US 20050108562A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2005/0108562 A1

Khazan et al. (43) Pub. Date: May 19, 2005

(54) TECHNIQUE FOR DETECTING EXECUTABLE MALICIOUS CODE USING A COMBINATION OF STATIC AND DYNAMIC ANALYSES

(76) Inventors: **Roger I. Khazan**, Somerville, MA (US); **Jesse C. Rabek**, Boston, MA (US); **Scott M. Lewandowski**, Reading, MA (US); **Robert K. Cunningham**, Lexington, MA (US)

Correspondence Address:
**Patent Group**
**Choate, Hall & Stewart**
**Exchange Place**
**53 State Street**
**Boston, MA 02109-2804 (US)**

(21) Appl. No.: **10/464,828**

(22) Filed: **Jun. 18, 2003**

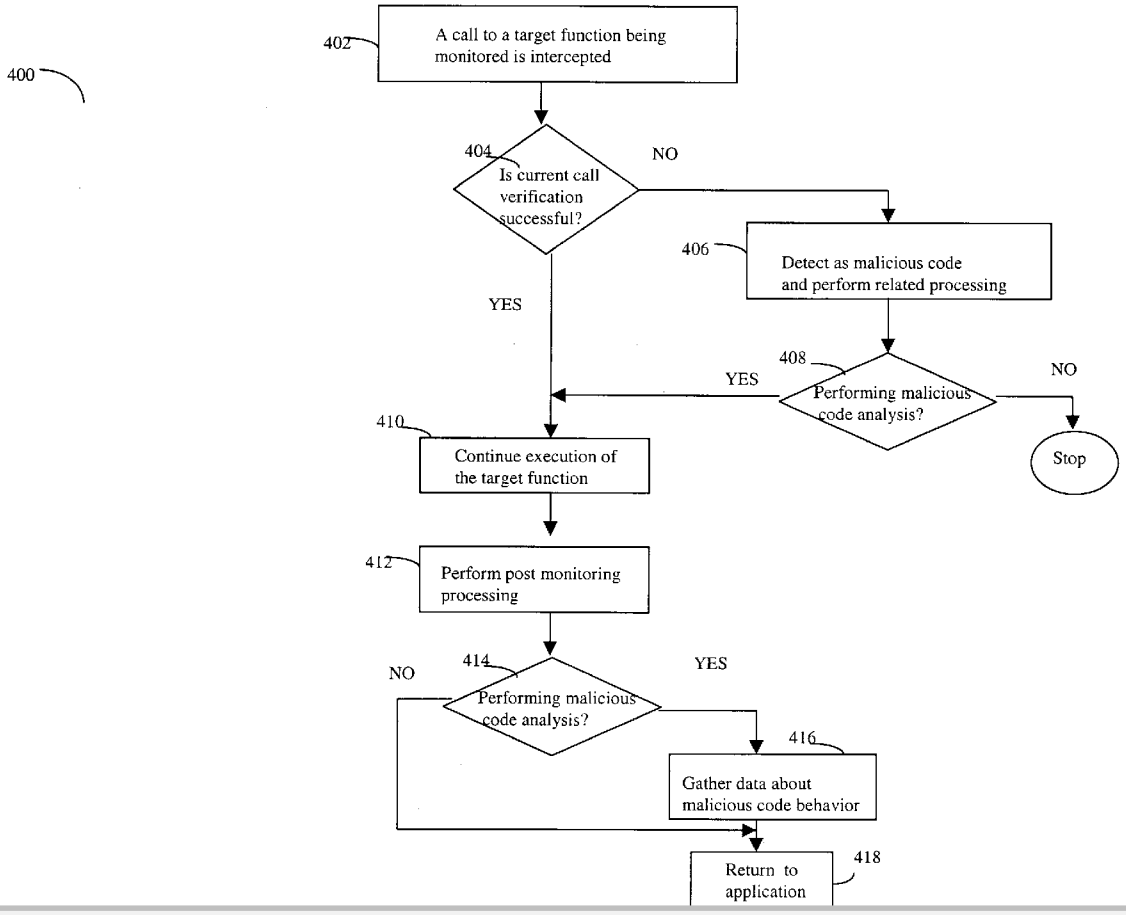
**Publication Classification**

(51) **Int. Cl.**[7] ..... **G06F 11/30**

(52) **U.S. Cl.** ..... **713/200**

(57) **ABSTRACT**

Described are techniques used for automatic detection of malicious code by verifying that an application executes in accordance with a model defined using calls to a predetermined set of targets, such as external routines. A model is constructed using a static analysis of a binary form of the application, and is comprised of a list of calls to targets, their invocation and target locations, and possibly other call-related information. When the application is executed, dynamic analysis is used to intercept calls to targets and verify them against the model. The verification may involve comparing the invocation and target location, as well as other call-related information, available at the time of call interception to the corresponding information identified by static analysis. A failed verification determines that the application includes malicious code. As an option, once detected, the malicious code may be allowed to execute to gather information about its behavior.



