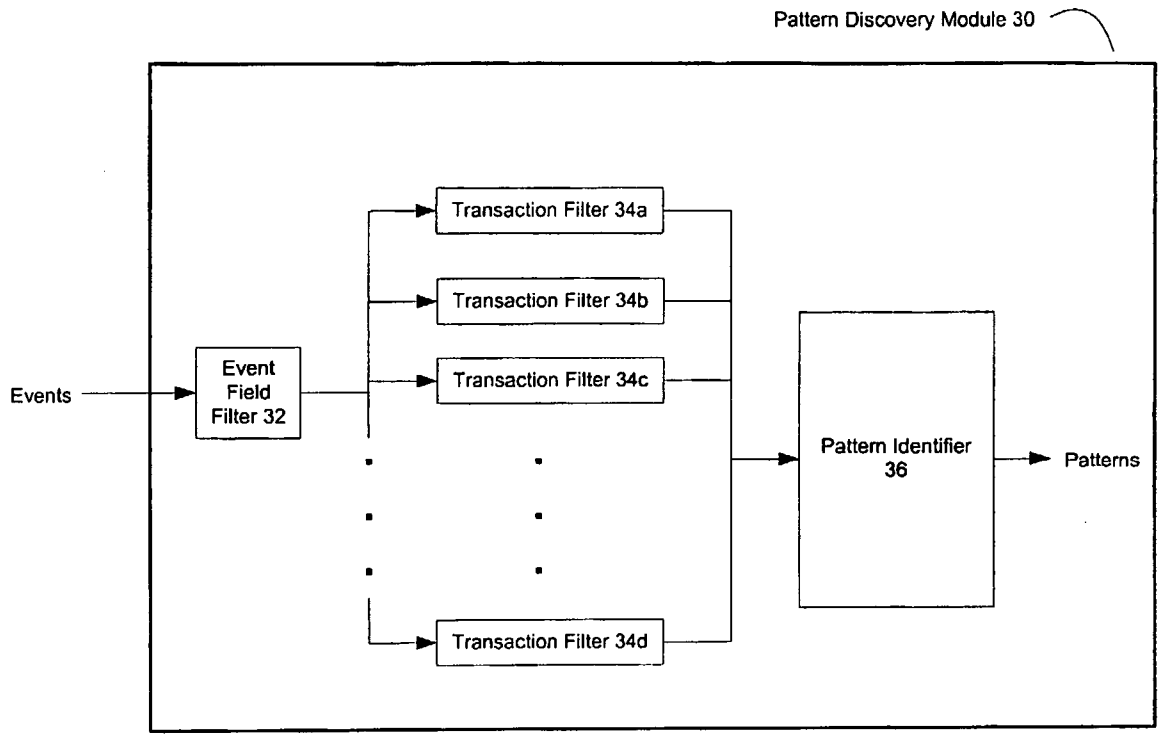
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, 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).

Published:
— *with international search report*

(88) Date of publication of the international search report:
2 March 2006

[Continued on next page]

(54) Title: PATTERN DISCOVERY IN A NETWORK SECURITY SYSTEM



(57) Abstract: Patterns can be discovered in security events collected by a network security system (10). In one embodiment, the present invention includes collecting and storing security events from a variety of monitor devices (12).In one embodiment , a subset of the stored security events is provided to a manager (14) as an event stream. In one embodiment, the present invention further includes the manager discovering one or more previously unknown event patterns in the event stream.

WO 2005/107424 A3

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.