US 20030182527A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0182527 A1**

Witt, Jr. (43) **Pub. Date: Sep. 25, 2003**

(54) **WRITE PROTECTION STATE CHANGE INITIATION SEQUENCE**

(75) Inventor: **Louis Perry Witt Jr.**, Orlando, FL (US)

Correspondence Address:
MORRIS, MANNING & MARTIN LLP
6000 FAIRVIEW ROAD
SUITE 1125
CHARLOTTE, NC 28210 (US)

(73) Assignee: **COLUMBIA DATA PRODUCTS, INC.**, Altamonte Springs, FL (US)

(21) Appl. No.: **10/248,424**

(22) Filed: **Jan. 18, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/350,434, filed on Jan. 22, 2002.

(30) **Foreign Application Priority Data**

Dec. 16, 2002 (WO) PCT/US02/40106

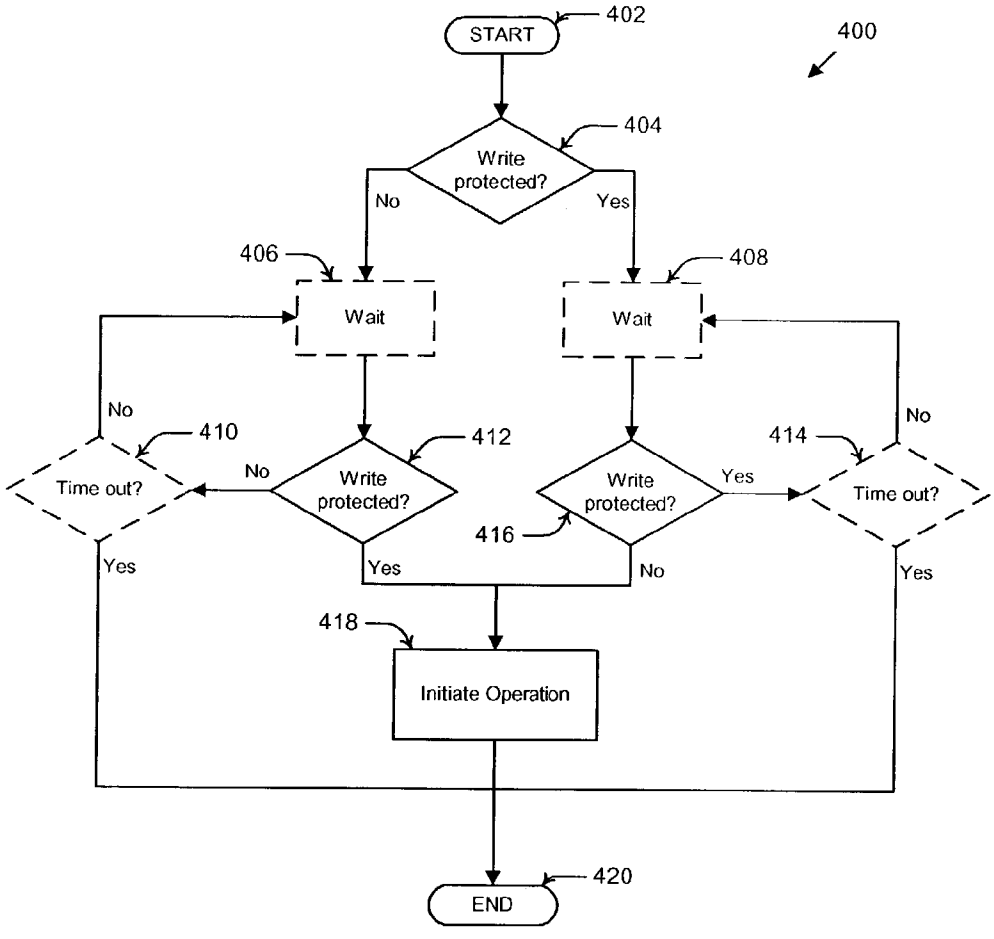
Publication Classification

(51) **Int. Cl.**[7] **G06F 13/28**

(52) **U.S. Cl.** **711/163**

(57) **ABSTRACT**

A user's intention to perform an operation is confirmed by determining within a computer configuration a change in state of a write protection status. The change in state of the write protection status may be either from enabled to disabled, or from disabled to enabled. Determining the change in state of the status includes initially checking the state of the write protection status; subsequently checking the state of the write protection status; and comparing the state determined in the initial check with the state determined in the subsequent check. A predetermined period between the initial check and the subsequent check is provided, and the subsequent check is repeated until a change in the status is determined, or until either a predetermined number of subsequent checks has occurred and/or a predetermined time period has expired. The method can be used in backing up and restoring data of a headless server.



