US005696822A

United States Patent [19]

Nachenberg

[11] Patent Number: 5,696,822

[45] Date of Patent: Dec. 9, 1997

[54] **POLYMORPHIC VIRUS DETECTION MODULE**

[75] Inventor: **Carey Nachenberg**, Northridge, Calif.

[73] Assignee: **Symantec Corporation**, Cupertino, Calif.

[21] Appl. No.: **535,340**

[22] Filed: **Sep. 28, 1995**

[51] **Int. Cl.**[6] **H04L 9/00**; G06F 3/00; H04K 3/00

[52] **U.S. Cl.** **380/4**; 364/709.05; 380/1; 380/25; 395/183.01; 395/183.09; 395/183.14

[58] **Field of Search** 380/49, 4, 25; 395/183.01, 183.09, 183.14; 364/709.05

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,975,950	12/1990	Lentz	380/4
5,121,345	6/1992	Lentz	364/550
5,144,660	9/1992	Rose	380/4
5,319,776	6/1994	Hile et al.	395/575
5,321,840	6/1994	Ahlin et al.	395/700
5,349,655	9/1994	Mann	395/575
5,359,659	10/1994	Rosenthal	380/4
5,398,196	3/1995	Chambers .	
5,408,642	4/1995	Mann	395/575
5,421,006	5/1995	Jablon et al.	395/575
5,440,723	8/1995	Arnold et al.	395/181
5,442,699	8/1995	Arnold et al.	380/4
5,485,575	1/1996	Chess et al.	395/183.14

FOREIGN PATENT DOCUMENTS

0636977 A2	2/1995	European Pat. Off.	G06F 11/00

OTHER PUBLICATIONS

Digitext, "Dr. Solomon's Anti-Virus Toolkit for Windows and DOS", *S&S International PLC*, Jan. 1995, pp. 1–15, 47–65, 75–77, 91–95 113–115, and 123–142, United Kingdom.

Veldman, Frans, "Virus Writing Is High-Tech Infosecurity Warfare", *Security on the I-Way '95*, 1995, pp. L-1—L-16, U.S.A.

Symantec Corporation, "Norton AntiVirus for Windows 95 & Special Subscription Offer", 1995, U.S.A.

(List continued on next page.)

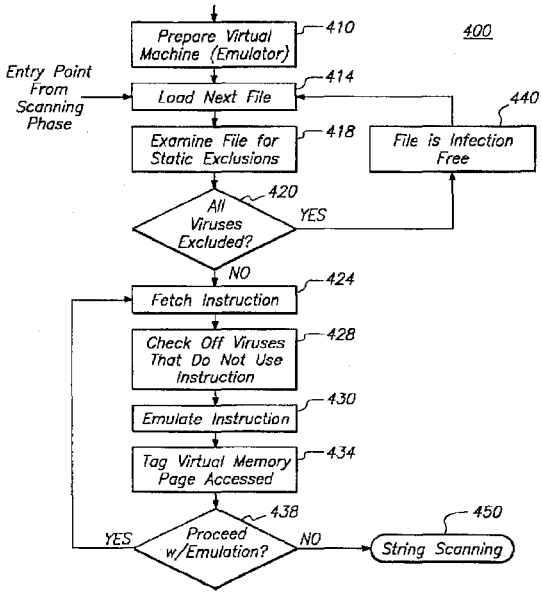
Primary Examiner—Stephen C. Buczinski

Attorney, Agent, or Firm—Fenwick & West LLP

[57] **ABSTRACT**

A Polymorphic Anti-Virus Module (PAM) (**200**) comprises a CPU emulator (**210**) for emulating the target program, a virus signature scanning module (**250**) for scanning decrypted virus code, and an emulation control module (**220**), including a static exclusion module (**230**), a dynamic exclusion module (**240**), instruction/interrupt usage profiles (**224**) for the mutation engines (**162**) of the known polymorphic viruses (**150**), size and target file types (**226**) for these viruses, and a table (**228**) having an entry for each known polymorphic virus (**150**). Prior to emulation, the static exclusion module (**230**) examines the gross characteristics of the target file for attributes that are inconsistent with the size/type data (**226**), and excludes polymorphic viruses (**150**) from the list (**228**) accordingly. During emulation, the dynamic exclusion module (**240**) compares fetched instructions with the instruction/interrupt usage profiles (**224**) to determine when emulation has proceeded to a point where at least some code from the decrypted static virus body (**160**) may be scanned for virus signatures.

