US005398196A

United States Patent [19]

Chambers

[11] Patent Number: 5,398,196

[45] Date of Patent: Mar. 14, 1995

[54] **METHOD AND APPARATUS FOR DETECTION OF COMPUTER VIRUSES**

[76] Inventor: **David A. Chambers**, 3655 Eastwood Cir., Santa Clara, Calif. 95054

[21] Appl. No.: **99,368**

[22] Filed: **Jul. 29, 1993**

[51] **Int. Cl.**[6] **G06F 15/20**

[52] **U.S. Cl.** **364/580**; 364/550; 364/578; 364/579; 395/500

[58] **Field of Search** 364/550, 578, 579, 580, 364/286.4; 371/16.2, 19; 395/500

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,080,650	3/1978	Beckett	395/500
4,773,028	9/1988	Tallman	364/578 X
5,086,502	2/1992	Malcom	395/575
5,121,345	6/1992	Lentz	364/550
5,144,660	9/1992	Rose	380/4
5,233,611	8/1993	Triantafyllos et al.	371/19 X

FOREIGN PATENT DOCUMENTS

9006430	4/1991	Brazil .
1057534	1/1992	China .
304033	2/1989	European Pat. Off. .
510244	10/1992	European Pat. Off. .
514815	11/1992	European Pat. Off. .
2629231	9/1989	France .
2632747	12/1989	France .
3736760	5/1989	Germany .
461879	4/1990	Sweden .
2231418	11/1990	United Kingdom .
2246901	2/1992	United Kingdom .
2253511	9/1992	United Kingdom .
9113403	9/1991	WIPO .
9221087	11/1992	WIPO .

OTHER PUBLICATIONS

Bowen, T., "Central Point Tool Unearths New Viruses," *P.C. Week*, May 31, 1993, pp. 41–42.

Excerpts From On-line Documentation for FProt Program, 1994.

Primary Examiner—Edward R. Cosimano

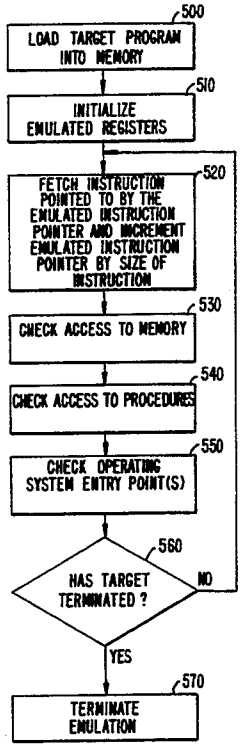
Attorney, Agent, or Firm—Townsend and Townsend Khourie and Crew

[57] **ABSTRACT**

A behavior analyzing antivirus program detects viral infection of a target program by emulating the execution of the target program and analyzing the emulated execution to detect viral behavior. The antivirus monitor program contains both variables corresponding to the CPU's registers and emulation procedures corresponding to the CPU's instructions. The target program is loaded into memory and its execution is emulated by the antivirus monitor program. Intelligent procedures contained in the monitor program are given control between every instruction emulated so as to detect aberrant or dangerous behavior in the target program in which case the danger of a viral presence is flagged and emulation is terminated.

27 Claims, 9 Drawing Sheets

Microfiche Appendix Included
(2 Microfiche, 167 Pages)



