(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 September 2005 (15.09.2005)

PCT

(10) International Publication Number
WO 2005/086005 A1

(51) International Patent Classification[7]: G06F 12/14, 9/445

(21) International Application Number: PCT/AU2005/000317

(22) International Filing Date: 4 March 2005 (04.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2004901143 5 March 2004 (05.03.2004) AU

(71) Applicant *(for all designated States except US)*: **SECURE SYSTEMS LIMITED** [AU/AU]; Level 1, 80 Hasler Road, Osborne Park, WA 6017 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WYNNE, Michael John** [AU/AU]; 352 Huntriss Road, Woodlands, Western Australia 6018 (AU). **GEDDES, Michael Ross** [AU/AU]; 1 Ullswater Glade, Joondalup, Western Australia 6027 (AU).

(74) Agent: **GRIFFITH HACK**; Level 6, 256 Adelaide Terrace, Perth, Western Australia 6000 (AU).

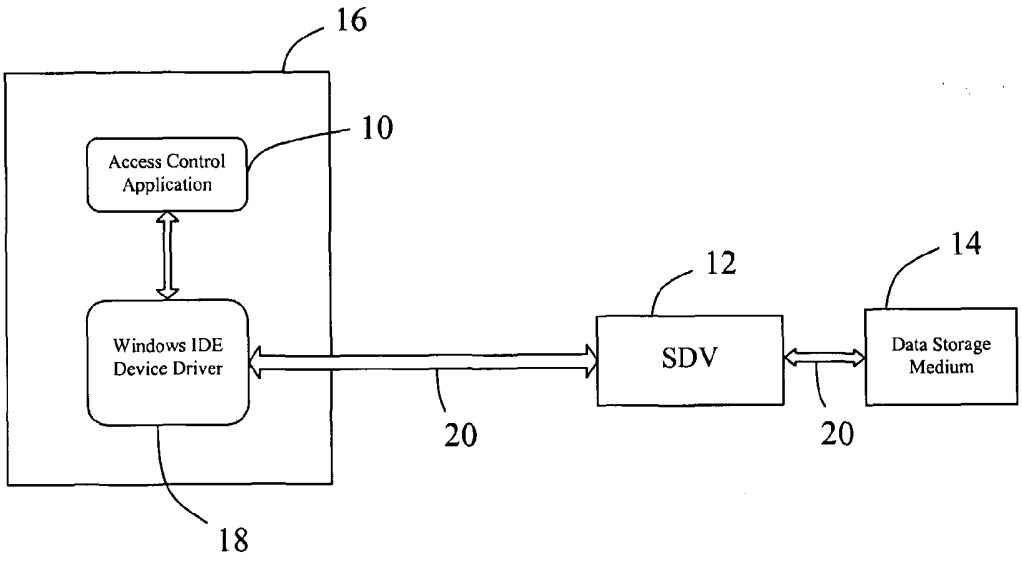
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PARTITION ACCESS CONTROL SYSTEM AND METHOD FOR CONTROLLING PARTITION ACCESS



(57) Abstract: An access control system (10)is disclosed for controlling access to data stored on at least one data storage medium (14)of a computing system. The access control system (10)comprises authentication means (25) to authenticate users permitted to access data stored in the at least one data storage medium (14) and database means (29)arranged to store data access profiles. Each data access profile is associated with a user permitted to access data stored in the at least one data storage medium (14), each data access profile includes information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium (14), and each data access profile includes a master data access profile (M)and a current data access profile (C). The current data access profile (C) is modifiable within parameters defined by the master data access profile (M).

WO 2005/086005 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PARTITION ACCESS CONTROL SYSTEM AND METHOD FOR CONTROLLING PARTITION ACCESS

Field of the Invention

The present invention relates to a partition access control system and method for computers that has particular utility for controlling user access to a data storage medium of a computing system.

Throughout the specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Background of the Invention

The following discussion of the background art is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was part of the common general knowledge as at the priority date of the present application.

With widespread developments in computer networking technology and computer use generally, the security of computer systems and especially accessing of data on storage media by such systems, has become of paramount importance to prevent unauthorised access by users and programs such as viruses, worms and other types of malware.

It is known to provide an operating system wherein a degree of protection against unauthorised access is

provided by defining access permission to data stored on a storage medium for each user, and requiring authentication of the users, for example using a user name and password, prior to authorising access to the storage medium.

However, such an arrangement provides only a minimal degree of protection against unauthorised access to data storage media.

It is known to provide a system and method for securing data and information stores in a computer system which involves the use of a discrete security device interposed between a host central processing unit (CPU) and a mass data storage medium of the computer system. The security device controls and coordinates access to the mass data storage medium based on pre-defined user access profiles.

It is also known to provide such a security device which is integrated into a bus bridge circuit provided on the motherboard of the computer system or into a bus bridge circuit provided in the hard disk drive itself.

With both arrangements, the security device under control of a system administrator is able to set data access permissions for partitions provided on the mass storage medium of the computer system and for each user of the computer system. The data access permissions include read only access, write only access, read and write access, or no access. In this specification, a set of data access permissions defined for a particular user is termed a "user access profile".

In order to ensure the integrity of the computer system incorporating the security device, the security device is configured to only authenticate users and assign user access profiles to users at start up of the computer system before loading the computer operating system.

Modification of the user access profile for a particular user after loading the operating system is not possible.

However, while such an arrangement provides a high degree of security, the arrangement is relatively inconvenient to a user in the event that the user is assigned multiple access profiles for various circumstances, such as when connected or not connected to the Internet. In this instance, if the user is logged in according to an access profile which does not allow Internet access, in order to obtain Internet access the user would be required to shut down the operating system and adopt a different user profile appropriate for connecting to the Internet during the authentication stage of the start up process.

Such a process is inconvenient to a user of the system and can significantly detract from operation efficiency.

Summary of the Invention

In accordance with a first aspect of the present invention, there is provided an access control system for controlling access to data stored on at least one data storage medium of a computer system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium; and

database means arranged to store data access profiles;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile, the current data access profile being modifiable within parameters defined by the master data access profile.

In one arrangement, the access control system further comprises profile setting means arranged to facilitate creation of the master and current access profiles.

The access control system may be incorporated into a computing system having an operating system and the master data access profile may be modifiable only prior to loading of the operating system.

In one embodiment, the control system is activatable so as to permit modification of the current access profile and deactivatable so as to prevent modification of the current access profile.

The access control system may be implemented at least in part in the form of software.

In addition, or alternatively, the access control system may be implemented at least in part in the form of hardware.

In one embodiment, the access control system is arranged to govern user access profiles used by a security device configured to control access to a data storage medium. The security device may be implemented at least in part in hardware and may be of a type located between a data storage medium of a computing system and a CPU of the computing system. Alternatively, the security device may be implemented at least in part in hardware and may be of a type incorporated into bus bridge circuitry of a computing system.

In one arrangement, the access control system is incorporated into a computing system having an operating system and the current access profile is modifiable after loading of the operating system.

In accordance with a second aspect of the present invention, there is provided a method of controlling access to data stored on at least one data storage medium of a computing system, the method comprising the steps of:

providing means for authenticating users permitted to access data stored in the at least one data storage medium;

storing data access profiles;

associating each data access profile with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile; and

facilitating modification of the current data access profile within parameters defined by the master data access profile.

In accordance with a third aspect of the present invention, there is provided computer program which when loaded into a computing system causes the computing system to operate in accordance with an access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium; and

database means arranged to store data access profiles;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile, the current data access profile being modifiable within parameters defined by the master data access profile.

In accordance with a fourth aspect of the present invention, there is provided computer useable medium having a computer readable program code embodied therein for causing a computer to operate in accordance with an access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium; and

database means arranged to store data access profiles;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile, the current data access profile being modifiable within parameters defined by the master data access profile.

Brief Description of the Drawings

The present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a block diagram showing a computing system including a partition access control system in accordance with a first embodiment of the invention, with the access control system shown in relation to a security device (SDV) of the type arranged to protect a computer system data storage medium;

Figure 2 is a block diagram of the logical structure of the access control system shown in Figure 1 and an SDV interfaced with the access control system;

Figure 3 is a depiction of a main screen displayed by a graphical user interface (GUI) of the access control system shown in Figures 1 and 2, the main screen showing partitions provided on the data storage medium of a computer system and the data access permissions available to a particular user of the computer system;

Figure 4 is a flow diagram showing an initialisation process for a computer system incorporating the access control system shown in Figures 1 and 2 and an SDV;

Figure 5 is a panel displayed by the GUI in order for a "super user" to access the computer system including the access control system shown in Figures 1 and 2 and initialise user access profiles;

Figure 6 is a panel displayed for the purposes of authenticating a "super user";

Figure 7 is a panel displayed to a "super user" for the purpose of configuring a user access profile;

Figure 8 is a panel superimposed upon the display panel of Figure 7 for the purpose of defining data access permissions for a specific partition during configuration of a user profile;

Figure 9 is a flow diagram showing the logical processes performed by a user when invoking the access control system;

Figure 10 shows a password entry box for authenticating a user to access the access control system;

Figure 11 shows a partition access control table for a user authenticated to use the access control system;

Figure 12 is a flow diagram showing normal system operation of a computer system incorporating SDV and access control system process flows; and

Figure 13 shows a user authentication box displayed to a typical user during authentication of the user to the SDV prior to booting of the operating system.

