US 20110238979A1

(19) **United States**

(12) **Patent Application Publication**

Harp et al.

(10) **Pub. No.: US 2011/0238979 A1**

(43) **Pub. Date: Sep. 29, 2011**

(54) **DEVICE FOR PREVENTING, DETECTING AND RESPONDING TO SECURITY THREATS**

(75) Inventors: **Steven Alex Harp**, Coon Rapids, MN (US); **J. Thomas Haigh**, Golden Valley, MN (US); **Johnathan A. Gohde**, Arden Hills, MN (US); **Richard C. O'Brien**, Brooklyn Park, MN (US); **Charles N. Payne, JR.**, Stillwater, MN (US); **Ryan A. VanRiper**, Bloomington, MN (US)

(73) Assignee: **ADVENTIUM LABS**, Minneapolis, MN (US)

(21) Appl. No.: **12/730,201**

(22) Filed: **Mar. 23, 2010**

Publication Classification

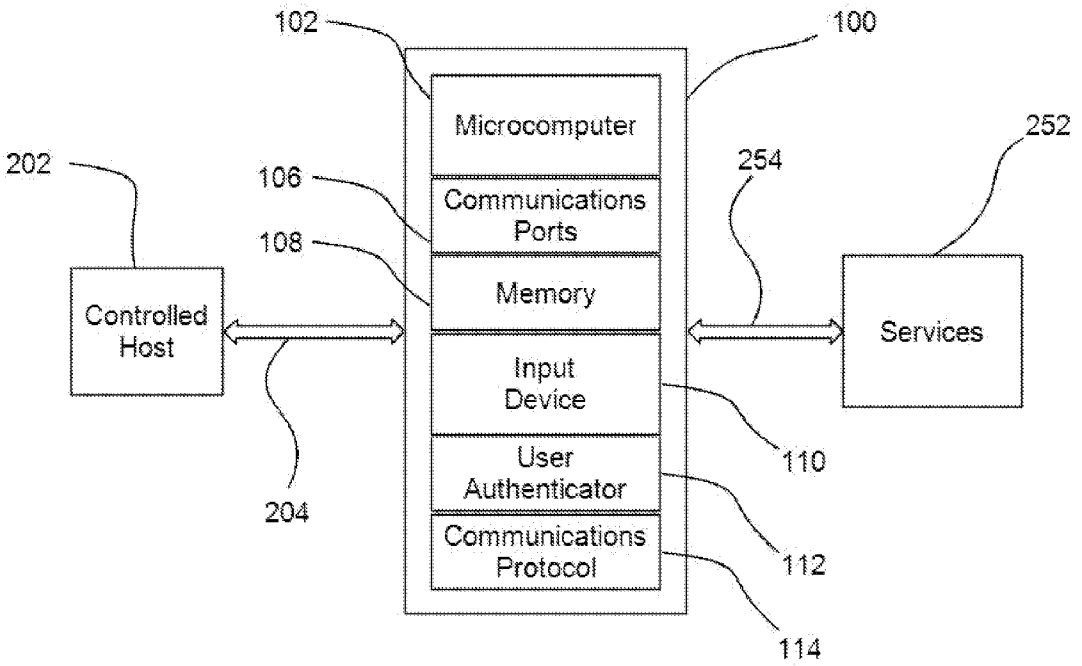
(51) **Int. Cl.**

H04L 9/32	(2006.01)
H04L 29/06	(2006.01)
G06F 21/20	(2006.01)

(52) **U.S. Cl.** **713/153**; 726/11; 713/171; 726/23

(57) **ABSTRACT**

A device to prevent, detect and respond to one or more security threats between one or more controlled hosts and one or more services accessible from the controlled host. The device determines the authenticity of a user of a controlled host and activates user specific configurations under which the device monitors and controls all communications between the user, the controlled host and the services. As such, the device ensures the flow of only legitimate and authorized communications. Suspicious communications, such as those with malicious intent, malformed packets, among others, are stopped, reported for analysis and action. Additionally, upon detecting suspicious communication, the device modifies the activated user specific configurations under which the device monitors and controls the communications between the user, the controlled host and the services.



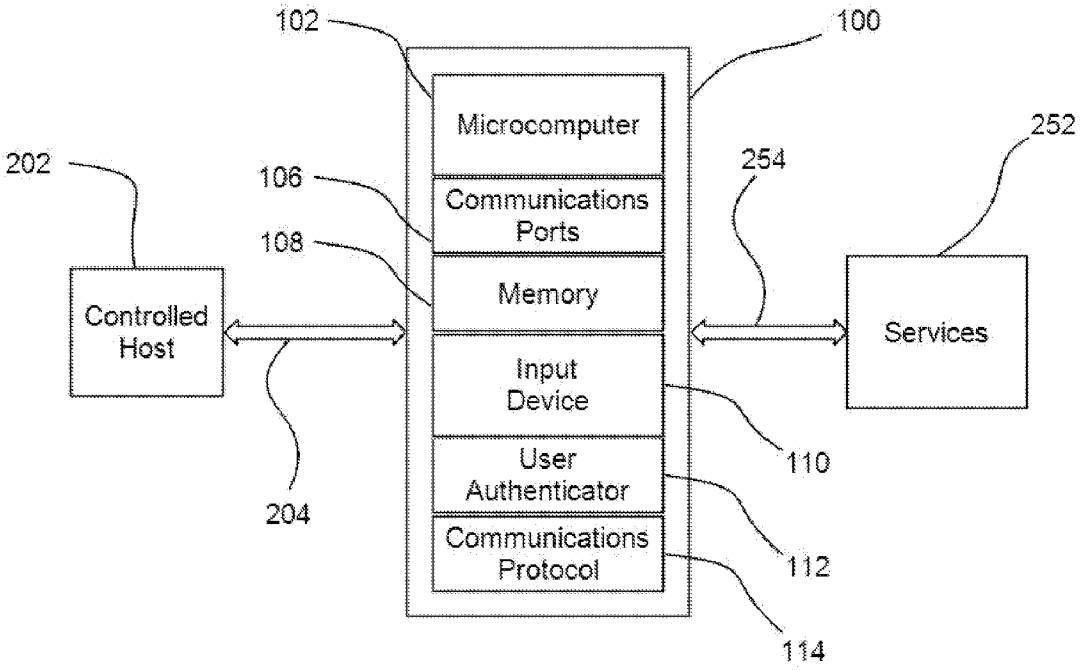

102
100
Microcomputer
252
202
106
254
Communications Ports
108
Memory
Controlled Host
Services
Input Device
110
User Authenticator
204
112
Communications Protocol
114

