



US007404212B2

(12) **United States Patent**
Radatti et al.

(10) **Patent No.:** **US 7,404,212 B2**
(45) **Date of Patent:** ***Jul. 22, 2008**

(54) **APPARATUS AND METHODS FOR INTERCEPTING, EXAMINING AND CONTROLLING CODE, DATA AND FILES AND THEIR TRANSFER**

(75) Inventors: **Peter V. Radatti**, Conshohocken, PA (US); **Timothy R. Eliseo**, Fair Oaks, CA (US)

(73) Assignee: **CyberSoft, Inc.**, Conshohocken, PA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 300 days.

This patent is subject to a terminal disclaimer.

5,481,735 A	1/1996	Mortensen et al.
5,511,163 A	4/1996	Lerche et al.
5,550,984 A	8/1996	Gelb
5,586,266 A	12/1996	Hershey et al.
5,623,600 A	4/1997	Ji et al.
5,682,428 A	10/1997	Johnson
5,761,424 A	6/1998	Adams et al.
5,802,178 A	9/1998	Holden et al.
5,832,208 A	11/1998	Chen et al.
5,832,228 A	11/1998	Holden et al.
5,889,943 A	3/1999	Ji et al.
5,916,305 A	6/1999	Sikdar et al.
5,931,917 A	8/1999	Nguyen et al.

(21) Appl. No.: **09/800,328**

(22) Filed: **Mar. 6, 2001**

(65) **Prior Publication Data**

US 2002/0129237 A1 Sep. 12, 2002

(51) **Int. Cl.**

G06F 21/00 (2006.01)
G06F 15/16 (2006.01)
G06F 11/30 (2006.01)

(52) **U.S. Cl.** **726/24**; 713/188; 713/189; 709/224

(58) **Field of Classification Search** 713/200, 713/201, 151, 152, 154, 188; 709/223–225, 709/227–232

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,070,528 A *	12/1991	Hawe et al.	713/161
5,126,728 A	6/1992	Hall	
5,278,901 A	1/1994	Shieh et al.	
5,319,776 A	6/1994	Hile et al.	
5,414,833 A	5/1995	Hershey et al.	

(Continued)

OTHER PUBLICATIONS

Microsoft Computer Dictionary third edition, 1997, p. 355.*

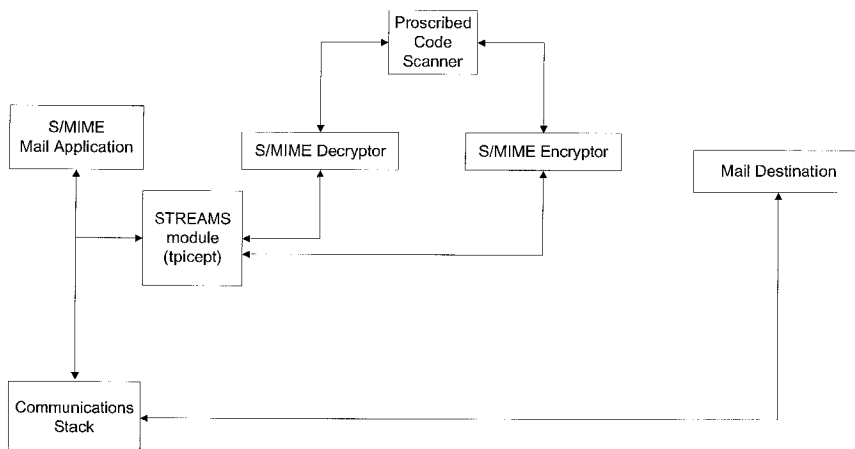
(Continued)

Primary Examiner—Christopher A Revak
(74) *Attorney, Agent, or Firm*—John F. A. Earley, III; Frank J. Bonini, Jr.; Harding, Early, Follmer & Frailey, P.C.

(57) **ABSTRACT**

The present invention comprises apparatus and methods for processing code, that is, for intercepting, examining and/or controlling code streams in a network. “Man in the middle” technology by use of decryptor/encryptor components are placed between client and server which permit alteration of the code as it passes through a communications channel. The code may then be examined by way of a proscribed code scanner. A protocol parser may also be implemented in order to intercept the code as it passes through the stack and transfer the code to the decryptor/encryptor components.