Description of an Embodiment of the Invention

Referring to the drawings, there is shown a partition access control system implemented in this example in the form of a software application and configured so as to operate in association with a security device arranged to control and coordinate access to a mass data storage medium of a computing system.

However, while the present embodiment is described in relation to an access control system implemented in the form of software, it will be understood that other arrangements are possible. For example, the access

control system may be implemented at least partially in hardware.

It will also be understood that the presence of a security device is not essential to the invention and other arrangements are possible. For example, the access control system in accordance with the present invention may be configured so as to operate in association with an appropriate access control application of an operating system.

The foregoing embodiments are directed towards an access control system arranged to control access by a user to a data storage medium, and which allows a user to modify a respective user data access profile within predefined parameters.

In the present embodiment, the computer system into which the access control system is incorporated is in the form of a standard personal computer (PC) comprising a central processing unit (CPU), standard peripheral devices such as monitor, keypad, mouse and printer, a data store in the form of a mass data storage medium such as a hard disk drive (HDD), and a security device (SDV) of the type described in patent specification WO 03/003242 for controlling and coordinating data access to the mass data storage medium.

As described in patent specification WO 03/003242, the SDV is interposed in the data access channel between the CPU and the HDD, and controls data access to the HDD by users. This control is effected using an authentication process, whereby a user having permission to access data on the HDD must be authenticated prior to booting of the PC operating system, and must be provided with a specific partition access profile that determines the data access permissions for the user in respect of the various partitions of the

data storage medium. Furthermore, the SDV is designed to enforce the data access regime for each particular user authenticated by the system, to deny access to portions of the data storage medium in accordance with the partition access profiles, and to deny access by users that are not authenticated and/or by spurious processes.

As described, the authentication process is invoked during operation of the basic input output system (BIOS) after the "drive ID" check is performed, and the authentication program is run by the CPU on loading the "custom" boot sector provided by the SDV in place of the normal boot sector or master boot record normally stored in the data storage medium.

As described, it is only after a user has been properly authenticated and the processes undertaken by the user during operation of the authentication application program have been completed that the BIOS program proceeds with permitting access to the data storage medium and loading of the operating system under which the user may subsequently operate the computer and access the data storage medium in accordance with the relevant data access profile.

As shown in Figure 1, a partition access control system in accordance with the present embodiment is specifically configured to interact with a security device (SDV) 12 of the type described above. In the present example, the access control system is implemented in software as a partition access control application 10 and stored in a location in a data storage medium 14 of a PC.

In the present embodiment, the access control application 10 is written as a Windows program developed in VC++ and MFC to operate within a Windows operating system 16, although it will be understood that other arrangements are

possible. The access control application 10 interfaces with a Windows IDE device driver 18 via a Windows Application Program Interface (API) and communicates with the data storage medium 14 along an IDE cable 20. As illustrated, the SDV 12 is connected in line with the IDE cable 20 so as to intercept all communications between the Windows IDE device driver 18 and the data storage medium 14.

The access control application 10 uses services provided by the Windows API of the host operating system, which may be Windows 2000 or Windows XP, for communicating with the SDV 12 and the user.

However, it will be appreciated that the access control application 10 may also be arranged to interface with other operating systems such as LINUX.

As shown in Figure 2 of the drawings, the access control application 10 comprises logical processes in the form of an authenticator 25 and a control system engine 27, the control system engine 27 communicating with a database 29 which may form part of the SDV 12 or may form part of the data storage medium 14.

The access control application 10 is invoked to operate normally under operation of a CPU 31 of a PC under control of the operating system 16, and interacts with an SDV engine 35, the SDV engine 35 controlling data access between the CPU 31 and the data storage medium 14.

As previously described, the data storage medium 14 may comprise a one or more HDDs, each having one or more partitions. In the present embodiment, the drives/partitions are C:\, D:\, E:\, F:\, G:\, H:\ and I:\.

The control system engine 27 of the access control application 10 comprises a profile setter 37 and an editor 39 which are arranged to populate the database 29 in a prescribed manner. These components will be described in more detail later.

The database 29 is designed to logically store two types of data access profile for each user permitted access to the data storage medium 14 of the PC. The data access profiles include a master data access profile M1 to Mn for users 1 to n, and a current data access profile C1 to Cn. Each data access profile defines the data access permissions of a particular user for those partitions that the user is permitted to access.

For example, as illustrated in Figure 3, a user profile screen 40 is shown wherein a user associated with a user profile has access to six partitions 42 indicated by the drives C:\, E:\, F:\, G:\, H:\ and I:\, with the relevant partition size 44 indicated for each partition. Further details 46 indicating whether the partition is bootable, whether partition access control is enabled or disabled, and the current permissions applying to the particular partition or drive are also shown. As indicated in the "current permissions" column, several data access permissions are available for each partition, namely "read only", "write only" "read/write" and "no access".

The authenticator 25 of the access control application 10 functions separately to the authentication program of the SDV 12 and is provided to authenticate users permitted to use the access control application 10. As will be described in more detail later, the SDV 12 is configured so that an administrator or "super user" of the SDV 12 is permitted to configure data access profiles of users permitted to access the data storage medium 14 of the PC.

The authenticator 25 works in conjunction with the control system engine 27 and interacts with the database 29 via the SDV engine 35 to permit either super user access or normal user access to the access control application 10 with corresponding functionality applicable to the status of the user and the relevant master data access profile.

Each data access profile stored within the database 29 includes the following information:

> a user name and password for each permitted user,

> the partitions of the data storage medium to which the user is permitted access, and

> the permissions state for each partition to which the user is permitted access.

The various permissions states serve to define different degrees of data access to the data stored within each partition, including low or no permission, permission to read data from a partition, permission to write data to the partition, or total permission to read or write data from or to the partition.

In the present embodiment, the range of possible permissions is as follows:

No access - no permission to read or write data.

Read Only - no permission to write but permission to read.

Read/Write - total permission to read and write data.

The profile setter 37 is particularly designed to allow setting of a master data access profile and a current data access profile. The master data access profile effectively sets the scope within which a user may change or alter the user's current data access profile using the access control application 10.

The editor 39 may be invoked by either a super user or normal user of the access control application 10 in order to edit the master data access profile or the current data access profile of a user respectively. Thus, if a super user is identified by the authenticator 25, the control system engine 27 allows the super user to operate the editor 39 in a manner so as to access and vary the master data access profiles of any permitted user of the PC stored within the database 29. If the authenticator 25 authenticates a user as a normal permitted user, the control system engine 27 permits the editor 39 to be operated by the user in a manner so as to allow the current data access profile of the authenticated user to be modified within the parameters defined by the master data access profile previously determined for the user.

It will therefore be understood that the parameters defined by the master data access profile only permit modification of the data access permission for a partition to the same or a lower degree of data access. Importantly, the parameters defined by the master data access profile do not permit a user to modify the data access permission for a particular partition to a higher degree of data access than specified for the permitted user in the master data access profile.

By way of example, if the master data access profile associated with a user specifies that the user has "read only" access for partition or drive E:\, then the user is only able to modify the current data access permission for

drive E:\ to "no access". It is not possible to change the data access permission for drive E:\ to "read/write" access.

It follows that if the master data access profile associated with a user specifies that the user has "no access" to drive or partition E:\, the user would be denied from making any change to the current data access permissions for drive or partition E:\.

Thus the profile setter 37 only permits a current user data access profile to be passed to the SDV engine 35 for subsequent use by the SDV 12 that conforms with the parameters of the master data access profile of the user.

In order to obtain a better understanding of how the access control application 10 is configured for process flow and interaction with a user via a graphical user interface (GUI) provided as part of the Windows API, operation of the access control application will now be described in relation to Figures 4 to 13.

The software flow performed by the SDV 12 during an initialisation phase is shown in Figure 4.

Installing the SDV hardware 12 by connecting it in line with the IDE cable 20 between the CPU 31 and the data storage medium 14 is represented at 41. The HDD's of the data storage medium 14 are then formatted with the required number of partitions at 43, the HDD's are installed under the control of the operating system of the PC at 45. A CD ROM containing set up software for the SDV 12 is inserted into the CD ROM drive of the PC at 47 and the set up program is loaded under the control of the operating system 16.

If the SDV 12 has not yet been initialised, the software flow at 49 invokes a process at 51 for setting up a super user for the SDV 12. The super user is able to set up user names and passwords for all permitted users of the PC and their associated master data access profiles. This process invokes a GUI at 53 to create a super user display panel 55 as shown in Figure 5 of the drawings. The display panel 55 allows a super user name to be created and a password to be set for the super user. The display panel 55 also allows the super user to enable access control for permitted users of the PC if desired and set an access control password for the super user with confirmation of the access control password and an identity string to authenticate the super user when invoking the access control application 12. A "finish" button 57 is also provided at the bottom of the screen to allow the super user to exit the process at 59.

