US006088804A

United States Patent [19]

Hill et al.

[11] Patent Number: 6,088,804

[45] Date of Patent: Jul. 11, 2000

[54] **ADAPTIVE SYSTEM AND METHOD FOR RESPONDING TO COMPUTER NETWORK SECURITY ATTACKS**

[75] Inventors: **Douglas W. Hill**, Scottsdale; **James T. Lynn**, Mesa, both of Ariz.

[73] Assignee: **Motorola, Inc.**, Schaumburg, Ill.

[21] Appl. No.: **09/006,056**

[22] Filed: **Jan. 12, 1998**

[51] **Int. Cl.**[7] **G06F 11/30**; H04L 9/00

[52] **U.S. Cl.** **713/201**; 713/200; 713/201

[58] **Field of Search** 713/201, 200; 714/38, 47, 48, 57; 380/4

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,062,147	10/1991	Pickett et al.	714/57
5,237,677	8/1993	Hirosawa et al.	714/57
5,414,833	5/1995	Heshey et al.	713/201
5,440,723	8/1995	Arnold et al.	714/2
5,452,442	9/1995	Kephart	380/4
5,491,791	2/1996	Glowny et al.	714/47
5,511,163	4/1996	Lerche et al.	714/39

FOREIGN PATENT DOCUMENTS

WO 93/22723	3/1993	WIPO .

OTHER PUBLICATIONS

Doumas et al. Design of a Neural Network for Recognition and Classification of Computer Virsul. pp. 435–448, 1995.

Tesauro et al. Neural networks for computer virusl recognition. pp. 5–6, Aug. 1996.

