EXHIBIT 7

US007975305B2

(12) **United States Patent**

Rubin et al.

(10) **Patent No.:**   **US 7,975,305 B2**

(45) **Date of Patent:**   **Jul. 5, 2011**

(54) **METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS**

(75) Inventors: **Moshe Rubin**, Jerusalem (IL); **Moshe Matitya**, Jerusalem (IL); **Artem Melnick**, Beit Shemesh (IL); **Shlomo Touboul**, Kefar-Haim (IL); **Alexander Yermakov**, Beit Shemesh (IL); **Amit Shaked**, Tel Aviv (IL)

(73) Assignee: **Finjan, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1016 days.

(21) Appl. No.: **11/009,437**

(22) Filed: **Dec. 9, 2004**

(65) **Prior Publication Data**

US 2005/0240999 A1   Oct. 27, 2005

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/930,884, filed on Aug. 30, 2004, which is a continuation-in-part of application No. 09/539,667, filed on Mar. 30, 2000, now Pat. No. 6,804,780, which is a continuation of application No. 08/964,388, filed on Nov. 6, 1997, now Pat. No. 6,092,194.

(51) **Int. Cl.**
G06F 11/00   (2006.01)
G06F 21/00   (2006.01)

(52) **U.S. Cl.** **726/25**; 726/22; 713/153

(58) **Field of Classification Search** .... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,077,677 A	12/1991	Murphy et al.	706/62
5,359,659 A	10/1994	Rosenthal	726/24
5,361,359 A	11/1994	Tajalli et al.	726/23
5,414,833 A *	5/1995	Hershey et al.	726/22
5,485,409 A	1/1996	Gupta et al.	726/25

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1091276	4/2001

(Continued)

OTHER PUBLICATIONS

D Grune, et al.—Parsing Techniques: A Practical Guide, 2000—John Wiley & Sons, Inc. New York, NY, USA, p. 1-326.*

(Continued)

*Primary Examiner* — Emmanuel L Moise
Assistant Examiner — Jeffery Williams
(74) *Attorney, Agent, or Firm* — Dawn-Marie Bey; King & Spalding LLP

(57)   **ABSTRACT**

A security system for scanning content within a computer, including a network interface, housed within a computer, for receiving content from the Internet on its destination to an Internet application running on the computer, a database of rules corresponding to computer exploits, stored within the computer, a rule-based content scanner that communicates with said database of rules, for scanning content to recognize the presence of potential exploits therewithin, a network traffic probe, operatively coupled to the network interface and to the rule-based content scanner, for selectively diverting content from its intended destination to the rule-based content scanner, and a rule update manager that communicates with said database of rules, for updating said database of rules periodically to incorporate new rules that are made available. A method and a computer readable storage medium are also described and claimed.

