US005421006A

United States Patent [19]

Jablon et al.

[11] Patent Number: 5,421,006

[45] Date of Patent: May 30, 1995

[54] **METHOD AND APPARATUS FOR ASSESSING INTEGRITY OF COMPUTER SYSTEM SOFTWARE**

[75] Inventors: **David P. Jablon; Nora E. Hanley,** both of Shrewsbury, Mass.

[73] Assignee: **Compaq Computer Corp.,** Houston, Tex.

[21] Appl. No.: **231,443**

[22] Filed: **Apr. 20, 1994**

Related U.S. Application Data

[63] Continuation of Ser. No. 880,050, May 7, 1992.

[51] **Int. Cl.**[6] **G06F 11/00;** H04K 1/00

[52] **U.S. Cl.** **395/575;** 380/4

[58] **Field of Search** 395/575, 700, 750, 425; 380/4

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,309,569	1/1982	Merkle .	
4,388,695	6/1983	Heinemann	364/900
4,590,552	5/1986	Guttag .	
4,651,323	3/1987	Goodman et al.	364/900
4,661,991	4/1987	Logemann .	
4,685,056	8/1987	Barnsdale, Jr. et al.	364/200
4,698,750	10/1987	Wilkie et al.	364/200
4,747,040	5/1988	Blanset et al.	364/200
4,819,267	4/1989	Cargile et al.	380/23
4,825,358	4/1989	Letwin et al.	364/200
4,885,788	12/1989	Takaragi et al.	380/23
4,908,861	3/1990	Brachtl et al.	380/25
4,930,073	5/1990	Cina	364/300
4,970,504	11/1990	Chen .	
4,975,950	12/1990	Lentz	380/4
5,022,077	6/1991	Bealkowski et al.	380/4
5,050,212	9/1991	Dyson	380/25
5,073,934	12/1991	Matyas et al.	380/30
5,121,345	6/1992	Lentz	364/550
5,138,706	8/1992	Melo et al. .	
5,144,659	9/1992	Jones	380/4
5,161,122	11/1992	Robertson	365/195
5,175,840	12/1992	Sawase et al.	395/425
5,204,966	4/1993	Wittenberg et al.	395/800
5,265,164	11/1993	Matyas et al.	380/30
5,278,973	1/1994	O'Brien et al.	395/500

OTHER PUBLICATIONS

Intel 386 SL Microprocessor SuperSet Programmer's Reference manual, 1990, ISBN 1-55512-129-2.

Compaq Computer Corporation, Security Standard for Hardware Configuration, pp. 1-6, 1990.

Flowchart of Operations of Computers According to the Security Standard for Hardware Configuraiton.

Chap. 13, Real Time Clock Interface, 386 SL Microprocessor Superset System Design Guide by Intel Corporation, pp. 13-1 to 13-2, 1990.

Using Password Security, Operations Guide for Compaq Deskpro 386s Personal Computer by Compaq Computer Corp., pp. 3-5 to 3-7, 1988.

Primary Examiner—Robert W. Beausoliel, Jr.