16 Claims, 4 Drawing Sheets



US 7,404,212 B2

Page 2

U.S. PATENT DOCUMENTS

5,983,348	A *	11/1999	Ji	713/200	6,721,424	B1 *	4/2004	Radatti	380/286
5,987,610	A *	11/1999	Franczek et al.	713/200	6,851,057	B1	2/2005	Nachenberg	
6,009,525	A	12/1999	Horstmann		2002/0004819	A1	1/2002	Agassy et al.	
6,067,410	A *	5/2000	Nachenberg	703/28	2002/0007453	A1	1/2002	Nemovicher	
6,088,803	A	7/2000	Tso et al.		2002/0073323	A1	6/2002	Myles	
6,178,505	B1	1/2001	Schneider et al.		2003/0131061	A1	7/2003	Newton et al.	
6,334,189	B1 *	12/2001	Granger et al.	713/200					
6,356,951	B1	3/2002	Gentry, Jr.						
6,357,008	B1 *	3/2002	Nachenberg	713/200					
6,389,534	B1	5/2002	Elgamal et al.						
6,393,568	B1 *	5/2002	Ranger et al.	713/188					
6,421,733	B1	7/2002	Tso et al.						
6,549,937	B1	4/2003	Auerbach et al.						
6,577,920	B1	6/2003	Hypponen et al.						
6,697,950	B1	2/2004	Ko						

OTHER PUBLICATIONS

PixelFusion Processor Now Hunting Network Apps, May 17, 200, p. 1-2.*
Redmond, T., "The Great Anti Virus Crusade", *Windows 2000 Magazine* (Apr. 2001) pp. 1-4.
Afzal, Motorola PowerPC Migration Tools—Emulation and Translation, 1996, IEEE, p. 145.

* cited by examiner

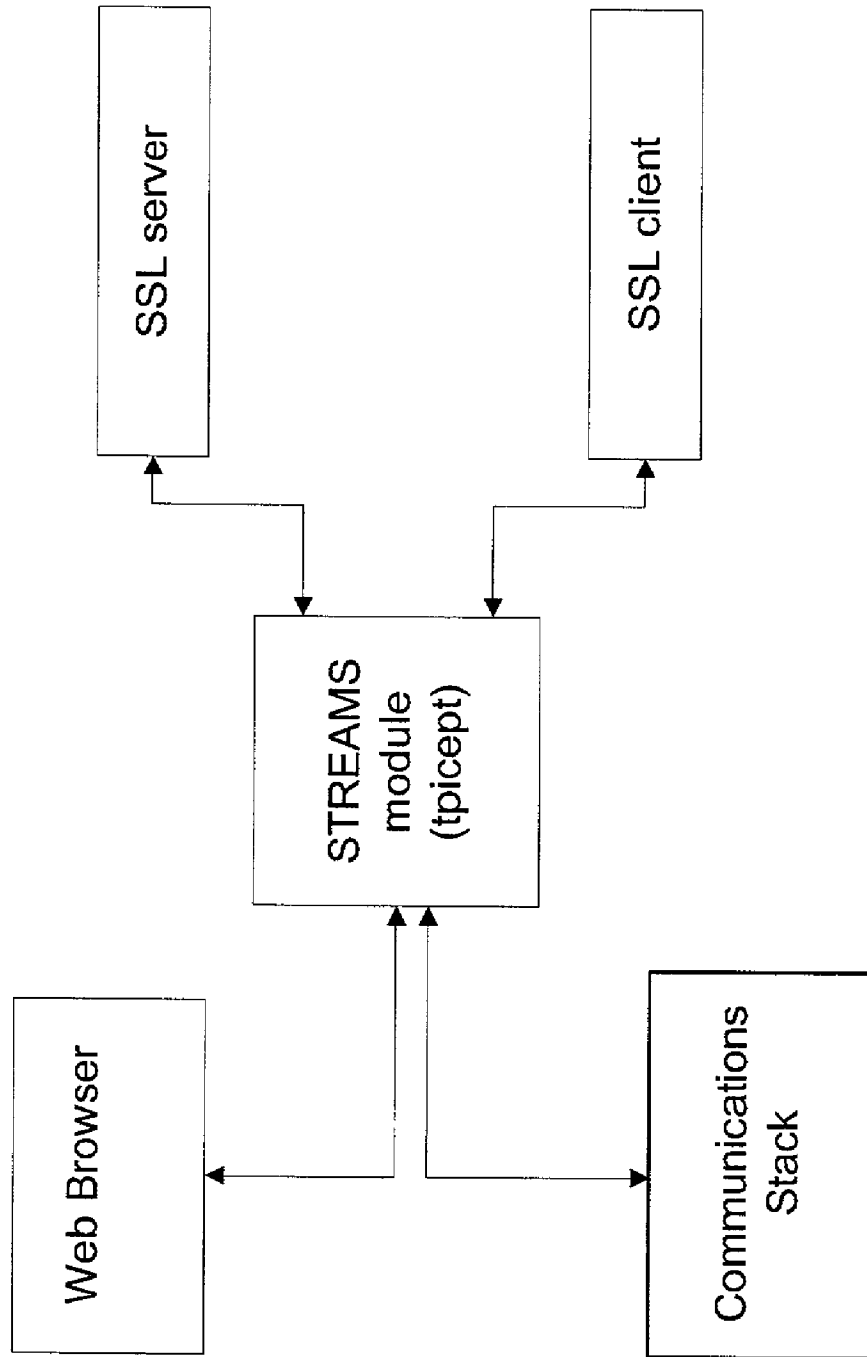


Figure 1

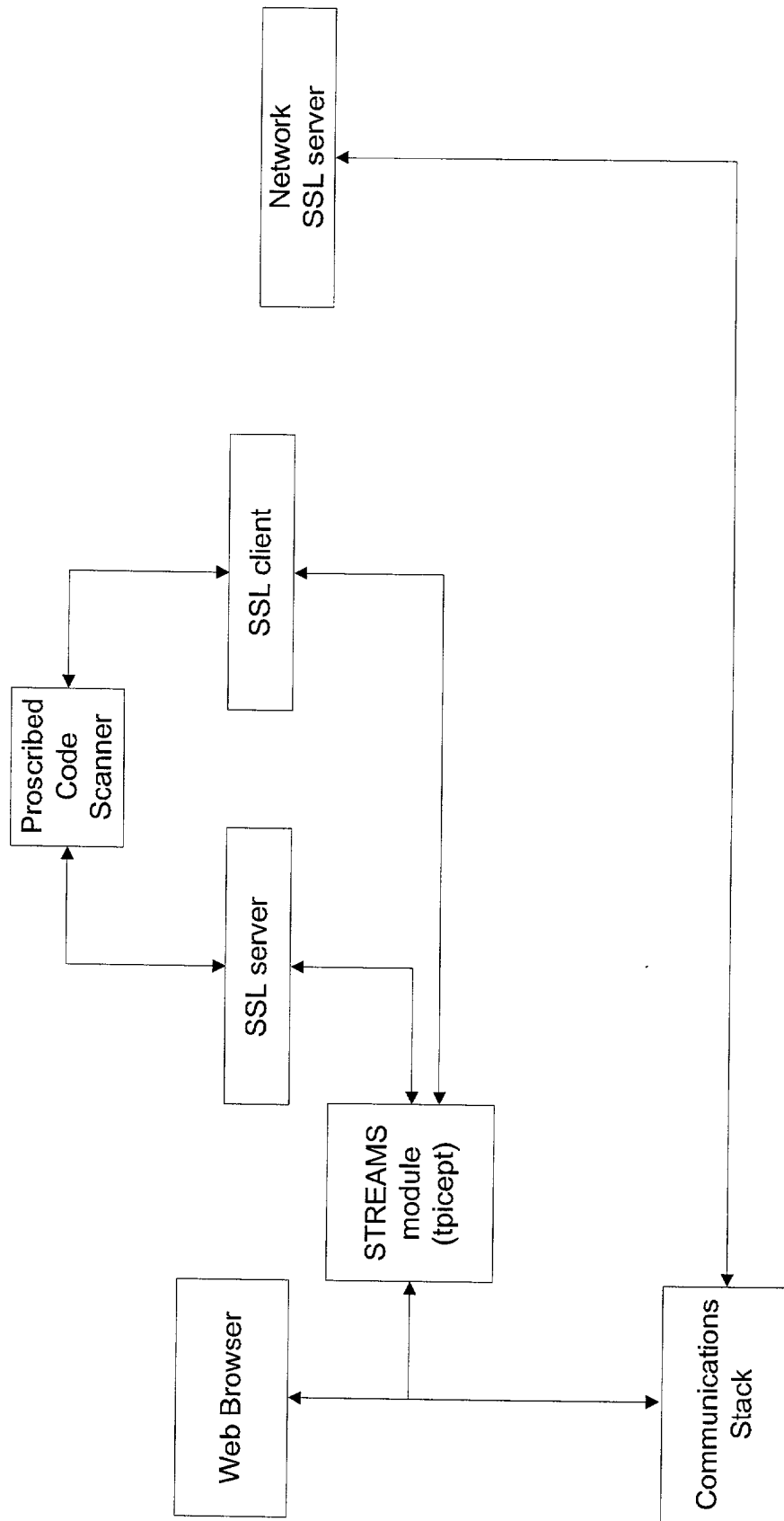


Figure 2

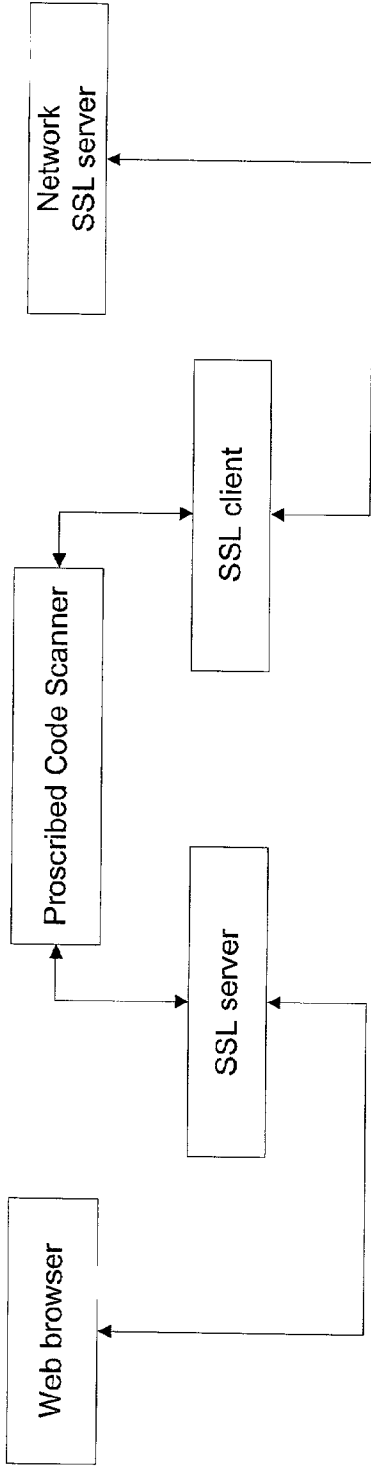


Figure 3



Figure 4

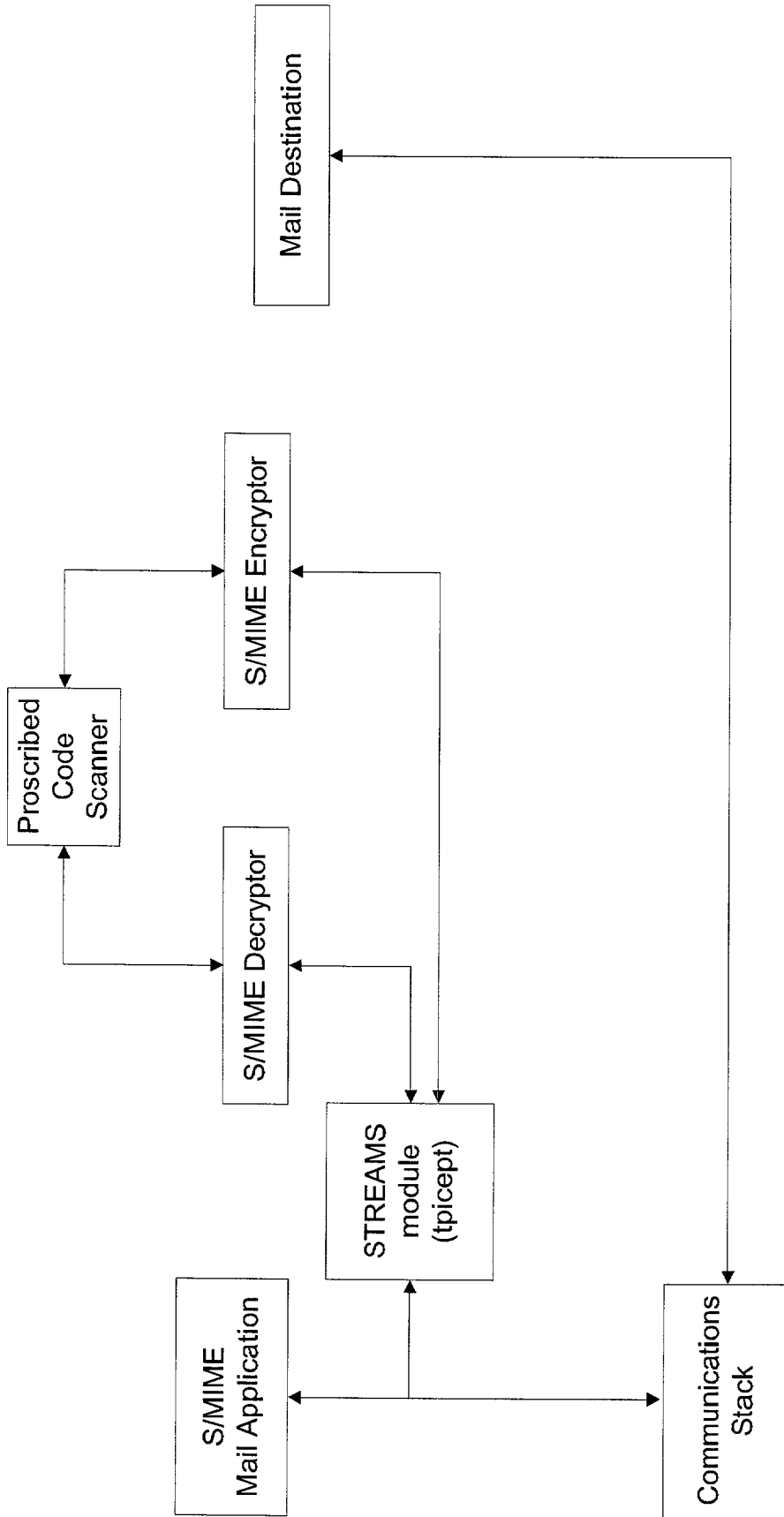


Figure 5

1

APPARATUS AND METHODS FOR INTERCEPTING, EXAMINING AND CONTROLLING CODE, DATA AND FILES AND THEIR TRANSFER

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. Ser. No. 09/244,154, entitled "NETWORK TRAFFIC INTERCEPTING METHOD AND SYSTEM," filed on Feb. 3, 1999, and issued as U.S. Pat. No. 6,763,467, on Jul. 13, 2004, by Peter V. Radatti and David J. Harding, which disclosure is incorporated herein by reference;

and is related to co-pending application Ser. No. 09/800314, entitled "APPARATUS AND METHODS FOR INTERCEPTING, EXAMINING AND CONTROLLING CODE, DATA AND FILES AND THEIR TRANSFER," filed on same date herewith, by Peter V. Radatti and Timothy R. Eliseo, which disclosure is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to apparatus and methods for intercepting, examining and controlling code, data and files and their transfer. More particularly, the present invention relates to apparatus and methods for intercepting, examining and controlling code, data and files and their transfer through secure connections.

BACKGROUND OF THE INVENTION

The rise of the Internet and networking technologies has resulted in the widespread transfer of code, data and files between computers. Transfer through the Internet and networking may be secured in a number of ways. Secure Sockets Layer (SSL) and Secure Multi-Purpose Internet Mail Extension (S/MIME) are two of the primary methods used to secure transfers. Both SSL and S/MIME use encryption to secure transfers. The transferred code, data and/or files ("code") are encrypted by the sender and decrypted by the receiver.

Secure transfers are, of course, rendered secure in order to make the code impenetrable to other applications and third parties. For example, encrypted code cannot be reviewed by a virus scanning application. The virus scanner cannot interpret the code and so cannot review the code for the presence of viruses. Accordingly, it would be desirable to provide an ability to review encrypted code.

Accordingly, it is an object of the present invention to provide apparatus and methods for intercepting, examining and controlling code and its transfer through secure connections in an efficient and effective manner transparently or almost transparently to the end-user, with little or no operational effort required by the user.

It is yet another object of the present invention to provide apparatus and methods that simply and effectively intercept, control, and/or examine incoming and outgoing secure code in an efficient and effective manner transparently or almost transparently to the end-user, with little or no operational effort required by the user.

SUMMARY OF THE INVENTION

The present invention comprises apparatus and methods for intercepting, examining, and controlling code transferred through a connection. The present invention may operate on a single computer system or multiple systems depending on

2

the operating system and other variables. The present invention may, in various embodiments, process, that is, intercept, examine, and/or control any or all code streams in a computer or network. Intercepting, examining and/or controlling code includes but is not limited to monitoring, blocking, logging, quarantining, discarding or transferring code. Although the present invention can be implemented on various platforms, the preferred embodiments are used in Unix® and various Windows® environments, such as NT, 2000, 95, 98 and Me.

The preferred embodiments monitor transfers from a system using a protocol parser which may be placed on the client system, the server system, or other intermediate system or component. In the especially preferred Unix® embodiments, the protocol parser is a Unix® STREAMS module and driver activated when an application opens a STREAMS device of the proper type. In the especially preferred Windows® NT embodiments, the protocol parser is a WinNT driver activated when an application opens a communications channel. When the parser intercepts a request from a client or server for an SSL transfer the parser creates a new SSL server that communicates with the original client and a new SSL client that communicates with the original server. The SSL server and SSL client may then intercept any and all communications that occur between the original SSL client and original SSL server.

The especially preferred embodiments insert a proscribed code scanner between the protocol server and protocol client. This proscribed code scanner may be an antivirus scanner, pattern scanner, and/or content scanner or other types and provides the ability to review the content of the SSL encrypted communications.

The preferred embodiments will also intercept and review S/MIME messages. The S/MIME messages will be intercepted by the protocol parser and sent to a S/MIME decryptor. The decrypted messages can then be scanned by a proscribed code scanner, which may be an antivirus scanner, pattern scanner, and/or content scanner or other types. The proscribed code scanner will then review the code and signal whether the S/MIME message may be released from interception.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of operation of a preferred embodiment.

FIG. 2 is a schematic diagram of operation of a preferred embodiment.

FIG. 3 is a schematic diagram of operation of a preferred embodiment.

FIG. 4 is a schematic diagram of a prior art embodiment.

FIG. 5 is a schematic diagram of operation of a preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments processes altered code. Altered code is defined herein as code altered by encryption or a communication protocol after being generated by an application or program for transmission to a complementary encryption or communication protocol. For example, both SSL and S/MIME alter code by securing code through encrypting and decrypting code on both the server and client ends of the communication. SSL is a protocol layer encryption used in TCP connections and implemented between the HTTP layer and the TCP layer. Code is encrypted as it passes