Once a super user account has been created, the SDV 12 is considered to be initialised and progresses to a user account configuration state, wherein the super user can set up individual user accounts for the users permitted access to the PC and to allow for their authentication.

As shown, the software flow may proceed to super user configuration of user accounts commencing at step 61 either immediately after the setup of the super user via the exit process 59, or via the decision box 49 if the SDV 12 has previously been initialised. The process commences at 61 by displaying a user authentication panel 63, as shown at Figure 6 of the drawings, and prompting the super user to enter their user name and pass phrase for correct authentication at 65. An authenticate button 67 is provided on the display panel 63 to effect authentication at 69. If a super user is not authenticated at this stage, the program flow exits at 71 and the setup program for the

SDV 12 needs to be restarted and the process repeated until such time as a super user is authenticated.

On valid authentication at 69, the software invokes a process at 73 that allows a super user to create each individual user account, assigning individual user pass phrases and access rights to configure the master data access profiles for the individual users.

This process uses a display panel 75 as shown in Figure 7 to configure each individual user profile at 77. The display panel 75 includes data entry fields for a user name, password, password confirmation, access control password, access control password confirmation and an identity string. The display panel 75 also includes two partition panels, a first partition panel 79 listing the various partitions formatted on the HDD of the data storage medium 14 and a second partition panel 81 the partitions that have been selected by the super user for access by a particular user.

As shown in Figure 7, the partition name and memory address map is provided for each formatted and selected partition. A "save" button 83 and a "return to main menu" button 85 are provided at the bottom of the display panel 75 to save the configuration and return to normal program flow respectively.

In order to select partition access, permissions and access control accessibility for individual users, a process 87 is invoked which causes the GUI to show a display panel 89 superimposed on the user profile configuration panel 77 as shown in Figure 8.

The display panel 89 allows the start sector address, the partition size, access mode and setting of the access control mode for the particular partition access of the

user to be identified. As indicated, drop down menus are provided for "access mode" and "access control mode" entry fields to allow selection of fixed permission access modes, i.e. read only, read/write and no access, for the purposes of setting the access mode, and "enabling" or "disabling" flags for the access control mode respectively. An "ok" button 93 and a "cancel" button 95 are provided at the bottom of the display panel 91 to allow for completion of the partition details selection of the highlighted partition.

After each user profile configuration has been completed, a check is made as to whether the super user has configured all users at 97 and, if not, the user profile configuration step 73 is carried out for another user. If profile configuration of all users has been completed, the initialisation procedure stops, as indicated at step 99.

As previously described, in the present example the access control application 10 operates as an application under the operating system 16 and interfaces with the Windows API to communicate with a user and the SDV engine 35. The software flow of the access control application 10 is shown in Figure 9.

The access control application 10 is invoked by a user at 101 and a password entry display panel 105 as shown in Figure 10 is displayed. The display panel 105 is used to enter the relevant access control password for user authentication.

The display panel 105 includes a "login" button 107 and an "exit" button 109 to continue or exit the access control authentication process. If continued by pressing the "login" button 107, the access control application 10 communicates with the SDV 12 for authentication at 111, whereupon verification of the authentication occurs at

113. If the user is not authenticated, the user is asked to enter the relevant access control password at 103. If the user is authenticated, the process continues and the control system engine 27 retrieves the partition access control information from the SDV 11 at 115.

The partition access control information for the authenticated user is then displayed to the user in the form of a table 117 as shown in Figure 11. The table 117 corresponds to the table described previously at Figure 3 of the drawings and only those partitions to which the user has been allocated access by the super user are displayed. The user is provided with the option to modify the permissions specified in the table to the extent permitted by the profile setter 37, that is, the degree of data access can be reduced or reasserted under the "current permissions" column in accordance with the master access profile. This is effected by clicking on the particular entry of the "current permissions", whereupon a drop down menu is presented providing the available permissions that are selectable for the particular drive are within the bounds of control determined by the master data access profile previously set for the user by the super user.

An "apply" button 121 and a "close" button 123 are provided at the base of the display panel 117 so that software flow may be progressed at 125. Moreover, if a user has not modified any partition access control and the "close" button 123 is asserted, then the access control application 10 is exited directly at 127. If the user has modified the current permissions and applied them by asserting the "apply" button 121, then the profile setter 37 sends new partition access control information to the SDV 12 at 129 so that the relevant current data access profile stored in the database 29 is modified as appropriate.

The integration of the normal software flow of the access control application, in conjunction with normal SDV system operation, is shown at Figure 12. Like steps are indicated with like reference numerals.

During normal operation of the SDV 12 and the access control application 10, the PC is powered up at 131 and the computer BIOS invoked which subsequently loads the start-up code from the SDV boot device at 133.

The user is prompted at 135 to enter the relevant name and pass phrase via the user authentication display panel 137 which is displayed to the user by the GUI at 139. On pressing the "authenticate" button 141 provided at the bottom of the display panel 137, the SDV authentication process is invoked to authenticate whether the user is a permitted user of the computer system.

If the user is not authenticated at 143, then an attempt counter is incremented (or decremented) and the permitted number of authentication attempts checked at 145. If the number of permitted authentication attempts are exceeded, the software process is exited at 147 and the computer system shutdown. If the number of permitted attempts to authenticate the user has not yet been reached, then the software flow returns to prompting the user to enter the relevant name and pass phase at 135 to provide the user with another authentication attempt.

On authentication of the user at 143, the SDV 12 decrypts the valid user partition access information, which in the present embodiment is stored in the database 29 in a hidden area of memory at 149, to control subsequent data access to the data store in accordance with the current user profile configured for the permitted user.

The computer operating system 16 is then started at 151, whereupon the SDV 12 checks all subsequent data access attempts to the data storage medium 14 at 153 in accordance with the current data access profile of the permitted user. If a data access attempt at 155 is not in accordance with the current data access profile of the user, then the data transfer process, being either a "read" or "write" is blocked at 157, without any access to the HDD being effected. The SDV 12 then returns to its data checking state at 153.

If data access is in conformity with the current data access profile of the user at 155, then the data is checked to ascertain wether the access control application is being invoked at 159. If not, data access to the HDD of the data store 15 is continued at 161, and the power down condition checked at 163. If the power down condition is asserted at 163, the software flow is exited at 165 and the power down process is effected by the computer system. If the power down condition is not asserted, then the software flow returns the SDV 12 to its data checking at 153.

If at 159 the SDV 12 determines that the access control application 10 is invoked, then the access control software flow process as described with respect to Figure 9 is progressed.

If the user has valid access to the access control application 10, the access control application 10 reads the partition access control information stored in the database 29 at 115, and displays the current data access profile of the user at 119.

If the user modifies the relevant access rights at 125 using the editor 39 then the access control application 10 updates the current data access rights stored in the

database 29 of the SDV using the profile setter 37 at 129, and proceeds to exit the access control application 10 at 127. Alternatively, if access rights are not modified at 125, then the access control application exits at 127 directly. On exiting the access control application 10, the power down condition is again checked at 163 and, if asserted, the program flow is exited at 165. If not asserted, the software flow returns the SDV 12 to its data checking state at 153.

In an alternative embodiment, an SDV 12 incorporated into the design of a bus bridge circuit is provided, either in the south bridge of the motherboard on the CPU side of the computer system or, alternatively, in the bridge circuit provided on the data store side, in the case of using a serial AT attachment (SATA) standard for communicating with the data store, as described in the applicant's international patent specification accompanying International Application PCT/AU2004/000210.

It will be appreciated that the control system described in either of the above embodiments allows an authenticated user to change the read and/or write access control partitions for which the user has authorisation during normal system operation under the operating system, without the need to change the user profile during a pre-boot process. Thus, the access control application 10 is installed as standard application software on the hard disk of a computer system and runs under the control of an operating system.

In this manner, only one master data access profile is required for each user, with each master data access profile defining the data access permissions for each partition accessible to the user and enabling access to the partitions within the confines of the master data access profile. This means that it is possible to obtain

complete control over data access that is allowed for the partitions by permitted users, whilst allowing each permitted user to alter their own profile within prescribed parameters governed by the master data access profile.

A further alternative embodiment of the invention may take the form of an access control application which performs all access control functions in relation to a data storage medium, or which operates in conjunction with an operating system instead of in conjunction with a security device such as the SDV described above. With this arrangement, permission or denial of access to drives and/or partitions will be exercised by the operating system within the confines of the master and current data access profiles controlled by the access control application.

A still further embodiment of the invention may take the form of a hardware implemented access control system which is connectable to a computing system and which includes appropriate software to cause the access control system to operate in conjunction with an operating system, an SDV type security device, or any other appropriate access control arrangement.

Some of the advantages provided by the present invention in allowing partition access control to a permitted user within limits as determined by the system administrator or super user are as follows:

- The system administrator has complete control over the users and partitions which may be controlled by the access control application.
- Each user requires only one profile for authentication at start-up.

- The number of passwords a user must remember are minimised.

- In order to protect data on the data store, a user may alter read or write access permissions for those partitions within their permitted bounds of control at any time during normal system operation.

- A user may disable access to all partitions allowing them to leave the computer in a secure state, without turning the power off. A third party must know the permitted users password to be able to gain access to the disabled partitions.