25 Claims, 14 Drawing Sheets
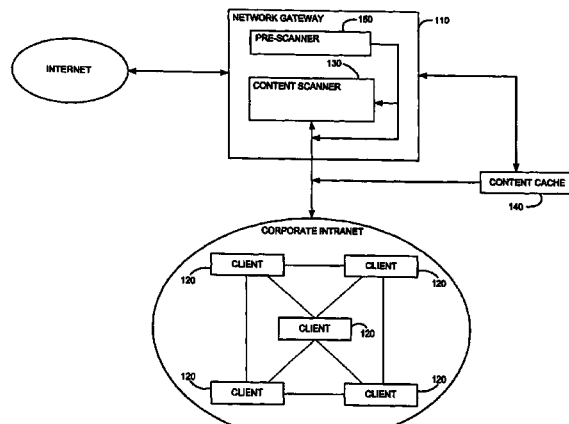
US 7,975,305 B2

Page 2

U.S. PATENT DOCUMENTS

5,485,575	A	1/1996	Chess et al.	714/38
5,572,643	A	11/1996	Judson	709/218
5,579,509	A	11/1996	Furtney et al.	703/27
5,606,668	A	2/1997	Shwed	726/13
5,623,600	A	4/1997	Ji et al.	726/24
5,638,446	A	6/1997	Rubin	705/51
5,675,711	A *	10/1997	Kephart et al.	706/12
5,692,047	A	11/1997	McManis	713/167
5,692,124	A	11/1997	Holden et al.	726/2
5,720,033	A	2/1998	Deo	726/2
5,724,425	A	3/1998	Chang et al.	705/52
5,740,248	A	4/1998	Fieres et al.	713/156
5,740,441	A *	4/1998	Yellin et al.	717/134
5,761,421	A	6/1998	van Hoff et al.	709/223
5,765,205	A	6/1998	Breslau et al.	711/203
5,784,459	A	7/1998	Devarakonda et al.	713/165
5,796,952	A	8/1998	Davis et al.	709/224
5,805,829	A	9/1998	Cohen et al.	709/202
5,832,208	A	11/1998	Chen et al.	726/24
5,832,274	A	11/1998	Cutler et al.	717/171
5,850,559	A	12/1998	Angelo et al.	713/320
5,859,966	A	1/1999	Hayman et al.	726/23
5,864,683	A	1/1999	Boebert et al.	709/249
5,881,151	A *	3/1999	Yamamoto	726/24
5,884,033	A *	3/1999	Duvall et al.	709/206
5,892,904	A	4/1999	Atkinson et al.	726/22
5,951,698	A	9/1999	Chen et al.	714/38
5,956,481	A	9/1999	Walsh et al.	726/23
5,963,742	A *	10/1999	Williams	717/143
5,974,549	A	10/1999	Golan	726/23
5,978,484	A	11/1999	Apperson et al.	705/54
5,983,348	A *	11/1999	Ji	726/13
5,987,611	A *	11/1999	Freund	726/4
6,088,801	A *	7/2000	Grecsek	726/1
6,088,803	A *	7/2000	Tso et al.	726/22
6,092,194	A	7/2000	Touboul	726/24
6,154,844	A	11/2000	Touboul et al.	726/24
6,167,520	A	12/2000	Touboul	726/23
6,339,829	B1	1/2002	Beadle et al.	726/15
6,425,058	B1	7/2002	Arimilli et al.	711/134
6,434,668	B1	8/2002	Arimilli et al.	711/128
6,434,669	B1	8/2002	Arimilli et al.	711/128
6,480,962	B1	11/2002	Touboul	726/22
6,487,666	B1	11/2002	Shanklin et al.	726/23
6,519,679	B2	2/2003	Devireddy et al.	711/114
6,598,033	B2 *	7/2003	Ross et al.	706/46
6,732,179	B1	5/2004	Brown et al.	709/229
6,804,780	B1	10/2004	Touboul	713/181
6,917,953	B2	7/2005	Simon et al.	707/204
7,058,822	B2	6/2006	Edery et al.	726/22
7,143,444	B2	11/2006	Porras et al.	726/30
7,210,041	B1 *	4/2007	Gryaznov et al.	713/188
7,308,648	B1	12/2007	Buchthal et al.	715/234
7,343,604	B2	3/2008	Grabarnik et al.	719/313
7,418,731	B2	8/2008	Touboul	726/22
2002/0059157	A1*	5/2002	Spooner et al.	706/45
2002/0066024	A1*	5/2002	Schmall et al.	713/200
2002/0073330	A1*	6/2002	Chandnani et al.	713/200
2003/0014662	A1	1/2003	Gupta et al.	726/23
2003/0101358	A1	5/2003	Porras et al.	726/4
2004/0073811	A1*	4/2004	Sanin	713/201
2004/0088425	A1*	5/2004	Rubinstein et al.	709/230
2005/0050338	A1	3/2005	Liang et al.	713/188
2005/0172338	A1	8/2005	Sandu et al.	726/22
2006/0031207	A1	2/2006	Bjarnestam et al.	707/3
2006/0048224	A1	3/2006	Duncan et al.	726/22
2008/0066160	A1	3/2008	Becker et al.	726/4
2010/0195909	A1*	8/2010	Wasson et al.	382/176

FOREIGN PATENT DOCUMENTS

EP	1132796	9/2001

OTHER PUBLICATIONS

International Search Report for Application No. PCT/IL05/00915, 4

Seventh IEEE Symposium on Reliable Distributed Systems, pp. 1-6, Oct. 1998.

Rubin, et al., "Mobile Code Security," *IEEE Internet*, pp. 30-34, Dec. 1998.

Schmid, et al. "Protecting Data From Malicious Software," *Proceeding of the 18th Annual Computer Security Applications Conference*, pp. 1-10, 2002.

Corradi, et al., "A Flexible Access Control Service for Java Mobile Code," *IEEE*, pp. 356-365, 2000.

International Search Report for Application No. PCT/IB97/01626, 3 pp., May 14, 1998 (mailing date).

Written Opinion for Application No. PCT/IL05/00915, 5 pp., dated Mar. 3, 2006 (mailing date).

International Search Report for Application No. PCT/IB01/01138, 4 pp., Sep. 20, 2002 (mailing date).

International Preliminary Examination Report for Application No. PCT/IB01/01138, 2 pp., dated Dec. 19, 2002.

Gerzic, Amer, "Write Your Own Regular Expression Parser," Nov. 17, 2003, 18 pp., Retrieved from the Internet: http://www.codeguru. com/Cpp/Cpp/cpp_mfc/parsing/article.php/c4093/.

Power, James, "Lexical Analysis," 4 pp., May 14, 2006, Retrieved from the Internet: http://www.cs.may.ie/~jpower/Courses/compilers/notes/lexical.pdf.

