

-1-

BUILT-IN DRIVE SECURITY SYSTEMFIELD OF THE INVENTION

5

The present invention relates generally to data storage devices. More particularly, the present invention relates to a disc drive with a built-in security password system.

10

BACKGROUND OF THE INVENTION

Mass storage devices are one of many components of modern computers. One type of mass storage device is the fixed disc drive. Such drives are used to store vast amounts of information relating to operating systems, applications, and user data. Most companies or individuals use electronic information extensively to support their daily business processes. Sensitive data on customers, products, contracts, financial results, and accounting are often stored on a fixed disc drive. If the confidentiality of this sensitive information were compromised, significant losses could occur. Thus, it is sometimes very important to ensure the confidentiality of data stored in a disc drive such that only authorized persons have access to the data.

Drive security has become even more important as fixed disc drives have become more interoperable and mobile. For example, a drive conforming to the AT Attachment Specification will operate with any system that supports the AT Attachment Specification. Modern systems generally detect fixed disc drives automatically and allow access with relative ease. With such systems drives can be swapped between systems with little effort.

As others have recognized the importance of drive security, disc drive security systems have been proposed to limit access to sensitive or confidential information. However, such systems require cooperation between the system Basic Input/Output System (BIOS) and drive firmware in order to enable/disable security features. This creates a significant problem where one system includes a BIOS that can enable security features on a drive, and a second system (typically an older system) does not include BIOS that can interact with the security features.

Another situation in which this problem arises, is when a given disc drive supports security features, such as the ATA5 Security Mode, and the system BIOS's do not support such features. For example, most BIOS' do not currently support the ATA Security Mode feature. Thus, incompatibilities occur that limit the interoperability and mobility of fixed disc drives with security features.

The present invention addresses these and other problems, and offers other advantages over the prior art.

20

SUMMARY OF THE INVENTION

The present invention relates to fixed disc drives which solve the above-mentioned problems.

In accordance with one embodiment of the invention, a fixed disc drive includes a built-in user level security system. The system includes instructions that create an user interface upon a computer thereby allowing user interaction with security features of the drive without relying upon system BIOS compatibility. In a specific embodiment, user level security interface software is

provided by the disc drive during the boot sequence of the computer system.

In another embodiment of the present invention, a method of disc drive security includes receiving a request from a computer to provide an operating system, and responsively providing user level security interface instructions. The user level security instruction are then executed by the computer to generate an user level security interface. If the drive is in a locked state, the interface requires the user to provide an acceptable password, otherwise access to data on the drive is forbidden or otherwise restricted.

In another embodiment a disc drive includes a system for reading data from and writing data to at least one disc. The drive also includes a system for generating a user level security interface to access one or more security features of the drive

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1 and 2 are diagrammatic and system block views, respectively, of an exemplary fixed disc drive for which embodiments of the present invention are useful.

FIG. 3 is a system block diagram of a disc drive controller in accordance with an embodiment of the present invention.

FIGS. 4 and 5 are system block diagrams of a method of providing a built-in user level security interface in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

FIG. 1 is a diagrammatic view of disc drive 100, which is adapted to couple to a computer 118 (shown in FIG. 2). When disc drive 100 is coupled to computer 118, computer 118 transfers data to and reads data from disc drive 100. Disc drive 100 includes discs 104, spindle 106, spindle motor 126 (shown in FIG. 2), transducer head 110, actuator 112, and board electronics 114. Board electronics 114 include disc controller 124 (shown in FIG. 2).

Discs 104 are fixed about spindle 106, which is coupled to spindle motor 126 such that energization of spindle motor 126 causes spindle 106 and discs 104 to rotate. When discs 104 rotate, heads 110 fly above/below discs 104 on thin films of air or liquid and carry heads 110 for communicating with the respective disc surface. Several alternative types of heads can be used, such as magnetic or optical heads. Actuator 112 is coupled to controller 124 and is adapted to move heads 110 relative to the surfaces of discs 104 in response to an actuation signal from controller 124.

FIG. 3 is a block diagram of disc controller 124 in accordance with an embodiment of the present invention. FIG. 3 shows disc controller 124 coupled to computer 118, spindle motor 126, actuator 112, and transducer head 110. FIG. 3 further shows disc controller 124 comprised of read/write circuitry 130, I/O port 132, control circuitry 128 and memory 134.

Control circuitry 128 provides an energization signal to spindle motor 126, and provides an actuation signal to actuator 112. Thus control circuitry 128 essentially controls all motion in drive 100. Control circuitry 128 also provides information which is to be written to discs 104, to read/write circuitry 130, and receives information read from discs 104 from read/write circuitry 130.

Control circuitry 128 is adapted to receive a request from I/O port 132 to read information from or write information to a specific address corresponding to a physical location within drive 100. Control circuitry 128 provides appropriate actuator and energization signals to position transducer head 110 over the specified location on disc 104. Once positioned, information is written to or read from discs 104 according to the request received from I/O port 132.