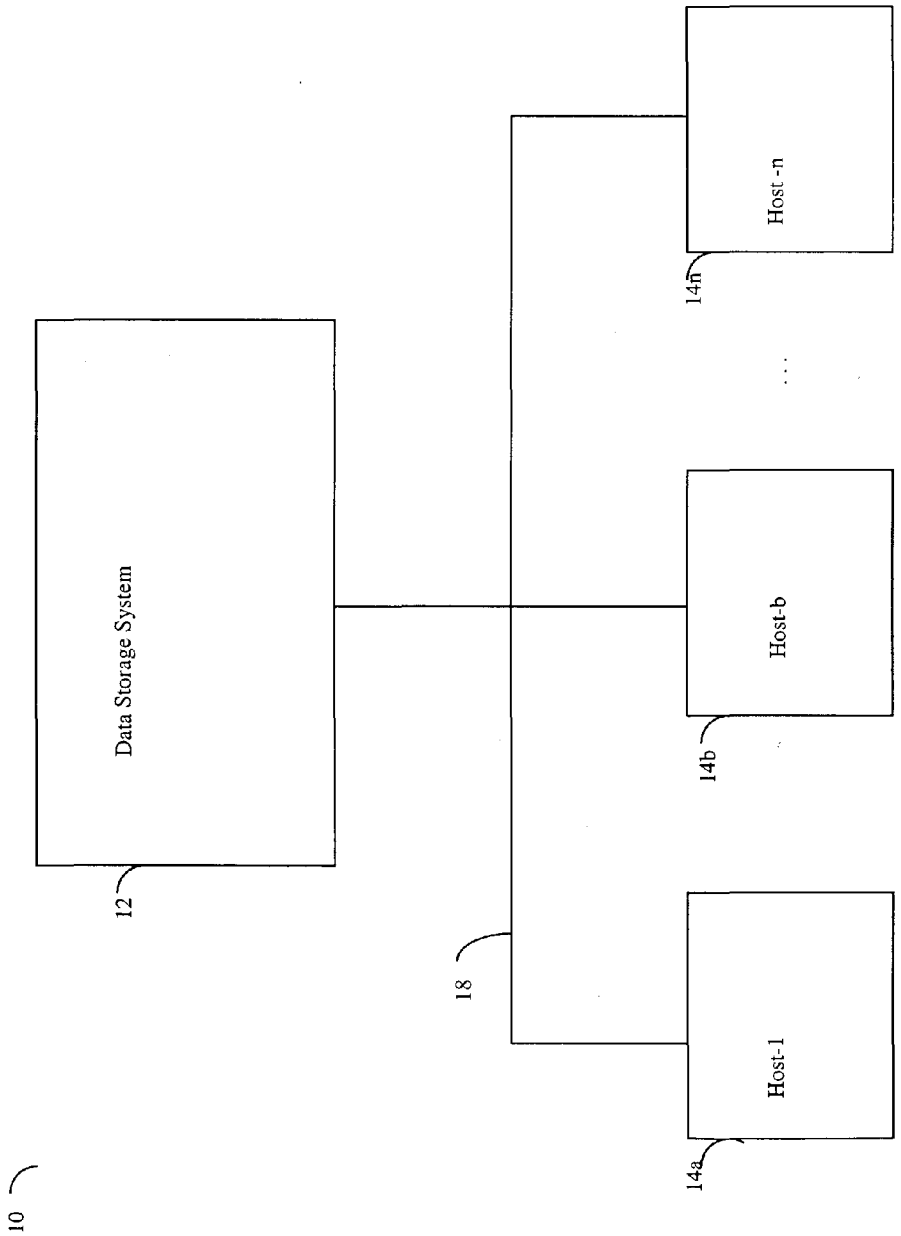



FIGURE 1

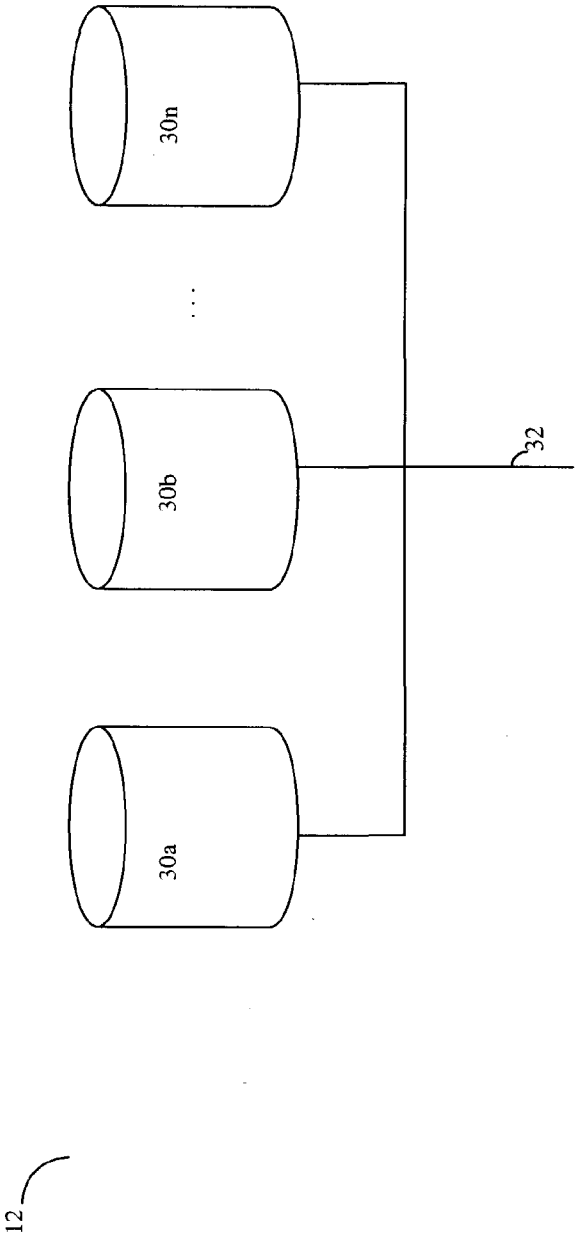