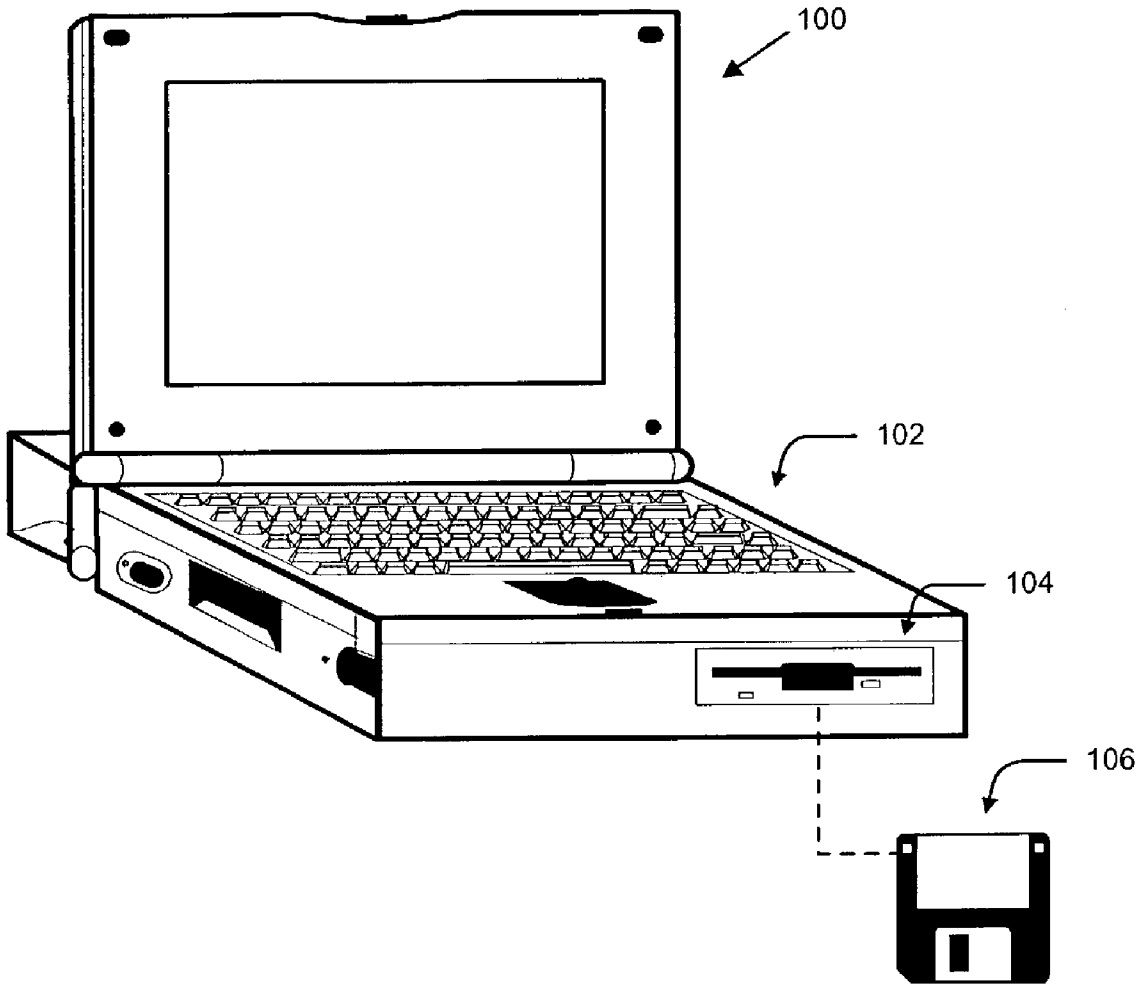


Fig. 1

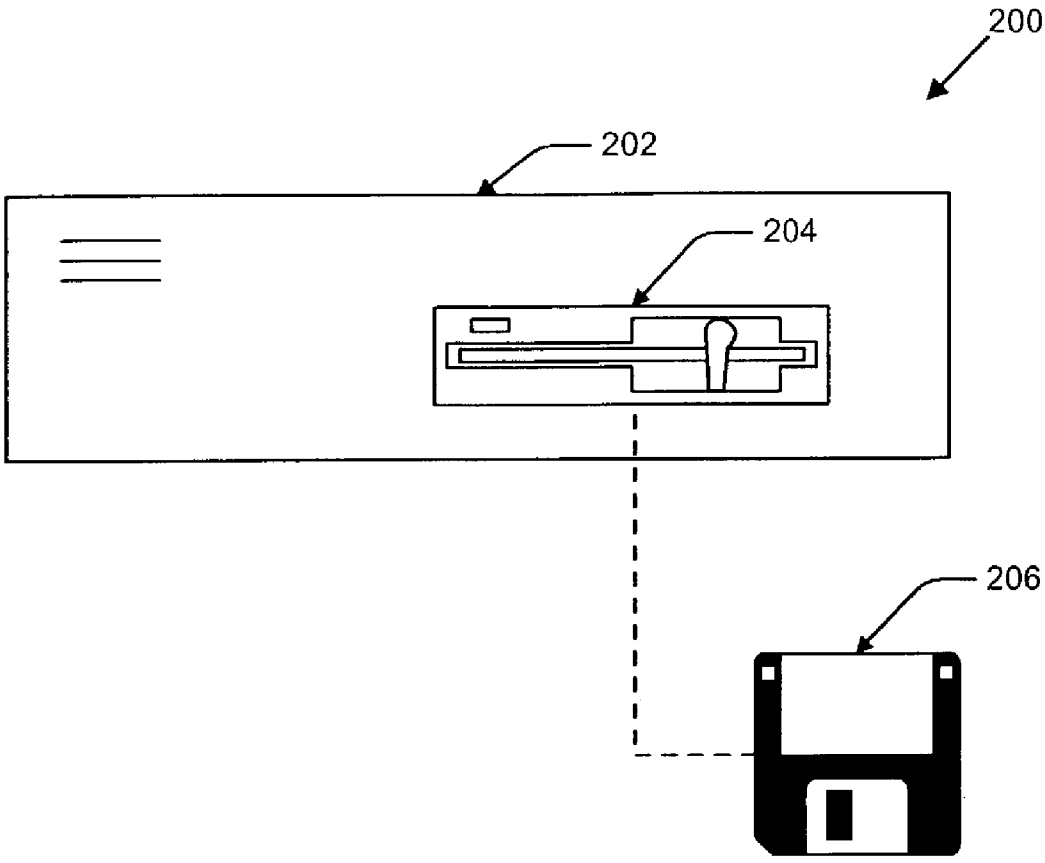


Fig. 2

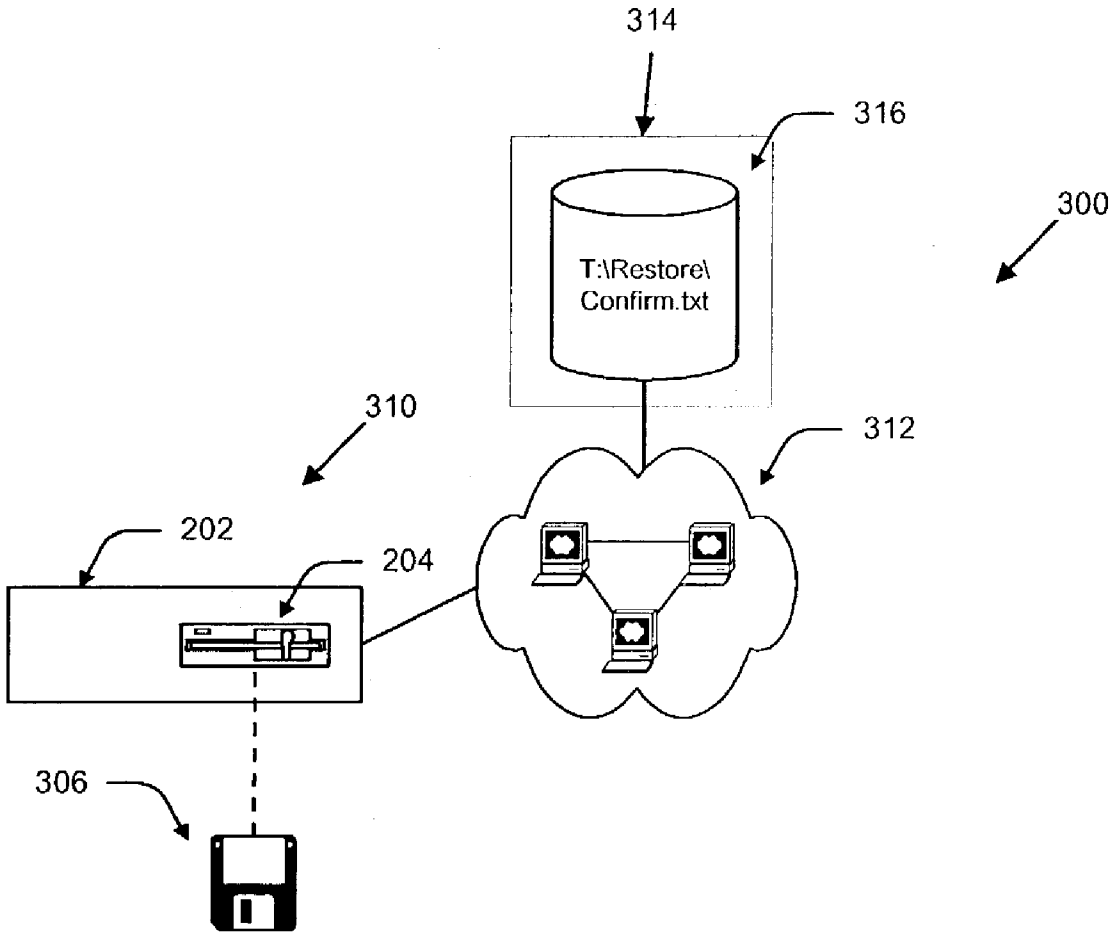


Fig. 3

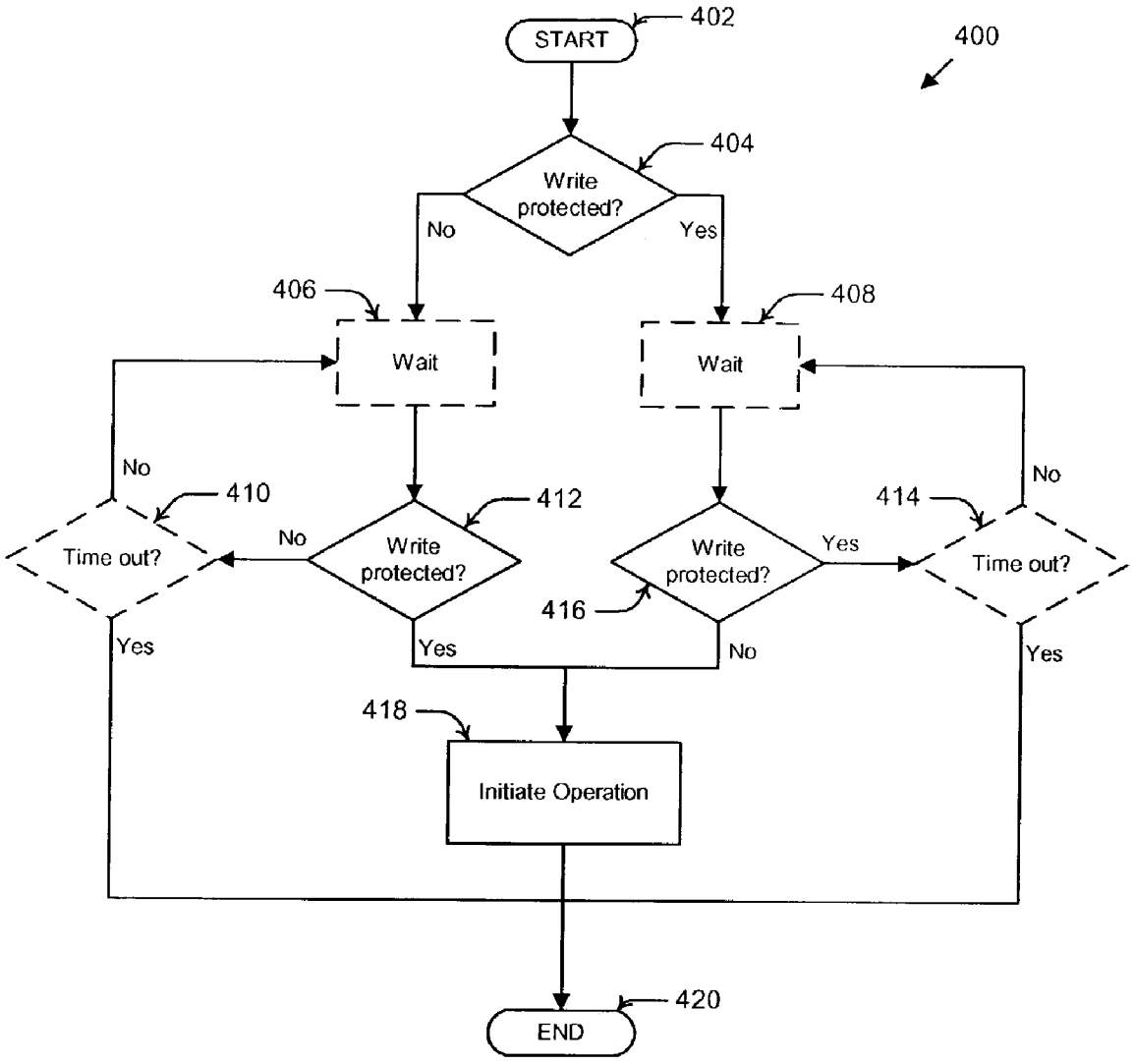

400
START
402
Write protected?
404
No
Yes
406
408
Wait
Wait
No
410
Time out?
No
412
Write protected?
Write protected?
Yes
414
No
Time out?
416
Yes
Yes
No
Yes
418
Initiate Operation
END
420

Fig. 4

WRITE PROTECTION STATE CHANGE INITIATION SEQUENCE

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority under 35 U.S.C. § 119(e) to U.S. provisional patent application serial No. 60/350,434, filed Jan. 22, 2002, which is incorporated herein by reference, and relates to the same field of the invention as the current assignee's International patent application serial no. PCT/US02/40106, filed Dec. 16, 2002, which is incorporated herein by reference.