I/O port 132 is adapted to communicate commands and data between system 118 and drive 100. Some commands are issued by computer system 118 during the boot sequence of computer system 118. One such boot command, issued by computer 118, generally instructs storage devices such as drive 100 to provide an operating system to computer 118. When this command is issued by computer system 118, I/O port 132 receives the command, and provides the command to control circuitry 128. Control circuitry 128 recognizes this specific command, and provides user level security interface software, which in one embodiment resides in memory 134 and/or on disc 104 to computer 118 through I/O port 132 instead of the system-requested operating system. Upon execution of the user level security interface software, computer system 118 causes a user interface to be displayed which provides access to security features of the drive. "Security Features," as used herein, is intended to mean any features that directly or indirectly provide selectable access to data on drive 100. Upon termination of the user level security interface, control circuitry 128 provides an operating system to computer 118 through I/O port 132 much as would any prior art storage disc

FIGS. 4 and 5 illustrate a method of providing user level security access in accordance with an embodiment of the present invention. The method begins at step 200 where the built-in security password system is invoked by system 118. Preferably, this invocation is generated during system boot, however those skilled in the art will recognize that invocation may be effected at other appropriate times as well. Once the password system has been invoked, control passes to state 202 which determines if drive 100 is in a locked state. This determination can be done in a number of ways, for example, drive 100 can query a non-volatile portion of memory 134 to determine if a Security Set Password command has been issued to cause a password to be stored within memory 134. Another alternative includes checking a location on disc(s) 104 that stores security information. In such an embodiment, security information is generally written upon a location of discs 104 that is always inaccessible to users, thus the hidden location functions as the non-volatile portion of memory 134. If drive 100 is locked, control passes to block 204. However, if drive 100 is not locked, control passes to block 206.

At block 204, the user level security interface prompts the user to enter the security password. Control then passes to block 208 where the Security Unlock command is sent to drive controller 128 along with the user-supplied password. If the user-supplied password matches the stored password recorded when the drive was locked, the Unlock command is successful and the drive becomes unlocked. However, if there is no match, the Unlock command fails and drive 100 remains locked. At state 210, the status of drive 100 is checked to see if it remains locked. If the drive is unlocked then control passes to state 212 where the entered security password is memorized, and where control is

passed to state 206. However, if drive 100 remains locked, then control passes to state 214 where a counter is incremented and checked to see if a pre-selected number of unsuccessful unlock attempts have occurred. In FIG. 4, the preselected number is five
5 attempts. If the number of unsuccessful attempts reaches the preselected threshold, then control passes to state 216 where the system is halted. Once system 118 is halted, the system must be reset in order for drive 100 to provide any user level security interface.

10 At block 206, drive 100 generates an user interface that allows a user to set a new password, disable password protection, or return to the host system. In one embodiment, the user interface generated at block 206 is a graphical user interface. Once the interface is displayed, the user is prompted to provide a
15 command related to the above options. At state 218, the command is evaluated to see if it is a request to set the password. If the command is indeed such a request, control passes to circle 300 which is set forth in detail in FIG. 5, which will be discussed later in the specification. If the user command is not Set Password, then
20 the command is evaluated, in state 220, to see if it is a Disable Password command. If the command is in fact a Disable Password command, then control passes to circle 302 which is also set forth in detail in FIG. 5. If the user command is neither Set Password nor Disable Password, then the command is checked at state 222
25 to see if it is a request to Return to Host. If so, control passes to state 224 where the operating system is provided to computer 118 and the boot process resumes as normal.

Circle 300, shown in FIG. 5, represents the state of drive 100 when an user has entered a command to Set Password at the user
30 interface prompt of block 206. The method begins at state 230

where the system determines whether drive security is disabled. If drive security is not disabled, then control passes to block 232, otherwise control passes to block 234. At block 232, the user interface prompts the user to enter the Current Password. At block 5 236, the Current Password and memorized security passwords are compared in order to verify user authorization. If the user has entered the correct password, then state 238 passes control to block 234, otherwise control passes to state 240 where a count of unsuccessful attempts is incremented and checked against a 10 preselected threshold, much like state 214 in FIG. 4. Once the number of preselected unsuccessful attempts has been reached, control passes to state 242 where system 118 is halted.

As illustrated in FIG. 5, block 234 can receive control from state 230 as well as state 238. Block 234 prompts the user to enter 15 the New Password. Once the user has entered the New Password, control passes to block 244 where the Security Set Password command is issued to drive 100, after which control returns to state 206 through state 245.

Circle 302 represents the state of drive 100 when a user has 20 entered a command to Disable Password at the user interface prompt of block 206. The method begins at state 246 where the system determines whether drive security is disabled. If drive security is disabled, then there is no reason to further execute the method, and control is returned to the user interface of state 206. 25 However, if drive security is not disabled, then control passes to block 248, which functions identically to block 232. At block 250, a Security Disable Password command is sent to drive 100 with the user-supplied password. At state 252, the system checks to see whether the command was successful. If the command was 30 successful, then control returns to the user interface of block 206

through state 254. However, if the command was not successful, then control passes to state 256 which functions similarly to state 240 in that unsuccessful attempts are counted, such that when the preselected number of unsuccessful attempts is reached, control
5 passes to state 242 where the system halts.

