

(19) World Intellectual Property Organization
International Bureau



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

PCT

(10) International Publication Number
WO 2008/052133 A2

(51) International Patent Classification:
G06F 17/30 (2006.01)

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

(21) International Application Number:
PCT/US2007/082560

(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.

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/862,932 25 October 2006 (25.10.2006) US
11/923,502 24 October 2007 (24.10.2007) US

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

(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, 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).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SINGLA, Anurag** [IN/US]; c/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US). **SAURABH, Kumar** [IN/US]; c/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US). **TIDWELL, Kenny, C.** [US/US]; c/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US).

Published:

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

(54) Title: TRACKING CHANGING STATE DATA TO ASSIST IN COMPUTER NETWORK SECURITY

	Key Field(s)		Timestamp Field(s)			Value Field(s)		
DHCP Schema	IP Address	Network Zone	Start Time	End Time	Creation Time	Host-name	MAC Address	
VPN Schema	IP Address	Network Zone	Start Time	End Time	Creation Time	Host-name	MAC Address	User
NAT Schema	IP Address	Network Zone	Start Time	End Time	Creation Time	Host-name	Actual IP Addr.	Source Port
Login Schema	IP Address	Network Zone	Start Time	End Time	Creation Time	Destin. User	Source User	Source Host.
Asset Ownership/Assignment Schema	MAC Address	Start Time	End Time	Creation Time	Person			

Legend

= Field

(57) Abstract: A session table includes one or more records, where each record represents a session. Session record information is stored in various fields, such as key fields, value fields, and timestamp fields. Session information is described as keys and values in order to support query/lookup operations. A session table is associated with a filter, which describes a set of keys that can be used for records in that table. A session table is populated using data contained in security information/events. Rules are created to identify events related to session information, extract the session information, and use the session information to modify a session table. A session table is partitioned so that the number of records in each session table partition is decreased. A session table is processed periodically so that active sessions are moved to the current partition.

WO 2008/052133 A2