Fig. 1

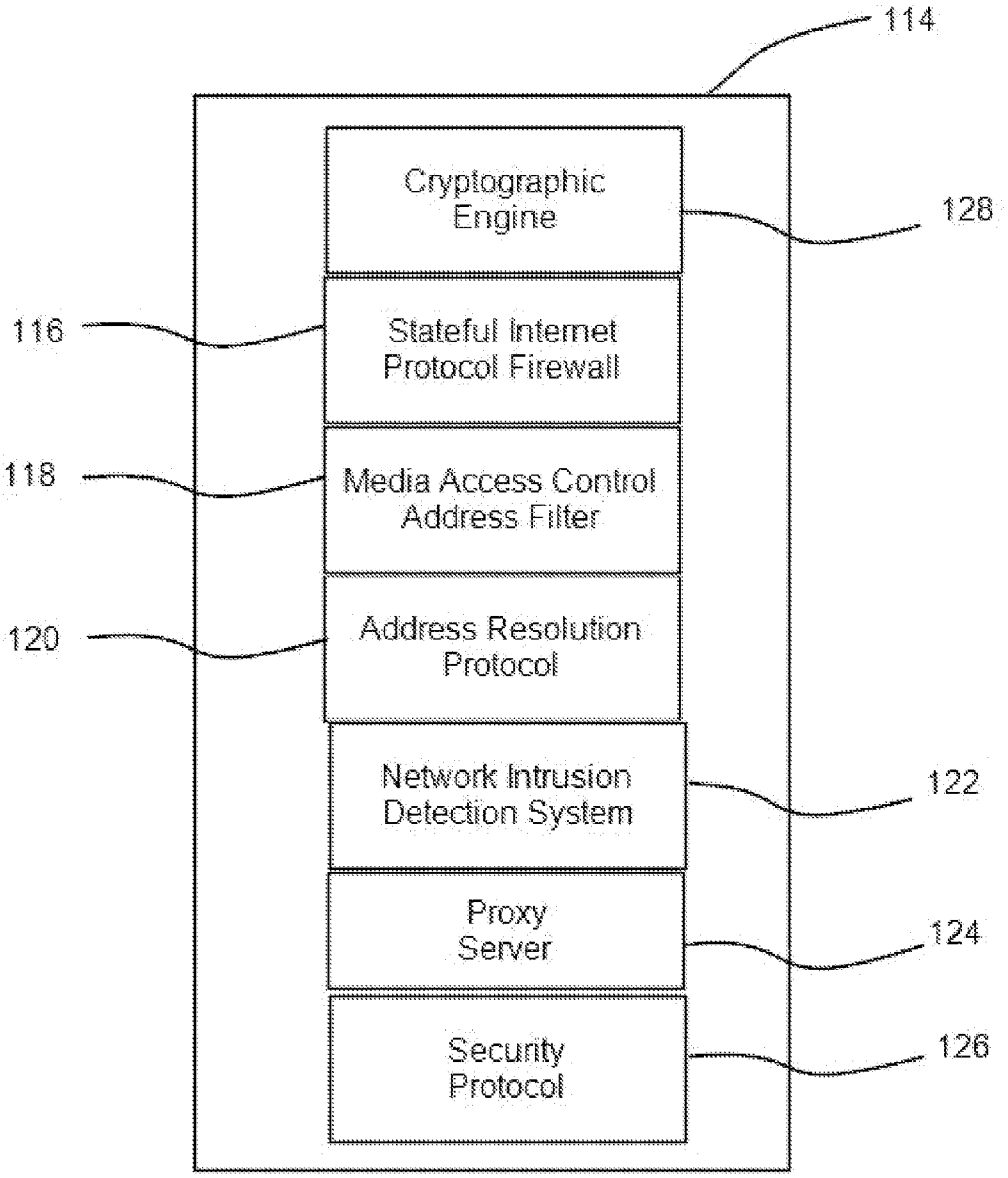

114
Cryptographic Engine
128
116
Stateful Internet Protocol Firewall
118
Media Access Control Address Filter
120
Address Resolution Protocol
Network Intrusion Detection System
122
Proxy Server
124
Security Protocol
126

