

5

Method for overcoming system administration blockage**Field of the Invention**

This invention relates to a method for overcoming system administrator blockage and refers particulars, though not exclusively, to a method for overcoming system administrator blockage of a device newly connected to a computer.

Background of the Invention

When a computer is operating not as part of a network, the computer operator is generally the administrator. Therefore, the user has control over system administration functions. However, when the computer is operating as part of network, be it a local network or a wide area network, the system administrator has control over some of the functions of each computer connected to the network.

In the "WINDOWS"™ operating system, the system administrator has an administrative privilege function to enable the system administrator to block certain services on the computer in which it is operating. The services that can be controlled by the system administrator in this way include directory services, files, printers, security, terminals management, and peripheral devices. This normally includes a blocking function for access to certain devices connected to the computer. For example, if a device with a private memory is connected to the computer, a password will be required to be entered to gain access to the private memory. Normally the password will not be able to be sent to the device, so access will be denied. Therefore, as a result the exercise of the blocking function by the system administrator the "WINDOWS"™ operating system might not be able to communicate with the peripheral or other device operatively connected to the computer.

Summary of the Invention

According to a first aspect there is provided a method for overcoming system administrator blockage of a device newly-connected to a host computer, operatively connected to a network controllable by a system administrator, the device having a first non-volatile memory comprising a private area, the private area being of a category for which communication by the host computer application is able to be blocked in an administrative privilege environment. The method allows

- 5 the device to be enumerated with the host computer application as a human interface device for enabling communication between the host computer application and the private area in a non-administrative privilege environment.

10 The communication between the host computer application and the private area may be through a mass storage driver. The device may enumerate itself as the human interface device during the configuration descriptor process. The feature report is used for communication between the device and the host computer operating system. The device preferably reports to the host computer operating system as an alphanumeric display in a usage selected from human interface
15 device usage, and usage page.

The device may be part of a composite device also having a second non-volatile memory comprising a public area. The public area may be able to communicate with the host computer operating system in the non-administrative privilege
20 environment. The composite device may be non-volatile memory external device for operative connection to the host computer. The public area and the private area may comprise a non-volatile memory, preferably a single non-volatile memory.

- 25 The device may be selected from: external disk drive, printer, game console, external read/write disk drive, external card reader, external USB hub, external sound card, media player, and MP3 player.

30 According to a second aspect there is provided a computer usable medium comprising a computer program code that is configured to cause a processor to execute one or more functions for the performance of the above method.

35 According to a third aspect there is provided a non-volatile memory device for operative connection to a host computer, and comprising a computer program code that is configured to cause processor of the non-volatile memory device to execute one or more functions for the performance of the above method.

According to a final aspect there is provided a non-volatile memory device comprising a public memory, a private memory, a controller for controlling the

5 public memory and the private memory as well as communication between the host computer and the non-volatile memory device, a connector for enabling connection of the non-volatile memory device to a host computer, and a connector interface. The non-volatile memory device is able to be enumerated to the host application as a composite device including a human interface device for enabling
10 the host computer application to communicate with the private memory. The host computer application may gain access to the private memory through a mass storage driver.

The host computer application system may be able to communicate with the public
15 memory in a non-administrative privilege environment. The host computer application may be able to communicate with the private memory in a non-administrative privilege environment only after enumeration. The connector may be a USB or IEEE 1394 connector.

The public memory and the private memory may be separate parts of the one
20 memory.

Brief Description of the Drawings

In order that the invention may be fully understood and readily put into practical effect, there shall now be described by way of non-limitative example only a
25 preferred embodiment of the present invention, the description being with reference to the accompanying illustrative drawings in which:

Figure 1 is schematic illustration of a preferred form of computer system with which the preferred embodiment is to be used;

Figure 2 is a schematic illustration of a second form of computer system which
30 preferred embodiment is to be used;

Figure 3 is a schematic illustration of a third form of computer system which preferred embodiment is to be used;

Figure 4 is block diagram of a preferred form of peripheral device;

Figure 5 is block diagram of an alternative form of peripheral device;

35 Figure 6 is a flow chart of the operation of the preferred embodiment in the three preferred forms of computer systems; and

Figure 7 is a flow chart for the operation of the preferred embodiment a peripheral device.