BACKGROUND OF INVENTION

[0002] It is desirable when a certain operation is to be performed on a computer to require user confirmation for such operation before initiation thereof. By way of example and not limitation, such operations include, for example, operations that are potentially damaging or result in irreversible changes to the computer, such as a low-level disk formatting of the computer's hard drive; restoring the computer to a previous, known state; reinstallation of the operating system of the computer; or performing emergency repair operations on the computer. Additional operations, for example, are set forth and discussed in the "Exemplary Commercial Utilizations" section below and in the incorporated international application.

[0003] By confirming an intention of a user to perform an operation on the computer, the operation is "protected" from accidentally being performed. User confirmation is determined by: (1) communicating by the computer a warning to the user through a user-output device associated with the computer; and (2) in response thereto, communicating by the user a signal to the computer through a traditional user-input device associated with the computer. A user-output device includes, for example, a video display monitor, a light, or a speaker and the like. A traditional user-input device includes, for example, a keyboard, a touch screen, a mouse, or a microphone and the like.

[0004] Unfortunately, there are circumstances in which a user's intention to perform an operation cannot be confirmed beforehand and, thus, the operation is unprotected from accidental performance. For example, a user's intention to perform an operation cannot be confirmed when there are no traditional user-input and/or user-output devices. A user's intention to perform an operation also cannot be confirmed when user-input and/or user-output devices associated with a computer malfunction or otherwise are disabled. A user's intention to perform an operation also cannot be confirmed when the operation itself must be successfully performed on the computer before the associated user-input and/or user-output devices may even be initialized.

[0005] Under these circumstances, allowing an operation to be performed on the computer without user confirmation is undesirable but, nevertheless, necessary.

[0006] The disadvantages of not being able to confirm a user's intentions to perform an operation are particularly apparent when an operation is to be performed on a "headless server" using a "bootstrap program." In this regard, a "headless server" is a computer that has neither monitor, keyboard, nor mouse and that functions as a server in a computer network. Headless servers are found in common computer networks. A bootstrap program is a program that automatically executes upon starting (or "booting") of a computer.

[0007] When an operation is to be performed on a headless server using a bootstrap program, the headless server is booted from auto-running bootstrap media, such as a floppy disk or ZIP disk having the bootstrap program, by placing the floppy disk or ZIP disk in a drive of the headless server and rebooting the server. Using such auto-running bootstrap media, a headless server can be initialized with a base operating system ("O/S") or otherwise restored to an operational condition. Once running, the server then can be configured, for example, by way of a network connected terminal.

[0008] The headless server then might run unattended for months or years. Unfortunately, if the bootstrap media is inadvertently left in the drive of the headless server (which frequently happens), then, upon reboot months or years later, the operation performed by the auto-running bootstrap program on the headless server automatically restarts contrary to the actual intention of the user. Such an accidental restarting of the bootstrap program (which does not seek to confirm a user's intention to perform again the operation) often indicates deletion of or damage to data and security information on the headless server.

[0009] A solution to the "forgotten media" problem is to require a reboot after execution of the operation in order for the headless server to resume normal operations. Leaving the bootstrap media in the drive then will place the computer in an endless loop of repeatedly rebooting and running the protected program until the bootstrap media is removed or otherwise disabled. While certainly not as costly as destroying months or years of data, the requirement of a reboot nonetheless proves wasteful and frustrating when the bootstrap media is inadvertently left in the drive.

[0010] In view of the foregoing, a need exists for a system and method for confirming a user's intention to perform a computer operation when there are no traditional user-input and/or user-output devices connected to a computer. A need further exists for system and method for confirming a user's intention to perform a computer operation when user-input and/or user-output devices associated with a computer malfunction, and/or when user-input and/or user-output devices associated with a computer are disabled. A need also exists for a system and method for confirming a user's intention to perform a computer operation when the operation itself must be successfully performed on a computer before the associated user-input and/or user-output devices may even be initialized.

[0011] Additionally, a particular need exists for a system and method for confirming a user's intention to perform an operation on a headless computer, especially one that functions as a server in a computer network.

[0012] One or more of these needs are met by one or more embodiments of the present invention.

SUMMARY OF INVENTION

[0013] The field of the present invention generally relates to performance of operations and, in particular, to a system and method for initiating an operation after a user's intention

to perform such operation is confirmed. Thus, the present invention guards against a computer operation being inadvertently performed.

[0014] Briefly described, the present invention broadly relates to a system and method in which a user's intention to perform an operation is confirmed. A user's intention is confirmed by determining a change in state of write protection (WP) status. Detection of the state change represents confirmation of the user's intention to perform the operation and forms part of the initiation sequence for the protected operation. The WP state change includes: (1) a change from "enabled" to "disabled," as well as (2) a change from "disabled" to "enabled." In this regard, "enabled" means writable or rewritable and "disabled" means read only. The WP state change preferably is accomplished by a physical act of a user. Accordingly, the WP state change tends to indicate: (1) that a user is present, and (2) that the protected computer operation is specifically intended by the user to be initiated.

[0015] In certain preferred embodiments, the WP state change pertains to a physical, computer-readable medium such as, for example, a floppy disk, a ZIP disk, a USB storage device, a hard disk drive, or the like. In other preferred embodiments, the WP state change pertains to a logical container having the capability of being write protected as well as being unprotected from writes. A logical container includes, for example, a file, a folder, a name space, a logical drive, a virtual device, or the like.

[0016] A method in accordance with the present invention for protecting against an unintentional operation being performed includes the step of initiating the operation only after a user's intention to perform the operation is confirmed. The user's intention to perform the operation is confirmed by: (i) initially checking a WP status of a computer-readable medium or logical container within a computer configuration; (ii) subsequently checking the WP status of the computer-readable medium or logical container within the computer configuration; and (iii) based on the initial and subsequent checks, determining whether there has been a state change in the WP status. The check preferably includes reading an attribute of the computer-readable medium or the logical container that is maintained within the computer configuration. Alternatively, the check of the computer-readable medium or the logical container preferably includes writing to the computer-readable medium or to the logical container. If the write is successful, then the WP status is determined to be enabled. If the write is unsuccessful, then the WP status is determined to be disabled. Upon a detection of the change in the write protection status, the user's intention is deemed confirmed. In a feature of the method, the user's intention is confirmed without requiring use of a user-input device.