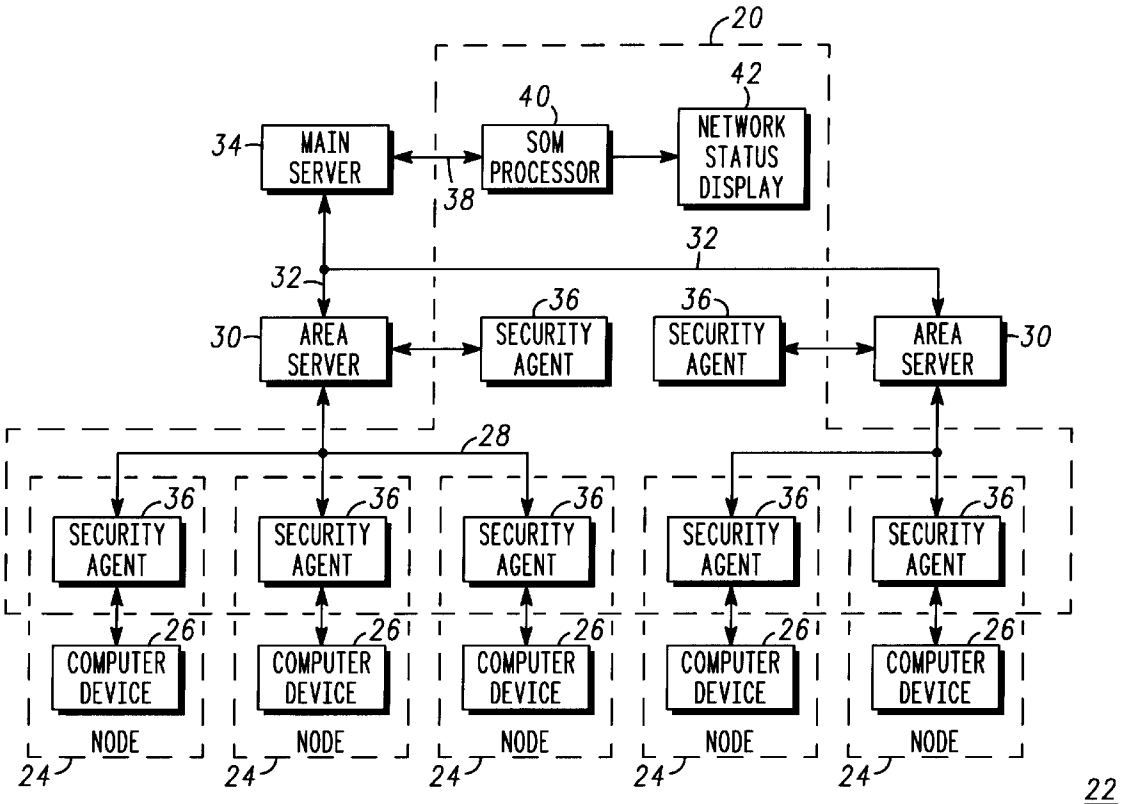
Primary Examiner—Ly V. Hua

Attorney, Agent, or Firm—Gregory J. Gorrie

[57] **ABSTRACT**

A dynamic network security system **(20)** responds to a security attack **(92)** on a computer network **(22)** having a multiplicity of computer nodes **(24)**. The security system **(20)** includes a plurality of security agents **(36)** that concurrently detect occurrences of security events **(50)** on associated computer nodes **(24)**. A processor **(40)** processes the security events **(50)** that are received from the security agents **(36)** to form an attack signature **(94)** of the attack **(92)**. A network status display **(42)** displays multi-dimensional attack status information representing the attack **(92)** in a two dimensional image to indicate the overall nature and severity of the attack **(92)**. The network status display **(42)** also includes a list of recommended actions **(112)** for mitigating the attack. The security system **(20)** is adapted to respond to a subsequent attack that has a subsequent signature most closely resembling the attack signature **(94)**.