Fig. 2

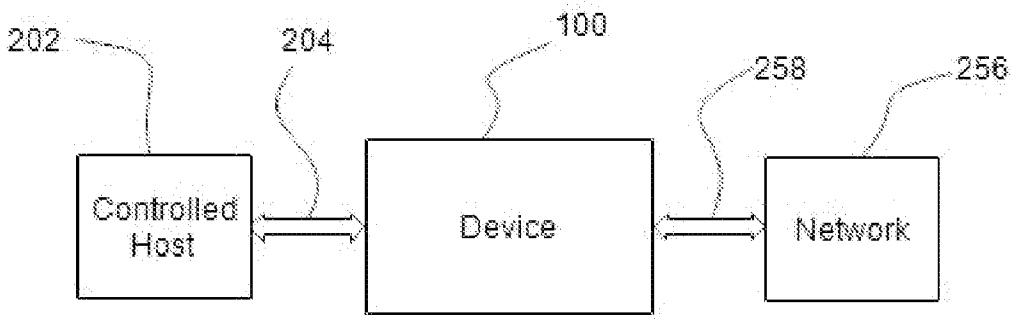


Fig. 3

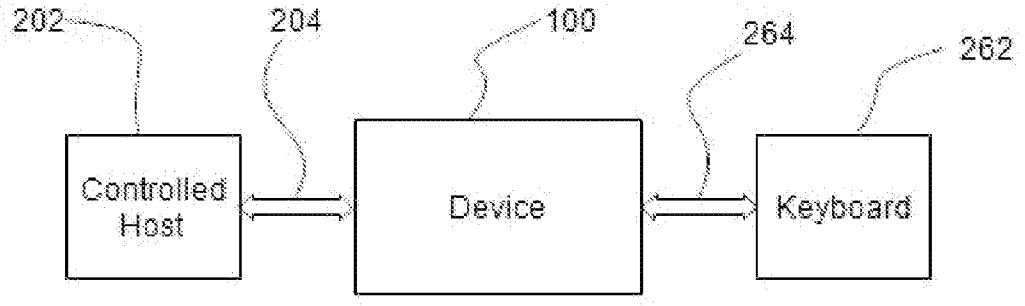


Fig. 4

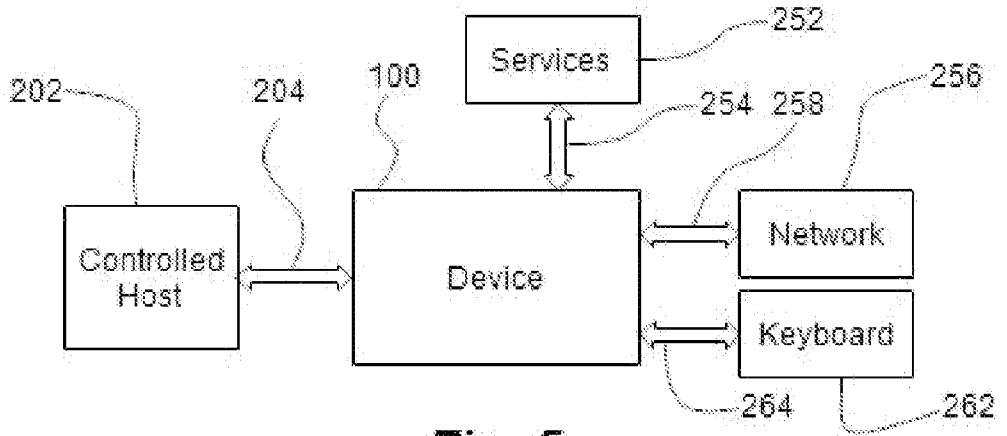


Fig. 5

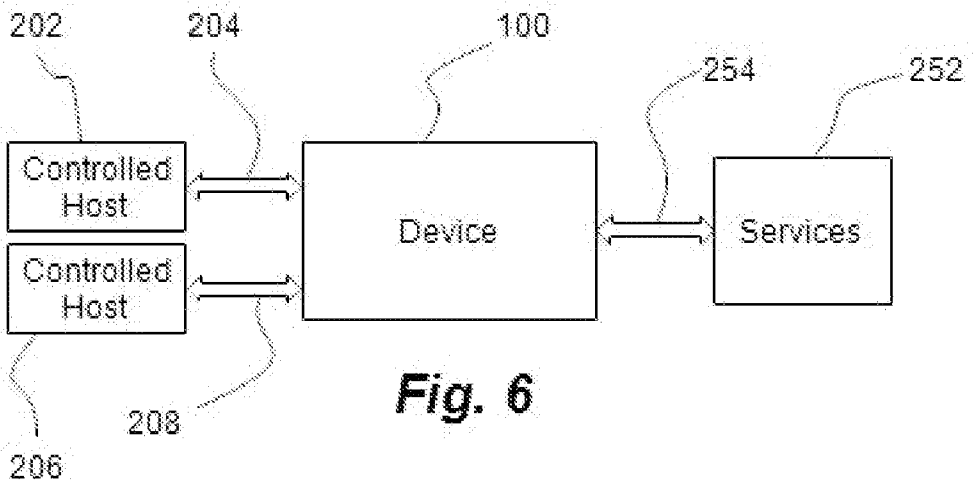


Fig. 6

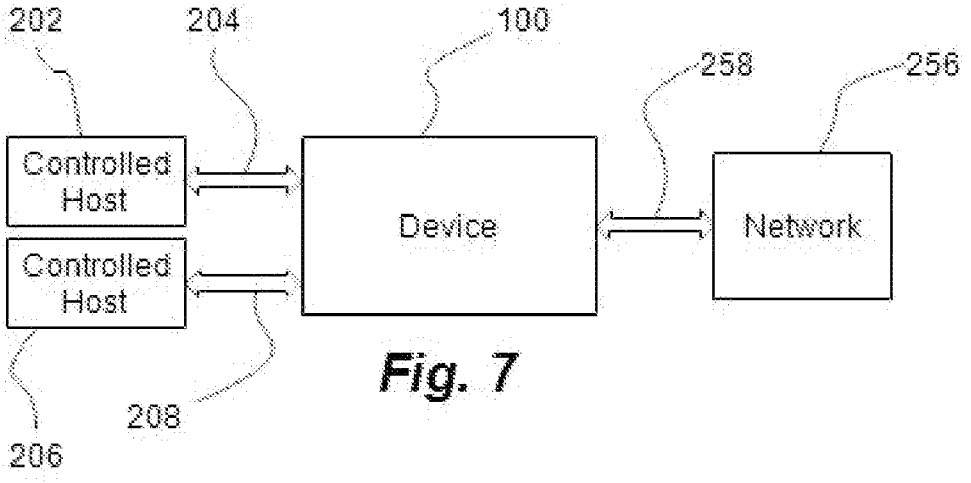


Fig. 7

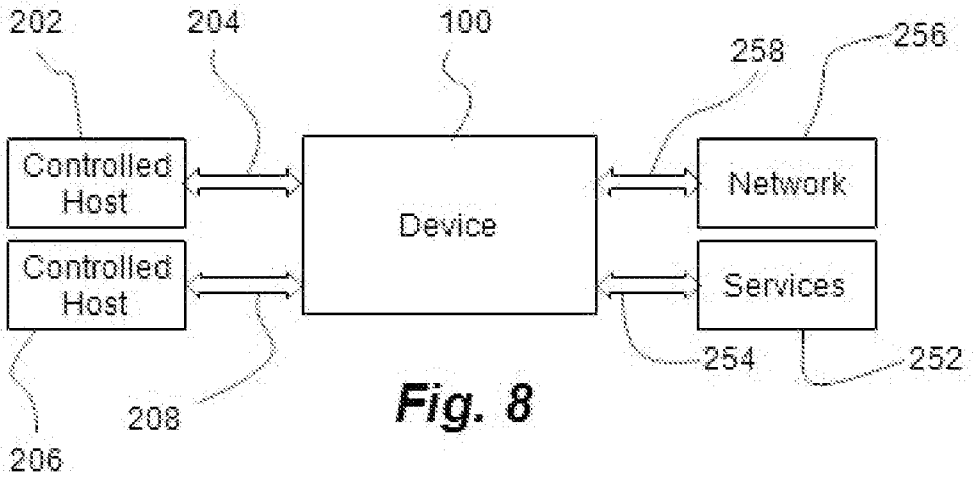


Fig. 8

DEVICE FOR PREVENTING, DETECTING AND RESPONDING TO SECURITY THREATS

TECHNICAL FIELD

[0001] The invention relates to security and safety of computer networks and computers.

BACKGROUND

[0002] In order to block intruders, computer networks have traditionally relied on a physical separation between the computer network and other networks and devices. Defenses located at the boundary of a computer network are unable to mediate secure access between controlled hosts they are trying to protect and the services that are accessible from the controlled host. As such, an intruder who gains a foothold on a controlled host can not be blocked from malicious activities.

[0003] U.S. Patent Application Publication No. 2007/0199061 (Byres et al.) teaches a network security appliance for providing security to end-point devices such as a node in an industrial environment. However, the appliance does not provide user authentication that is independent of the device being protected, and it does not provide security protections to traffic between devices being protected.

[0004] U.S. Pat. No. 7,536,715 (Markham) teaches a network interface card installed in a computer to protect the computer in which the card is installed and to protect the card itself. However, the device does not provide user authentication that is independent of the computer being protected.

[0005] In view of the foregoing, there exists a need for devices providing sophisticated prevention, detection and response capabilities against security threats.

SUMMARY

[0006] The present invention is a device to prevent, detect and respond to one or more security threats between a controlled host and one or more services connected to the controlled host. In an embodiment of the invention, the device collects information for authenticating a user of the controlled host and compares the collected information with the information for one or more user permitted to use the controlled host. If the information for the user of the controlled host matches the information for the one or more user permitted to use the controlled host, then the user is designated as an authorized user. Otherwise, the user is designated as an unauthorized user. The one or more configurations assigned for the authorized or unauthorized user of the controlled host is then activated by the device for controlling the communication between the controlled host and the one or more services. Additionally, the activated configurations also include those for identifying and preventing malicious intent.

[0007] The device includes a mechanism for cryptographically ensuring the privacy and integrity of communications between the controlled host and the one or more services. The communication is configured into one or more packets and the packets are evaluated against the rules and filters included in one or more utilities such as internet protocol tables, media access control address filters, address resolution protocol, network intrusion detection system, proxy server, and security protocol. As such, the device detects suspicious communications such as those with malicious intent, malformed packets, unauthorized activities, etc. Suspicious communications are stopped and their characteristics are logged, reported and analyzed. Suspicious communications are also used to modify the activated configurations under which the device controls the communication between the controlled host and the one or more services. The communication between the controlled host and the one or more services is compared with the activated configuration for compliance. Compliant communications are permitted to proceed and non-compliant communications are stopped.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. **1** is a block diagram of an embodiment of the invention.

[0009] FIG. **2** is a block diagram of an embodiment of the communications protocol in accordance with an embodiment of the invention.

[0010] FIG. **3** is a block diagram of another embodiment of the invention.

[0011] FIG. **4** is a block diagram of yet another embodiment of the invention.

[0012] FIG. **5** is a block diagram of an alternate embodiment of the invention.

[0013] FIG. **6** is a block diagram of another embodiment of the invention.

[0014] FIG. **7** is a block diagram of yet another embodiment of the invention.

[0015] FIG. **8** is a block diagram of an alternate embodiment of the invention.

DETAILED DESCRIPTION

[0016] While the present invention is subject to various modifications, embodiments illustrating the best mode contemplated for carrying out the invention are described in detail herein below by way of examples with reference to the included drawings. While multiple embodiments of the instant invention are disclosed, still other embodiments may become apparent to those skilled in the art. It should be clearly understood that there is no intent, implied or otherwise, to limit the invention in any form or manner to that disclosed herein. As such, all alternative embodiments of the invention are considered falling within the spirit, scope and intent of the disclosure as defined by the appended claims.

[0017] With reference to FIG. **1**, device **100**, in accordance with an embodiment of the invention, prevents, detects and responds to one or more security threats between controlled host **202** and services **252** available to a user of controlled host **202**. Device **100** includes microcomputer **102**, one or more communications ports **106**, memory **108**, input device **110**, user authenticator **112** and communications protocol **114**. As used herein, and unless stated otherwise, communications protocol **114** refers to a means for monitoring and regulating communications between controlled host **202** and services **252**.

[0018] In an embodiment of the invention, device **100** is an inline device. In another embodiment, device **100** is embedded within controlled host **202**. In an alternate embodiment, device **100** is a bump-in-the-wire device. In yet another embodiment, device **100** is a virtual device on controlled host **202**. In an embodiment of the invention, device **100** includes anti-tamper or other security features to enforce and enhance the isolation of device **100** from controlled host **202** and services **252**.