- The access control application can be distributed on CD or downloaded from a website provided on the Internet.

- The access control application can be stored in an encrypted "read only" partition on the HDD to help maintain system integrity.

Where methods and systems of the present invention may be implemented by software applications, or partly implemented by software, then they may take the form of program code stored or available from computer readable media, such as CD-ROMS or any other machine readable media, the program code comprising instructions which, when loaded into a machine such as a computer, the machine then becomes a system for carrying out the invention. The computer readable media may include transmission media, such as cabling fibre optics or any other form of transmission media.

It should be appreciated that the present invention is not limited to the specific embodiments described herein. Accordingly, alternative embodiments and variations from the best mode may be envisaged in accordance with conventional software and computer engineering practice, without departing from the spirit or scope of the present invention.

CLAIMS:

1. An access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium; and

database means arranged to store data access profiles;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile, the current data access profile being modifiable within parameters defined by the master data access profile.

2. An access control system as claimed in claim 1, further comprising profile setting means arranged to facilitate creation of the master and current access profiles.

3. An access control system as claimed in claim 2, wherein the access control system is incorporated into a computing system having an operating system and the master data access profile is modifiable only prior to loading of the operating system.

4. An access control system as claimed in any one of claims 1 to 3, wherein said control system is activatable so as to permit modification of the current access profile and deactivatable so as to prevent modification of the current access profile.

5. An access control system as claimed in any one of the preceding claims, wherein the access control system is implemented at least in part in the form of software.

6. An access control system as claimed in any one of the preceding claims, wherein the access control system is implemented at least in part in the form of hardware.

7. An access control system as claimed in any one of the preceding claims, wherein the access control system is arranged to govern user access profiles used by a security device configured to control access to a data storage medium.

8. An access control system as claimed in claim 7, wherein the security device is implemented at least in part in hardware and is of a type located between a data storage medium of a computing system and a CPU of the computing system.

9. An access control system as claimed in claim 7, wherein the security device is implemented at least in part in hardware and is of a type incorporated into bus bridge circuitry of a computing system.

10. An access control system as claimed in any one of the preceding claims, wherein the access control system is incorporated into a computing system having an operating system and the current access profile is modifiable after loading of the operating system.

11. A method of controlling access to data stored on at least one data storage medium of a computing system, the method comprising the steps of:

providing means for authenticating users permitted to access data stored in the at least one data storage medium; and

storing data access profiles;

associating each data access profile with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile; and

facilitating modification of the current data access profile being within parameters defined by the master data access profile.

12. A method as claimed in claim 11, further comprising the step of facilitating creation of the master and current access profiles.

13. A method as claimed in claim 12, wherein the access control system is incorporated into a computing system having an operating system, and the step of facilitating modification of the current data access profile includes the step of facilitating modification of the master data access profile only prior to loading of the operating system.

14. A method as claimed in any one of claims 11 to 13, further including the steps of facilitating activation of said control system so as to permit modification of the current access profile and facilitating deactivation of said control system so as to prevent modification of the current access profile.

15. A method as claimed in any one of claims 11 to 14, wherein the access control system is implemented at least in part in the form of software.

16. A method as claimed in any one of claims 11 to 15, wherein the access control system is implemented at least in part in the form of hardware.

17. A method as claimed in any one of claims 11 to 16, further comprising the step of arranging the access control system so as to govern user access profiles used by a security device configured to control access to a data storage medium.

18. A method as claimed in claim 17, wherein the security device is implemented at least in part in hardware and is of a type located between a data storage medium of a computing system and a CPU of the computing system.

19. A method as claimed in claim 17, wherein the security device is implemented at least in part in hardware and is of a type incorporated into bus bridge circuitry of a computing system.

20. A method as claimed in any one of claims 11 to 19, further comprising the steps of incorporating the access control system into a computing system having an operating system and facilitating modification of the current access profile after loading of the operating system.

21. A computer program which when loaded into a computing system causes the computing system to operate in accordance with an access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium; and

database means arranged to store data access profiles;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile, the current data access profile being modifiable within parameters defined by the master data access profile.

22. A computer useable medium having a computer readable program code embodied therein for causing a computer to operate in accordance with an access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium; and

database means arranged to store data access profiles;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

each data access profile including information indicative of the degree of access permitted by a user to data stored in the at least one data storage medium; and

each data access profile including a master data access profile and a current data access profile, the current data access profile being modifiable within parameters defined by the master data access profile.

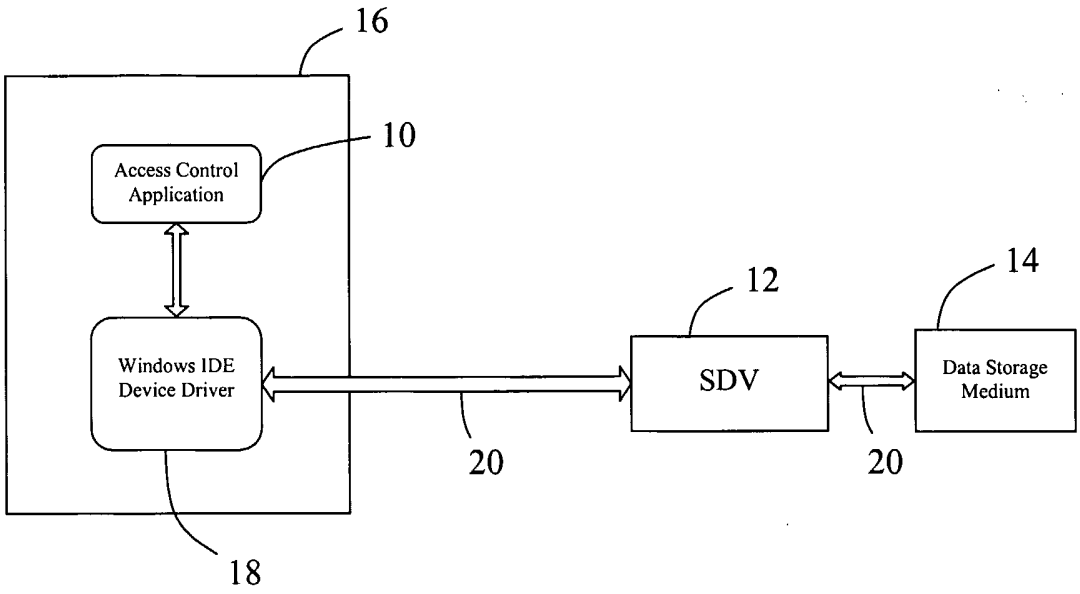

16
10
Access Control Application
Windows IDE Device Driver
18
20
12
SDV
20
14
Data Storage Medium