19 Claims, 6 Drawing Sheets



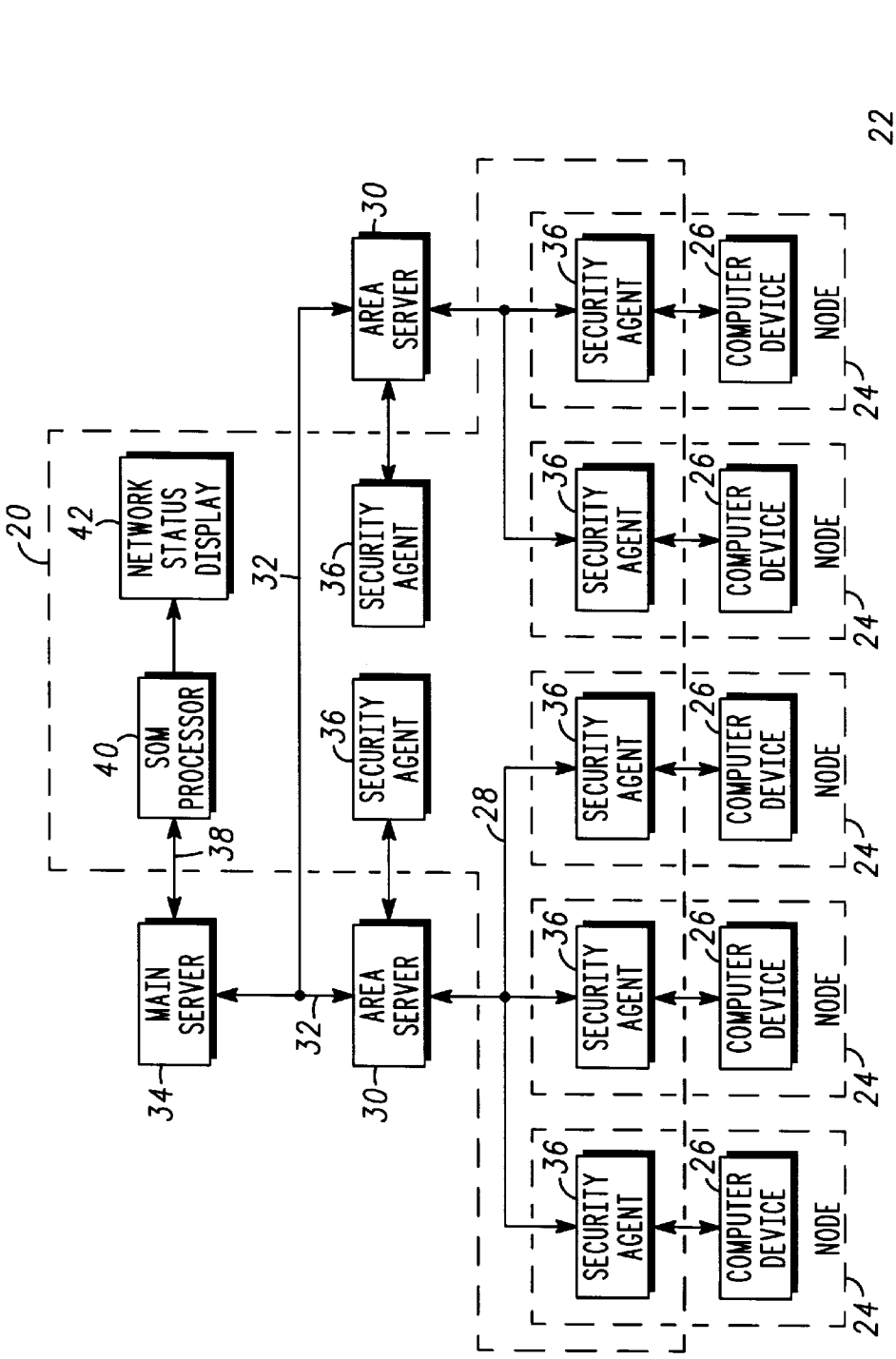


FIG. 1

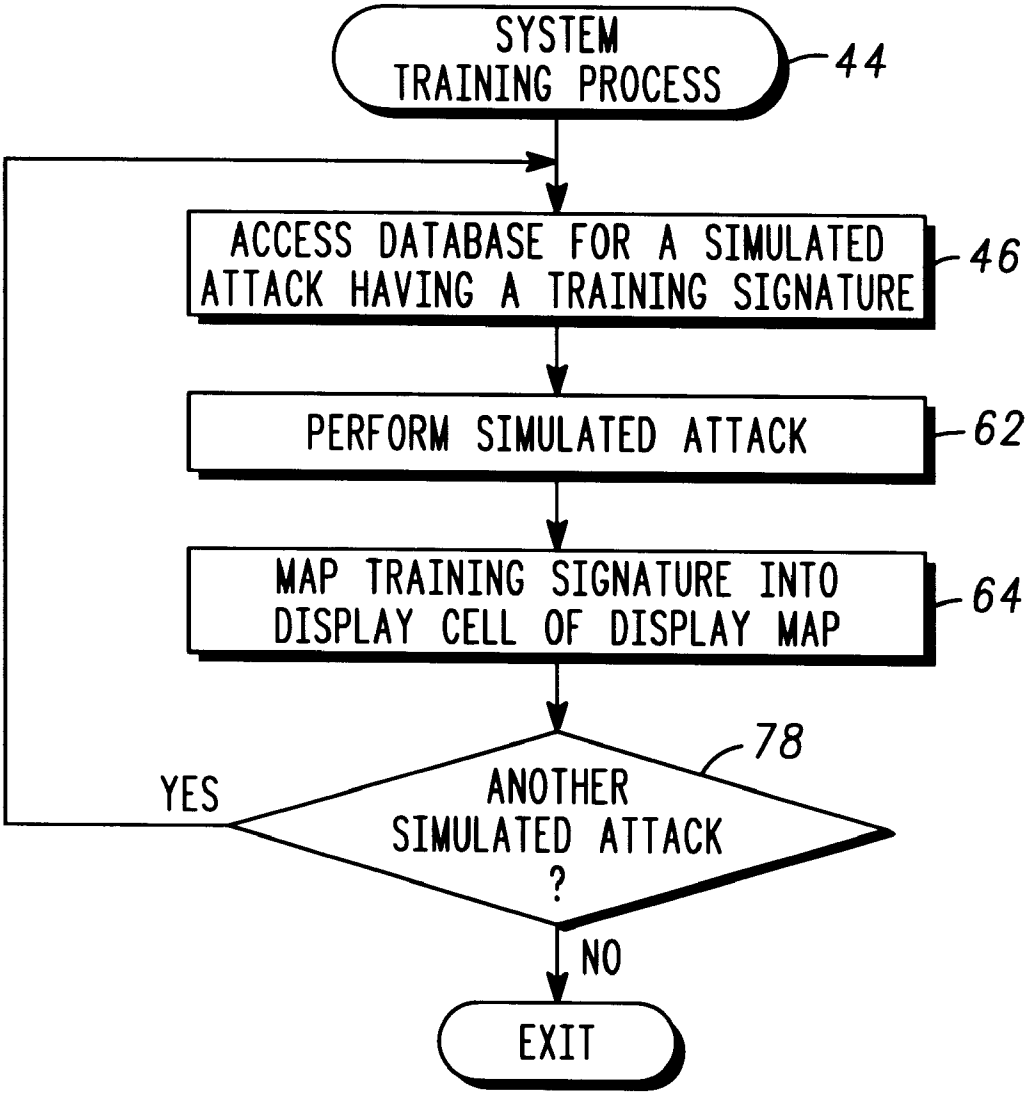


FIG. 2

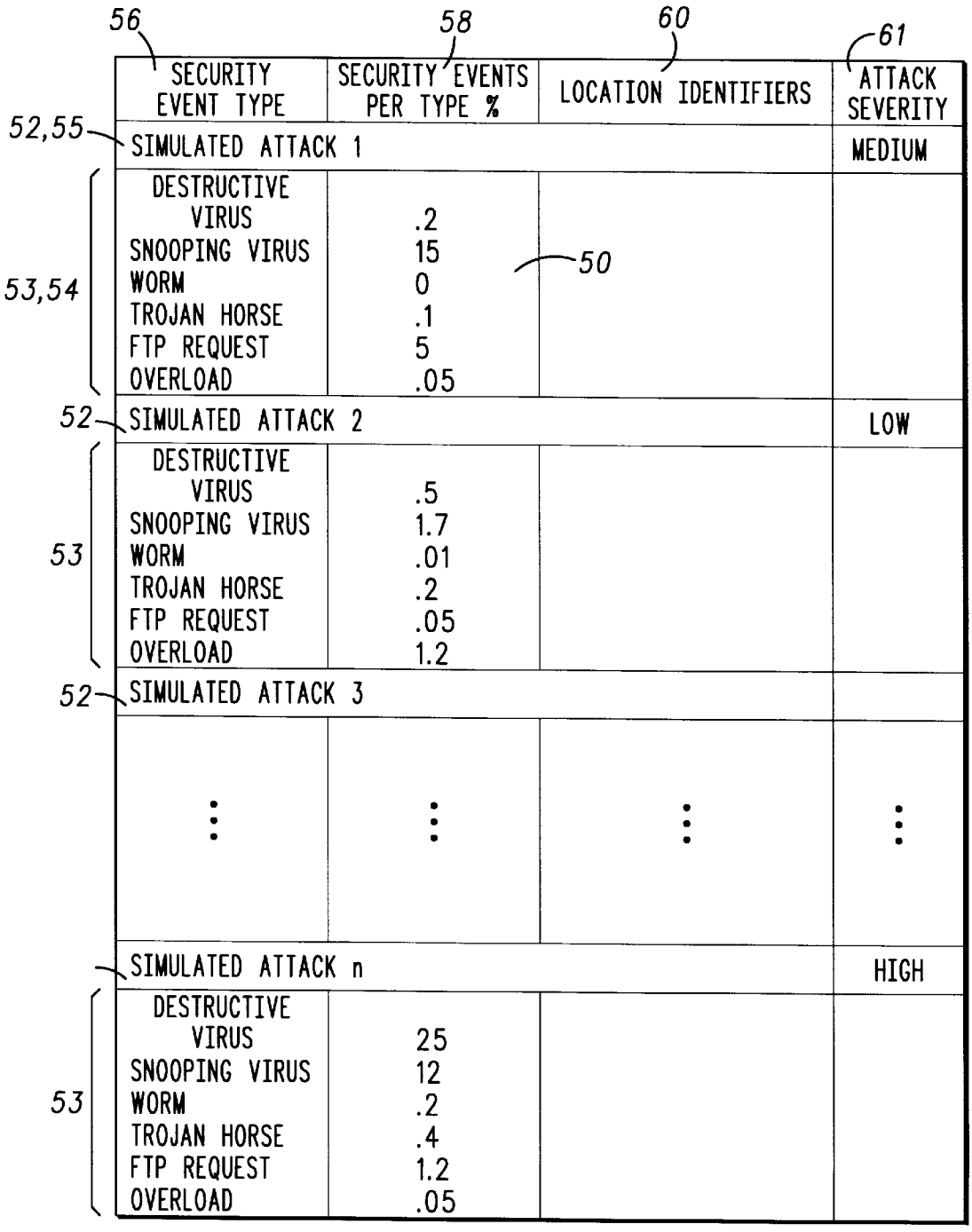


FIG. 3

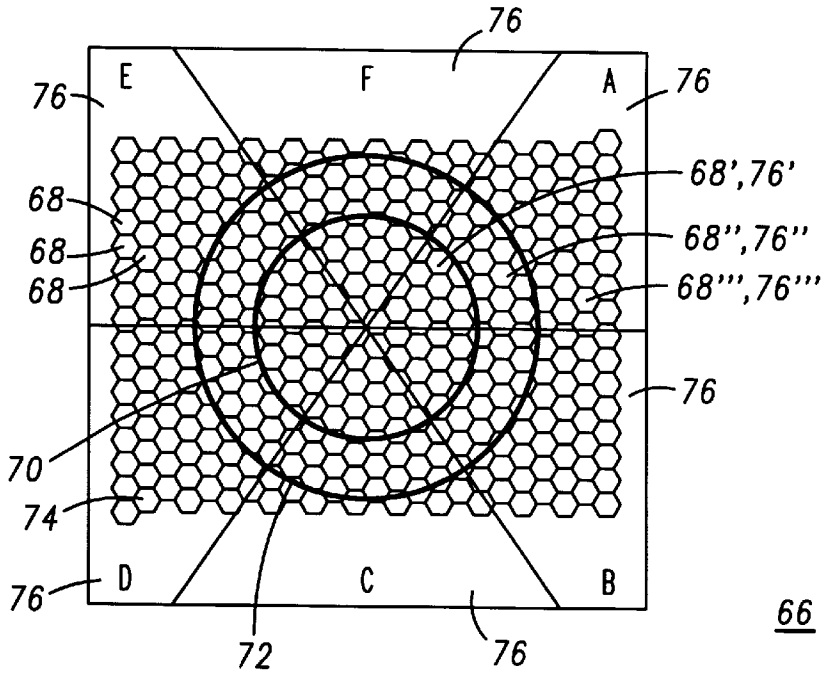