Sitaker, Kragen, "Rapid Genetic Evolution of Regular Expressions" [online], *The Mial Archive*, Apr. 24, 2004 (retrieved on Dec. 7, 2004), 5 pp., Retrieved from the Internet: http://www.mail-archive.com/kragen-tol@canonical.org/msg00097.html.

"Lexical Analysis: DFA Minimization & Wrap Up" [online], Fall, 2004 [retrieved on Mar. 2, 2005], 8 pp., Retrieved from the Internet: http://www.owlnet.rice.edu/~comp412/Lectures/L06LexWrapup4. pdf.

"Minimization of DFA" [online], [retrieved on Dec. 7, 2004], 7 pp., Retrieved from the Internet: http://www.cs.odu.edu/~toida/nerzic/390teched/regular/fa/min-fa.html.

"Algorithm: NFS -> DFA" [online], Copyright 1999-2001 [retrieved on Dec. 7, 2004], 4 pp., Retrieved from the Internet: http://rw4.cs. uni-sb.de/~ganimal/GANIFA/page16_e.htm.

"CS 3813: Introduction to Formal Languages and Automata—State Minimization and Other Algorithms for Finite Automata," 3 pp., May 11, 2003, Retrieved from the Internet: http://www.cs.msstate.edu/~hansen/classes/3813fall01/slides/06Minimize.pdf.

Watson, Bruce W., "Constructing Minimal Acyclic Deterministic Finite Automata," [retrieved on Mar. 20, 2005], 38 pp., Retrieved from the Internet: http://www.win.tue.nl/~watson/2R870/downloads/madfa_algs.pdf.

Chang, Chia-Hsiang, "From Regular Expressions to DFA's Using Compressed NFA's," Oct. 1992, 243 pp., http://www.cs.nyu.edu/web/Research/Theses/chang_chia-hsiang.pdf.

"Products," Articles published on the Internet, "Revolutionary Security for a New Computing Paradigm" regarding SurfinGate™, 7 pp.

"Release Notes for the Microsoft ActiveX Development Kit," Aug. 13, 1996, activex.adsp.or.jp/inetsdk/readme.txt, pp. 1-10.

Doyle, et al., "Microsoft Press Computer Dictionary," Microsoft Press, 2d Edition, pp. 137-138, 1993.

Finjan Software Ltd., "Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™," Article published on the Internet by Finjan Software Ltd., 2 pp. 1996.

Finjan Sofrtware Ltd., "Finjan Announces a Personal Java™ Firewall for Web Browsers—the SurfinShield™ 1.6 (formerly known s SurfinBoard)," Press Release of Finjan Releases SurfinShield 1.6, 2 pp., Oct. 21, 1996.

Finjan Software Ltd., "Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0," Las Vegas Convention Center/Pavillion 5 P5551, 3 pp., Nov. 18, 1996.

Finjan Software Ltd., "Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product for the World Wide Web," Article published on the Internet by Finjan Software Ltd., 1 p., Jul. 29, 1996.

Finjan Software Ltd., "Java Security: Issues & Solutions," Article published on the Internet by Finjan Software Ltd., 8 pp. 1996.

Finjan Software Ltd., Company Profile, "Finjan—Safe Surfing, The

"IBM AntiVirus User's Guide, Version 2.4,", International Business Machines Corporation, pp. 6-7, Nov. 15, 1995.

Khare, R., "Microsoft Authenticode Analyzed" [online], Jul. 22, 1996 [retrieved on Jun. 25, 2003], 2 pp., Retrieved from the Internet: http://www.xent.com/FoRK-archive/smmer96/0338.html.

LaDue, M., Online Business Consultant: Java Security: Whose Business is It?, Article published on the Internet, Home Page Press, Inc., 4 pp., 1996.

Leach, Norvin, et al., "IE 3.0 Applets Will Earn Certification," *PC Week*, vol. 13, No. 29, 2 pp., Jul. 22, 1996.

Moritz, R., "Why We Shouldn't Fear Java," *Java Report*, pp. 51-56, Feb. 1997.

Microsoft, "Microsoft ActiveX Software Development Kit" [online], Aug. 12, 1996 [retrieved on Jun. 25, 2003], pp. 1-6, Retrieved from the Internet: activex.adsp.or.jp/inetsdk/help/overview.htm.

Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet," Microsoft Corporation, Oct. 1996, including Abstract, Contents, Introduction, and pp. 1-10.

Microsoft Corporation, Web Page Article "Frequently Asked Questions About Authenticode," last updated Feb. 17, 1997, printed Dec. 23, 1998, URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9, pp. 1-13.