Fig. 1

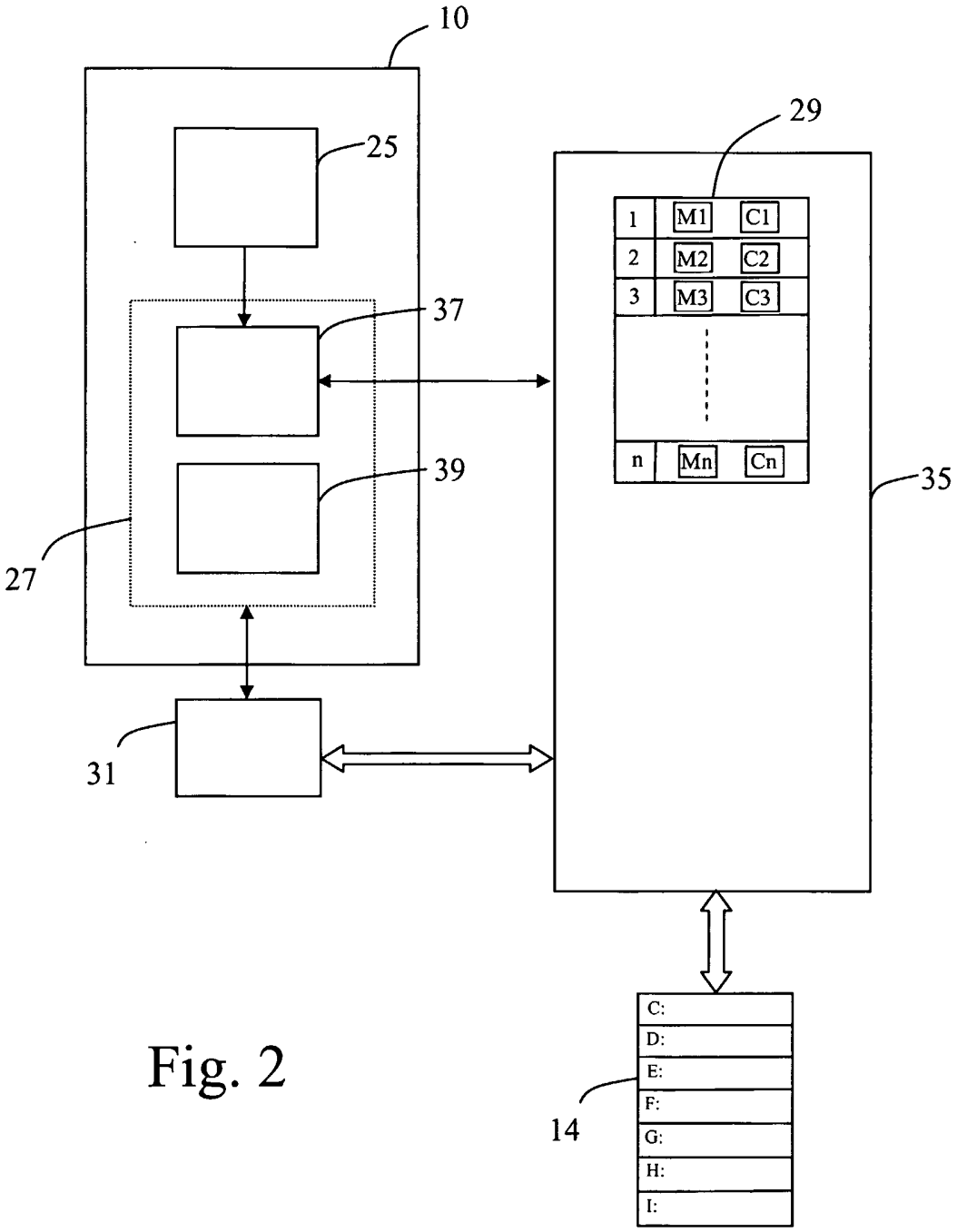


Fig. 2

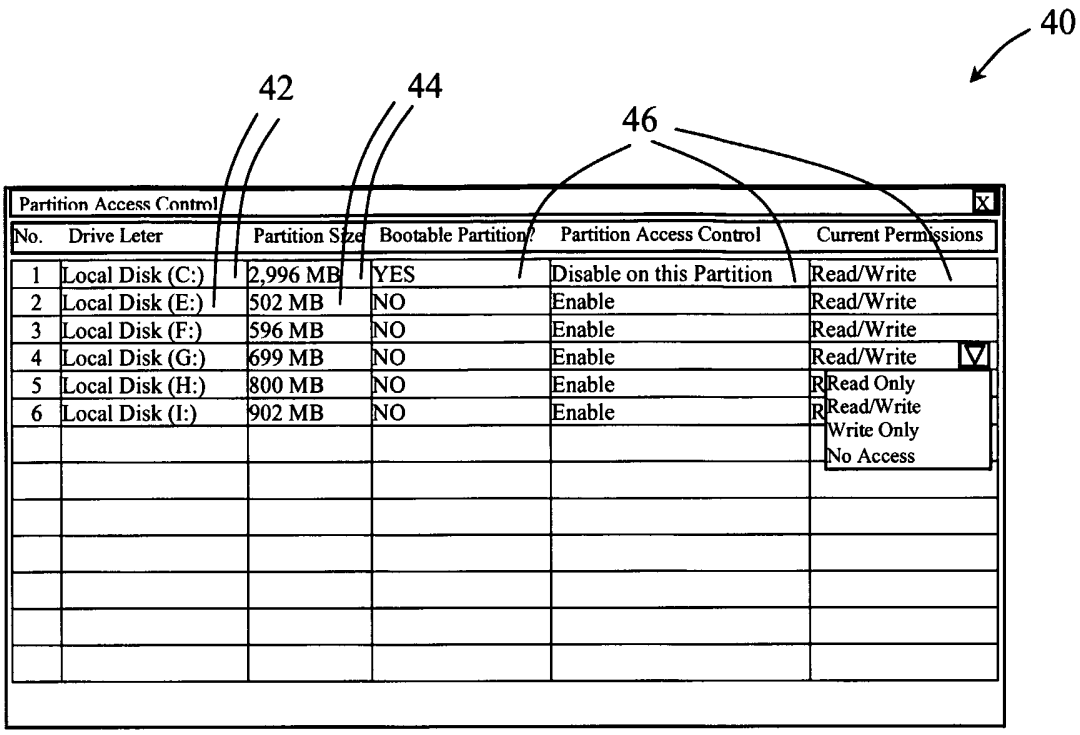

40
42
44
46
Partition Access Control
No.
Drive Leter
Partition Size
Bootable Partition?
Partition Access Control
Current Permissions
1 Local Disk (C:) 2,996 MB YES Disable on this Partition Read/Write
2 Local Disk (E:) 502 MB NO Enable Read/Write
3 Local Disk (F:) 596 MB NO Enable Read/Write
4 Local Disk (G:) 699 MB NO Enable Read/Write
5 Local Disk (H:) 800 MB NO Enable
6 Local Disk (I:) 902 MB NO Enable
Read Only
Read/Write
Write Only
No Access

Fig. 3

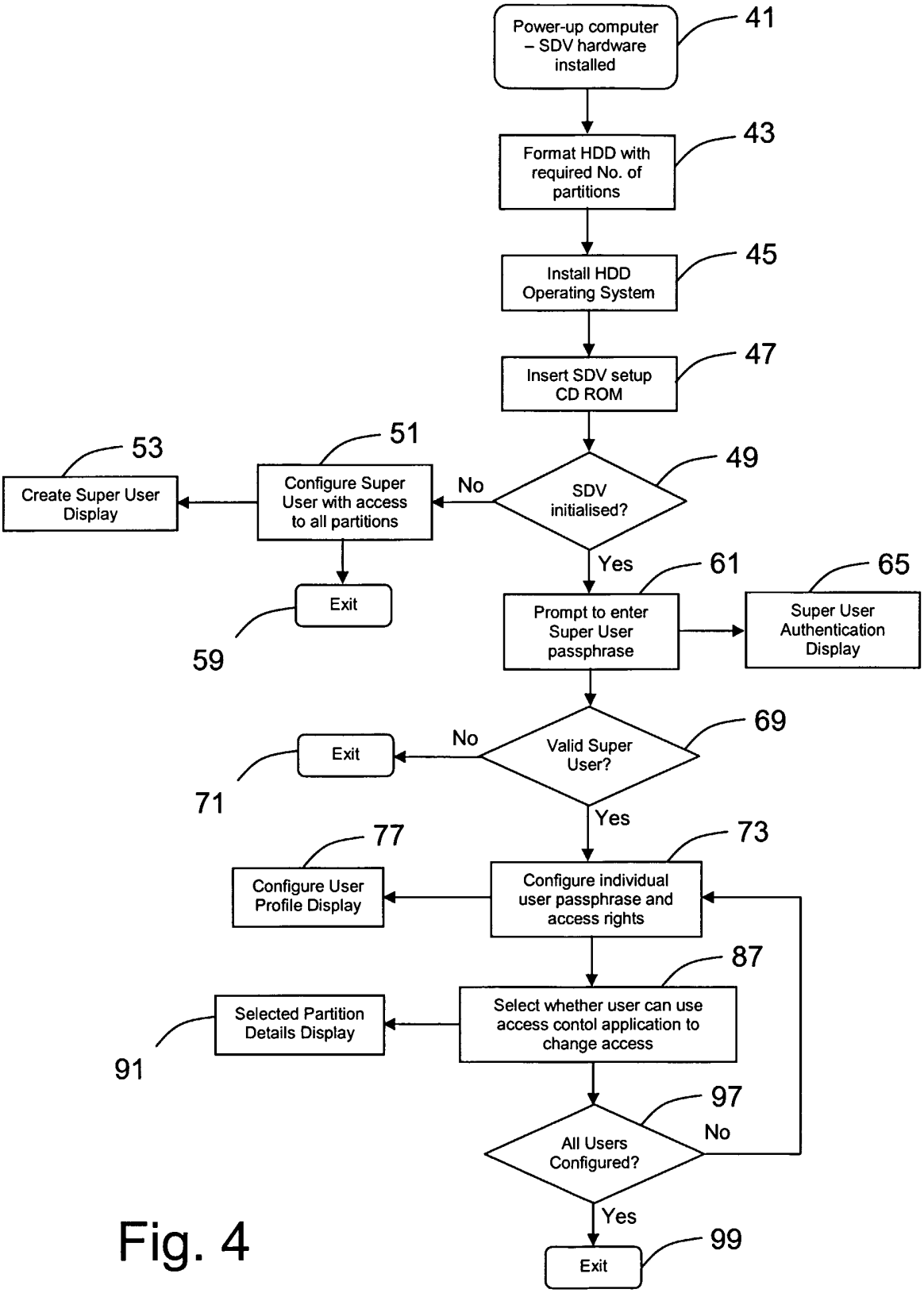

Power-up computer – SDV hardware installed
41
Format HDD with required No. of partitions
43
Install HDD Operating System
45
Insert SDV setup CD ROM
47
SDV initialised?
49
No
Configure Super User with access to all partitions
51
Create Super User Display
53
Exit
59
Yes
Prompt to enter Super User passphrase
61
Super User Authentication Display
65
Valid Super User?
69
No
Exit
71
Yes
Configure individual user passphrase and access rights
73
Configure User Profile Display
77
Select whether user can use access contol application to change access
87
Selected Partition Details Display
91
All Users Configured?
97
No
Yes
Exit
99