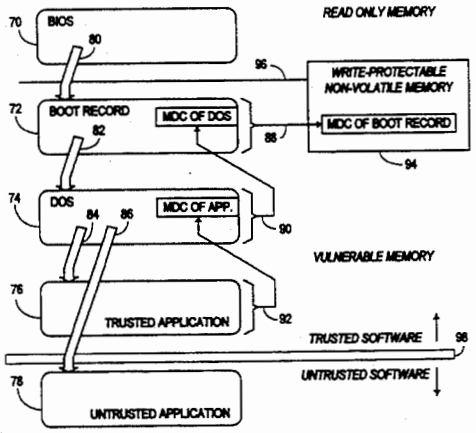
Assistant Examiner—Joseph E. Palys

Attorney, Agent, or Firm—Pravel, Hewitt, Kimball & Krieger

[57] **ABSTRACT**

A method and device for reliably assessing the integrity of a computer system's software prevents execution of corrupted programs at time of system initialization, enhancing system security. Programs and data comprising the system's trusted software, including all startup processes, are verified before being utilized. Methods to verify the trusted software use a hierarchy of both modification detection codes and public-key digital signature codes. The top-level codes are placed in a protectable non-volatile storage area, and are used by the startup program to verify the integrity of subsequent programs. A trusted initialization program sets a hardware latch to protect the codes in the non-volatile memory from being overwritten by subsequent untrusted programs. The latch is only reset at system restart, when control returns to the bootstrap program. Software reconfiguration is possible with trusted programs that write new top-level codes while the latch is open. The mechanism itself is immune to malicious software attack when the write-protect latch is closed before running untrusted software. Preferred embodiments in an IBM-compatible personal computer uses the reset switch to initiate a trusted path between the user and a program. Damage from certain classes of computer virus and trojan horse attacks is prevented. A system recovery process is described. A related improved method for user authentication uses a read-and -write memory protection latch to prevent access to sensitive authentication data.

19 Claims, 8 Drawing Sheets



DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

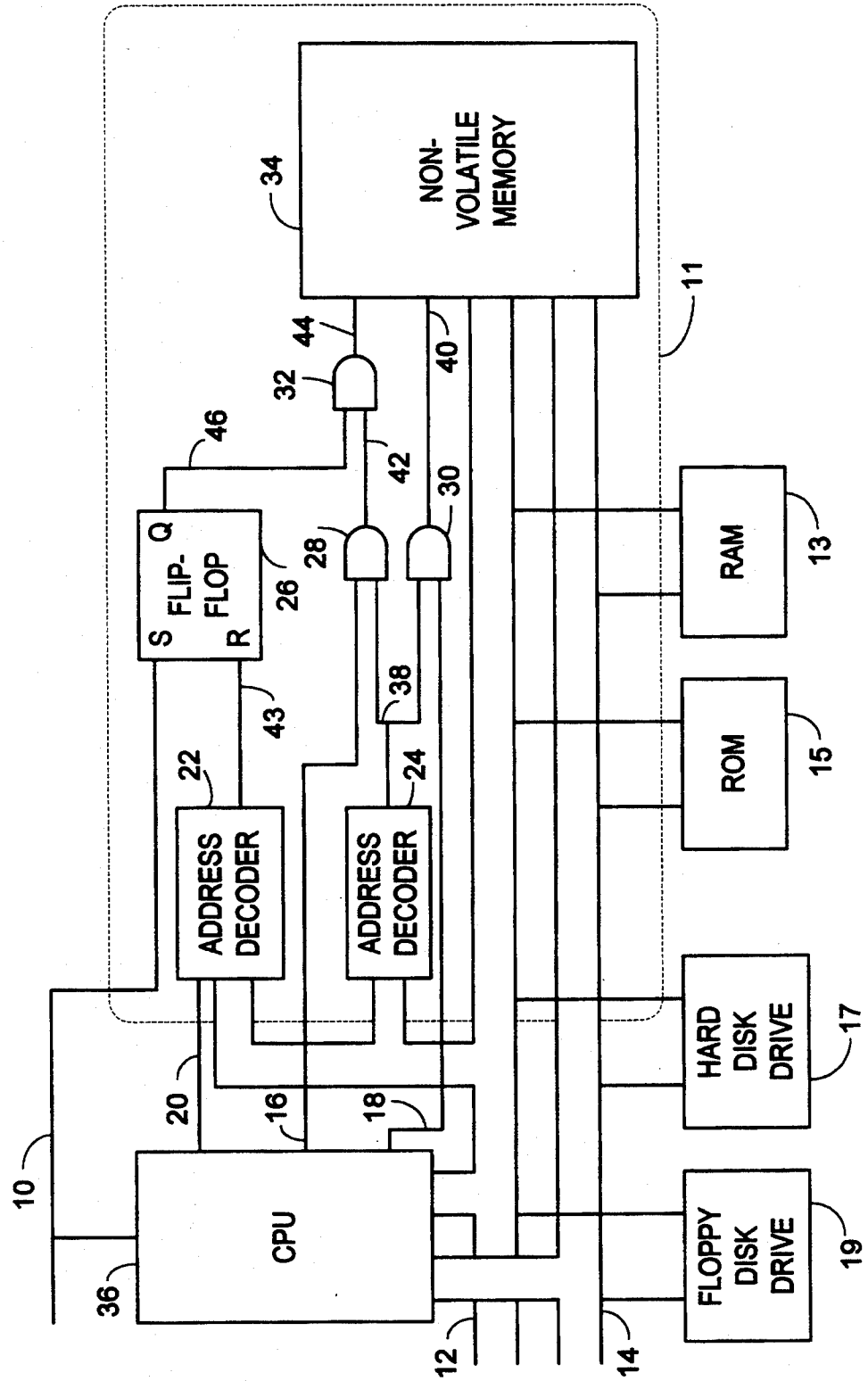
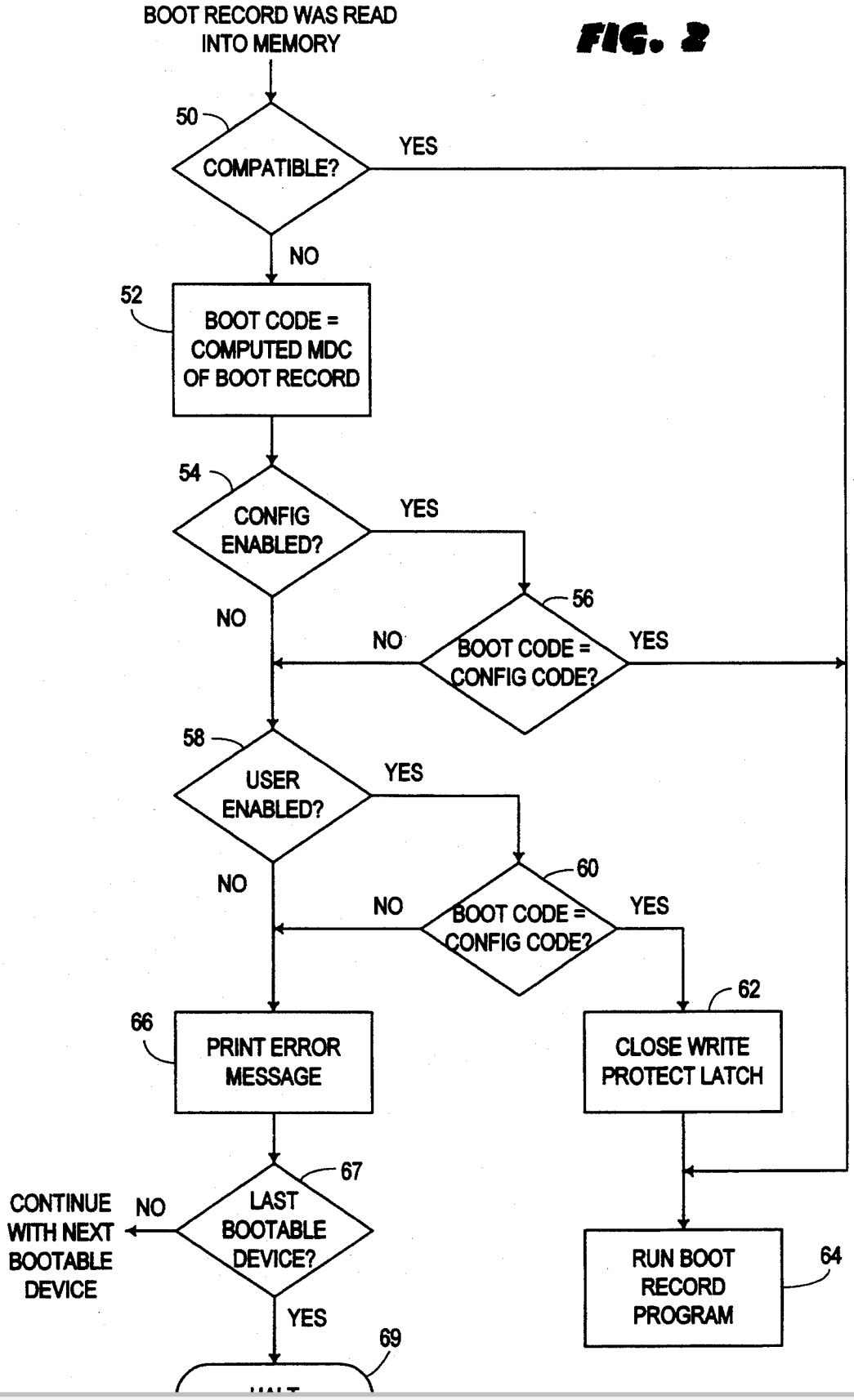


FIG. 1

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

FIG. 2



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

A SECURE CONFIGURATION:

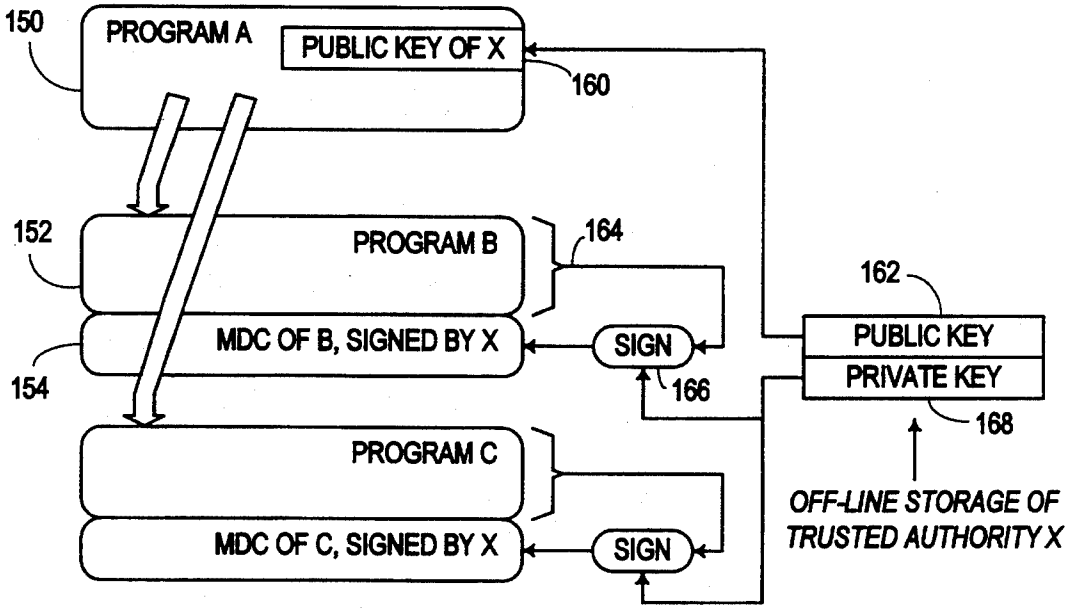
VARIABLE	VALUE	
COMPATIBLE	FALSE	110
USER ENABLED	TRUE	111
USER CODE	A6339DE4DBE72231	112
CONFIG ENABLED	TRUE	113
CONFIG CODE	15088428267F00BA	114

FIG. 3

COMPATIBLE CONFIGURATION:

VARIABLE	VALUE	
COMPATIBLE	TRUE	120
USER ENABLED	UNDEFINED	121
USER CODE	UNDEFINED	122
CONFIG ENABLED	UNDEFINED	123
CONFIG CODE	UNDEFINED	124

FIG. 4



DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

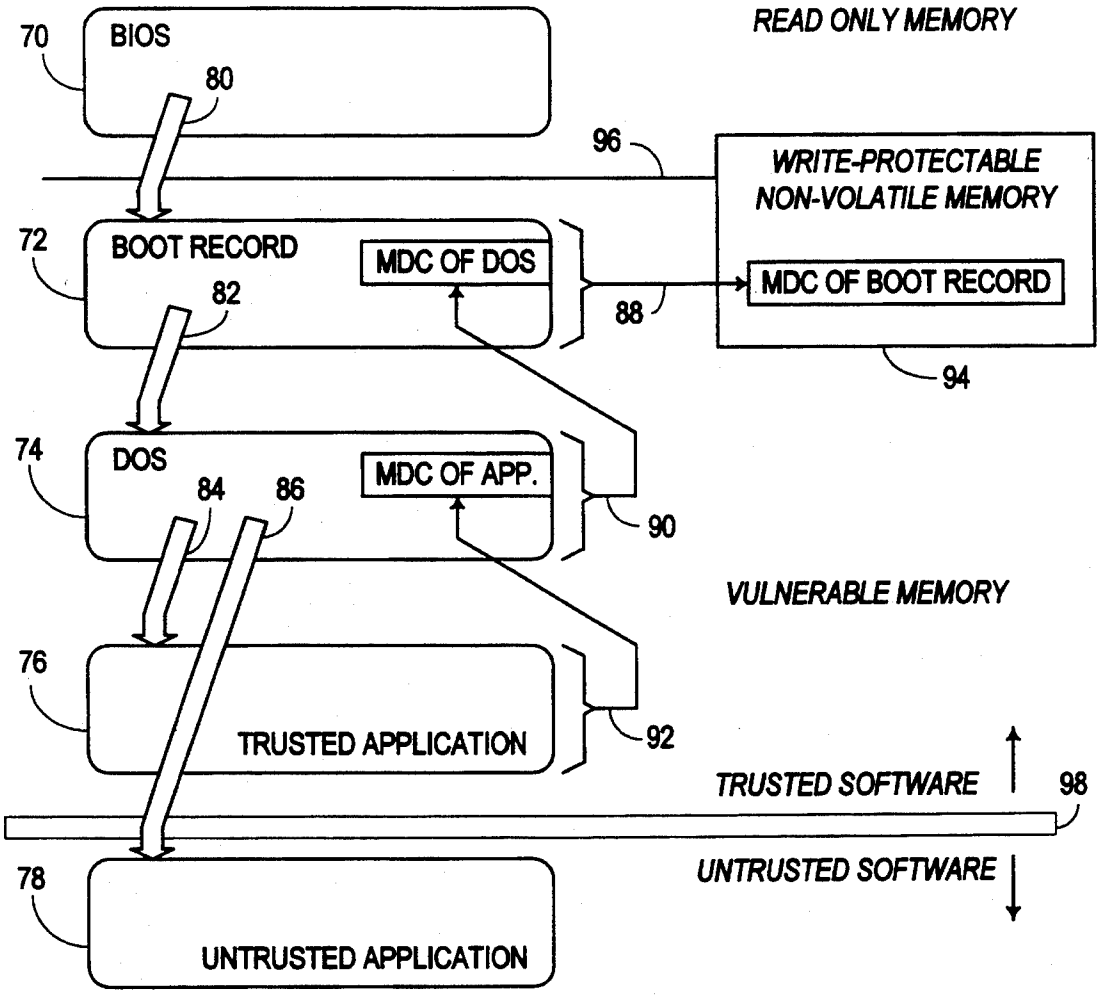


FIG. 5

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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.