[0017] The subsequent check of the WP status preferably occurs after a predetermined period of time. Additionally, the check preferably is made for a predetermined number or times, or for a predetermined period of time, before the method times out and results in the subsequent termination of the initiation sequence without performance of the operation. Following termination of the initiation sequence, the initiation sequence preferably must begin again in order to perform the protected operation. Thus, the initiation sequence preferably is a prerequisite to performing the operation.

[0018] An apparatus in accordance with the present invention includes a computer-readable medium having computer-executable instructions for performing the steps of the preferred method described above. Preferably, this computer-readable medium is a bootstrap medium and the computer-executable instructions are part of a bootstrap program or are part of a program that is run by the bootstrap program during boot up. In a preferred embodiment, the operation that is protected by the initiation sequence is a restore operation from a backup medium onto a headless server. Another apparatus in accordance with the present invention includes a computer configuration including a computer-readable medium having computer-executable instructions for performing the preferred method described above.

BRIEF DESCRIPTION OF DRAWINGS

[0019] Further features and benefits of the present invention will be apparent from a detailed description of preferred embodiments thereof taken in conjunction with the following drawings, wherein similar elements are referred to with similar reference numbers, and wherein:

[0020] **FIG. 1** illustrates a first preferred embodiment of a digital computer configuration of the invention;

[0021] **FIG. 2** illustrates a second preferred embodiment of a digital computer configuration of the invention;

[0022] **FIG. 3** illustrates a third preferred embodiment of a digital computer configuration of the invention; and

[0023] **FIG. 4** illustrates a flow diagram of steps of a preferred embodiment of a method of the invention.

DETAILED DESCRIPTION

[0024] As a preliminary matter, it will readily be understood by those persons skilled in the art that the present invention is susceptible of broad utility and application in view of the following detailed description of preferred embodiments of the present invention. Many devices, methods, embodiments, and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements thereof, will be apparent from or reasonably suggested by the present invention and the following detailed description thereof, without departing from the substance or scope of the present invention. Accordingly, while the present invention is described herein in detail in relation to preferred embodiments, it is to be understood that this disclosure is illustrative and exemplary and is made merely for purposes of providing a full and enabling disclosure of the invention. The detailed disclosure herein is not intended nor is to be construed to limit the present invention or otherwise to exclude any such other embodiments, adaptations, variations, modifications and equivalent arrangements, the present invention being limited only by the claims appended hereto and the equivalents thereof.

[0025] A First Preferred Embodiment of a Computer Configuration of the Present Invention

[0026] Referring to **FIG. 1, a** first preferred computer configuration **100** is shown in accordance with the present invention. The computer configuration **100** includes a digital computer **102** illustrated as a laptop computer and hardware **104** comprising a ZIP drive that can read from and write to

Zip disks. Removable storage medium **106** is illustrated as a Zip disk. The disk is insertable into the drive of the computer configuration **100** for reading thereof and writing thereto by the computer **102**. The computer configuration **100** includes computer-readable media having computer-executable instructions for performing the preferred method of the present invention described in detail below.

[**0027**] A Second Preferred Embodiment of a Computer Configuration of the Present Invention

[**0028**] A second preferred computer configuration **200** is shown in **FIG. 2** in accordance with the present invention. Similar to the computer configuration **100** of **FIG. 1**, the computer configuration **200** of **FIG. 2** includes a digital computer **202** having hardware **204** in which a removable storage medium **206** is insertable for reading therefrom and writing thereto by the computer **202**. Unlike the computer configuration **100** of **FIG. 1**, the computer **202** is illustrated as a headless server, as the computer configuration **200** includes no user-input or output devices; the hardware **204** comprises a floppy drive; and the removable storage medium **208** comprises a floppy disk. The computer configuration **200** includes computer-readable media having computer-executable instructions for performing the preferred method of the present invention described in detail below.

[**0029**] A Third Preferred Embodiment of a Computer Configuration of the Present Invention

[**0030**] A third preferred computer configuration **300** is shown in **FIG. 3** in accordance with the present invention and includes a computer network **312**. The computer configuration **200** of **FIG. 2** forms part of the computer configuration **300** illustrated **FIG. 3**, as the computer configuration **200** represents a node **310** of the computer network **312**. The computer configuration **200** includes the digital computer **202** and hardware **204** in which removable storage medium **306** is insertable for reading thereof and writing thereto by the computer **202**.

[**0031**] The computer network **312** also includes a network attached device (NAD) **318** with network attached storage (NAS) **316**. The NAS **316** includes therein a logical container comprising a file titled "confirm.txt" and, in turn, this file is located within another logical container comprising a folder. The folder is titled "Restore" and, in turn, the folder is located within another logical container comprising a logical drive or volume titled "T" (also referred to as the "T drive"). The file "confirm.txt" preferably includes an attribute that is recorded within the computer configuration that identifies a WP status of the file. This attribute typically is part of the metadata associated with the file. Alternatively, the folder includes an attribute that is recorded within the computer configuration that identifies a WP status of the files contained within the folder, or the T drive includes an attribute that is recorded within the computer configuration that identifies a WP status of all of the folders and/or of all of the files contained within the T drive. The computer configuration **300** includes computer-readable media having computer-executable instructions for performing the preferred method of the present invention described in detail below.

[**0032**] A Preferred Embodiment of a Method of the Present Invention

[**0033**] Referring now to **FIG. 4**, steps of a preferred method **400** in accordance with the present invention are illustrated. The preferred method **400** begins at Step **402** when a protected operation is to be performed. At Step **404** a WP status is determined. With regard to the preferred computer configuration **100** of **FIG. 1**, the WP status of the disk **106** is determined; with regard to the preferred computer configuration **200** of **FIG. 2**, the WP status of the disk **206** is determined; and with regard to the preferred computer configuration **300** of **FIG. 3**, the WP status of either the disk **306** or of one of the logical structures of the NAS **316** is determined. Preferably, the WP status is determined by reading an attribute of the computer-readable medium or of the logical structure that indicates the WP status. Alternatively, the WP status is determined by attempting to write to the computer-readable medium or to the logical structure. If the write is successful, then the WP status is determined to be enabled. Thus, for instance, the WP status of the file "confirm.txt" on the T drive of the NAS **316** may be determined by writing to the file.