The embodiments described above allow an user to access a user level security interface on the drive without relying upon system BIOS compatibility. This stand-alone capacity of the drive facilitates interoperability as well as mobility of drives that contain
10 sensitive or confidential information.

In conclusion, a disc drive 100 is disclosed including a built-in drive security system. The drive 100 generally includes at least one disc 104 having a disc surface. A spindle motor 126 is coupled to the disc 104 for causing rotation of the disc 104. A head 110
15 reads information from the surface of the disc 104. An actuator 112 is coupled to the head 110 for responsively positioning the head 110 over the surface of the at least one disc 104. A non-volatile memory 134 contains security state information. A disc controller 124 within the drive 100 includes control circuitry 128
20 coupled to the non-volatile memory 134, the spindle motor 126 and the actuator 112 for controlling operation of the drive 100 in response to security state information. The disc controller 124 also includes read circuitry 130 coupled to the head 110 to receive information from the head 110. An Input/Output (I/O) port 132 is
25 coupled to the control circuitry 128 and the computer 118 such that information can be transferred between the I/O port 132 and the computer 118 to provide user level security interface software to the computer 118. The interface software, when executed by the computer 118, generates an user level security interface upon the
30 computer 118, which interface allows selectable access to data on

the at least one disc 104 based upon user input from the user level security interface and the security state information. The interface software can be stored in the non-volatile memory 134. The drive 100 can include built in security features that operate with
5 compatible BIOS, while using the built-in interface for computers having BIOS's that do not support the built-in security features. One example of a built-in security feature is the ATA5 Security Mode feature. The built-in interface can allow authorized users to change passwords as well as disable drive security. The user
10 interface can count unsuccessful access attempts and halt operation of the computer 118 if the number of unsuccessful attempts reaches a preselected threshold.

In accordance with another aspect of the invention, a method includes a number of steps for providing security on a disc drive
15 100. One step receives a request from the computer 118 for the disc drive 100 to provide an operating system to the computer 118. Another step responds to the computer's request by providing user level security interface software instead of the operating system. The computer executes the interface software and generates an
20 interface that allows user level security information to be modified by an authorized user. Upon termination of the user interface, the drive provides the requested operating system and the boot process resumes.

It is to be understood that even though numerous
25 characteristics and advantages of various embodiments of the present invention have been set forth in the foregoing description, together with details of the structure and function of various embodiments of the invention, this disclosure is illustrative only and changes may be made in detail, especially in matters of
30 structure and arrangement of parts within the principles of the

present invention to the full extent indicated by the broad general meaning of the terms in which the appended claims are expressed. For example, the particular elements may vary depending on the particular application for the disc drive while
5 maintaining substantially the same functionality without departing from the spirit and scope of the present invention. Further, although embodiments of the present invention have been described with respect to a single password and absolute access, it is expressly contemplated that any suitable number of
10 passwords can be provided any varying degrees of user access can be allowed in response thereto. Additionally, different users can be granted access to different physical or logical portions of the disc drive depending on their individual passwords.



WHAT IS CLAIMED IS:

1. A storage device comprising:
 - at least one rotatable disc having a disc surface;
 - a head supported relative to the disc surface;
 - 5 a non-volatile memory containing security state information; and
 - a disc controller adapted to provide user level security interface software, wherein the security interface software includes program instructions for generating a user level security interface and wherein the controller provides selectable access to data on the at least one disc based upon the security state information and user input from the user level security interface.
 - 15
2. The device of claim 1 wherein the user level security interface software is stored in non-volatile memory.
- 20 3. The device of claim 2, wherein the user level security interface provides access to a built-in security feature in the drive.
4. The device of claim 1, wherein the user interface allows an authorized user to change passwords.
- 25 5. The device of claim 1, wherein the user interface allows an authorized user to disable drive security.



-13-

6. The device of claim 1, wherein the drive operates in accordance with ATA-5 specification.
7. The device of claim 1, wherein the user interface allows a
5 preselected number of unsuccessful access attempts before halting operation of a connected system.
8. A method of providing security for data stored on a storage device, the method comprising steps of:
- 10 a) receiving, in the storage device, a request for the storage device to provide an operating system;
- b) responding to the request by providing an user level security interface software instead of the requested operating system;
- 15 c) executing the user level security interface software;
- d) creating a user interface that displays user level security information and selectably allows modification thereto; and
- e) upon authorized termination of the user level security interface, the storage device providing the operating
20 system such that the operating system is executed.
9. The method as recited in claim 8 wherein the user interface prompts a user to enter a password if the drive is in a locked state.
- 25
10. The method as recited in claim 9, wherein the user interface allows the user to change passwords if the user enters the correct password.



-14-

11. The method as recited in claim 9, wherein the user interface allows the user to disable drive security if the user enters the correct password.
- 5 12. The method as recited in claim 9, wherein operation of a connected system is halted if the user reaches a preselected number of unsuccessful access attempts.
13. The method as recited in claim 8, wherein the storage drive
10 operates in accordance with the ATA-5 specification.
14. A disc drive comprising:
at least one rotatable disc having a disc surface;
a head supported relative to the disc surface; and
15 means for generating a user level security interface to
access one or more security features of the drive.