Fig. 4

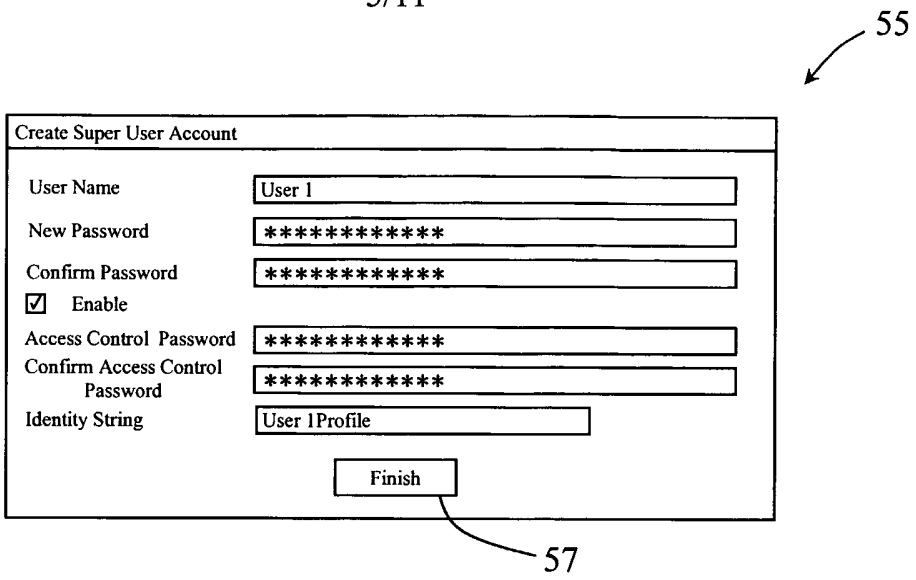

55
Create Super User Account
User Name
User 1
New Password
****
Confirm Password
****
Enable
Access Control Password
****
Confirm Access Control Password
****
Identity String
User 1Profile
Finish
57

Fig. 5

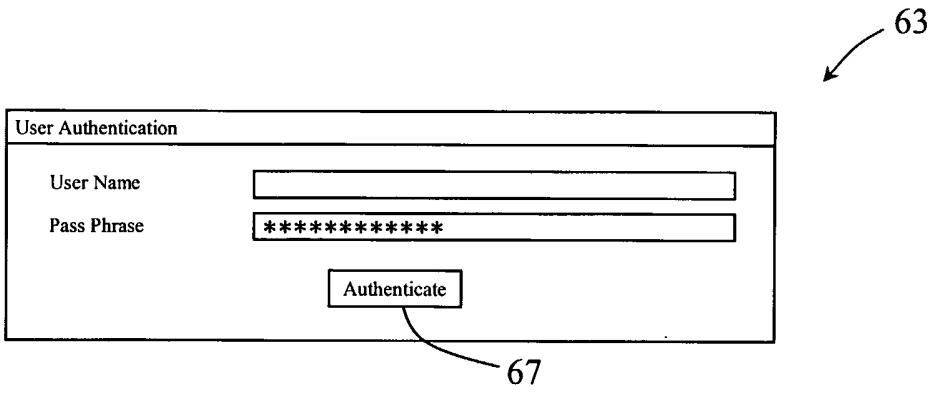

63
User Authentication
User Name
Pass Phrase
****
Authenticate
67

Fig. 6

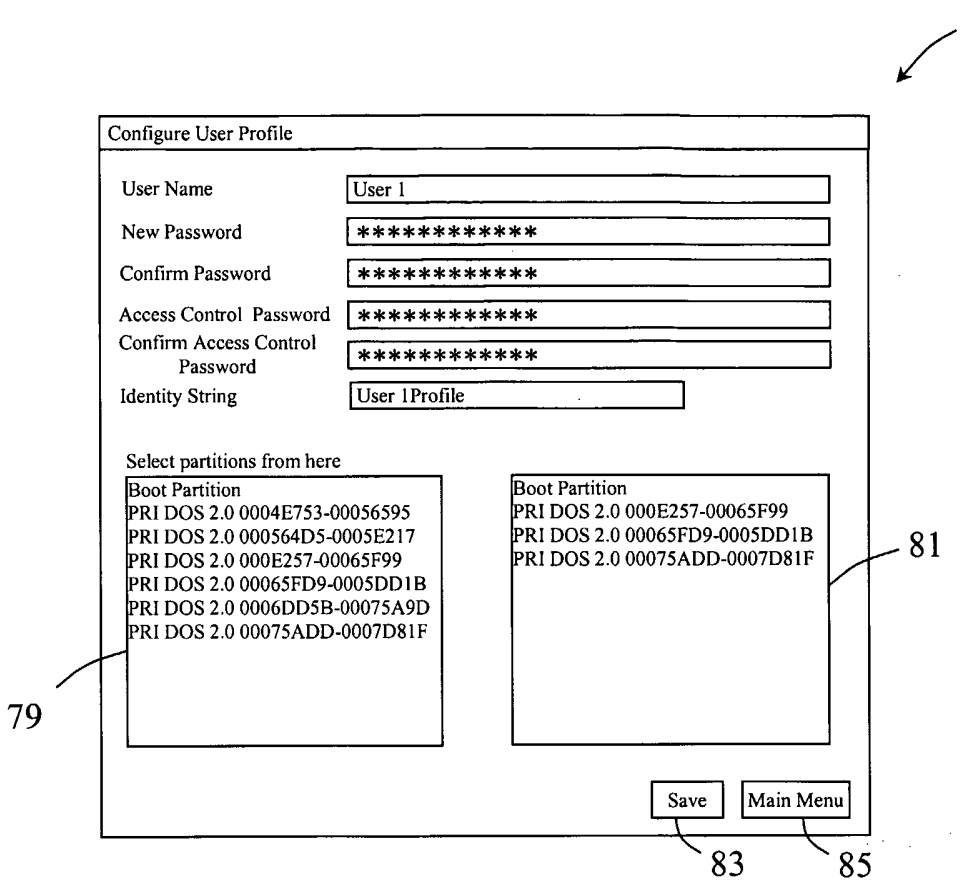

75
Configure User Profile
User Name
User 1
New Password
****
Confirm Password
****
Access Control Password
****
Confirm Access Control Password
****
Identity String
User 1Profile
Select partitions from here
Boot Partition
PRI DOS 2.0 0004E753-00056595
PRI DOS 2.0 000564D5-0005E217
PRI DOS 2.0 000E257-00065F99
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 0006DD5B-00075A9D
PRI DOS 2.0 00075ADD-0007D81F
Boot Partition
PRI DOS 2.0 000E257-00065F99
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 00075ADD-0007D81F
81
79
Save
Main Menu
83
85

Fig. 7

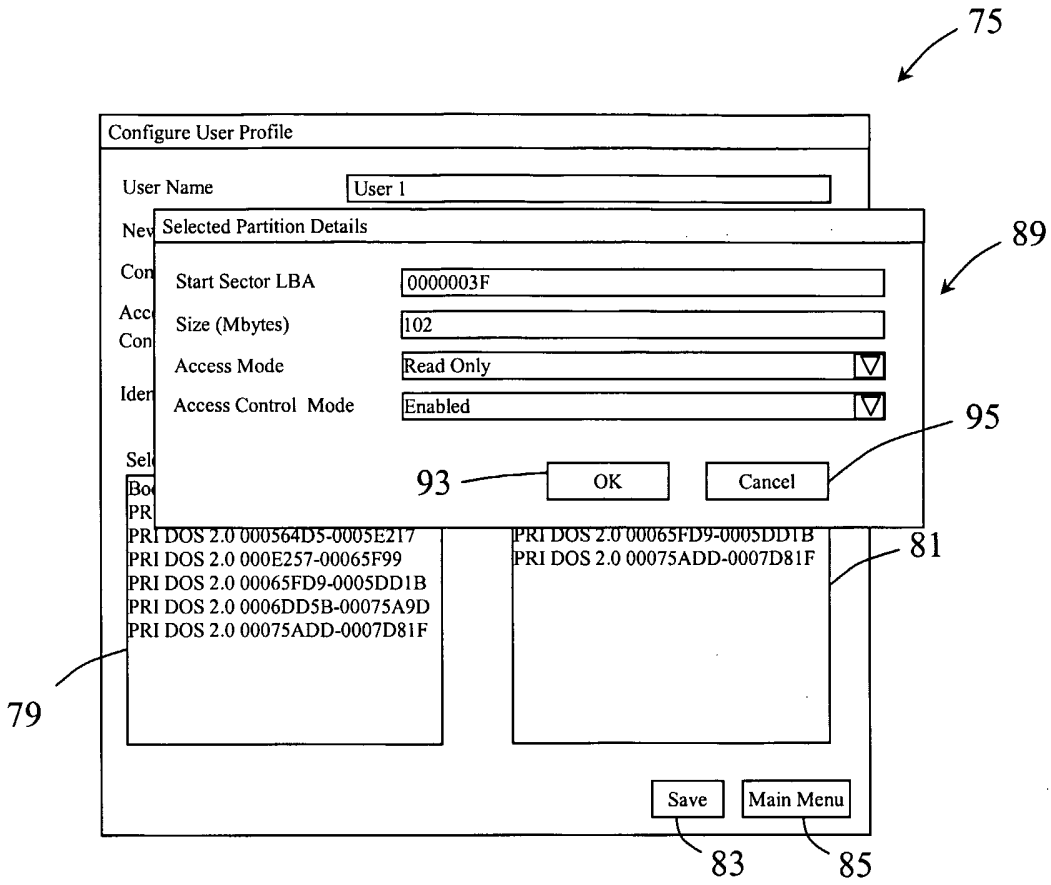

75
Configure User Profile
User Name
User 1
Selected Partition Details
89
Start Sector LBA
0000003F
Size (Mbytes)
102
Access Mode
Read Only
Access Control Mode
Enabled
95
93
OK
Cancel
PRI DOS 2.0 000564D5-0005E217
PRI DOS 2.0 000E257-00065F99
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 0006DD5B-00075A9D
PRI DOS 2.0 00075ADD-0007D81F
81
79
Save
Main Menu
83
85