[0019] Device **100** monitors all communications between controlled host **202** and services **252**. As such, device **100** prevents, detects and responds to security threats independent

of the source and/or destination of the security threats. Security threats include any attack, failure, mistake, or other action by services **252** on controlled host **202**. Security threats also include any attack, failure, mistake, or other action by controlled host **202** on services **252**. Accordingly, device **100** prevents, detects and responds to security threats initiated from controlled host **202** and destined for one or more services **252**. Alternatively, device **100** prevents, detects and responds to security threats initiated from one or more services **252** and destined for controlled host **202**.

[0020] In an embodiment of the invention, device **100** includes communications ports **106** for connecting device **100** to controlled host **202** and services **252**. As shown in FIG. **1**, communications channels **204** and **254** respectively connect device **100** to controlled host **202** and services **252**. Communications channels **204** and **254** include, for example, one or more cross over cables, universal serial bus (USB) connections, serial cables, parallel cables, and wireless connectivity. Alternate means for communications channels **204** and **254** will be apparent to one skilled in the art. All such alternate communications channels are considered to be within the scope, spirit and intent of the instant invention.

[0021] In device **100**, memory **108** serves the typical purpose and function as in any microcomputer based device as is well known in the art. For instance, memory **108** contains information pertaining to one or more users who are permitted to use controlled host **202**. Memory **108** also contains information such as one or more configurations for each user of controlled host **202**. Additionally, memory **108** includes information and instructions for operating microcomputer **102** and device **100**. Memory **108** also contains the functional instructions for communications protocol **114** as described herein with reference to FIG. **2**.

[0022] Input device **110** is used for collecting information for authenticating a user of controlled host **202**, which information is processed by user authenticator **112** to identify the user of controlled host **202**, and to activate a configuration for that user. In an embodiment of the invention, input device **110** is one or more of a smart card reader, a biometric device, a retina scanner, a finger print scanner, a palm print scanner, and a face scanner. Alternate forms of input device **110** for collecting information for authenticating the user of controlled host **202** will be apparent to one skilled in the art. All such alternate forms of input device **110** for collecting information for authenticating the user of controlled host **202** are considered to be within the scope, spirit and intent of the instant invention.

[0023] User authenticator **112** compares the information collected about the user of controlled host **202**, as obtained through input device **110**, with the information for one or more user permitted to use controlled host **202**. If the information about the user of controlled host **202**, as obtained through input device **110**, matches the information for one or more user permitted to use the controlled host **202**, then user authenticator **112** designates the user of controlled host **202** as an authorized user. However, if the information about the user of controlled host **202**, as obtained through input device **110**, does not match the information for one or more user permitted to use the controlled host **202**, then user authenticator **112** designates the user of controlled host **202** as an unauthorized user.

[0024] As can be seen, input device **110** and user authenticator **112** in an embodiment of device **100** are independent from controlled host **202**. Such an embodiment prevents tampering or circumvention of device **100**.

[0025] In an embodiment of the invention, device **100** includes communications protocol **114** comprising means for controlling communication between controlled host **202** and services **252**. As illustrated in FIG. **2**, an embodiment of communications protocol **114** includes cryptographic engine **128**, stateful internet protocol firewall **116**, media access control address filter **118**, address resolution protocol **120**, network intrusion detection system **122**, proxy server **124** and security protocol **126**.

[0026] Cryptographic engine **128** encrypts all communications and negotiates the cryptographic keys used between controlled host **202** and services **252**. As such, cryptographic engine **128** cryptographically ensures the privacy and integrity of communications between controlled host **202** and services **252**. All communications are monitored to ensure any rogue connection is blinded. As such, only encrypted communications are permitted by device **100** and only device **100** possesses the cryptographic keys required for accessing service **252** to and from controlled host **202**.

[0027] Stateful internet protocol firewall **116** contains chains of rules for the treatment of all communications packets between controlled host **202** and service **252**. As such, device **100** has the ability to monitor the state of a connection and redirect, modify or stop communications packets based on the state of the connection, not just on the source, destination or data content of the packet. Each communications packet arriving at or leaving controlled host **202** is processed by sequentially traversing the chain of rules and each packet traverses at least one chain. Each rule in a chain contains a specification corresponding to each communication packet. As a packet traverses a chain, each rule in turn is examined. If a rule does not match the packet, the packet is passed to the next rule. If a rule does match the packet, the rule takes the action indicated by the specification, which may result in the packet being allowed to be transmitted or it may not. The packet continues to traverse the chain until either a rule matches the packet and decides the ultimate fate of the packet or the end of the chain is reached. If the end of the chain is reached without any match between the communications packet and the rules in the chain, device **100** prevents transmission of the communications packet.

[0028] Media access control addresses are unique identifiers assigned to most network adapters or network interface cards. Media access control address filter **118** filters media access control addresses and performs stateful, deep-packet inspection on its interface to controlled host **202** and its interface to services **252**.

[0029] Address resolution protocol **120** is a computer networking protocol for determining a network host's link layer or hardware address when only its internet layer or network layer address is known. In an embodiment of the invention, address resolution protocol **120** includes the address resolution protocol tables for maintaining the address resolution protocol packet filter rules. The address resolution protocol tables utility is used to create, update and view the tables that contain the filtering rules, similar to the previously described stateful internet protocol firewall **116**.

[0030] Network intrusion detection system **122** detects security threats and attacks launched from controlled host **202** such as for instance by a malicious insider. In an embodiment of communications protocol **114**, network intrusion detection system **122** performs protocol analysis, content

searching, content matching, packet logging, and real-time traffic analysis. Network intrusion detection system **122** includes both network intrusion prevention systems and network intrusion detection systems for actively blocking and/or passively detecting a variety of attacks and probes such as buffer overflows, stealth port scans, web application attacks, server message block probes, operating system fingerprinting attempts, amongst other features.

