US006904529B1

(12) **United States Patent**
Swander

(10) **Patent No.: US 6,904,529 B1**
(45) **Date of Patent: Jun. 7, 2005**

(54) **METHOD AND SYSTEM FOR PROTECTING A SECURITY PARAMETER NEGOTIATION SERVER AGAINST DENIAL-OF-SERVICE ATTACKS**

(75) Inventor: **Brian D. Swander**, Kirkland, WA (US)

(73) Assignee: **Microsoft Corporation**, Redmond, WA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/561,046**

(22) Filed: **Apr. 28, 2000**

(51) **Int. Cl.**[7] **G06F 11/30**
(52) **U.S. Cl.** **713/201**; 713/151; 713/200
(58) **Field of Search** 713/200, 201, 713/151

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,923,849 A * 7/1999 Venkatraman 709/224
5,958,053 A * 9/1999 Denker 713/201
6,330,562 B1 * 12/2001 Boden et al. 707/10

OTHER PUBLICATIONS

"Analysis of a Denial of Service Attack on TCP", Proceedings of the 1997 IEEE Symposium on Security and Privacy, 1997, pp. 208–223.*

Computer Communications 22(10): "TCP/IP Security Threats and Attack Methods", Jun. 25, 1999, 885–97.

"Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks", Proceedings of the 1999 Network and Distributed System Security Symposium, pp. 151–65.

"Analysis of a Denial of Service Attack on TCP", Proceedings of the 1997 IEEE Symposium on Security and Privacy, 1997, pp. 208–223.

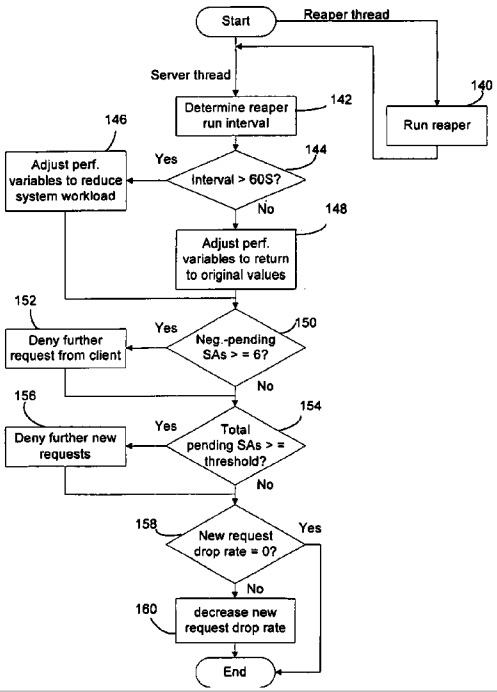
* cited by examiner

Primary Examiner—Justin T. Darrow
(74) *Attorney, Agent, or Firm*—Leydig, Voit & Mayer, Ltd.

(57) **ABSTRACT**

A method and system protects a security parameter negotiation server that stores states for connection requests pending negotiations from malicious denial-of-service attacks that attempt to flood the server with false requests. The degradation of performance of the server is dynamically detected, such as by monitoring the running intervals of a reaper that removes unneeded states. When performance degradation of the system is detected, relevant performance variables such as negotiation delay, extra retransmission delay and packet drop percentage are dynamically adjusted to reduce the workload on the negotiation server. Limiting the number of states with incomplete negotiation status for each client and the total number of such states further enhances the effectiveness of the protection against denial-of-service attacks.

16 Claims, 3 Drawing Sheets



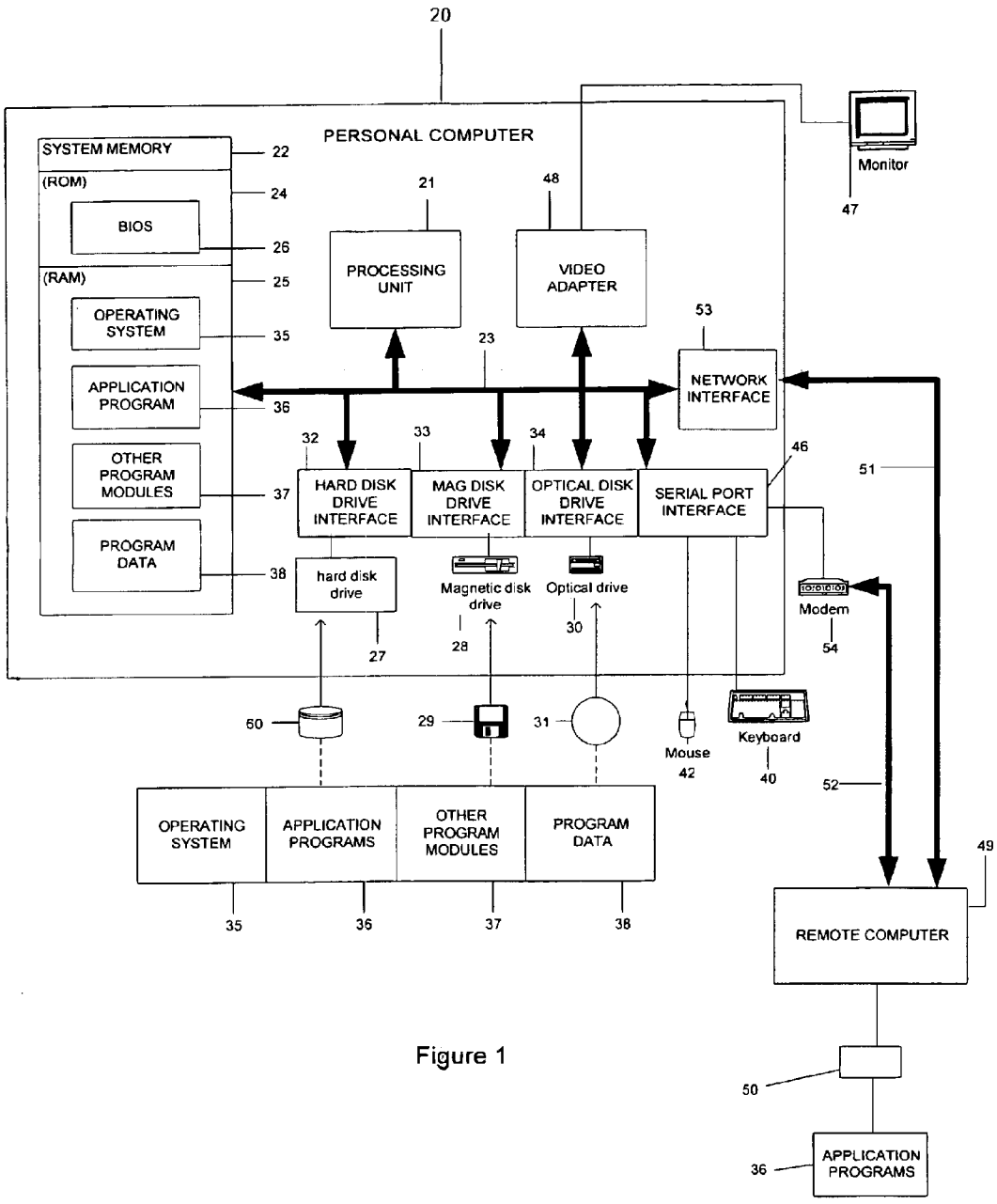


Figure 1

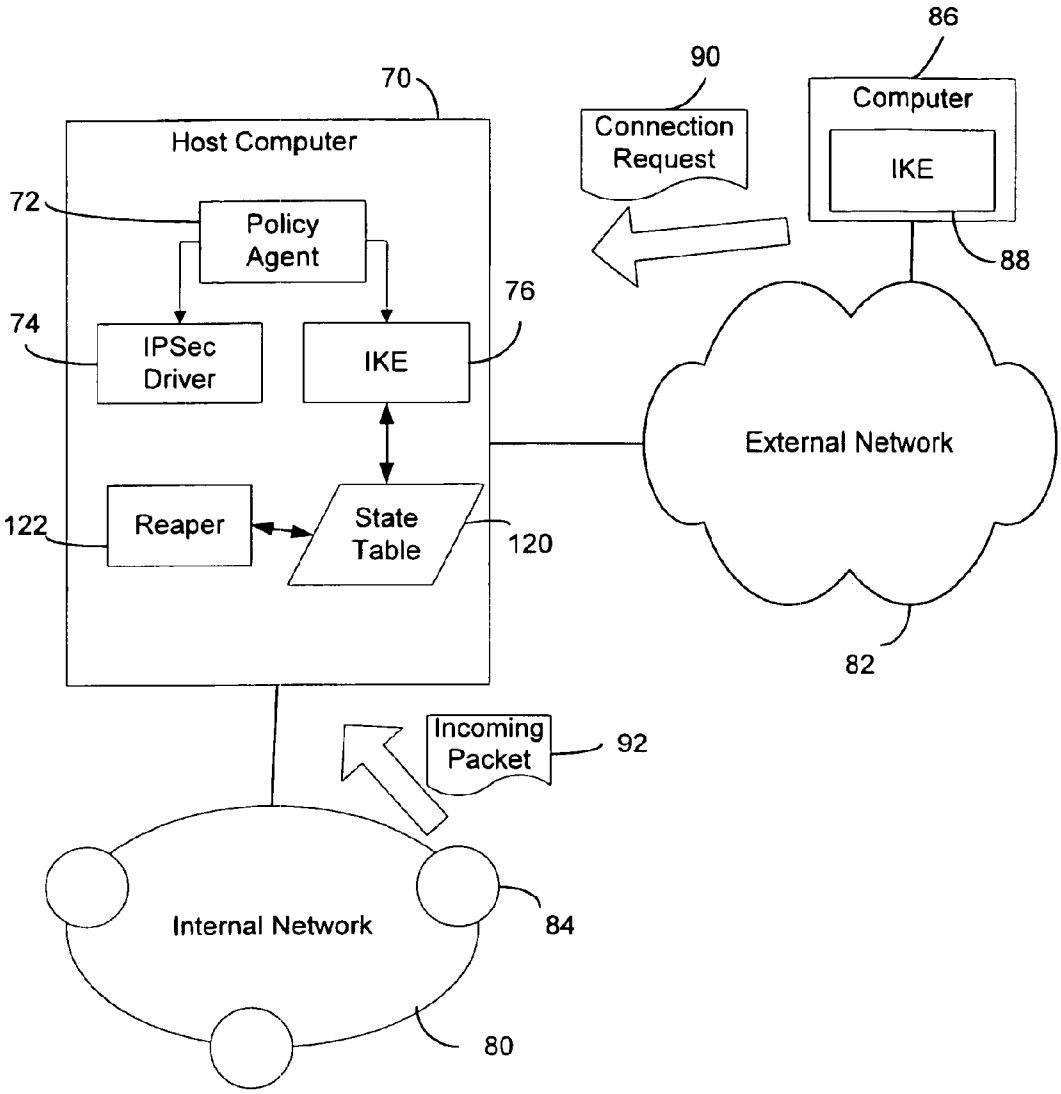


FIG. 2

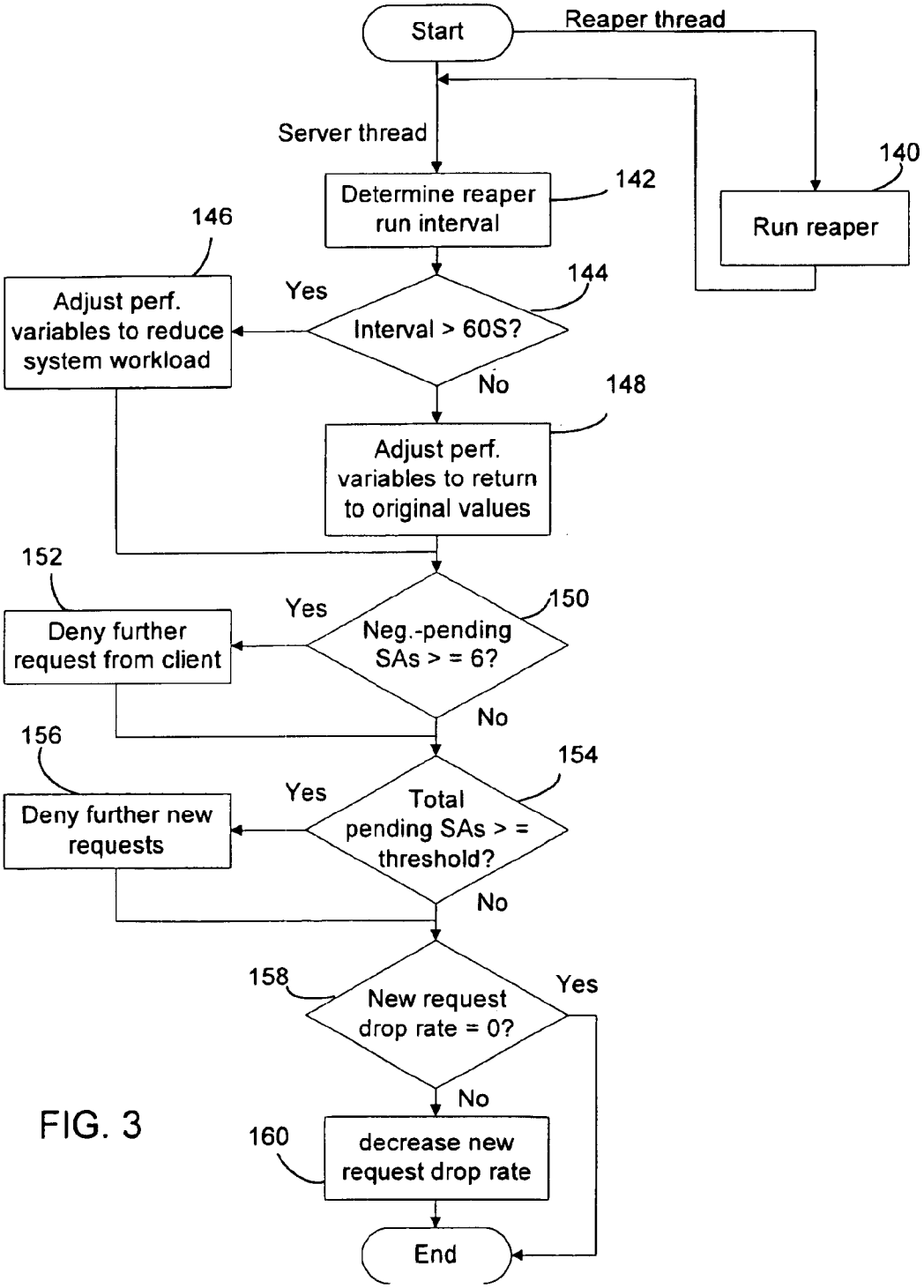


FIG. 3

METHOD AND SYSTEM FOR PROTECTING A SECURITY PARAMETER NEGOTIATION SERVER AGAINST DENIAL-OF-SERVICE ATTACKS

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to network communications, and more particularly to security threats to communication servers in a network environment.

BACKGROUND OF THE INVENTION

The Internet has entered the new millenium as the most important computer network of the world. Everyday, millions of people use the Internet to communicate with each other and to gather or share information. Moreover, electronic commerce ("E-commerce") using the World-Wide Web (WWW) of the Internet as its backbone is rapidly replacing and changing the conventional brick-and-mortar stores.

The security of communications through the Internet, however, has always been a major concern. This problem is related to the underlying network communication protocol of the Internet, the Internet Protocol ("IP"), which is responsible for delivering packets across the Internet to their destinations. The Internet Protocol was not designed to provide security features at its level of network communication operation. Moreover, the flexibility of IP allows for some creative uses of the protocol that defeat traffic auditing, access control, and many other security measures. IP-based network data is therefore wide open to tampering and eavesdropping. As a result, it substantial risks are involved in sending sensitive information across the Internet.

To address the lack of security measures of the Internet Protocol, a set of extensions called Internet Protocol Security ("IPSec") Suite has been developed to add security services at the IP level. The IPSec Suite includes protocols for an authentication header (AH), encapsulating security protocol (ESP), and a key management and exchange protocol (IKE). A significant advantage of the IPSec Suite is that it provides a universal way to secure all IP-based network communications for all applications and users in a transparent way. Moreover, as the IPSec Suite is designed to work with existing and future IP standards, regular IP networks can still be used to carry communication data between the sender and recipient. The IPSec Suite is also scalable and can therefore be used in networks ranging from local-area networks (LANS) to global networks such as the Internet.

Even though the IPSec standard provides a comprehensive and robust way to secure network communications against tampering and eavesdropping, the components implementing the IPSec Suite themselves may be subjected to various security threats in the network environment. For instance, the IPSec layer includes a component called an "Internet Key Exchange" ("IKE") server, which is responsible for negotiating with another IKE for security parameters, collectively called a "Security Association" ("SA"), of security operations for securing a given network communication stream. For each secured communication stream, a separate SA has to be negotiated and maintained. Because of the system resources required for handling each communication requests, it is possible for an attacker to construct and send a large number of false communication

the server to the extent that it is no longer able to serve legitimate users.

SUMMARY OF THE INVENTION

In view of the foregoing, the present invention provides a method and system for protecting a network security server for negotiating network security parameters, such as an Internet Key Exchange ("IKE") server of the IPSec suite, from denial-of-service attacks that flood the server with false connection requests. The vulnerability of the security server to such attacks comes from the need for the server to maintain state data for on-going negotiations in response to requests from unknown clients. In accordance with the invention, the resilience of the negotiation server to such attacks is significantly enhanced