Fig. 8

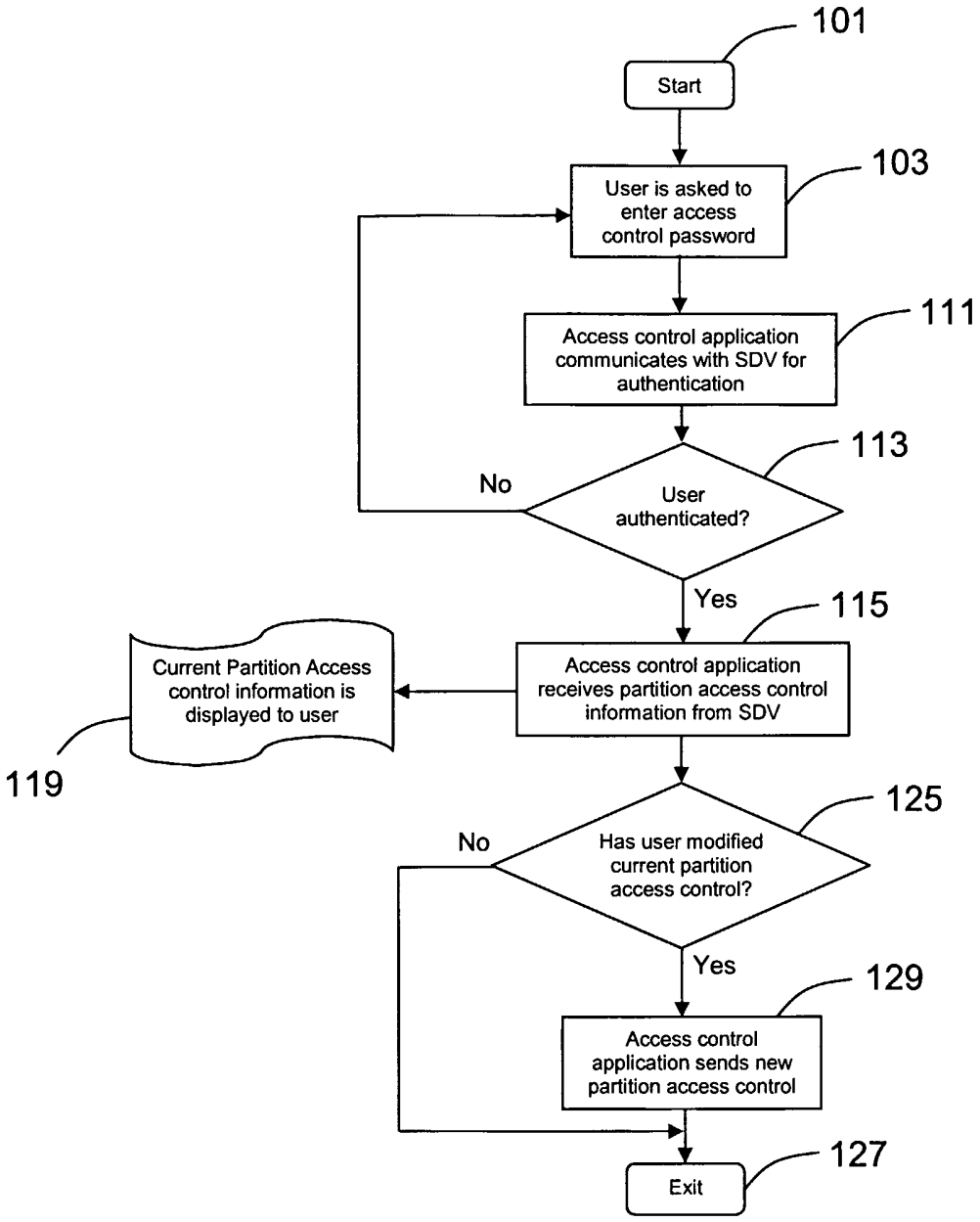

101
Start
103
User is asked to enter access control password
111
Access control application communicates with SDV for authentication
113
User authenticated?
No
Yes
115
Access control application receives partition access control information from SDV
Current Partition Access control information is displayed to user
119
125
Has user modified current partition access control?
No
Yes
129
Access control application sends new partition access control
127
Exit

Fig. 9

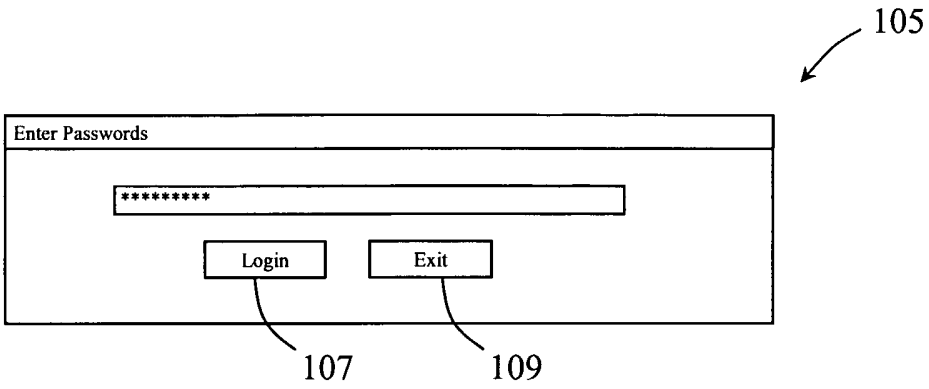

105
Enter Passwords
****
Login
Exit
107
109

Fig. 10

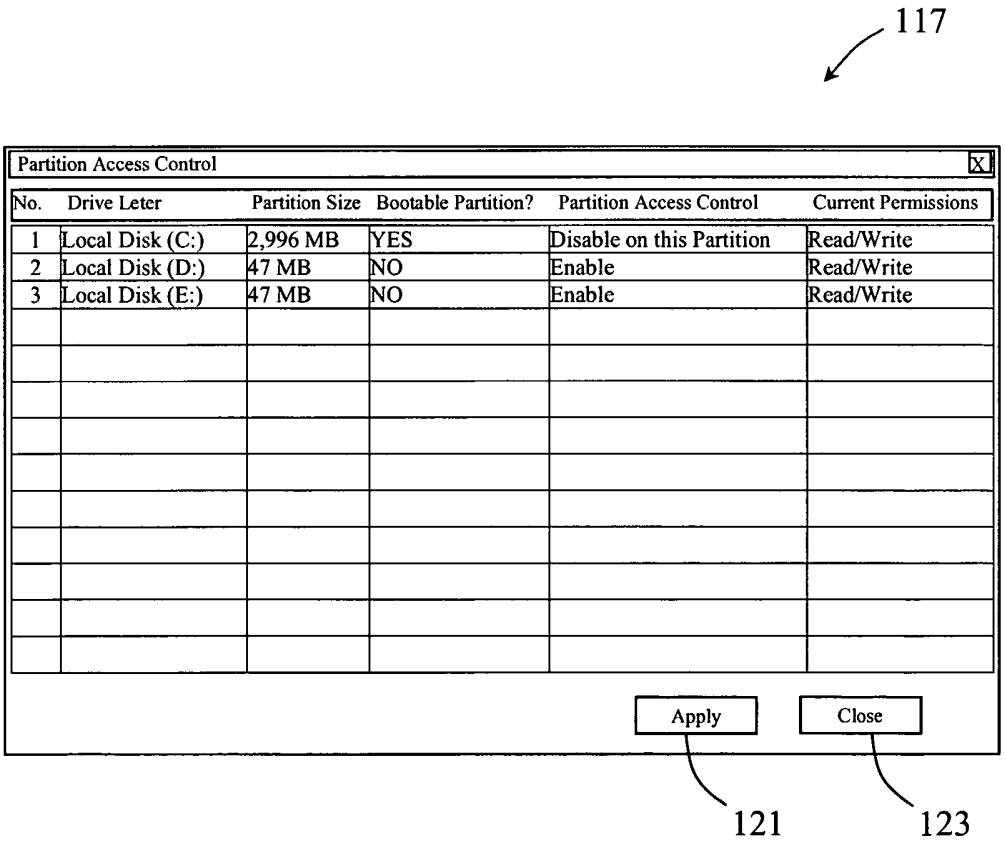

117
Partition Access Control
No. Drive Leter Partition Size Bootable Partition? Partition Access Control Current Permissions
1 Local Disk (C:) 2,996 MB YES Disable on this Partition Read/Write
2 Local Disk (D:) 47 MB NO Enable Read/Write
3 Local Disk (E:) 47 MB NO Enable Read/Write
Apply
Close
121
123