[**0034**] If the WP status is "disabled," then the method determines again (Step **412**) the WP status. If the WP status is changed based on a comparison of the initial and subsequent checks, i.e., if the WP status is now "enabled," then the method initiates the operation at Step **418**, and the method then ends at Step **420**.

[**0035**] On the other hand, if the WP status is determined to be "disabled" at Step **412**, i.e., if the WP status is determined not to have changed based on a comparison of the initial and subsequent checks, then the method ends at Step **420** without the operation being initiated.

[**0036**] Alternatively, if the WP status is "enabled" as initially determined in Step **404**, then the method determines again (Step **416**) the WP status. If the WP status is changed based on a comparison of the initial and subsequent checks, i.e., if the WP status is now "disabled," then the method initiates the operation at Step **418**, and the method then ends at Step **420**.

[**0037**] On the other hand, if the WP status is determined to be "enabled" at Step **416**, i.e., if the WP status is determined not to have changed based on a comparison of the initial and subsequent checks, then the method ends at Step **420** without the operation being initiated.

[**0038**] In order for a user to change the WP status of the computer-readable medium or logical container for which the WP status is determined, a sufficient period preferably is provided before the respective subsequent checks at Steps **412** and **416**.

[**0039**] Accordingly, if the WP status is determined to be "disabled" at Step **404**, then the method waits (Step **406**) for some period of time, and if the WP status is determined to be "enabled" at Step **404**, then the method waits (Step **408**) for some period of time. Thereafter, a subsequent check respectively is made at Step **412** and Step **416**. Furthermore, the method continues to check the WP status until either the WP status is determined to have changed or the method times out. The method times out at Steps **410**,**414** after a predetermined period of time or after a predetermined number of subsequent checks of the WP status have been

made. If the method times out at Step **410** or Step **414**, then the method ends at Step **420** without the operation being initiated.

[**0040**] With regard to the preferred computer configuration **100** of **FIG. 1**, the WP status of the disk **106** is changed by the user by unchecking a "read only" attribute in the properties box for the disk **106**; with regard to the disk **206** of **FIG. 2** or to the disk **306** of **FIG. 3**, the WP status of the disk is changed by the user physically toggling a write protection tab on the disk; and with regard to one of the logical containers of **FIG. 3**, the WP status of the logical structure is changed by the user by unchecking a "read only" attribute in the properties box for the particular logical container.

[**0041**] In view of the foregoing detailed description, it will be apparent that the operation will not be initiated without the successful determination of a change in state of the WP status and, hence, confirmation of the user's intention to perform the operation. Preferably, the operation can only be initiated following confirmation of the user's intention to perform the operation.

[**0042**] Moreover, in view of the foregoing detailed description, it will be apparent that, at least with regard to certain embodiments of the present invention, a user's intention to perform the operation actually is confirmed without requiring the use of user-input and user-output devices. No keyboard, mouse, monitor, microphone, speaker, touch screen, or the like is required in order to perform the initiation sequence for the operation. Nor is an on-screen user prompt required in order to confirm the user's intention to perform the operation on the computer. The physical toggling of the write protection tab on disks **206**, **306206,306**, for instance, is an act that necessarily must be performed by a user at the time of the initialization of the operation, and represents confirmation of the user's intentions to initiate and perform the operation at that time.

[**0043**] Exemplary Commercial Utilizations of the Present Invention

[**0044**] The following represent examples of contemplated commercial utilizations of the present invention.

[**0045**] Keystroke Emulation Program

[**0046**] In certain circumstances, it is desirable to emulate keystrokes, especially when a keyboard or keypad is absent, malfunctioning, or otherwise unavailable. For instance, one may desire to create a backup of one's hard drive on a laptop computer using a backup program on the hard drive. This may be impossible, or at least very difficult, without the use of a keyboard. Utilizing a method of the present invention, a first removable storage medium such as disk **206** in **FIG. 2** comprising a bootstrap disk is inserted into a floppy drive of the laptop and the laptop then is started. During booting of the laptop, the laptop boots from the bootstrap disk. The bootstrap disk includes a program that is executed by the laptop that causes the computer to determine the WP status of the disk and then to determine, again, the WP status of the disk. The subsequent determination is made after a sufficient period of time in which the user can remove the disk from the drive, physically toggle the write protection tab of the disk, and then reinsert the disk into the drive. Accordingly, when the subsequent check is made to determine the WP status of the disk, a comparison of the initial and subsequent checks reveals a change in the state of the WP status. Following successfully determining the change in state of the WP status, the bootstrap program emulates keystrokes of a user. In this regard, the sequence of keystrokes is predetermined and results in the execution of the backup program on the laptop's hard disk drive. Moreover, the sequence of keystrokes preferably identifies a backup location external to the laptop, such as, for example, a network storage device or a USB hard drive attached directly to a USB port of the laptop. The determination of the change in state of the WP status of the bootstrap disk is a prerequisite to initiation of the keystroke emulation. Consequently, inadvertently booting the laptop with the disk does not result in an unintended performance of the backup operation.

[**0047**] Headless Server Restore and Backup

[**0048**] Another example of a commercial utilization of the present invention includes backup and restore operations on a headless server. Inadvertent or unauthorized restoration of a backup image on a headless or blind server can destroy valuable data. In this context, the restore program is stored on a first bootstrap computer-readable medium such as a floppy disk. Upon booting from this disk, a bootstrap program thereon determines the WP status of the disk and then determines, again, the WP status of the disk in accordance with the method of **FIG. 4**. The second determination is made after a sufficient period of time in which the user can remove the disk from the drive of the headless server, toggle a write protection tab of the disk, and then reinsert the disk into the drive. Accordingly, when the comparison is made for a change in state of the WP status of the disk, such a change is determined. Following this successful determination, the bootstrap program initiates a restore operation in which backup data is written to the headless server. The backup data could be written from a secondary drive of the headless server or from a remote location, such as network attached storage. In this way, the physical change in the write protection tab of the disk ensures that it is impossible to inadvertently perform a restore operation to the headless server by simply leaving the bootstrap disk in the drive and later rebooting the headless server. Indeed, even if the bootstrap disk is inadvertently left in the drive, the restore operation nevertheless will not be executed upon a later reboot, as the state of the WP status of the disk will not change absent user action. In such case, the initiation sequence simply will time out and, if the restore operations is indeed desired, the headless server will have to reboot with the bootstrap disk in the drive.