FIGURE 2

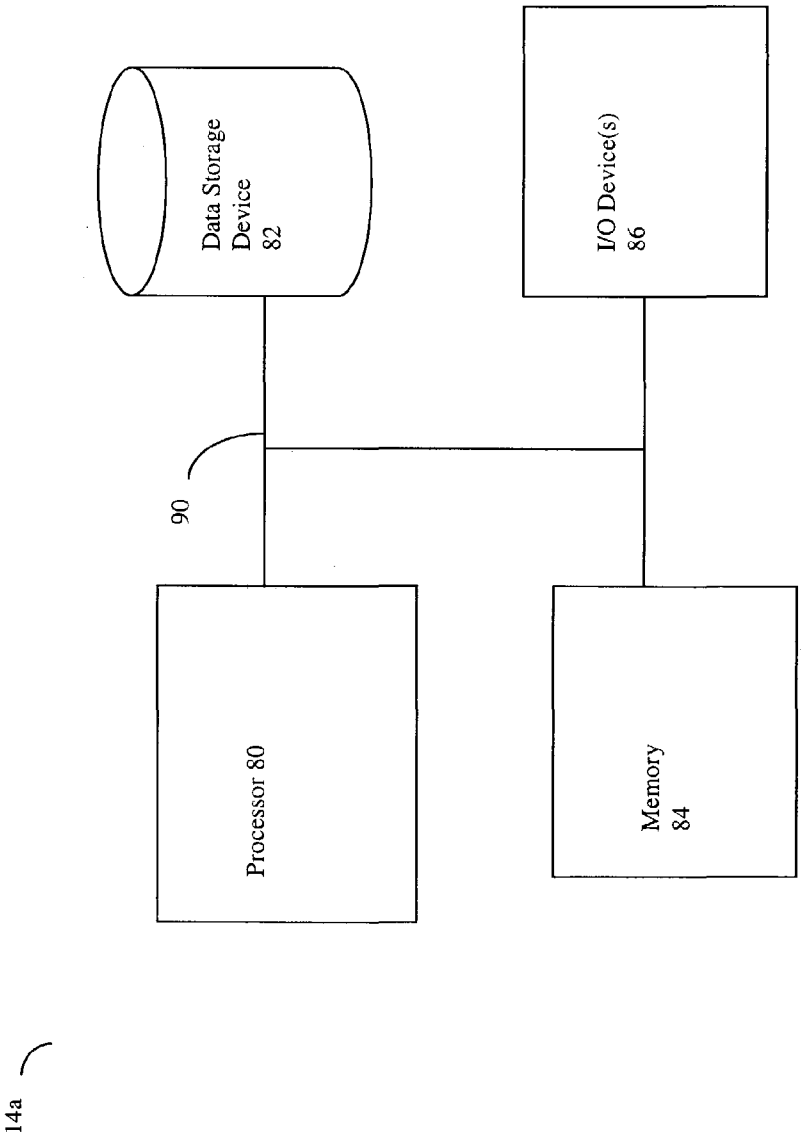



FIGURE 3