5

Detailed Description of the preferred Embodiments

To refer to the Figure 1, there is shown a normal computer system comprising a CPU 10, monitor 12, keyboard 14, mouse 16, and printer 18. Each of the peripheral devices 12, 14, 16 and 18 may be connected to the CPU 10 by cables 10 20, or wirelessly. The CPU 10 has a number of ports 22 to which a memory device 24 may be operatively connected. The computer CPU 10 is connected to a network 11 that is controlled by a system administrator 13.

Figure 2 shows a laptop or notebook computer 26 having a display screen 28 and 15 a keyboard 30 mounted within a hinged case 32. A number of ports 34 may be provided to which the memory device 24 may be operatively connected. The computer 26 is also connected to the network 11 that is controlled by the system administrator 13.

20 Figure 3 illustrates a personal digital assistant 36 having a display 38 and keypad 40 mounted within a casing 42. At least one port 44 may be provided for connection thereto by a peripheral or separable device – in this case the memory device 24. The personal digital assistant is also connected to the network 11 that is controlled by the system administrator 13.

25

The memory device 24 is shown in Figures 4 and 5. It comprises a body 46 having a male connector 48 at one end. Mounted within the body 46 is an interface 50 for connector 48, a controller 52 operatively connected to interface 50, and non-volatile memory generally shown as 54. The memory 54 comprises a protected or private area 56 and a public area 58 that may be parts of the same physical memory (Figure 4); or may be two (or more) physically separate memory devices (Figure 5). The memory 54 may be a disk drive, flash memory, or otherwise. The connector 52 may be a USB or IEEE 1394 connector, or otherwise as required or desired. The protection or private area 56 may be used for the storage of 30 confidential or private data or information.

35

Although the following description relates to the memory device 24, it applicable to all devices for attachment to a computer and that have a memory such as, for example, external disk drives, printers, games consoles, external read/write disk

- 5 drives, external card readers, external USB hubs, external sound cards, media players, and MP3 players.

Due to the memory device 24 having the protected or private area 56, when the device 24 is connected to a corresponding port 22, 34, 44, the computer's
10 operating system or application will block all relevant commands to the protected area 56 such as, for example, a password, as it doesn't recognize the protected area 56 due to setting by or instructions from the system administrator 13. As such, an administration right or privilege (hereinafter "administration privilege") is involved and the protected area 56 is in an administrative privilege environment.
15 Such commands are usually SCSI commands.

To reduce the likelihood of this problem, and referring to Figure 5, after the device 24 is operatively connected to host computer 10, 26, 36 hereinafter "host 10" (51), the host 10 sends a setup token to device 24 during the configuration descriptor
20 request (52). During the enumeration of the device it enumerates as a composite device (53) that has two interfaces in the one device: one as a mass storage device (for public area 58) and one as a human interface device (for the private area 56). This will be as a part of the configuration descriptor. A human interface device does not require a device driver as the "WINDOWS"™ operating system
25 has a devices driver for human interface devices.

During the string descriptor, the device 24 will report as the human interface device to the host 10 (54). As a consequence, the host 10 will request the report descriptor for the human interface device at (55).

30

The device 24 reports to the host 10 as an alphanumeric display in human interface device usage (56). It may report as other usages as required or desired. During the report descriptor process, feature report is used for communication between the device 24 and the host 10 (57). Alternatively, the input or output
35 reports may be used. The report ID may be used as a command set and the mass storage operational code may be used as the report ID (58).

The host 10 commences the enumeration of device 24 (59). The device 24 is enumerated as a composite device (60) and therefore there will be no blockage of

5 commands to the protected area 56 and thus the device 24 is able to accept
 commands for both the mass storage device (public) area 58 and the human
 interface device (private) area 56 (61). Each component 58, 56 is enumerated (63,
 64) and when a mass storage command for either component 56, 58 is sent to
 device 24 (65, 66), the controller 52 is able to service and perform the task. After
 10 the tasks are performed, the process stops (67). As such the device 24 is
 operating in a non-administrative privilege environment and the system
 administrator 13 is not able to block commands to the protected area 56.

Figure 6 shows the process as it occurs on the device 24. Here, the composite
 15 device 24 is the mass storage (public) device 58 and the human interface (private)
 device 56 (70). The mass storage (public) device 58 (71) can perform all normal
 mass storage functions: read, write, transfer files to and from host 10, and so forth
 (72).

