Title (en)

SYSTEMS AND METHODS FOR PROCESSING DATA FLOWS

Title (de)

SYSTEME UND VERFAHREN ZUR VERARBEITUNG VON DATENFLÜSSEN

Title (fr)

SYSTEMES ET PROCEDES POUR TRAITER DES FLUX DE DONNEES

Publication

EP 1960867 A4 20101013 (EN)

Application

EP 06846609 A 20061213

Priority

- US 2006062053 W 20061213
- US 74991505 P 20051213
- US 75066405 P 20051214
- US 79588506 P 20060427
- US 79570806 P 20060427
- US 79588606 P 20060427
- US 79570706 P 20060427
- US 79571206 P 20060427

Abstract (en)

[origin: WO2007070838A2] A flow processing facility, which uses a set of artificial neurons for pattern recognition, such as a self-organizing map, in order to provide security and protection to a computer or computer system supports unified threat management based at least in part on patterns relevant to a variety of types of threats that relate to computer systems, including computer networks. Flow processing for switching, security, and other network applications, including a facility that processes a data flow to address patterns relevant to a variety of conditions are directed at internal network security, virtualization, and web connection security. A flow processing facility for inspecting payloads of network traffic packets detects security threats and intrusions across accessible layers of the IP-stack by applying content matching and behavioral anomaly detection techniques based on regular expression matching and self- organizing maps. Exposing threats and intrusions within packet payload at or near real-time rates enhances network security from both external and internal sources while ensuring security policy is rigorously applied to data and system resources. Intrusion Detection and Protection (IDP) is provided by a flow processing facility that processes a data flow to address patterns relevant to a variety of types of network and data integrity threats that relate to computer systems, including computer networks.

IPC 8 full level

H04L 29/06 (2006.01); **G06N 3/04** (2006.01)

CPC (source: EP)

G06F 21/55 (2013.01); **G06N 3/047** (2023.01); **H04L 63/1416** (2013.01); **H04L 63/1441** (2013.01); **H04L 63/1483** (2013.01); H04L 63/0227 (2013.01); H04L 2463/141 (2013.01)

Citation (search report)

- [A] HUFF J ET AL: "Hierarchical Kohonenen Net for Anomaly Detection in Network Security", IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS. PART B:CYBERNETICS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US LNKD- DOI:10.1109/TSMCB.2005.843274, vol. 35, no. 2, 1 April 2005 (2005-04-01), pages 302 - 312, XP011128464, ISSN: 1083-4419
- [A] LEI J Z ET AL: "Network intrusion detection using an improved competitive learning neural network", COMMUNICATION NETWORKS AND SERVICES RESEARCH, 2004. PROCEEDINGS. SECON D ANNUAL CONFERENCE ON FREEERICTON, NB, CANADA 19-21 MAY 2004, PISCATAWAY, NJ, USA,IEEE LNKD- DOI:10.1109/DNSR.2004.1344728, 19 May 2004 (2004-05-19), pages 190 - 197, XP010732731, ISBN: 978-0-7695-2096-4
- See references of WO 2007070838A2

Cited by

CN104967589A

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

WO 2007070838 A2 20070621; **WO 2007070838 A3 20080703**; EP 1960867 A2 20080827; EP 1960867 A4 20101013; EP 2432188 A1 20120321; EP 2432188 B1 20160420; EP 2442525 A1 20120418; IL 192117 A0 20081229; IL 192117 A 20130930

DOCDB simple family (application)

US 2006062053 W 20061213; EP 06846609 A 20061213; EP 11002731 A 20061213; EP 11007048 A 20061213; IL 19211708 A 20080612