PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06 | A1

(11) International Publication Number: WO 00/05852

(43) International Publication Date: 3 February 2000 (03.02.00)

(21) International Application Number: PCT/US99/12394

(22) International Filing Date: 20 July 1999 (20.07.99)

(30) Priority Data:
60/093,554 21 July 1998 (21.07.98) US

(71) Applicant: RAYTHEON COMPANY [US/US]; 141 Spring Street, Lexington, MA 02421 (US).

(72) Inventors: MALONEY, Michael, P.; 248 Poe Court, Severna Park, MD 21146 (US). SUIT, John, M.; 7873 Dero Drive, Pasadena, MD 21122 (US). SCOTT, Christopher, J.; 265 Steeplechase Drive, Pleasant Gap, PA 16823 (US). WOODUS, Francis, M.; 9733 Sherwood Farm Road, Owings Mill, MD 21117 (US). RUBEL, Rich; 205 Fox Ridge Court, Glen Burnie, MD 21061 (US). KAROLCHIK, Joseph; 890 The Old Station Court, Woodbine, MD 21797–8762 (US).

(74) Agents: MEIER, Harold, E. et al.; Baker & Botts, L.L.P., 2001 Ross Avenue, Dallas, TX 75201–2980 (US).

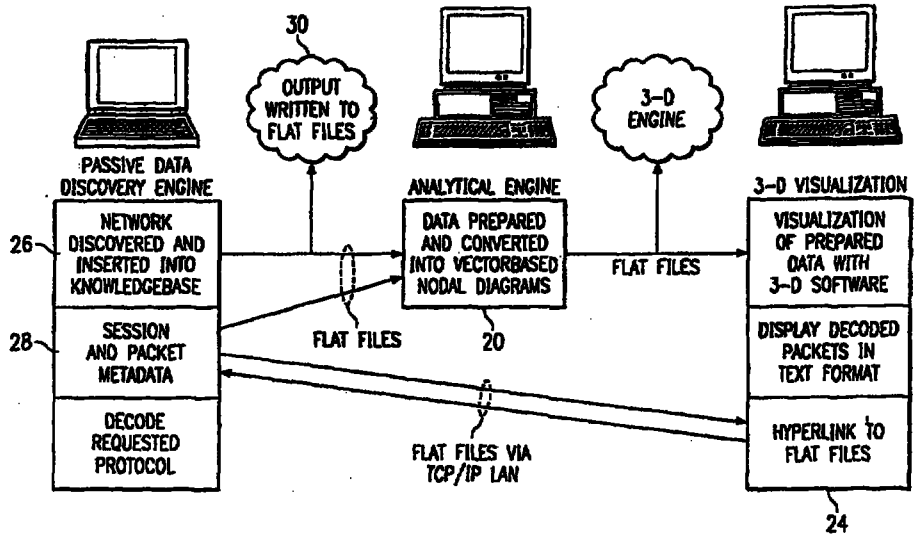
(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: INFORMATION SECURITY ANALYSIS SYSTEM



(57) Abstract

The analysis system is a collection, configuration and integration of software programs that reside on multiple interconnected computer platforms. The software, less computer operating systems, is a combination of sensor, analysis, data conversion, and visualization programs. The hardware platforms consist of several different types of interconnected computers, which share the software programs, data files, and visualization programs via a Local Area Network (LAN). This collection and integration of software and the migration to a single computer platform results in an approach to LAN/WAN monitoring in either a passive and/or active mode. The architecture permits digital data input from external sensors for analysis, display and correlation with data and displays derived from four major software concept groups. These are: Virus Computer Code Detection; Analysis of Computer Source and Executable Code; Dynamic Monitoring of Data Communication Networks; 3–D Visualization and Animation of Data.