US005440723A

United States Patent [19]

Arnold et al.

[11] **Patent Number: 5,440,723**

[45] **Date of Patent: Aug. 8, 1995**

[54] **AUTOMATIC IMMUNE SYSTEM FOR COMPUTERS AND COMPUTER NETWORKS**

[75] Inventors: **William C. Arnold**, Mahopac; **David M. Chess**, Mohegan Lake; **Jeffrey O. Kephart**, Yorktown Heights; **Steven R. White**, New York, all of N.Y.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **4,872**

[22] Filed: **Jan. 19, 1993**

[51] **Int. Cl.**[6] **G06F 11/00**

[52] **U.S. Cl.** **395/181;** 395/700; 395/183.09; 395/183.14

[58] **Field of Search** 395/575; 371/16.5, 19, 371/11.2, 8.2

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,062,045	10/1991	Janis et al.	371/16.5
5,084,816	1/1992	Boese et al.	395/575
5,121,345	1/1992	Lentz	364/550
5,200,958	4/1993	Hamilton et al.	371/16.5
5,218,605	1/1993	Low et al.	371/19
5,255,208	10/1993	Thakore et al.	371/16.5
5,278,901	1/1994	Shieh et al.	380/4
5,291,590	3/1994	Ohnishi et al.	371/16.5
5,297,150	3/1994	Clark	371/19
5,319,776	6/1994	Hile et al.	395/575
5,359,659	10/1994	Rosenthal	380/4
5,361,359	11/1994	Tajallie et al.	395/700

OTHER PUBLICATIONS

Qasem et al. "AI Trends in Virus Control" 1991 IEEE Proc. of Southeaston pp. 99–103 vol. 1.

Crocker et al. "A Proposal for a Verification-Based Virus Filler" 1989 IEEE Symposium on Security & Privacy pp. 319–324.

Kephort et al. "Directed Graph Epidemiological Module of Computer Viruses" 1991 IEEE Computer Society Symposium on Research in Security & Privacy pp. 343–359.

Kumor et al. "A Generic Virus Scanner in C++" 1992 8th Ann. Computer Security Applications Proceedings pp. 210–219.

Shoutkov et al. "Computer Viruses: Ways of Reproduction in MS DOS" 25th Ann. 1991 IEEE International Carnahan Conf. on Security Tech. pp. 168–176.

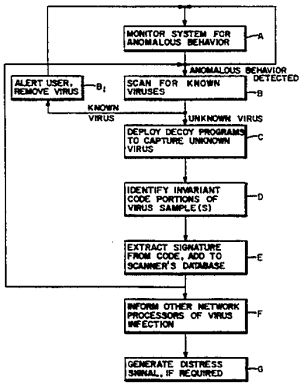
(List continued on next page.)

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Joseph E. Palys
Attorney, Agent, or Firm—Perman & Green

[57] **ABSTRACT**

A method includes the following component steps, or some functional subset of these steps: (A) periodic monitoring of a data processing system (**10**) for anomalous behavior that may indicate the presence of an undesirable software entity such as a computer virus, worm, or Trojan Horse; (B) automatic scanning for occurrences of known types of undesirable software entities and taking remedial action if they are discovered; (C) deploying decoy programs to capture samples of unknown types of computer viruses; (D) identifying machine code portions of the captured samples which are unlikely to vary from one instance of the virus to another; (E) extracting an identifying signature from the executable code portion and adding the signature to a signature database; (F) informing neighboring data processing systems on a network of an occurrence of the undesirable software entity; and (G) generating a distress signal, if appropriate, so as to call upon an expert to resolve difficult cases. A feature of this invention is the automatic execution of the foregoing steps in response to a detection of an undesired software entity, such as a virus or a worm, within a data processing system. The automatic extraction of the identifying signature, the addition of the signature to a signature data base, and the immediate use of the signature by a scanner provides protection from subsequent infections of the system, and also a network of systems, by the same or an altered form of the undesirable software entity.