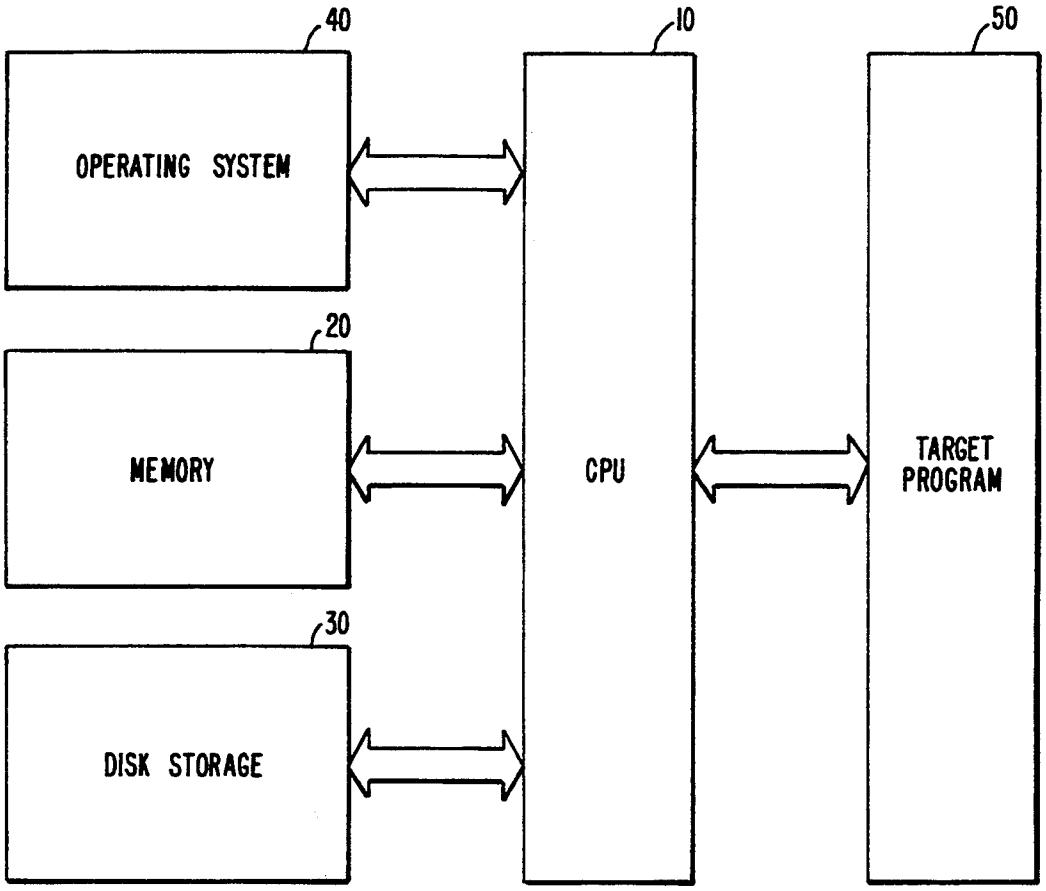


FIG. 1A.
(PRIOR ART)