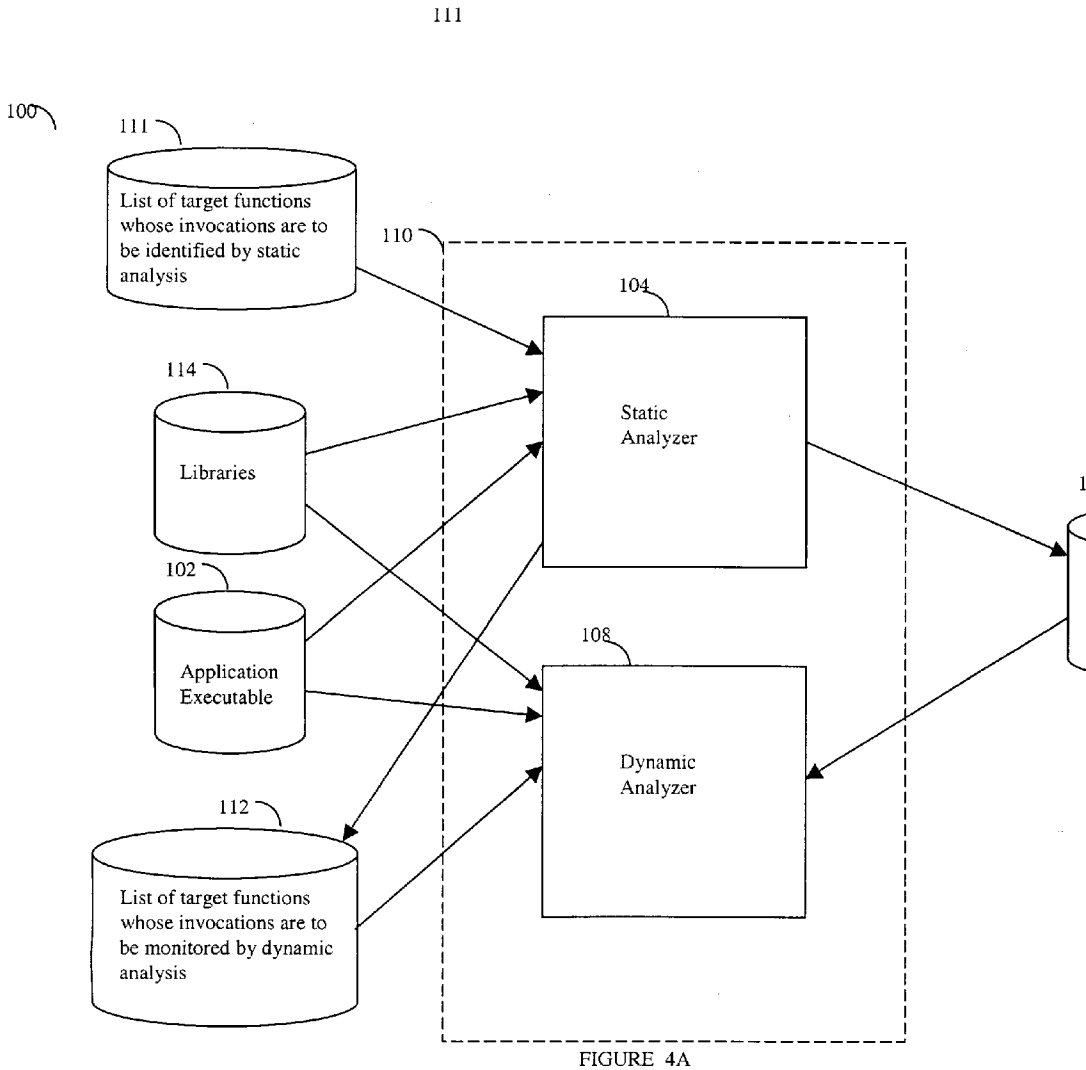



FIGURE 4A

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.