**Method, Apparatus And System For Authentication Of External Storage Devices**

**Field of the Invention**

This invention relates to a method, apparatus and system for authentication of external storage devices and relates particularly, though not exclusively, to such a method apparatus and system for preventing unauthorized use of external storage devices with a host computer.

**Background to the Invention:**

There is many external storage devices on the market. These include optical-based storage devices such as hard disk drives, and flash-based storage devices including USB flash drives. Various standard interfaces may be used to connect them to a host computer including, but not limited to, USB, Firewire, and PCMCIA. There are also proprietary interface such as, for example, the "Memory Stick" interface, SD card interface, and so forth.

As the download rate may be quite high, and the storage device form factor becomes quite small a significant security and confidentiality threat is raised for companies. The threats include the unauthorized copying of sensitive or confidential information, and the uploading of malicious or malignant applications including viruses, and so forth. For example, an employee of a company can easily carry a small USB flash drive that is hidden from view. It can be inserted into a USB port on any company computer to download and save a copy of sensitive or confidential data; and/or to upload a virus thereby bypassing all virus filters. There is no way the company can control the situation

unless they block all external interfaces, physically close all external interfaces, or deny users the ability to download data from or upload data to the company computer system. By doing so significant limitations will be created for those who are authorized to perform such acts.

## Summary of the Invention

According to a preferred aspect there is provided a method for authentication of an external storage device operatively connected to a port of a host computer, the method comprising: the host computer conducting a handshake with the external storage device seeking an authentication key from the external storage device; electrically disconnecting the external storage device from the host computer if the authentication key is at least one selected from the group consisting of: incorrect, and not provided within a predetermined period; and allowing access to the host computer by the external storage device if the authentication key is correct and provided within the predetermined period.

According to a second preferred aspect there is provided an external storage device able to be operatively connected to a port of a host computer by use of a connector of the external storage device, the external storage device comprising an authentication module configured to communicate with an authentication application of the host computer; the authentication module being configured to comprise an authentication key for sending to the authentication application for authentication of the external storage device.

According to a third preferred aspect there is provided a system for authentication of an external storage device operatively connected to a port of a host computer by use of a connector of the external storage device, the external storage device comprising an authentication module to communicate with an authentication application of the host computer; the authentication module comprising an authentication key for sending to the authentication application for authentication of the external storage device.

For all aspects, correct authentication keys may be maintained in a lookup table. The lookup table may be maintained in one of: the host computer, and a server of a network to which the host computer is connected. The authentication key may be restricted by at least one of: a particular user, a particular host computer, a particular terminal of a network to which the host computer is connected. The particular user may be determined by user login code, the particular host computer may be determined by host computer identity, and the particular terminal of the network may be determined by network terminal identity. The user login code, the host computer identity, and the network terminal identity may be stored in the lookup table.

Access to the host computer may be restricted to certain applications or certain data of the host computer, the restrictions being maintained in the lookup table. Access to the network may be restricted to certain applications or certain data, the restrictions being maintained in the lookup table.

The authentication key may be allocated to an external storage device that does not have the authentication key by querying if the authentication key is required and, upon a positive response within the predetermined period, checking the external storage device and, if the external storage device is clear, allocating the authentication key to the external storage device. Checking of the external storage device may include at least one of: external storage device identity, user identity, host computer identity, network terminal identity, and scans for viruses or other malignant applications or data.

The authentication module may be downloaded to the external storage device before the authentication key is sent to the external storage device.

The external storage device may be electrically disconnected from the host computer if the response is negative or if the response is not provided within the predetermined period.

**Brief Description of the Drawings**

In order than the invention may be fully understood and readily put into practical effect there shall now be described by way of non-limitative example only preferred embodiments of the present invention, the description being with reference to the accompanying illustrative drawings.

In the drawings:

Figure 1 is a perspective view of an embodiment of an external storage device about to be used with an embodiment of a host computer;

Figure 2 is a block diagram of the external storage device of Figure 1;

Figure 3 is a partial block diagram of the host computer of Figure 1;

Figure 4 is a flow chart of an embodiment; and

Figure 5 is a flow chart of another embodiment.

**Detailed Description of the Preferred Embodiments**

To first refer to Figure 1 there is shown a computer 10 connected to a LAN 12. The computer 10 has a number of ports 14 for connection of an external storage device such as the USB flash memory storage device 16. By use of the external storage device 16 data may be downloaded from the computer 10 and/or the network 12, and/or data may be uploaded to the computer 10 and/or network 12. As shown, the external storage device 16 has a connector 18 which, in this case, is a USB connector. However, it may be any suitable connector able to operatively mate with one or more of the ports 14.

In Figure 2 the external storage device 16 is shown in more detail. The device 16 has a connector interface 20 as well as storage 22. The storage may be a hard disc, flash memory, or otherwise as required or desired. The storage 22 is controlled by a storage controller 26. A microprocessor 24 controls the overall operation of the device 24. An authentication module 28 is for authentication of the device 16. The authentication module 28 may be firmware, may be included in the microprocessor 24, or may be in a processor separate from the microprocessor 24.

The computer 10 includes a controller 30 that includes an authentication application 32 that is able to communicate with the authentication module 28 when connector 18 is operatively engaged in a port 14. The application 32 will block access to any of the systems of the computer 10 and/or network 12 by any external storage device 16 that is operatively connected to any one of the ports 14 and that is not authenticated; but will allow access any of the systems of the computer 10 and/or network 12 by any external storage device 16 that is operatively connected to any one of the ports 14 and that is authenticated. Authentication may be limited to particular individuals by login codes and/or particular computers by the computer identifier.