FIG. 4

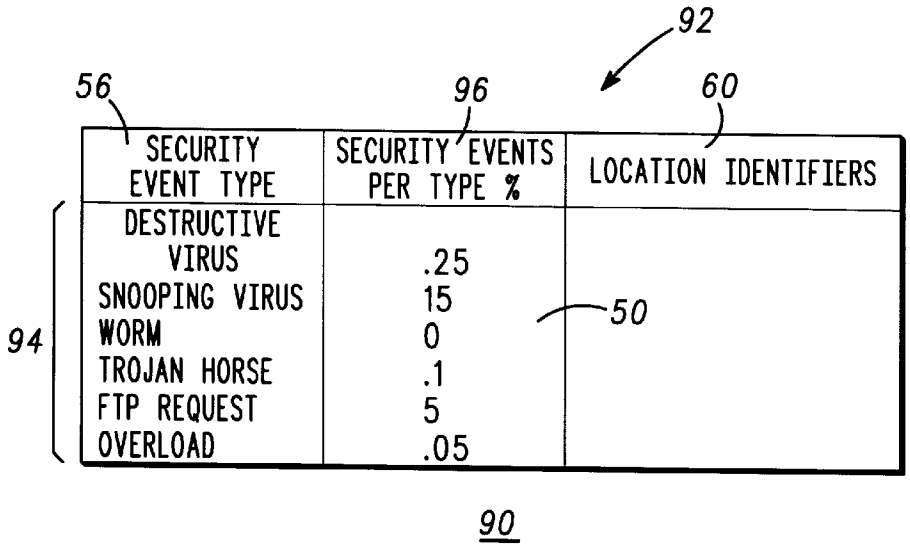


FIG. 6

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.