20 For the human interface (private) device 56 (73), when the controller 52
 communicates with host 10 (74) it will ask for get-report-request or set-report-
 request to enable communication between host 10 and device 24 for the human
 interface (private) device 56. This will normally be through setup token and
 endpoint 0. All command codes communication with the device 24 for the human
 25 interface (private) device 56 is through the human interface get-report-request and
 set-report-request (75). The device 24 receives the human interface commands
 code (76) and performs the necessary task. As the command code is under a non-
 administrative privilege environment, the operating system of host 10 is not able to
 block the human interface (private) device 56. Communication between the host
 30 computer 10 application and the private area 56 may be through a mass storage
 driver. As such the device 24 is operating in a non-administrative privilege
 environment and the system administrator 13 is not able to block commands to the
 protected area 56.

35 Whilst there has been described in the foregoing description preferred
 embodiments of the present invention, it will be understood by those skilled in the
 technology that many variations or modifications in details of design or construction
 or operation may be made without departing from the present invention.

5 The Claims

1. A method for overcoming system administrator blockage of a device newly-connected to a host computer operatively connected to a network controllable by a system administrator, the device having a first non-volatile memory comprising a private area, the private area being of a category for which communication by the host computer application is able to be blocked in an administrative privilege environment, the method comprising enumerating the device with the host computer application as a human interface device for enabling communication between the host computer application and the private area in a non-administrative privilege environment.
2. A method as claimed in claim 1, wherein the communication between the host computer application and the private area is through a mass storage driver.
3. A method as claimed in claim 1 or claim 2, wherein the device enumerates itself as the human interface device during the configuration descriptor process.
4. A method as claimed in claim 3, wherein a feature report is used for communication between the device and the host computer application.
5. A method as claimed in claim 4, wherein the device reports to the host computer application as an alphanumeric display in a usage selected from the group comprising: human interface device usage, and usage page.
6. A method as claimed in anyone of claims 1 to 5, wherein the device is part of a composite device, the composite device further comprising a second non-volatile memory comprising a public area, the public area being able to communicate with the host computer application in the non-administrative privilege environment.

- 5 7. A method as claim in any one of claims 1 to 6, wherein the host computer application is in a "WINDOWS"™ operating system.
8. A method as claimed in any one of claims 1 to 7, wherein the public area and the private area comprise separate parts of a single memory.
- 10
9. A method as claimed in claim 6, wherein the composite device is a non-volatile memory external device for operative connection to the host computer, the non-volatile memory external device comprising the public and the private area.
- 15
10. A method as claimed in any one of claims 1 to 8, wherein the device is selected from the group consisting of: external disk drive, printer, game console, external read/write disk drive, external card reader, external USB hub, external sound card, media player, and MP3 player.
- 20
11. A computer usable medium comprising a computer program code that is configured to cause a processor to execute one or more functions for the performance of the method of any one of claims 1 to 10.
- 25
12. A non-volatile memory device for operative connection to a host computer, and comprising a processor and a computer program code that is configured to cause the processor of the non-volatile memory device to execute one or more functions for the performance of the method of any one of claims 1 to 10.
- 30
13. A non-volatile memory device comprising:
- (a) a public memory;
- (b) a private memory;
- (c) a controller for controlling the public memory and the private memory as well as communication between a host computer connected to a network controllable by a system administrator, and the non-volatile memory device;
- 35

5 (d) a connector to enable connection of the non-volatile memory device to the host computer; and

 (e) a connector interface;

 wherein

 (f) the non-volatile memory device is able to be enumerated to the
10 host computer application as a composite device including a human interface device for enabling the host computer application to communicate with the private memory in a non-administrative privilege environment.

15 14. A non-volatile memory device as claimed in claim 13, wherein the private memory and the host computer application communicate through a mass storage driver.

20 15. A non-volatile memory device as claimed in claim 13 or claim 14, wherein the public memory is able to communicate with the host computer operating system in an administrative privilege environment.

25 16. A non-volatile memory device as claimed in any one of claims 13 to 15, wherein the connector is selected from the group consisting of: USB, and IEEE 1394.

30 17. A non-volatile memory device as claimed in any one of claims 13 to 16, wherein the public memory and the private memory comprise parts of a single memory.