18 Claims, 4 Drawing Sheets



OTHER PUBLICATIONS

ThunderBYTE B.V., "User Manual", 1995, pp. i—191, Wijchen, The Netherlands.
"Virus Infection Techniques: Part 3", *Virus Bulletin,* 1995, pp. 006–007, Oxfordshire, England.
Cohen, Frederick B., "A Short Course on Computer Virus—2d Ed.", *John Wiley & Sons, Inc.,,* pp. 54–55, 199–209, 1994, U.S.A.
Veldman, Frans, "Heuristic Anti–Virus Technology", *Proceedings of the International Virus Protection and Information Security Council,* Apr. 1, 1994.
Wells, Joseph, "Viruses in the Wild", *Proceedings of the International Virus Protection and Information Security Council,* Apr. 1, 1994.
Gordon, Scott, "Viruses & Netware", *Proceedings of the International Virus Protection and Information Security Coucil,* Mar. 31, 1994.
Solomon, Alan, "Viruses & Polymorphism", *Proceedings of the International Virus Protection and Information Security Council,* Mar. 31, 1994.
Case, Tori, "Viruses: An Executive Brief", *Proceedings of the International Virus Protection and Information Security Council,* Mar. 31, 1994.
Skulason, Fridrik, "For Programmers", *Virus Bulletin,* Jul. 1990, pp. 10–11, Oxon, England.
"Automated Program Analysis for Computer Virus Detection", *IBM Technical Disclosure Bulletin,* vol. 34, No. 2, Jul. 1991, pp. 415–416.
"Artificial Immunity for Personal Computers", *IBM Technical Disclosure Bulletin,* vol. 34, No. 2, Jul. 1991, pp. 150–154.
Marshall, G., "Pest Control", *LAN Magazine,* Jun. 1995, pp. 54–67.
Gotlieb, L., "End Users and Responsible Computing", *CMA—the Management Accounting Magazine,* vol. 67, No. 7, Sep. 1993, pp. 13.
Karney, J., "Changing the Rules on Viruses", *PC Magazine,* vol. 13, No. 14, Aug. 1994, pp. NE36.
Schnaidt, P., "Security", *LAN Magazine,* vol. 7, No. 3, Mar. 1992, pp. 19.
"UK–Sophos Intros Unix Virus Detection Software Jan. 26, 1995", *Newsbytes News Network,* Jan. 26, 1995.
"Anti–Virus Company Claims Polymorphic Breakthrough Jul. 10, 1992", *Newsbytes News Network,* Jul. 10, 1992.
"LAN Buyers Guide: Network Management", *LAN Magazine,* vol. 7, No. 8, Aug. 1992, pp. 188.

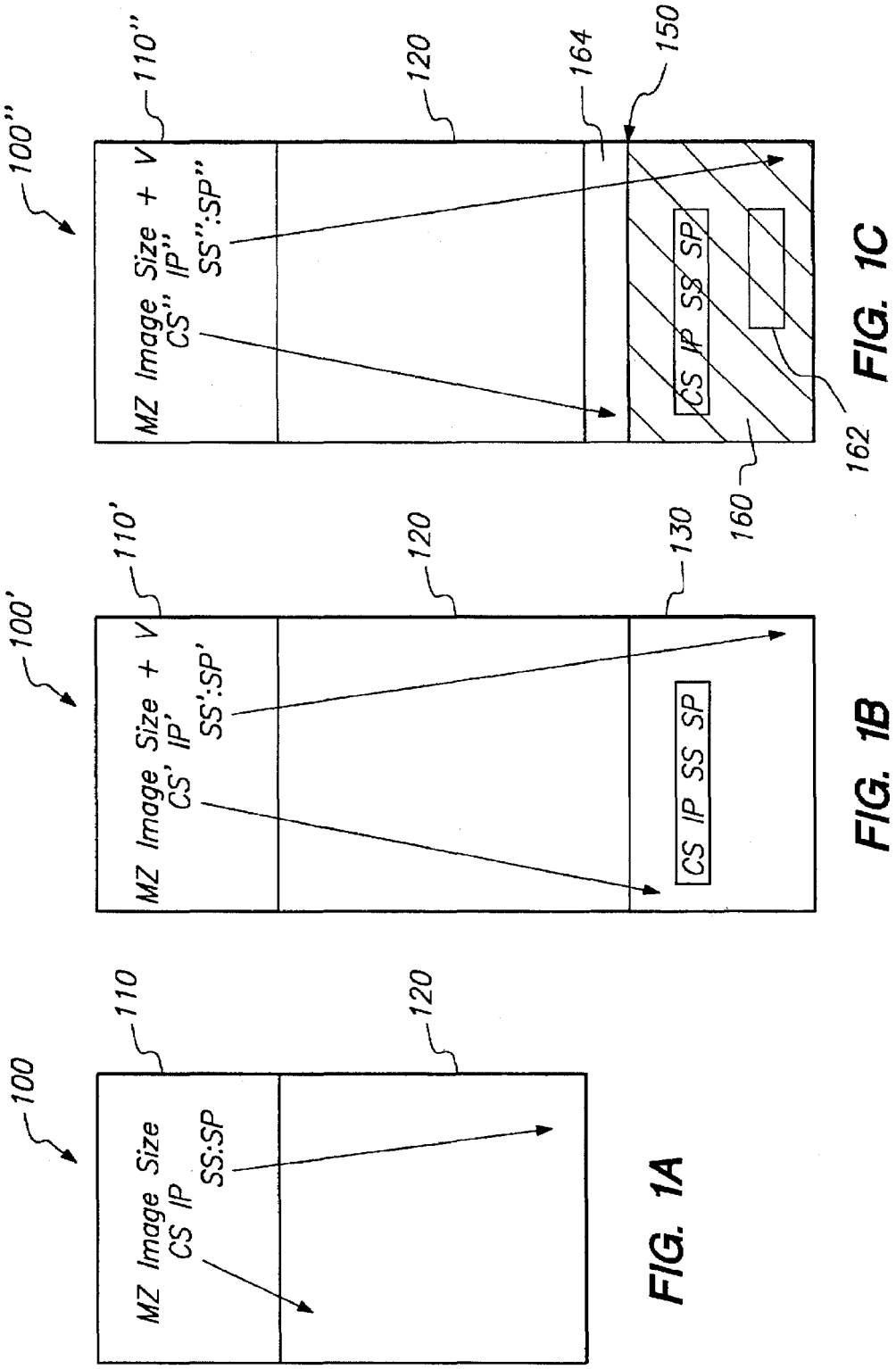


FIG. 1C

FIG. 1B

FIG. 1A

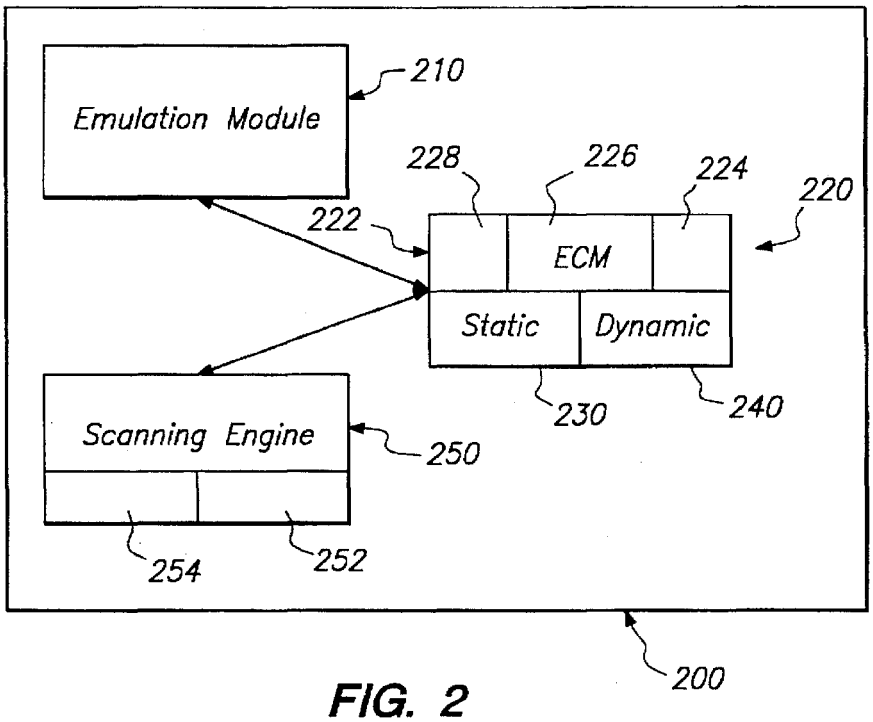


FIG. 2

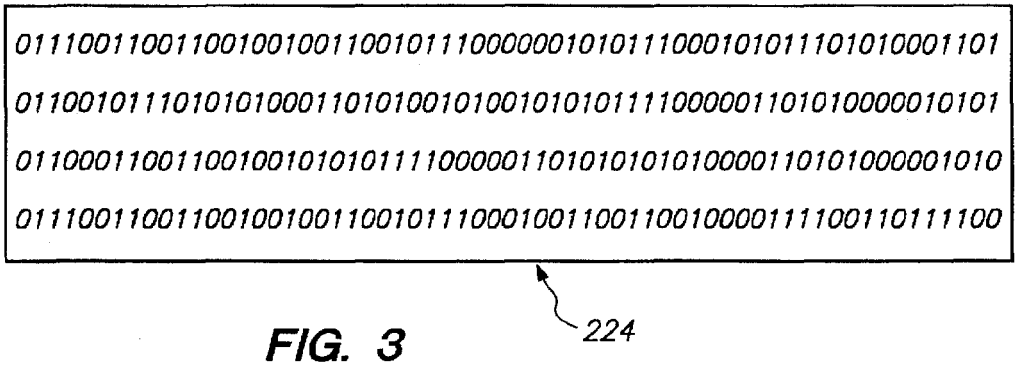


FIG. 3

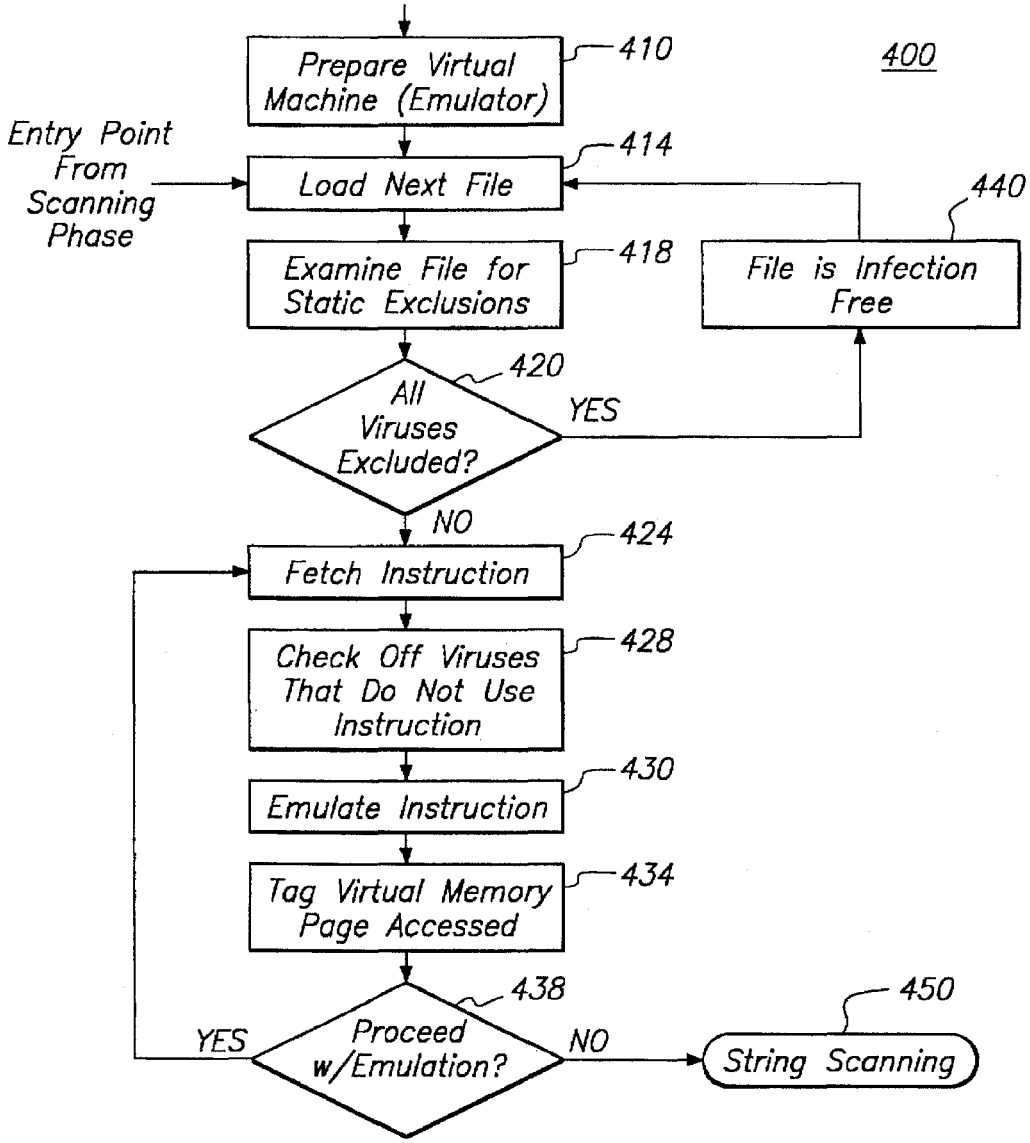


FIG. 4A

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.