Okamoto, E., et al., "ID-Based Authentication System for Computer Virus Detection," *IEEE/IEE Electronic Library online, Electronics Letters*, vol. 26, Issue 15, ISSN 0013-5194, Jul. 19, 1990, Abstract and pp. 1169-1170, URL: http://iel.ihs.com:80/cgi-bin/iel_cgi?se...2ehts%26ViewTemplate%3ddocview%5fb%2ehts.

Omura, J. K., "Novel Applications of Cryptography in Digital Communications," *IEEE Communications Magazine*, pp. 21-29, May 1990.

Schmitt, D.A., ".EXE files, OS-2 style," *PC Tech Journal*, vol. 6, No. 11, p. 76(13), Nov. 1988.

Zhang, X. N., "Secure Code Distribution," *IEEE/IEE Electronic Library online, Computer*, vol. 30, Issue 6, pp. 76-79, Jun. 1997.

Power, James, "Notes on Formal Language Theory and Parsing," National University of Ireland, pp. 1-40, 1999.
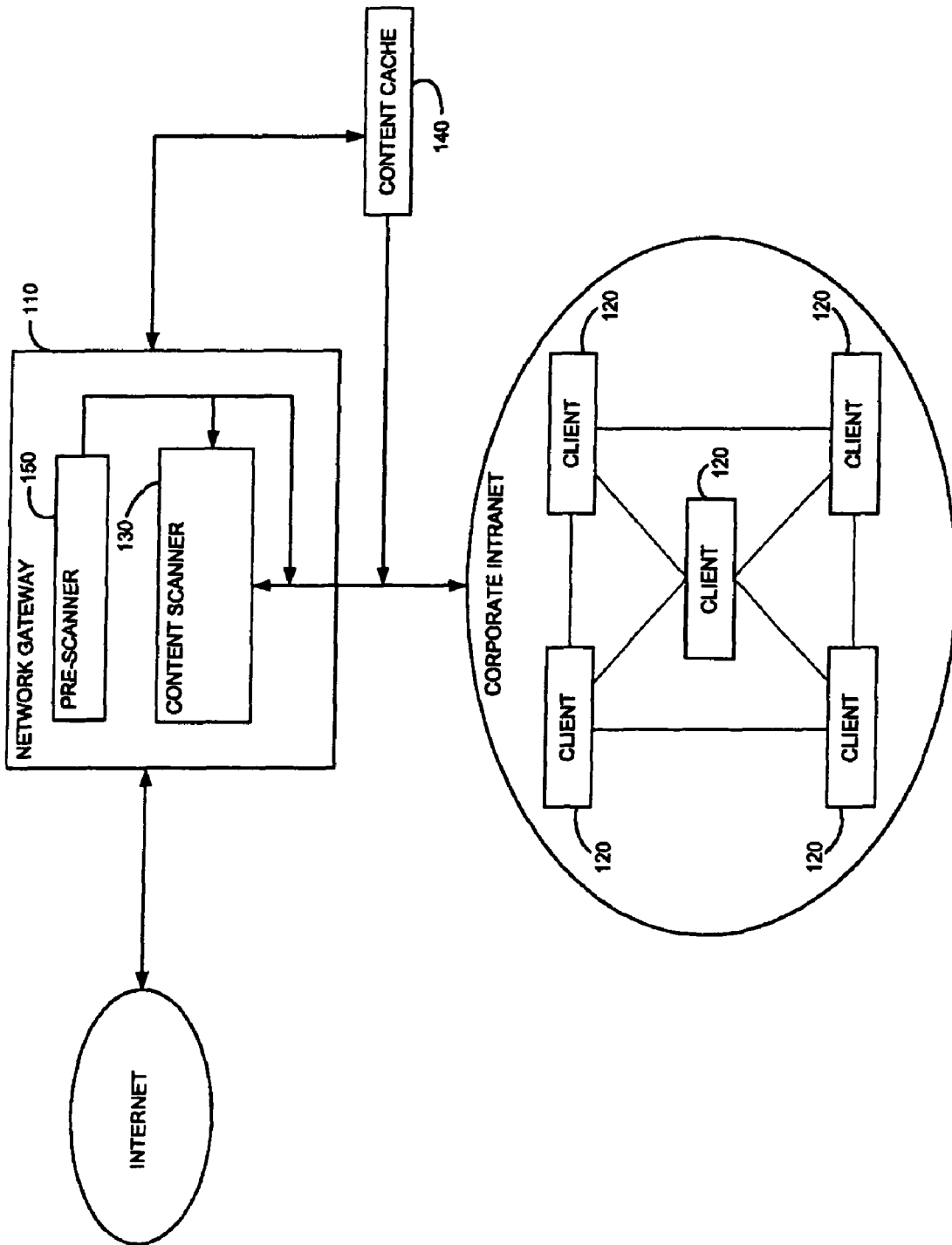
* cited by examiner

FIG. 1

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.