46 Claims, 7 Drawing Sheets



OTHER PUBLICATIONS

S. W. Shieh et al. "A Pattern-Oriented Intrusion-Detection Model and its Applications", Proceedings of the 1991 IEEE Computer Society Symposium on Reserach and Privacy, pp. 327-342.

H. S. Javitz et al. "The SRI IDES Statistical Anomaly Detector", Proceedings of the 1991 IEEE Computer Symposium on Research in Security and Privacy, pp. 316-326.

W. Arnold et al. "System for Detecting Undesired Alteration of Software", IBM TDB, vol. 32, No. 11, Apr. 1990, pp. 48-50.

S. M. Katz, "Estimation of Probabilities from Sparse Data for the Language Model Component of a Speech Recognizer", IEEE Trans. ASSP-35, No. 3, Mar. 1987, pp. 400-401.

F. Cohen, A Short Course on Computer Viruses, ASP Press, Pittsburg, 1990, pp. 9-15.

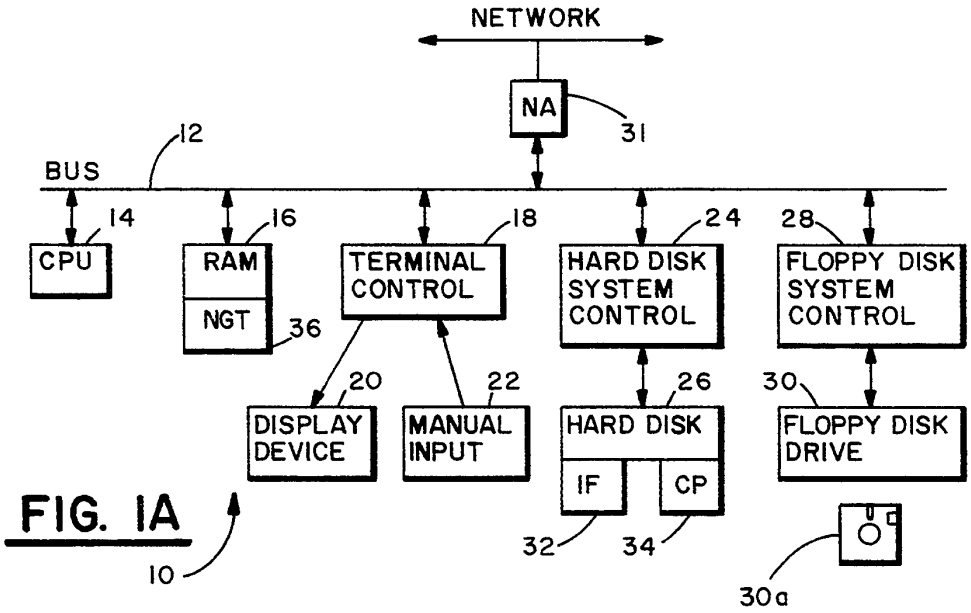


FIG. 1A

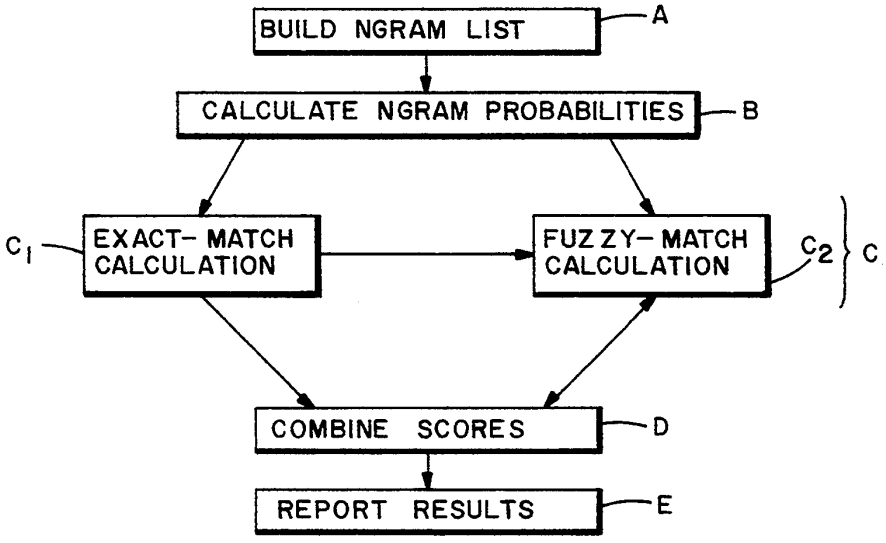


FIG. 5

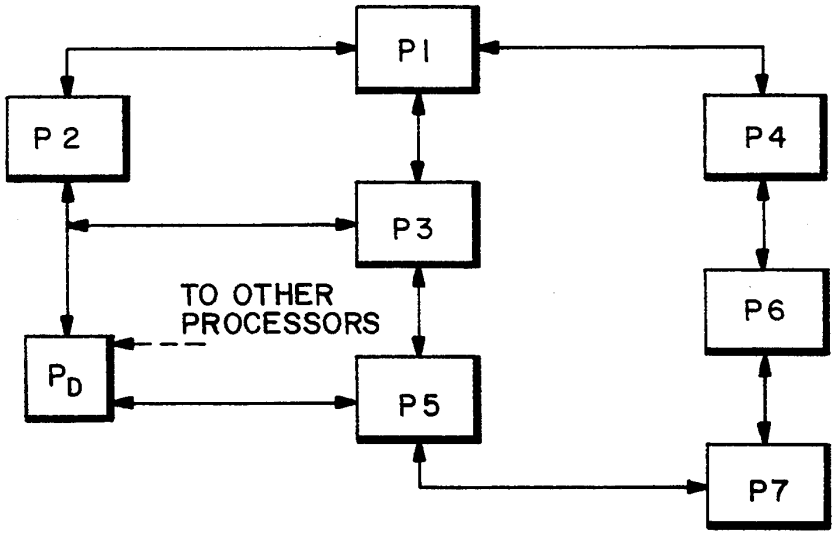


FIG. 1B

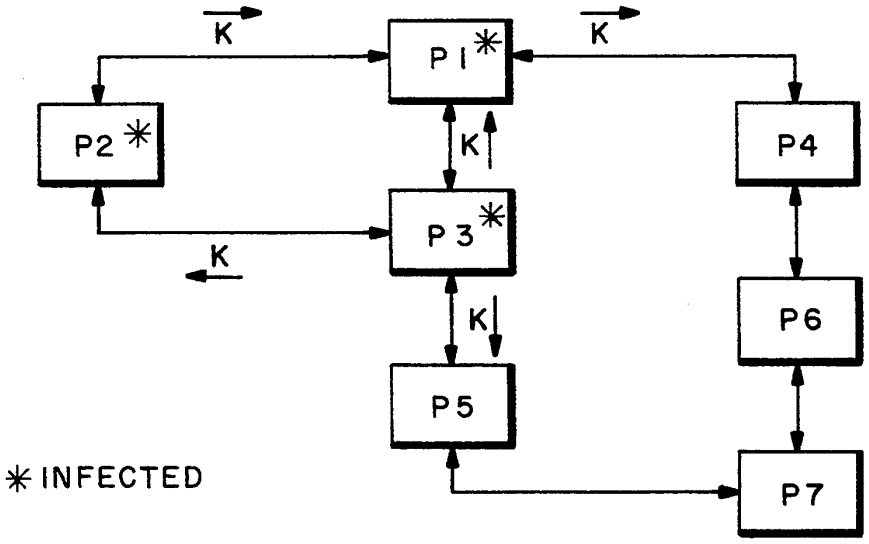


FIG. 1C

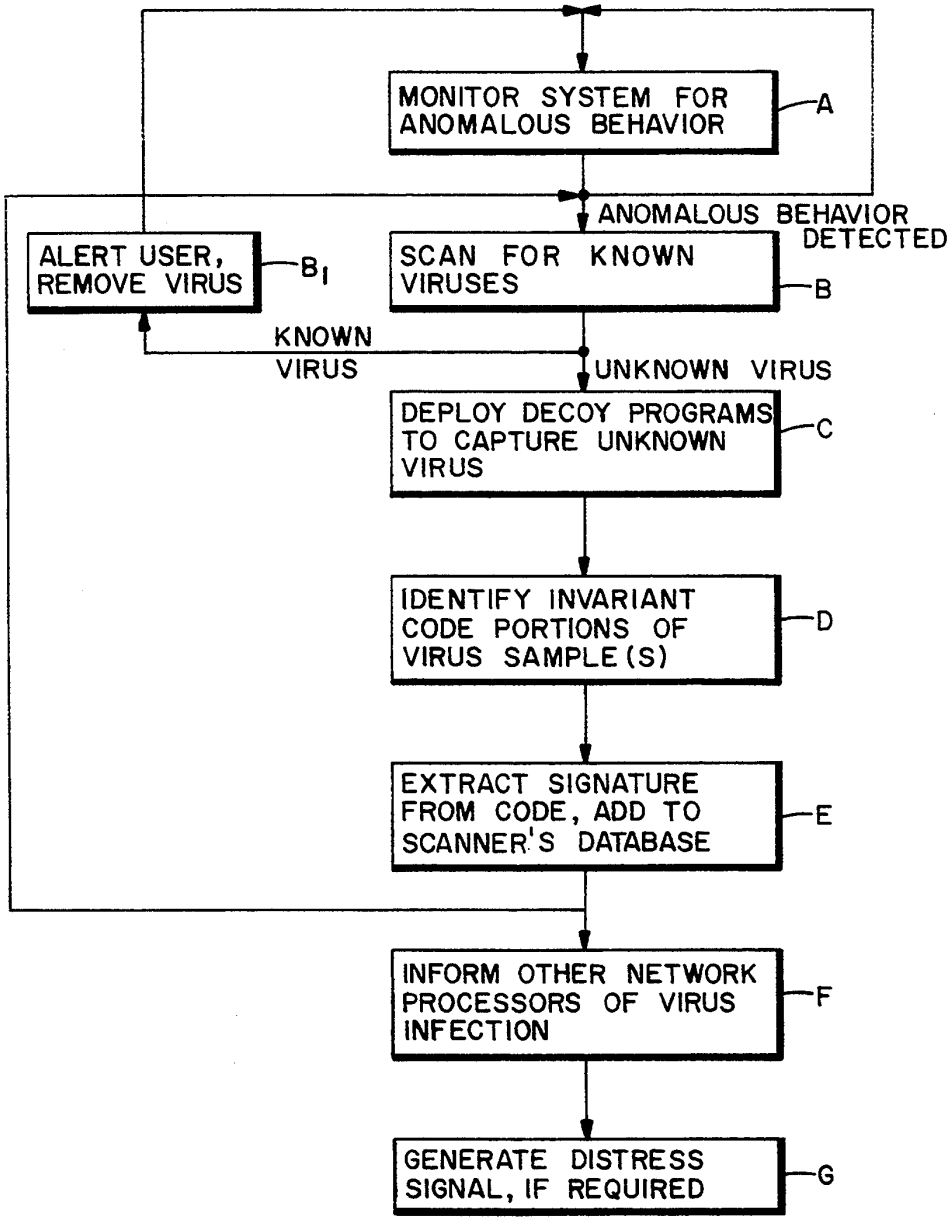


FIG. 2

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.