[0031] Proxy server **124** in an embodiment of communications protocol **114** acts as an intermediary for requests from clients seeking resources from providers. During any communication on a computer network, the client is controlled host **202** and the provider is services **252**. Alternatively, during a different communication, the client is services **252** and the provider is controlled host **202**. When the client requests some service from the provider, proxy server **124** evaluates the request according to its filtering rules. If the request is validated, proxy server **124** provides the resources by connecting to the relevant provider and requesting the service on behalf of the client. In an embodiment of device **100**, proxy server **124** controls and manipulates all network communication associated with an application running on controlled host **202**. Proxy server **124** compares the communication against the one or more activated configuration and permits the communication to complete if there is a match. Communication that does not match the one or more activated configuration is stopped and not permitted to proceed. As such, proxy server **124** detects and blocks malformed communication and alerts other security or monitoring components about such communication. Proxy server **124** also monitors the legitimacy of the communication to and from controlled host **202**. Communication not conforming to the rules of proxy server **124** are stopped and not permitted to proceed. In an embodiment of device **100**, proxy server **124** maintains the anonymity of the client and/or the provider, speeds up access to resources, applies access policies to services **252** or to the content of the communication, logs and/or audits usage, amongst other functions.

[0032] As shown in FIG. **2**, an embodiment of communications protocol **114** includes security protocol **126** for securing internet protocol communications by authenticating and encrypting the communication into one or more packets of data streams. Security protocol **126** also includes protocols for establishing mutual authentication between a client and a provider at the beginning of the session. During any communication on a computer network, the client is controlled host **202** and the provider is services **252**. Alternatively, during a different communication, the client is services **252** and the provider is controlled host **202**. Security protocol **126** is used to protect data flow between a client and a provider using encryption to ensure that any rogue connection between controlled host **202** and services **252** is blinded. In an embodiment of the invention, security protocol **126** is the Internet Protocol Security (IPSec) as is well known in the art.

[0033] As described in the foregoing with reference to FIGS. **1** and **2**, an embodiment of device **100** of the instant invention includes one or more mechanisms to control and manipulate communication between controlled host **202** and services **252**. In an embodiment of device **100**, memory **108** contains one or more configurations for each authorized user of controlled host **202**. Each configuration specifies how controlled host **202** can be used by each user and further specifies the one or more services **252** that are accessible to that user.

[0034] In operation, device **100** uses input device **110** and user authenticator **112** in combination to identify the user of controlled host **202** as either an authorized user or an unauthorized user. Until device **100** identifies the user as an authorized user, communications protocol **114** activates the configurations that provide only limited access to services **252** from controlled host **202**. For example, configurations enforcing a strict concept of "least privilege" are used. Alternatively, network connectivity is turned off or user inputs on controlled host **202** are not processed. Alternate embodiments of device **100** can activate configurations that provide limited access to the network or services **252** when no authorized user has been identified. For example support tasks and house-keeping functions such as back-up and patch management are permitted. In other embodiments, the activated configurations direct device **100** to ban a user from, for example, using one or more controlled hosts **202** or one or more services **252**. In another embodiment, the activated configurations direct device **100** to block network access from one or more controlled host **202** or from one or more services on controlled host **202**.

[0035] Once the user has been identified, communications protocol **114** activates configurations in accordance with the identity of the user of controlled host **202**. Such user specific configurations include, for example, filtering rules, monitoring rules, authorization rules and proxy configuration. Communications protocol **114** further activates configurations that define rogue connections and communications with malicious intent. If the authorized user is a system or network administrator, the configurations permit, for example, tasks related to auditing or tasks pertaining to security monitoring and enforcement or tasks associated with maintaining configurations for authorized users or configurations for identifying malicious communications. To one skilled in the art, it will be apparent that communications protocol **114** can activate additional, fewer, or different configurations under which device **100** prevents, detects and responds to security threats. All such alternative embodiments are considered to be within the spirit, scope and intent of the present invention. As can be seen, by activating user specific configurations, device **100** authorizes only the services **252** required by the user, the user's role, or other user specific discriminators.

[0036] Device **100** monitors and encrypts all communications between controlled host **202** and services **252** to ensure any rogue connection is blinded. As such, only encrypted communications are permitted by device **100** and only device **100** possesses the cryptographic keys required for accessing service **252** to and from controlled host **202**. Accordingly, device **100** cannot be bypassed because all communication is consistent with the user-based network authorization policies enforced by device **100**, and all communication is examined by device **100** for malicious content and/or intent. Information pertaining to such malicious communications is sent to the security and monitoring components of device **100** for examining the attributes of attacks and for implementing corrective actions. Authentication records from device **100** provide information such as which users were apparently present and which controlled host **202** the users were using before or during a particular series of events, time frame, or other criteria. For example, an attempt to transmit a maliciously crafted communication is detected by proxy server **124** and attributed to service **252** and controlled host **202** that

caused the inconsistency. Network intrusion detection system **122** detects attempts to probe the network and identify where the scans originated from.

[0037] In accordance with an embodiment of the invention, device **100** checks the integrity of communications between controlled host **202** and services **252** while preserving message metadata to help identify the nature, source and cause of a failure such as for example, the user, controlled host **202**, or service **252** responsible for the failure. Failures can include, but are not limited to, compromised or corrupted data or other inputs. Failures can also result from a delay in providing inputs or outputs. Accordingly, device **100** inspects each communication and sends the metadata about the message to security and monitoring components.

[0038] Alternate embodiments of device **100** play a key role in activities such as mitigating threats from one or more of a user, controlled host **202**, services **252**, and the nature of the communication between controlled host **202** and services **252**. In such embodiments, responses by device **100** are determined based on the activated configuration or are directed by the network security and monitoring components. For instance, device **100** reports such activities to the network security and monitoring component which, for example, conducts additional analysis of such activities. The network security and monitoring components apply reasoning to such activities and the extent to which any activity indicates malicious intent by one or more of the user, controlled host **202**, services **252**, the nature of the communication between controlled host **202** and services **252**. For activities determined to be suspicious and/or having malicious intent, the activated configurations are modified thereby changing the operation of device **100**. Such changes to the operation of device **100** include isolating controlled host **202**, isolating services **252**, and preventing the user from using controlled host **202** and/or accessing services **252**. In some embodiments, the network security and monitoring component of device **100** alerts a system administrator or a duty officer to investigate the suspicious activities. Accordingly, device **100** assures users engage only in authorized actions and thereby reduces the range of activities that can be performed by a malicious insider and simplifies analysis (manual or automated) of user activities.

[0039] Other embodiments of device **100** enable monitoring and tracking of a user's conformance (or not) to that user's known patterns of operation and workflows by reporting the user's activities between controlled host **202** and services **252**. Alternate embodiments of device **100** enable the network security and monitoring components detect when any activity fails to register completion by its deadline (or is started out of order) and report such failures.

[0040] While FIG. **1** shows one controlled host **202** and one service **252** respectively connected to device **100** via communications channels **204** and **252**, it should be understood that FIG. **1** illustrates one of many possible embodiments of network configurations wherein device **100** prevents, detects and responds to one or more security threats. Alternate embodiments of network configurations for device **100** are described herein below with reference to FIGS. **3** through **8**, inclusive.

[0041] FIG. **3** illustrates an embodiment of a network configuration wherein controlled host **202** and network **256** are respectively connected to an embodiment of device **100** via communications channels **204** and **258**. Accordingly, device **100** prevents, detects and responds to one or more security threats between controlled host **202** and network **256**.

[0042] FIG. **4** illustrates another embodiment of a network configuration wherein controlled host **202** and keyboard **262** are respectively connected to an embodiment of device **100** via communications channels **204** and **264**. Accordingly, device **100** prevents, detects and responds to one or more security threats between controlled host **202** and keyboard **262**.

[0043] FIG. **5** illustrates an alternate embodiment of a network configuration wherein communications channels **204**, **254**, **258** and **264** respectively connect device **100** to controlled host **202**, services **252**, network **256** and keyboard **262**. Accordingly, device **100** prevents, detects and responds to one or more security threats between controlled host **202** and services **252**, network **256** and keyboard **262**. Additionally, in an alternate embodiment of the network configuration of FIG. **5**, device **100** further prevents, detects and responds to one or more security threats, for example, between keyboard **262** and network **256**, between keyboard **262** and services **252**, between network **256** and services **252**, amongst others.

[0044] FIG. **6** illustrates yet another embodiment of a network configuration wherein device **100** is respectively connected to controlled host **202**, controlled host **206** and services **252** via communications channels **204**, **208** and **254**. Accordingly, device **100** prevents, detects and responds to one or more security threats between controlled host **202** and services **252** and between controlled host **206** and services **252**. Additionally, in an alternate embodiment of the network configuration of FIG. **6**, device **100** further prevents, detects and responds to one or more security threats between controlled host **202** and controlled host **206**.

[0045] FIG. **7** illustrates an embodiment of a network configuration wherein controlled host **202**, controlled host **206** and network **256** are respectively connected to device **100** via communications channels **204**, **208** and **258**. Accordingly, device **100** prevents, detects and responds to one or more security threats between controlled host **202** and network **256** and between controlled host **206** and network **256**. Additionally, in an alternate embodiment of the network configuration of FIG. **7**, device **100** further prevents, detects and responds to one or more security threats between controlled host **202** and controlled host **206**.

[0046] FIG. **8** illustrates another embodiment of a network configuration wherein communications channels **204**, **208**, **254** and **258** respectively connect device **100** to controlled host **202**, controlled host **206**, services **252**, and network **256**. Accordingly, device **100** prevents, detects and responds to one or more security threats between controlled host **202** and services **252** and network **256**, and device **100** prevents, detects and responds to one or more security threats between controlled host **206** and services **252** and network **256**. Additionally, in an alternate embodiment of the network configuration of FIG. **8**, device **100** further prevents, detects and responds to one or more security threats, for example, between controlled host **202** and controlled host **206**, between services **252** and network **256**, amongst others.

[0047] As can be seen, alternate network configurations include one or more controlled host **202** even though only one such controlled host **202** has been shown and discussed with reference to some of the embodiments described in the foregoing. Controlled host **202** is one or more of a computer, a laptop, a processing device, or other device with one or more processors embedded therein. Similarly, alternate network configurations include one or more service **252** even though only one such service **252** has been shown and discussed with

reference to some of the embodiments described in the foregoing. Accordingly, as used throughout this disclosure and as discussed in the foregoing, services **252** implies one or more of network **256**, one or more keyboard **262**, one or more network switches, one or more servers, amongst others.

[0048] Embodiments of network configurations described in the foregoing with reference to FIGS. **3** through **8**, inclusive, have been limited for discussion and illustrative purposes. Additional and alternate embodiments of the various network configurations will be apparent to one skilled in the art, and all such embodiments are considered to be within the spirit, scope and intent of the present invention.

[0049] Various modifications can be made to the embodiments presented herein without departing from the spirit, scope and intent of the present invention. All such alternatives, modifications, and variations are considered as being within the spirit, scope and intent of the instant invention as defined by the appended claims and all equivalents thereof.

What is claimed is:

1. A device to prevent, detect and respond to one or more security threats between a controlled host and one or more services connected to the controlled host, the device comprising

a microcomputer;

one or more communications ports for connecting the device to

the controlled host; and

the one or more services connected to the controlled host;

memory for storing

information pertaining to one or more user permitted to use the controlled host; and

one or more configuration for communication between the controlled host and the one or more services;

input device for collecting information for authenticating a user of the controlled host;

a user authenticator; and

communications protocol for controlling communications between the controlled host and the one or more services.

2. The device of claim **1**, wherein the communications protocol

includes a cryptographic engine;

monitors communication between the controlled host and the one or more services;

includes stateful internet protocol firewall;

filters communications based on media access control addresses;

proxies address resolution protocol;

includes a network intrusion detection system;

includes a proxy server; and

applies security protocol to the communication between the controlled host and the one or more services.

3. The device of claim **2**, wherein the security protocol is the Internet Protocol Security (IPSec).

4. The device of claim **3**, wherein the cryptographic engine

negotiates cryptographic keys between the controlled host and the one or more services;

encrypts communications between the controlled host and the one or more services; and

ensures privacy and integrity of communications between the controlled host and the one or more services.

5. The device of claim **4**, wherein the user authenticator

compares the information pertaining to the user of the controlled host with the information pertaining to the one or more user permitted to use the controlled host; and

designates the user of the controlled host as one of

an authorized user if the information pertaining to the user of the controlled host matches the information pertaining to the one or more user permitted to use the controlled host; and

an unauthorized user if the information pertaining to the user of the controlled host does not match the information pertaining to the one or more user permitted to use the controlled host.

6. The device of claim **5**, wherein the one or more user specific configuration for communication comprises one or more of

filtering rules;

monitoring rules;

authorization rules; and

proxy configurations.

7. The device of claim **6**, wherein

the one or more configuration for communication is for the authorized user;

the one or more configuration for communication is for the unauthorized user; and

the one or more configuration for communication is for preventing malicious intent.

8. The device of claim **7**, wherein the communications protocol activates and controls communication between the controlled host and the one or more services with

the one or more configuration for communication for preventing malicious intent;

the one or more configuration for communication for the authorized user if the user authenticator designates the user of the controlled host as the authorized user; and

the one or more configuration for communication for the unauthorized user if the user authenticator designates the user of the controlled host as the unauthorized user.

9. The device of claim **8**, wherein the communications protocol

compares the one or more activated configuration with the communication between the controlled host and the one or more services;

authorizes the communication if the communication is in compliance with the one or more activated configurations;

prevents the communication if the communication is not in compliance with the one or more activated configurations; and

changes the activated configurations upon detecting communications comprising one or more of

malicious intent; and

malformed packets.

10. The device of claim **9**, wherein the user is prevented from using one or more of

the controlled host; and

one or more services.

11. The device of claim **10**, wherein the controlled host is prevented from accessing one or more services.

12. The device of claim **11**, wherein the means for connecting the device to the controlled host and to the one or more services comprises one or more of

a cross-over cable;
a universal serial bus connection;
a serial cable;
a parallel cable; and
wireless connectivity.

13. The device of claim **12**, wherein the input device for collecting information for authenticating a user of the controlled host includes one or more of
a smart card reader;
a biometric device;
a retina scanner;
a finger print scanner;
a palm print scanner; and
a face scanner.

14. The device of claim **13**, wherein the one or more services includes one or more of
a computer network;
a display unit;
a keyboard; and
a mouse.

15. The device of claim **14** connected to a network switch, wherein the device prevents, detects and responds to one or more security threats between one or more controlled host and one or more services connected to the network switch.

16. A method for preventing, detecting and responding to one or more security threats between a controlled host and one or more services connected to the controlled host, the method comprising the steps of
collecting information for authenticating a user of the controlled host;
comparing the information of the user of the controlled host with information for one or more user permitted to use the controlled host;
designating the user of the controlled host as one of
an authorized user if the information pertaining to the user of the controlled host matches the information pertaining to the one or more user permitted to use the controlled host; and
an unauthorized user if the information pertaining to the user of the controlled host does not match the information pertaining to the one or more user permitted to use the controlled host;
activating one or more configurations for communication between the controlled host and the one or more services, wherein the one or more activated configuration comprises
configurations associated with the user of the controlled host;
configuration for preventing malicious intent; and
configuration for one of
the authorized user; and
the unauthorized user.

17. The method of claim **16**, further comprising the steps of
negotiating cryptographic keys between the controlled host and the one or more services;
monitoring communication between the controlled host and the one or more services;
configuring the communication between the controlled host and the one or more services into one or more packets;
evaluating internet protocol tables;
filtering media access control address;
applying address resolution protocol;
checking for network intrusion detection;
evaluating the one or more packets with a proxy server; and
applying security protocol to the communication between the controlled host and the one or more services.

18. The method of claim **17**, further comprising the steps of
comparing the one or more activated configuration with the communication between the controlled host and the one or more services;
authorizing the communication if the communication is in compliance with the one or more activated configuration;
preventing the communication if the communication is not in compliance with the one or more activated configuration; and
changing the activated configurations upon detecting communications comprising one or more of
malicious intent; and
malformed packets.

19. A device to prevent, detect and respond to one or more security threats between a controlled host and one or more services connected to the controlled host, the device comprising
means for collecting information for authenticating a user of the controlled host;
means for comparing the information of the user of the controlled host with information for one or more user permitted to use the controlled host;
means for designating the user of the controlled host as one of
an authorized user if the information pertaining to the user of the controlled host matches the information pertaining to the one or more user permitted to use the controlled host; and
an unauthorized user if the information pertaining to the user of the controlled host does not match the information pertaining to the one or more user permitted to use the controlled host;
means for activating one or more configurations for communication between the controlled host and the one or more services, wherein the one or more activated configuration comprises
configurations associated with the user of the controlled host;
configuration for preventing malicious intent; and
configuration for one of
the authorized user; and
the unauthorized user.

20. The device of claim **19**, further comprising
means for negotiating cryptographic keys between the controlled host and the one or more services;
means for monitoring communication between the controlled host and the one or more services;
means for configuring the communication between the controlled host and the one or more services into one or more packets;
means for evaluating internet protocol tables;
means for filtering media access control address;
means for applying address resolution protocol;
means for checking for network intrusion detection;
means for evaluating the one or more packets with a proxy server;

means for applying security protocol to the communication between the controlled host and the one or more services;

means for comparing the one or more activated configuration with the communication between the controlled host and the one or more services;

means for authorizing the communication if the communication is in compliance with the one or more activated configuration;

means for preventing the communication if the communication is not in compliance with the one or more activated configuration; and

means for changing the activated configurations upon detecting communications comprising one or more of malicious intent; and

malformed packets.

* * * * *