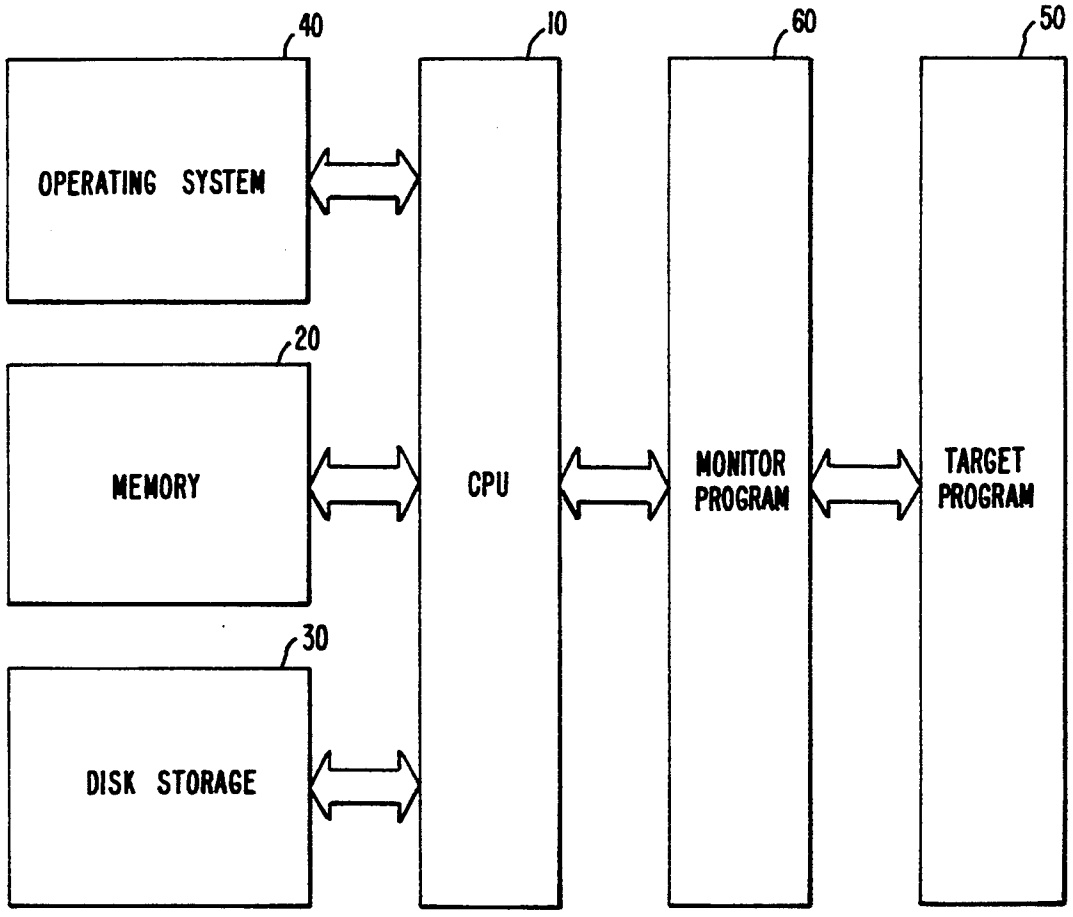


FIG. IB.

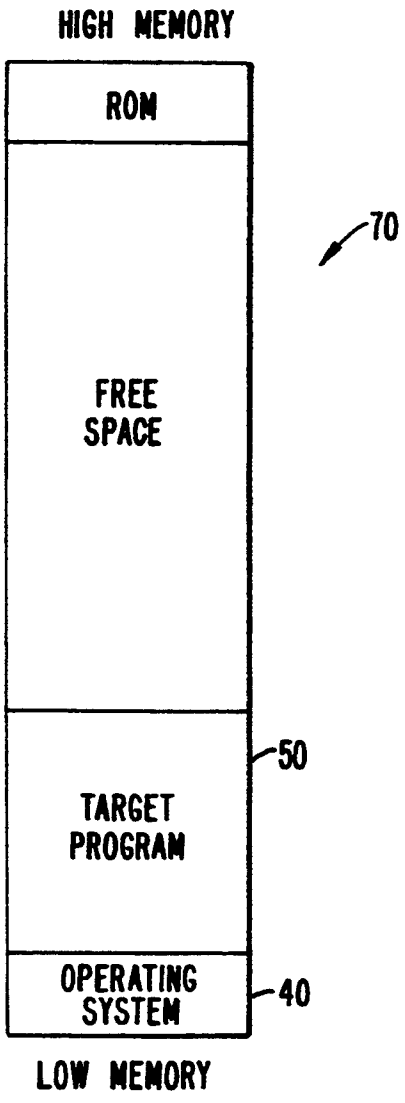


FIG. 2A.
(PRIOR ART)

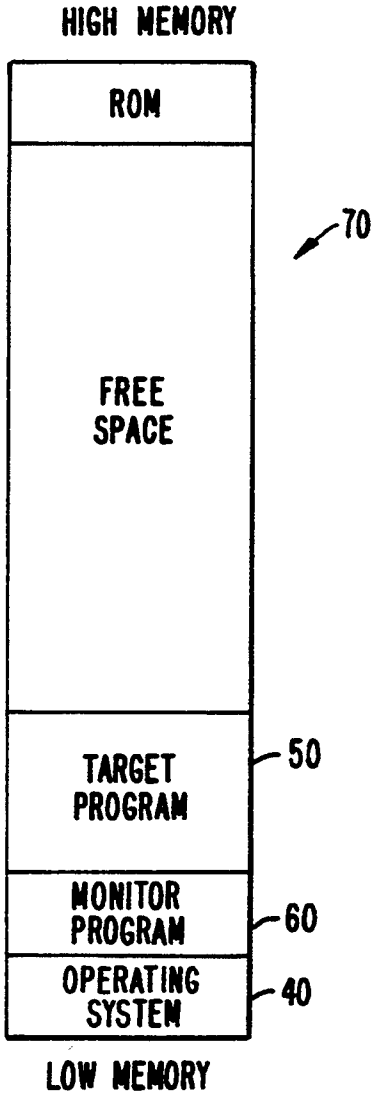


FIG. 2B.