Fig. 11

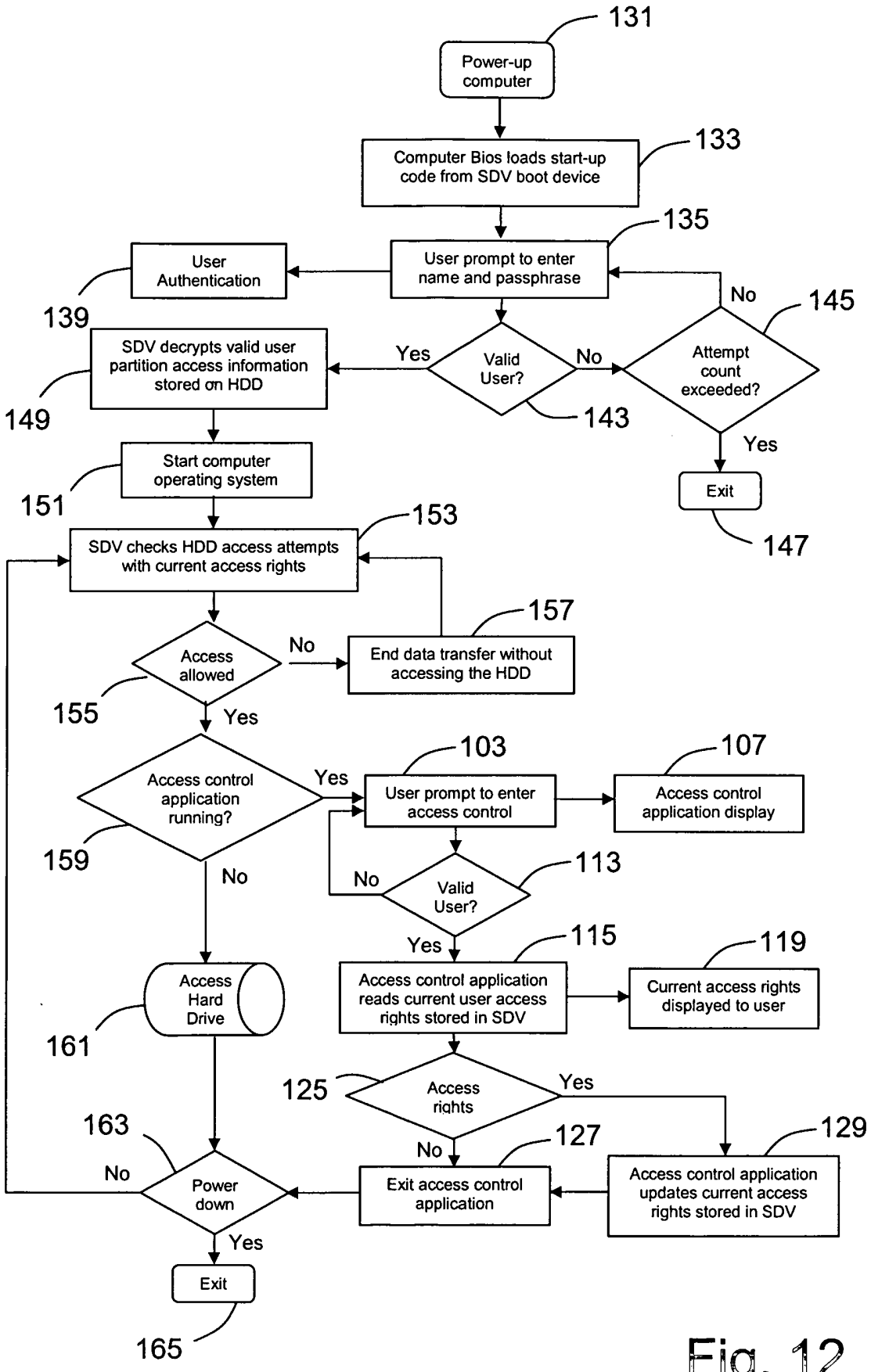

131
Power-up computer
133
Computer Bios loads start-up code from SDV boot device
135
User prompt to enter name and passphrase
User Authentication
139
Valid User?
Yes
No
143
Attempt count exceeded?
No
145
Yes
Exit
147
SDV decrypts valid user partition access information stored on HDD
149
Start computer operating system
151
SDV checks HDD access attempts with current access rights
153
Access allowed
155
No
End data transfer without accessing the HDD
157
Yes
Access control application running?
159
Yes
No
103
User prompt to enter access control
107
Access control application display
No
Valid User?
113
Yes
Access Hard Drive
161
Access control application reads current user access rights stored in SDV
115
Current access rights displayed to user
119
Access rights
125
Yes
No
127
Access control application updates current access rights stored in SDV
129
Exit access control application
Power down
163
No
Yes
Exit
165

Fig. 12

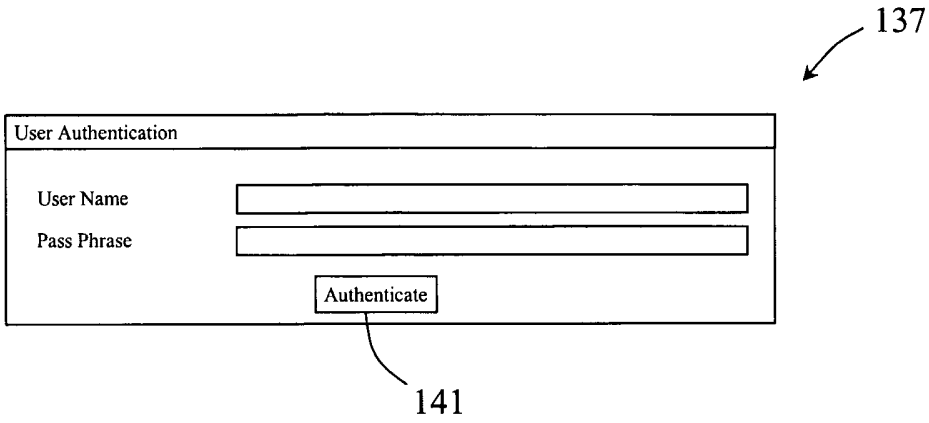

137
User Authentication
User Name
Pass Phrase
Authenticate
141

Fig. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2005/000317

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 12/14, 9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DWPI,USPTO,ESP@CE, GOOGLE, IEEE XPLORE (access, profile, storage, user, secure, authentication and like terms)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Pointsec PC 4.3 Security Target" Version 1.08 Pointsec Mobile Technologies, Inc. (Prepared by SAIC) Published 12 January 2004 URL http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID4010-ST.pdf Downloaded on 25 May 2005. Sections 6.1.X, particularly page 45, page 53 section 6.1.7	1,2,11,12, 21,22
Y	WO 2003/100544 A2 (TELEFONAKTIEBOLAGET LM ERICSSON) 4 December 2003 Whole document	1,2,11,12, 21,22
Y	US 6463537 B1 (TELLO) 8 October 2002 Abstract, figures 13Q,R,S,T,U, column 32 line 4 to column 34 line 47	1,2,11,12, 21,22
Y	WO 2002/019064 A2 (BUCKLEY) 7 March 2002 Abstract, page 3 lines 17-22, page 4 lines 15-30, page 9 lines 1-3,18-21 Page 10 line 29 to page 11 line 11	1,2,11,12, 21,22

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2005	0 1 JUN 2005
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer DALE SIVER Telephone No : (02) 6283 2196

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2005/000317

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2001/065375 A1 (BIONETRIX SYSTEMS CORPORATION) 7 September 2001 Abstract, page 28 line 24 to page 29 line 29	1,2,11,12, 21,22
Y	GB 2281645 A (IBM CORP) 8 March 1995 Whole document, especially page 13	1,2,11,12, 21,22
A	WATSON, R. et al. "Design and implementation of the Trusted BSD MAC Framework" DARPA Information Survivability Conference and Exposition 2003 Published 22-24 April 2003	1
A	WO 2001/029731 A1 (3COM CORPORATION) 26 April 2001 Abstract, figures	1
A	US 6134549 A (REGNIER et al.) 17 October 2000 Abstract, claims	1
A	US 6092189 A (FISHER et al.) 18 July 2000 Abstract	1
A	US 5434562 (REARDON) 18 July 1995 Abstract	1
A	US 5163147 A (ORITA) 10 November 1992 Abstract, figures, claims	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2005/000317

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	03100544	AU	2003245887	EP	1508236		
US	6463537	AU	11686/01	WO	0233522		
WO	0219064	AU	87444/01	CA	2420889		
WO	0165375	AU	41870/01				
GB	2281645	EP	0647901	JP	7084960	US	5774650
WO	0129731		NONE				
US	6134549		NONE				
US	6092189		NONE				
US	5434562		NONE				
US	5163147	JP	3088052				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX