US 20020188866A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0188866 A1**

Ca et al. (43) **Pub. Date: Dec. 12, 2002**

(54) **METHOD AND APPARATUS FOR PROTECTING A DEVICE CONNECTED TO A NEWTWORK**

(76) Inventors: **Jalaludeen Ca**, Karnataka (IN); **Nandakumar Gn**, Karnataka (IN)

Correspondence Address:
Kevin M. Mason
Ryan, Mason & Lewis, LLP
Suite 205
1300 Post Road
Fairfield, CT 06430 (US)

(21) Appl. No.: **09/876,568**

(22) Filed: **Jun. 7, 2001**

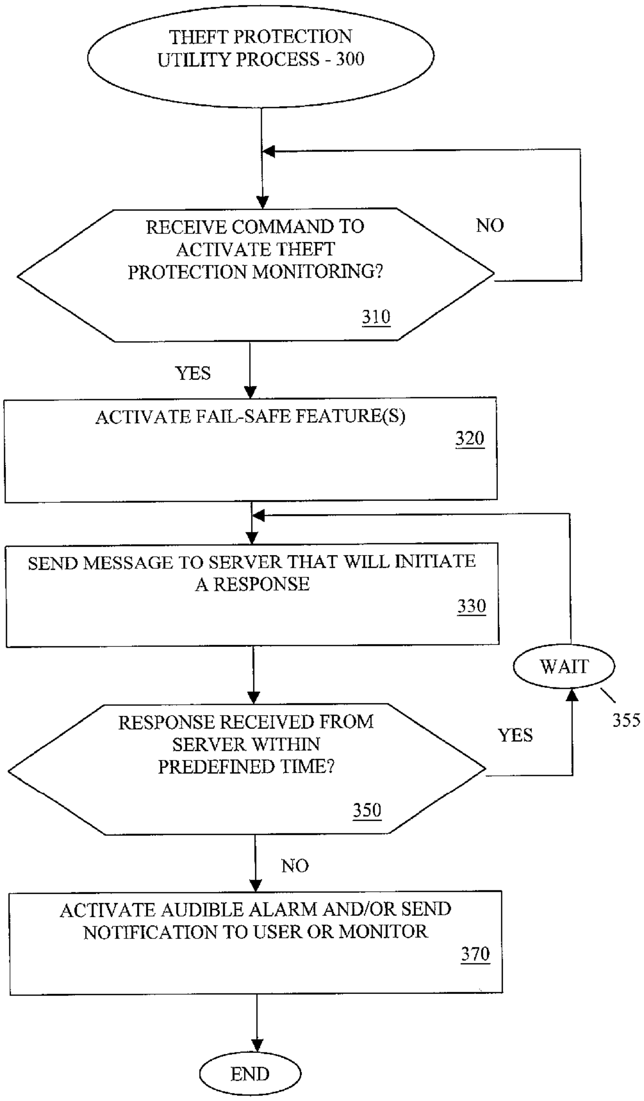
Publication Classification

(51) **Int. Cl.^{7}** **G06F 11/30**

(52) **U.S. Cl.** **713/201**

(57) **ABSTRACT**

A method and apparatus are disclosed for detecting the removal of a device connected to a network. The present invention generates an alarm on a protected device when an unauthorized user disconnects the device from a network connection. The network connection is monitored and an alarm is generated if the protected device is disconnected from the network connection without proper notification to the theft protection utility. A number of fail-safe features can optionally be employed to ensure that the theft protection aspects of the present invention are not bypassed. For example, the theft protection utility process can employ speaker, volume and/or power control features to ensure that the alarms generated by the present invention, or the theft protection feature itself, cannot be bypassed.


THEFT PROTECTION UTILITY PROCESS - 300
RECEIVE COMMAND TO ACTIVATE THEFT PROTECTION MONITORING?
310
NO
YES
ACTIVATE FAIL-SAFE FEATURE(S)
320
SEND MESSAGE TO SERVER THAT WILL INITIATE A RESPONSE
330
WAIT
355
RESPONSE RECEIVED FROM SERVER WITHIN PREDEFINED TIME?
350
YES
NO
ACTIVATE AUDIBLE ALARM AND/OR SEND NOTIFICATION TO USER OR MONITOR
370
END

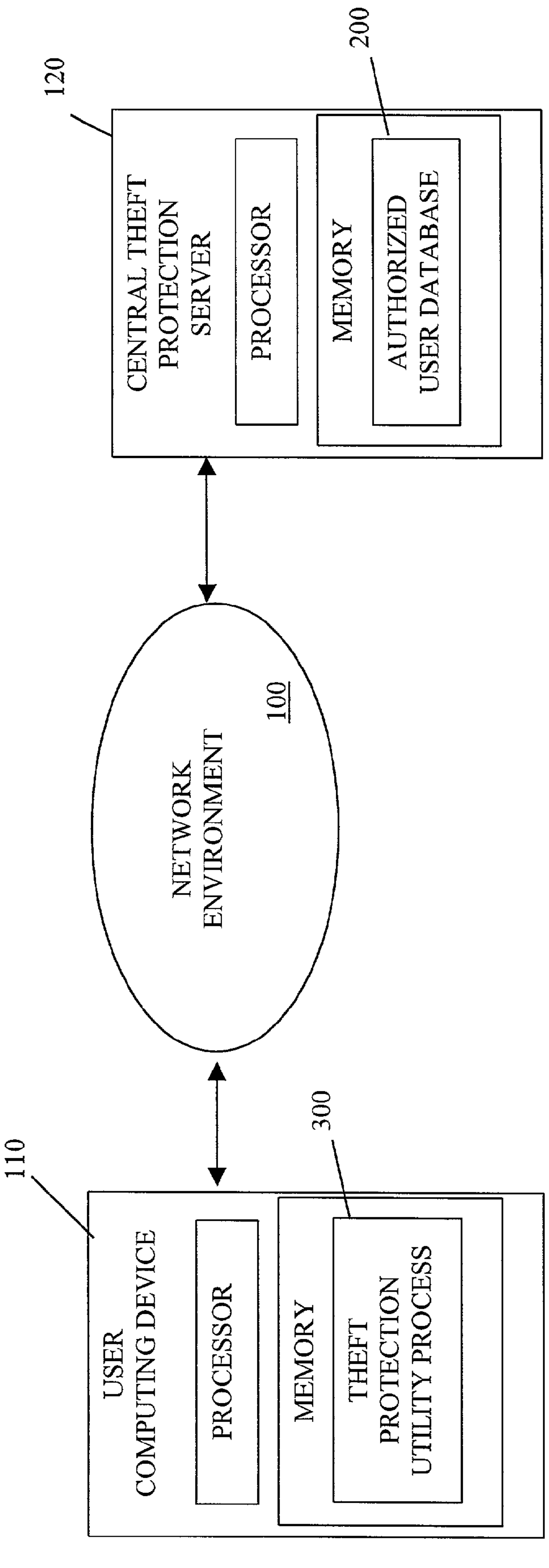
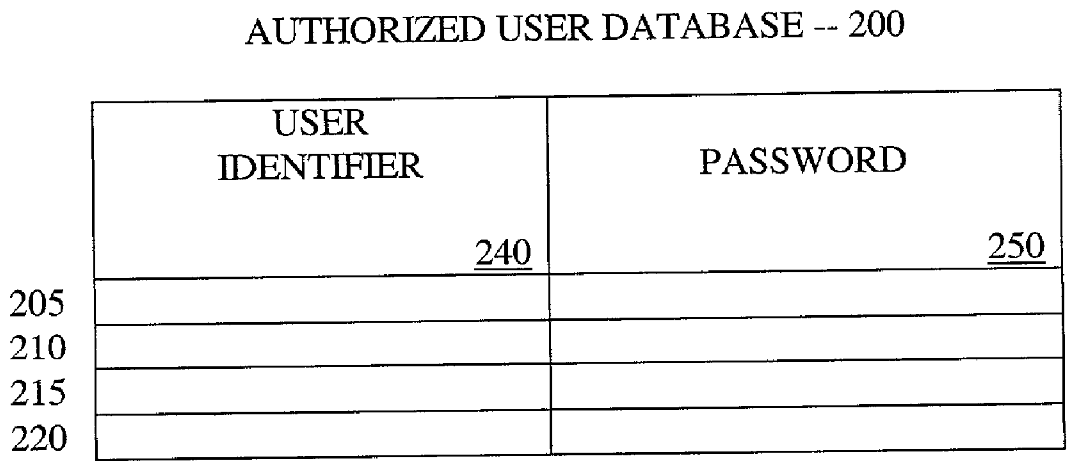

120
CENTRAL THEFT PROTECTION SERVER
PROCESSOR
MEMORY
200
AUTHORIZED USER DATABASE
NETWORK ENVIRONMENT
100
110
USER COMPUTING DEVICE
PROCESSOR
MEMORY
300
THEFT PROTECTION UTILITY PROCESS

FIG. 1



AUTHORIZED USER DATABASE -- 200

	USER IDENTIFIER 240	PASSWORD 250
205		
210		
215		
220		

FIG. 2

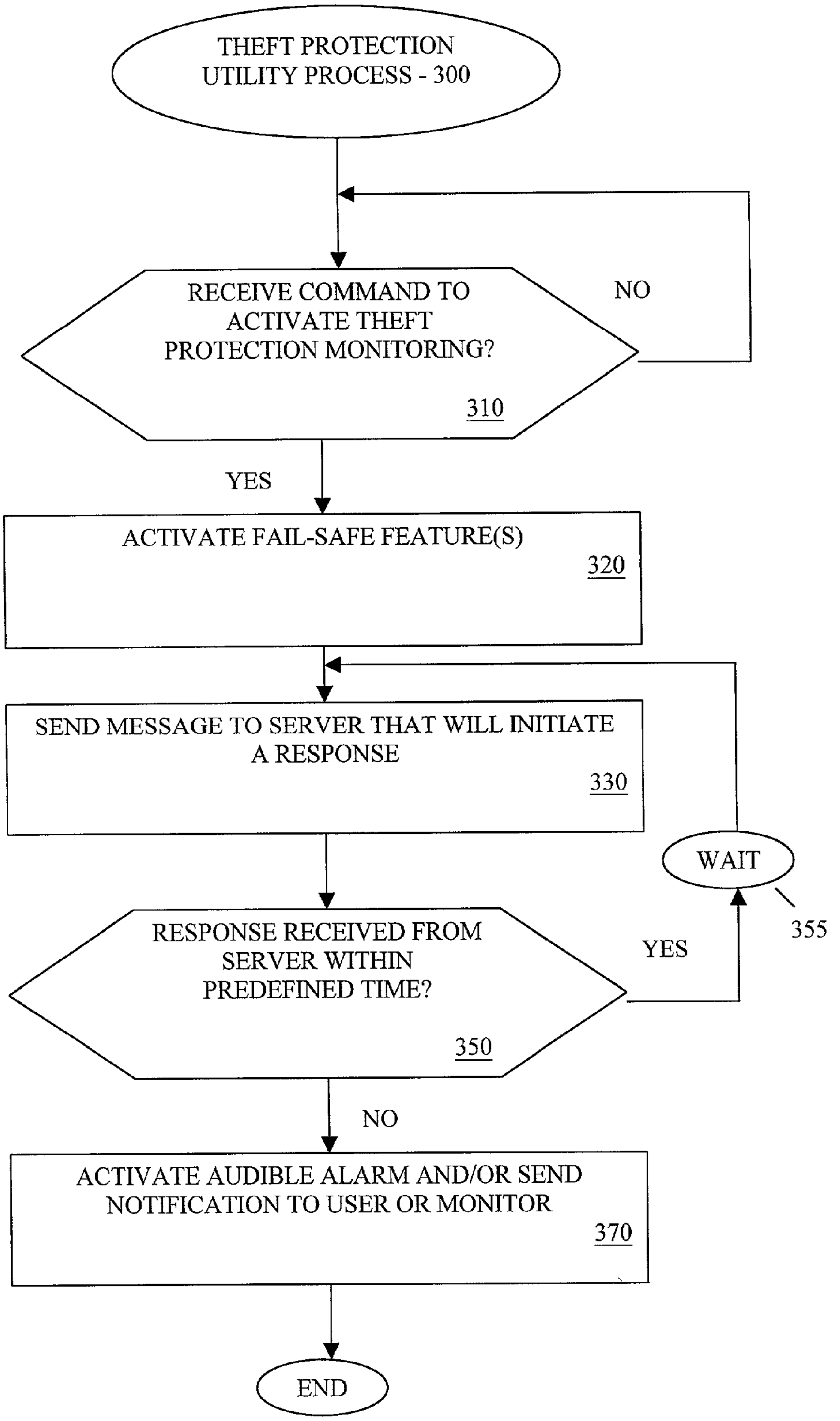

THEFT PROTECTION UTILITY PROCESS - 300
RECEIVE COMMAND TO ACTIVATE THEFT PROTECTION MONITORING?
310
NO
YES
ACTIVATE FAIL-SAFE FEATURE(S)
320
SEND MESSAGE TO SERVER THAT WILL INITIATE A RESPONSE
330
WAIT
355
RESPONSE RECEIVED FROM SERVER WITHIN PREDEFINED TIME?
350
YES
NO
ACTIVATE AUDIBLE ALARM AND/OR SEND NOTIFICATION TO USER OR MONITOR
370
END

FIG. 3

METHOD AND APPARATUS FOR PROTECTING A DEVICE CONNECTED TO A NEWTWORK

FIELD OF THE INVENTION

[0001] The present invention relates generally to computer security techniques, and more particularly, to methods and apparatus for preventing the removal of a portable computer connected to a network.

BACKGROUND OF THE INVENTION

[0002] It is an unfortunate fact of modern life that laptop computers and other portable devices are often stolen. The financial loss to the owner of the device must be measured in terms of the fair market value of the stolen item, as well as the value of any data or other information that was stored on the stolen device. Thus, the actual costs of such a loss can often be significant, especially when the data or information stored on the stolen device includes proprietary or non-recoverable information. Significantly, the trend in the consumer marketplace is towards ever smaller and lighter electronic devices, thereby making such devices even easier to conceal and steal.

[0003] A number of mechanical techniques have been proposed to prevent the theft of such devices. For example, a number of physical locks are commercially available that allow a user to secure a laptop or another device. Such hardware solutions, however, require the user to carry around additional hardware and increase the size and weight of the portable device. A need therefore exists for a mechanism to prevent the theft of a portable device that does not require the user to carry around additional hardware. A further need exists for a software-based mechanism to prevent theft of a portable device. Yet another need exists for a method and apparatus for preventing theft of a portable device that does not increase the size or weight of the portable device.

SUMMARY OF THE INVENTION

[0004] Generally, a method and apparatus are disclosed for detecting the removal of a device connected to a network. The present invention generates an alarm on a protected device when an unauthorized user disconnects the device from a network connection. A theft protection utility process monitors the network connection and generates an alarm if the protected device is disconnected from the network connection without proper notification to the theft protection utility process.

[0005] The present invention optionally incorporates a number of fail-safe features that ensure that the theft protection aspects of the present invention cannot be bypassed. For example, the theft protection utility process of the present invention can employ speaker, volume and/or power control features to ensure that the alarms generated by the present invention, or the theft protection feature itself, cannot be bypassed.

[0006] A more complete understanding of the present invention, as well as further features and advantages of the present invention, will be obtained by reference to the following detailed description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] **FIG. 1** illustrates an exemplary network environment in which the present invention can operate;

[0008] **FIG. 2** is a sample table from the authorized user database maintained by the central theft protection server of **FIG. 1**; and

[0009] **FIG. 3** is a flow chart describing an exemplary theft protection utility process incorporating features of the present invention and implemented by the user computer device of **FIG. 1**.

DETAILED DESCRIPTION

[0010] **FIG. 1** illustrates a network environment **100** in which the present invention can operate. As shown in **FIG. 1, a** user computing device **110** is connected over a network **100** to one or more servers **120**. According to one aspect of the present invention, an alarm on the user computing device **110** is automatically triggered when the device is disconnected from a network connection by an unauthorized user. It is noted that the user computing device **110** is only one example of a device that may be protected using the present invention. The present invention may be employed to prevent the unauthorized removal of any device having a connection to a network, as would be apparent to a person of ordinary skill in the art based on the disclosure herein.

[0011] Thus, the user computing device **110** may be embodied, for example, as any device that can be connected to a network **100**, such as a portable computer, workstation or personal digital assistant (PDA). The network **100** may be embodied as any wired or wireless local or wide area network (LAN or WAN, respectively), including the Public Switched Telephone Network (PSTN), a corporate intranet or the Internet (World Wide Web), or any combination of the foregoing. In another variation, the network **100** may be embodied as a cable network, an optical network or a digital satellite service (DSS) network for distributing media content. In such as media distribution network environment, the user computing device **110** may be embodied, for example, as a set-top terminal, cable-enabled media player (e.g., a television) or another decryption device. In the exemplary embodiment of the present invention, the user computing device **110** communicates with a special-purpose central theft protection server **120** over the network **100**. However, the functions performed by the central theft protection server **120** in accordance with the present invention can be performed by any server or computer connected to a network, as would be apparent to a person of ordinary skill in the art based on the disclosure herein.

[0012] As shown in **FIG. 1**, the memory of the central theft protection server **120** includes an authorized user database **200**, discussed below in conjunction with **FIG. 2**. Generally, the authorized user database **200** identifies each authorized user of the network **100** and provides a corresponding password that may be utilized in various embodiments of the present invention to prevent theft of the user computing device **110**. In addition, the memory of the user computing device **110** includes a theft protection utility process **300**, discussed below in conjunction with **FIG. 3**. In the exemplary embodiment, the user computing device **110** employs the theft protection utility process **300** to monitor the network connection and generate an alarm if the user computing device **110** is disconnected from the network connection without proper notification to the theft protection utility process **300**.

[0013] **FIG. 2** is a sample table from the authorized user database **200** maintained by the central theft protection server **120** of **FIG. 1**. Generally, the authorized user database **200** identifies each authorized user of the network **100** and provides a corresponding password that may be utilized in various embodiments of the present invention to prevent theft of the user computing device **110**. Thus, as shown in **FIG. 2**, the authorized user database **200** includes a plurality of records **205-220**, each associated with a different authorized user. For each user identified in field **240**, the authorized user database **200** indicates the user's password in field **255**. In this manner, when the user attempts to remove the user computing device **110** from the network connection, the user can optionally be prompted by the central theft protection server **120** to enter a password.

[**0014**] **FIG. 3** is a flow chart describing an exemplary theft protection utility process **300** incorporating features of the present invention. Generally, the user computing device **110** employs the theft protection utility process **300** to monitor the network connection and generate an alarm if the user computing device **110** is disconnected from the network connection without proper notification to the theft protection utility process **300**.

[**0015**] As shown in **FIG. 3**, the theft protection utility process **300** initially performs a test during step **310** to determine if a command is received to activate the theft monitoring protection feature provided by the utility process **300**. For example, a command to activate the theft protection utility process **300** may be automatically generated when power is applied to the user computing device **110** or whenever a network connection is present. In addition, the activation may be passive or active, as would be apparent to a person of ordinary skill in the art, and may optionally be combined with password protection to activate and deactivate the theft protection utility process **300**. In an active embodiment, the user can manually invoke the utility before leaving the device **110**. In a passive embodiment, the theft protection utility process **300** can be automatically activated, for example, if the user computing device **110** is inactive for a period of time, such as when a screensaver is activated.

[**0016**] If it is determined during step **310** that such a command is not received to activate the theft monitoring protection feature, then program control returns to step **310**, which will be periodically reexecuted to determine if the process is activated. If, however, it is determined during step **310** that a command is received to activate the theft monitoring protection feature, then fail-safe features of the present invention are optionally activated during step **320**. The theft protection utility process **300** optionally incorporates a number of fail-safe features that ensure that the theft protection aspects of the present invention cannot be bypassed. For example, the theft protection utility process **300** can employ:

[**0017**] (i) a speaker control feature that ensures that a speaker associated with the user computing device **110** cannot be disconnected, to thereby prevent an alarm from being heard;

[**0018**] (ii) a volume control feature that ensures that the volume of the speaker cannot be turned down or muted;

[**0019**] (iii) a power control feature that ensures that an unauthorized user cannot turn off the power of the device and bypass the theft protection utility (e.g., disable the power/reset switch automatically while the theft protection utility process **300** is active); or

[**0020**] (iv) a combination of the foregoing.

[**0021**] Thereafter, the theft protection utility process **300** will send a message to the central theft protection server **120** during step **330** that will initiate a response. In this manner, the theft protection utility process **300** polls the server **120** to ensure that a network connection is present. In further variations, the theft protection utility process **300** can poll one or more network ports on the user computing device **110** to see if they are connected or listen for a "heartbeat" message from a remote device, such as a server.

[**0022**] A test is performed during step **350** to determine if a response was received from the central theft protection server **120**. If it is determined during step **350** that a response was received from the central theft protection server **120**, then the network connection is still present (and the user computing device **110** is still connected to the network **100**). The polling process should be performed at periodic or intermittent time intervals, so a wait command is performed during step **355** before program control returns to step **330**.

[**0023**] If, however, it is determined during step **350** that a response was not received from the central theft protection server **120**, then the network connection is no longer present (and the user computing device **110** is no longer connected to the network **100**). Thus, an audible alarm on the user computing device **110** is activated during step **370** or a notification is sent to the user or a monitor, for example, using a cellular connection. Program control then terminates.

[**0024**] As is known in the art, the methods and apparatus discussed herein may be distributed as an article of manufacture that itself comprises a computer readable medium having computer readable code means embodied thereon. The computer readable program code means is operable, in conjunction with a computer system, to carry out all or some of the steps to perform the methods or create the apparatuses discussed herein. The computer readable medium may be a recordable medium (e.g., floppy disks, hard drives, compact disks, or memory cards) or may be a transmission medium (e.g., a network comprising fiber-optics, the world-wide web, cables, or a wireless channel using time-division multiple access, code-division multiple access, or other radio-frequency channel). Any medium known or developed that can store information suitable for use with a computer system may be used. The computer-readable code means is any mechanism for allowing a computer to read instructions and data, such as magnetic variations on a magnetic media or height variations on the surface of a compact disk.

[**0025**] The memories shown in **FIG. 1** will configure the processors to implement the methods, steps, and functions disclosed herein. The memory could be distributed or local and the processor could be distributed or singular. The memory could be implemented as an electrical, magnetic or optical memory, or any combination of these or other types of storage devices. Moreover, the term "memory" should be construed broadly enough to encompass any information able to be read from or written to an address in the addressable space accessed by processor. In an alternate implementation, the present invention can be implemented using an application specific integrated circuit (ASIC), as would be apparent to a person of ordinary skill in the art.

[**0026**] It is to be understood that the embodiments and variations shown and described herein are merely illustrative of the principles of this invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention.

What is claimed is:

1. A method for detecting removal of a device connected to a network by a network connection, comprising:

monitoring said network connection; and

generating an alarm if said network connection is disconnected.

2. The method of claim 1, further comprising the step of preventing a volume of said device from being reduced below a predefined minimum level.

3. The method of claim 1, further comprising the step of preventing said device from being turned off.

4. The method of claim 1, wherein said monitoring step is automatically activated in a passive manner.

5. The method of claim 1, wherein said monitoring step is manually activated by a user.

6. The method of claim 1, wherein said generating step can be prevented by entering a password.

7. The method of claim 1, wherein said monitoring step further comprises the step of sending a message to a remote device and awaiting a response.

8. The method of claim 1, wherein said monitoring step further comprises the step of receiving a message from a remote device.

9. The method of claim 1, wherein said monitoring step further comprises the step of receiving a signal from a remote device.

10. The method of claim 1, wherein said monitoring step further comprises the step of polling one or more local network ports on said device.

11. The method of claim 1, wherein said generating step is performed only if said network connection is disconnected by an unauthorized user.

12. A method for detecting removal of a device connected to a network by a network connection, comprising:

sending a message to a second device connected to said network that will initiate a response; and

generating an alarm if said response is not received within a predefined time interval.

13. The method of claim 12, further comprising the step of preventing a volume of said device from being reduced below a predefined minimum level.

14. The method of claim 12, further comprising the step of preventing said device from being turned off.

15. The method of claim 12, wherein said generating step can be prevented by entering a password.

16. The method of claim 12, wherein said generating step is performed only if said network connection is disconnected by an unauthorized user.

17. A method for detecting removal of a device connected to a network by a network connection, comprising:

monitoring a signal received on said network connection from a remote device over said network connection; and

generating an alarm if said signal is no longer received.

18. The method of claim 17, further comprising the step of preventing a volume of said device from being reduced below a predefined minimum level.

19. The method of claim 17, further comprising the step of preventing said device from being turned off.

20. The method of claim 17, wherein said generating step can be prevented by entering a password.

21. The method of claim 17, wherein said generating step is performed only if said network connection is disconnected by an unauthorized user.

22. A system for detecting removal of a device connected to a network by a network connection, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

monitor said network connection; and

generate an alarm if said network connection is disconnected.

23. The system of claim 22, wherein said processor is further configured to prevent a volume of said device from being reduced below a predefined minimum level.

24. The system of claim 22, wherein said processor is further configured to prevent said device from being turned off.

25. The system of claim 22, wherein said processor is further configured to prevent said alarm by entering a password.

26. The system of claim 22, wherein said processor is further configured to send a message to a remote device and await a response.

27. The system of claim 22, wherein said processor is further configured to receive a message from a remote device.

28. The system of claim 22, wherein said processor is further configured to receive a signal from a remote device.

29. The system of claim 22, wherein said processor is further configured to poll one or more local network ports on said device.

30. The system of claim 22, wherein said processor is further configured to generate said alarm only if said network connection is disconnected by an unauthorized user.

31. An article of manufacture for detecting removal of a device connected to a network by a network connection, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to monitor said network connection; and

a step to generate an alarm if said network connection is disconnected.

32. A system for detecting removal of a device connected to a network by a network connection, comprising:

means for monitoring said network connection; and

means for generating an alarm if said network connection is disconnected.

* * * * *