by dynamically detecting the degradation of the performance of the system, and dynamically adjusting relevant performance variables, such as negotiation delay, retransmission delay, and packet drop percentage, etc., to reduce the states maintained by the negotiation server when performance degradation is detected. A useful indicator of the system health may be the interval between consecutive runs of a reaper for removing states that are no longer useful. To further enhance the effectiveness of the protection against denial-of-service attacks, the maximum number of states pending negotiation responses for outstanding new negotiation requests from a client may be limited, and the total number of stored states pending negotiation responses may also be limited.

Additional features and advantages of the invention will be made apparent from the following detailed description of illustrative embodiments, which proceeds with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

While the appended claims set forth the features of the present invention with particularity, the invention, together with its objects and advantages, may be best understood from the following detailed description taken in conjunction with the accompanying drawings of which:

FIG. **1** is a block diagram generally illustrating an exemplary computer system on which the present invention may be reside;

FIG. **2** is a schematic diagram showing a networked computer having a negotiation server for negotiation of security parameters for securing network communications; and

FIG. **3** is a flow diagram showing a process embodying a method of the invention for protecting the negotiation server against denial-of-service attacks.

DETAILED DESCRIPTION OF THE INVENTION

Turning to the drawings, wherein like reference numerals refer to like elements, the invention is illustrated as being implemented in a suitable computing environment. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system

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.