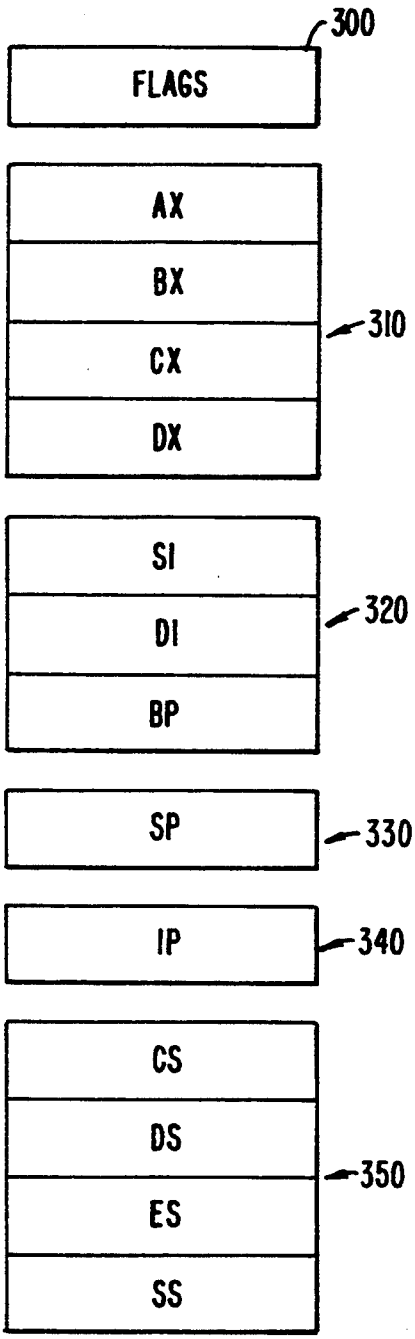


FIG. 3.
(PRIOR ART)

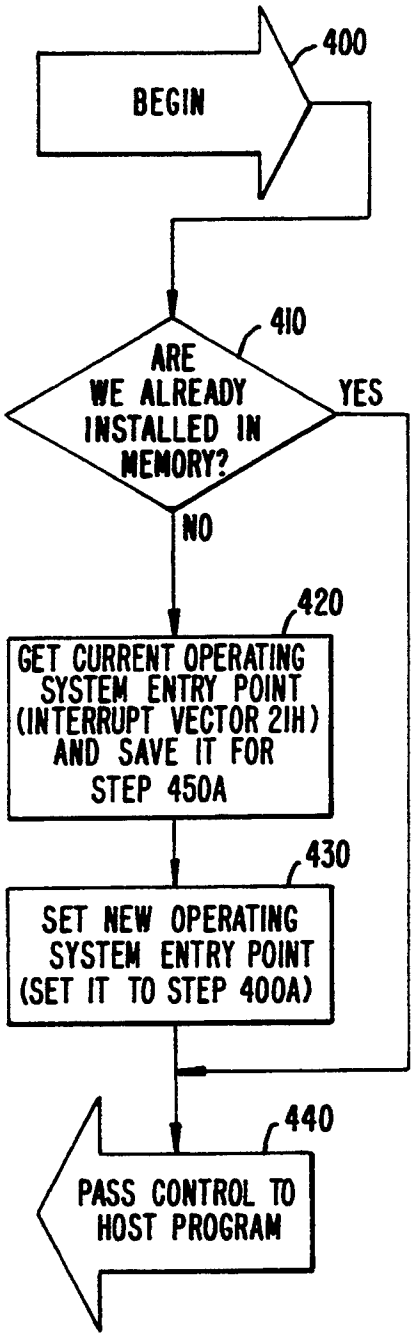


FIG. 4A.
(PRIOR ART)

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.