[**0049**] Correspondingly, an inadvertent or unauthorized saving of backup data from a headless server can likewise destroy previously saved backup data. As in the restore operation, the present invention can be utilized to safeguard against this type of disaster. In this regard, the backup operation to successfully execute requires, as a prerequisite, the change in state of the WP status of a disk. This disk also can be additionally used to load backup parameters and to save operational results of the backup for review by a user on another computer.

[**0050**] Remote Network Install on Local Machine

[**0051**] In certain arrangements it may be desirable to install a program on a local machine that is connected to a network, wherein the installation program itself is centrally located on a network attached device. The installation,

however, may destroy important data on the local machine if inadvertently performed, or if inadvertently performed remotely on the wrong local machine (hundreds or even thousands of local machines can exist on a network). The present invention can be utilized to ensure installation to the proper machine and to limit unintentional installations. When an installation is to be performed at a local machine, a technician physically disposed at the local machine inserts a computer-readable medium comprising a disk into a drive associated with the local machine. The computer reads an identifier from the drive that is unique to, and thereby identifies to the local computer, the program to be installed on the local machine from the central network location. The computer also checks the WP status of the disk. Thereafter, the technician changes the state of the WP status of the disk and, after a predetermined period, the computer again checks the WP status of the disk.

[0052] Upon the successful determination of a change in state of the WP status of the disk, the computer initiates the installation program for installation to the local machine from the central network location. Furthermore, the identifier read from the disk is checked at the central network location against a list of identifiers that are associated with local machines to insure that the identifier read from the disk is, in fact, associated with the particular local machine so that the appropriate program will be installed for that machine. On the other hand, if the determination of a change in the state of the WP status of the disk is unsuccessful, or if a timeout occurs, which would occur in the absence of the technician, then the initiation sequence ends and the installation operation simply is not initiated.

[0053] Dangerous Program Isolation

[0054] Execution of programs that, if inadvertently or maliciously executed would cause severe damage, may be contained by utilizing the present invention. In this regard, such a program is stored on a removable storage medium such as a floppy disk and not, for example, on a hard disk drive of a computer. This physical isolation of the program safeguards against malicious execution of the program by someone who merely gains access to the computer and its non-removable storage media. To execute the program utilizing the present invention, the floppy disk is inserted into a drive of the computer and the program including the initiation sequence is run. Upon running, the program first determines the WP status of a predetermined file on the disk. Thereafter, the program again determines the WP status of the predetermined file. If the WP status of the predetermined file does not change between the initial and subsequent checks, then the program ends without the dangerous program being successfully executed. If the WP status of the disk changes, then the dangerous program is then successfully initiated.

[0055] In this example, the program of the initiation sequence may or may not comprise a bootstrap program and/or may or may not reside upon a bootstrap disk. However, if the program does comprise a bootstrap program, or resides on a bootstrap disk and is called by the bootstrap program, then the required change in state of the WP status of the predetermined file on the disk ensures that the dangerous program cannot be inadvertently executed upon a reboot of the computer merely by leaving the disk within the drive; someone also must be present to change the state of the WP status of the predetermined file between the initial check and subsequent check performed as part of the initiation sequence.

[0056] Scope of the Present Invention

[0057] In view of the foregoing detailed description of preferred embodiments of the present invention, it readily will be understood by those persons skilled in the art that the present invention in all its aspects is susceptible of broad utility and application. While various embodiments of the present invention have been described herein in certain contexts, the embodiments may be useful in other contexts as well. Many embodiments and adaptations thereof other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the foregoing description thereof, without departing from the substance or scope of the present invention. Furthermore, any sequence(s) and/or temporal order of steps of various processes described and claimed herein are those considered to be the best mode contemplated for one or more preferred embodiments of the present invention. It should also be understood that, although steps of various processes may be shown and described as being in a preferred sequence or temporal order, the steps of any such processes are not limited to being carried out in any particular sequence or order, absent a specific indication of such. In many cases, the steps of such processes may be able to be carried out in various different sequences and orders, while still falling within the scope of the present invention. Accordingly, while the present invention has been described herein in detail in relation to preferred embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made merely for purposes of providing a full and enabling disclosure of the invention. The foregoing disclosure is not intended nor is to be construed to limit the present invention or otherwise to exclude any such other embodiments, adaptations, variations, modifications and equivalent arrangements thereof, the present invention being limited only by the claims appended hereto and the equivalents thereof.

[0058] Thus, the use of "program" herein may refer not only to a standalone set of code, but also, for example, to a snippet of code or a module forming part of a larger program. Furthermore, for example, a laptop computer **102** is shown in **FIG. 1** only for purposes of illustrating a digital computer. The laptop computer **102** further represents, for example, a desktop, a tower computer, and a headless server, as well as an embedded computer such as those computers found in ATMs, cash registers, vending machines, gaming machines, autos, appliances, etc. Similarly, the headless server **202** of **FIG. 2** equally could be the laptop computer **102** as shown in **FIG. 1**, etc. The Zip disk **106** and the floppy disk **206** are shown only for purposes of illustrating different types of computer-readable media. These further represent, for example, optical discs, floppy disks, Zip disks, and the like, with the drive **104** and disk drive **204** each representing the appropriate type of hardware of the computer configuration for reading thereof and writing thereto by the computer. In general, the Zip disk **106** and disk **206** represent any type of computer-readable media that can be read and written by the computer **102**, such as USB hard disk drives, USB memory devices, and the like.

[0059] Thus, for example, when the computer-readable media include USB devices, the computer configuration includes a USB port as the hardware for reading of the USB devices; when the computer-readable media include serial devices, the computer configuration includes a serial port as the hardware for reading the serial devices; when the computer-readable media include parallel devices, the computer configuration includes a parallel port as the hardware for reading the parallel devices; when the computer-readable media include a SCSI device, the computer configuration includes a SCSI connection as the hardware for reading the SCSI devices; and when the computer-readable media include infrared devices, the computer configuration includes an infrared port as the hardware for reading the infrared devices, etc.

[0060] In addition to a user effecting a change in the WP status within the computer configuration, it is also contemplated that, within certain embodiments of the present invention, a software program effects the change in the WP status rather than a user. Such a software program may run remotely or within the computer configuration, and preferably is executed by the user to run at one or more specified times when the user intends the operation to be initiated. In this situation, the software program that effects the state change in the WP status does not itself confirm the intention of the user to perform the operation by determining that a state change of the WP status has occurred.

[0061] One or more methods also have been described as including the booting of a computer from a bootstrap storage medium. A variation of the present invention further includes such methods absent the actual booting of the computer from such storage media. Instead, it is contemplated within the scope of the invention that in each such method the computer be booted from another storage medium, such as a hard disk drive of the computer configuration, a remote server in a networked computer configuration, etc., while otherwise still performing the other steps of the respective method described herein. Booting from a removable storage medium clearly is not a necessary element of the invention in its broadest scope. Moreover, it will be recognized that embodiments of the present invention may overlap to various extents and, accordingly, are not mutually exclusive.

What is claimed is:

1. An invention comprising a method of initiating an operation after a user's intention to perform the operation is confirmed, the method comprising the step of confirming the user's intention by determining within a computer configuration a change in state of a write protection (WP) status.

2. An invention comprising a computer-readable medium including computer-executable instructions for performing a method of initiating an operation after a user's intention to perform the operation is confirmed, the method comprising the steps of

(a) confirming the user's intention by determining within the computer configuration a change in state of a write protection (WP) status, and

(b) after the user's intention is confirmed, initiating the operation.

3. An invention comprising a computer configuration in which an operation is initiated only after a user's intention to perform the operation is confirmed, the computer configuration comprising a computer-readable medium and means for confirming the user's intention by determining within the computer configuration a change in state of a write protection (WP) status.

4. The invention of claim 1, wherein the operation is performed only after the user's intention to perform the operation is confirmed.

5. The invention of claim 1, wherein confirming the user's intention by determining within the computer configuration a change in state of the WP status consists of determining a change in state of the WP status from enabled to disabled.

6. The invention of claim 1, wherein confirming the user's intention by determining within the computer configuration a change in state of the WP status consists of determining a change in state of the WP status from disabled to enabled.

7. The invention of claim 1, wherein confirming the user's intention by determining within the computer configuration a change in state of the WP status comprises determining a change in state of the WP status from enabled to disabled.

8. The invention of claim 1, wherein confirming the user's intention by determining within the computer configuration a change in state of the WP status comprises determining a change in state of the WP status from disabled to enabled.

9. The invention of claim 1, wherein confirming the user's intention by determining within the computer configuration a change in state of the WP status comprises determining a change in state of the WP status either (a) from enabled to disabled, or (b) from disabled to enabled.

10. The invention of claim 1, wherein determining within the computer configuration a change in state of the WP status comprises,

(a) initially checking the state of the write protection status;

(b) subsequently checking the state of the write protection status; and

(c) comparing the state determined in the initial check with the state determined in the subsequent check.

11. The invention of claim 10, wherein determining within the computer configuration a change in state of the WP status further comprises (d) waiting a predetermined period between the initial check and the subsequent check.

12. The invention of claim 11, wherein determining within the computer configuration a change in state of the WP status further comprises (d) repeating the subsequent check until

(i) a change in the WP status is determined, or

(ii) until either,

(A) a predetermined number of subsequent checks has occurred, and/or

(B) a predetermined time period has expired.

13. The invention of claim 10, wherein determining within the computer configuration a change in state of the WP status further comprises (d) repeating the subsequent check until

(i) a change in the WP status is determined, or

(ii) until either,

(A) a predetermined number of subsequent checks has occurred, and/or

(B) a predetermined time period has expired.

14. The invention of claim 1, wherein the state of the WP status must be changed by the user.

15. The invention of claim 14, wherein the state of the WP status is changed by a physical act of the user.

16. The invention of claim 1, wherein the user's intention is confirmed without requiring the use of a user-input device of a computer.

17. The invention of claim 1, wherein the WP status is of a computer-readable storage medium.

18. The invention of claim 17, wherein the computer-readable storage medium is a bootstrap medium.

19. The invention of claim 17, wherein the computer-readable storage medium is a non-removable storage medium.

20. The invention of claim 17, wherein the computer-readable storage medium comprises a removable storage medium.

21. The invention of claim 20, wherein the removable computer-readable storage medium is a bootstrap medium.

22. The invention of claim 20, wherein the removable storage medium comprises one of the type of floppy disks, ZIP disks, optical discs, USB devices, serial devices, parallel devices, and SCSI devices.

23. The invention of claim 1, wherein the WP status is of a logical container.

24. The invention of claim 23, wherein the logical container comprises a virtual device.

25. The invention of claim 23, wherein the logical container comprises a logical drive.

26. The invention of claim 23, wherein the logical container comprises a partition.

27. The invention of claim 23, wherein the logical container comprises a name space.

28. The invention of claim 23, wherein the logical container comprises a folder.

29. The invention of claim 23, wherein the logical container comprises a file.

30. The invention of claim 1, wherein the operation is performed on a computer.

31. The invention of claim 30, wherein the computer has no user-input devices connected thereto.

32. The invention of claim 30, wherein the computer has a user-input device that is disabled or malfunctioning.

33. The invention of claim 30, wherein the computer that has no user-output devices connected thereto.

34. The invention of claim 30, wherein the computer comprises a laptop computer.

35. The invention of claim 30, wherein the computer configuration includes a computer comprising a headless server.

36. The invention of claim 1, wherein the operation is one of the group of hard disk drive partitioning; low level disk formatting; logical container deleting; restoring a computer to a previous, known state; reinstallation of the operating system of a computer; and performing emergency repair operations on a computer.

37. The invention of claim 1, wherein the operation includes backing up data from a computer-readable medium to a backup medium.

38. The invention of claim 37, wherein the backup medium comprises network attached storage.

39. The invention of claim 37, wherein the operation includes restoring data of a backup to the computer-readable medium.

40. The invention of claim 39, wherein the computer configuration comprises a computer network and the computer-readable medium of which the backup is made comprises a headless server of the network.

41. The invention of claim 1, wherein a change in WP status is effected by a software program.

42. The invention of claim 41, wherein the software program that effects the change in WP status does not confirm the user's intention to perform the operation.

* * * * *