Upon operative connection of the device 16 to the computer 10, authentication may be by a number of different methods. The device 16 may have previously been authenticated in which case the process of Figure 4 is followed. An alternative is for the device 16 to be authenticated when it is operatively connected to the computer 10, the authentication being able to be relied upon for subsequent uses of the device 16. This is shown in Figure 5.

Preferably, all initial authentications of devices 16, whether or not for particular users and/or computers is by an administrator that has the functionality and ability to allow the devices 16 to functionally interact with the computer 10 and/or network 12; and to authenticate devices 16 not issued by them but that are able to be authenticated. For the embodiment of Figure 5, all subsequent authentications are by the process of Figure 4.

To refer to Figure 4, the authentication application 32 automatically starts when the computer 10 is booted (401). It runs in the computer 10 isolated from user access except for the administrator mentioned above. In this way a user cannot tamper with, interfere with or otherwise hinder or prevent the operation of the application 32. This may be in the same manner as other "secured" applications that normally run on the computer 10. The application 32 includes a monitoring module 34 whereby it will monitor the ports 14 to detect when an external storage device 16 is connected to any one of the ports 14 (402). This may be done by, for example, regular polling of the ports 14 (403). If no insertion is detected (404), polling continues. When an insertion of a device 16 into a port 14 is detected (405) the application 32 will then try to establish an authentication handshake with the device 16 by performing a challenge and response (406). If the device 16 was inserted into the port 14 before the booting of the computer 10, the process will be the same, and access to the systems of the computer 10 and/or network 12 by the storage device 16 will be denied until authentication has taken place.

During the authentication process (406) the application 32 calls for the device16 to provide an authentication code or key. If an authentication code or key is provided by the authentication module 28 (407), the application 32 checks a lookup table of current authentication codes or keys to determine if the authentication code or key is listed (408). If there is a match (409), the device 16 may be given access to the computer 10 and/or the network 12 (410). The lookup table may include restrictions (411). For example, the authentication key or code of the device 16 may be linked to a particular individual and/or computer 10. This can be checked by reference to the user login code,

and the identity of the computer 10 and/or the terminal of the network 12 to which it is connected. Access may be limited to certain applications and/or data of the computer 10 and/or network 12. If there are restrictions, the application 32 checks the lookup table to ensure they are correct (412).

If the authentication module 28 is not able to respond correctly to the application 32 in the handshake procedure at (407), or if there is no match at (409), or if the restrictions are not correct at (412), the application 32 will immediately electrically disconnect, or isolate, the device 16 from the computer 10 to prevent the device 16 from having access to any of the systems of the computer 10 (413) and/or network 12. However, the device 16 may still remain inserted in the port 14.

In the embodiment of Figure 5, there may be authentication of the device 16 during the authentication process. Here like reference numerals are used for like processes but the prefix number is changed from 4 to 5.

Again, the authentication application 32 automatically starts when the computer 10 is booted (501). It runs in the computer 10 isolated from user access except for the administrator mentioned above. In this way a user cannot tamper with, interfere with or otherwise hinder or prevent the operation of the application 32. This may be in the same manner as other "secured" applications that normally run on the computer 10. The application 32 again includes the monitoring module 34 whereby it will monitor the

ports 14 to detect when an external storage device 16 is connected to any one of the ports 14 (502). This may be done by, for example, regular polling of the ports 14 (503). If no insertion is detected (504), polling continues. When an insertion of a device 16 into a port 14 is detected (505) the application 32 will then try to establish an authentication handshake with the device 16 by performing a challenge and response (506). If the device 16 was inserted into the port 14 before the booting of the computer 10, the process will be the same, and access to the systems of the computer 10 and/or network 12 by the storage device 16 will be denied until authentication has taken place.

During the authentication process (506) the application 32 calls for the device16 to provide an authentication code or key. If an authentication code or key is provided by the authentication module 28 (507), the application 32 checks a lookup table of current authentication codes or keys to determine if the authentication code or key is listed (508). If there is a match (509), the device 16 may be given access to the computer 10 and/or the network 12 (510). The lookup table may include restrictions (511). For example, the authentication key or code of the device 16 may be linked to a particular individual and/or computer 10. This can be checked by reference to the user login code, and the identity of the computer 10 and/or the terminal of the network 12 to which it is connected. Access may be limited to certain applications and/or data of the computer 10 and/or network 12. If there are restrictions, the application 32 checks the lookup table to ensure they are correct (512).

If the authentication module 28 is not able to respond correctly to the application 32 in the handshake procedure at (507) due to the device 16 not having previously been authenticated, authentication may take place by a query from the application 32 to the device 16 (517). This will be displayed on a monitor and will require user input. If there is no response within a predetermined period such as, for example, thirty seconds, or if the response is in the negative, the application 32 will immediately electrically disconnect, or isolate, the device 16 from the computer 10 to prevent the device 16 from having access to any of the systems of the computer 10 (515) and/or network 12. However, the device 16 may still remain inserted in the port 14.

If at 515 the response is within the predetermined period and is positive, the application 32 checks the device 16. This may include one or more of: device identity, user identity, computer identity, and network terminal identity; and may include scans for viruses or other malignant applications or data. If all are in order, the administrator can allocate a key for the device 16 and record the key in the lookup table. Any restrictions on the user and/or computer/terminal may be created at this time and included in the lookup table. The necessary module 28 is then downloaded to the device 16, if not previously downloaded. The application then sends the key to the device 16 for storage in the authentication module 28 or memory 22. Access to the computer 10 and/or network 12 is then granted within the scope of the restrictions created.

If there is no match at (509), or if the restrictions are not correct at (512), the application 32 will immediately electrically disconnect, or isolate, the device 16 from the computer

10 to prevent the device 16 from having access to any of the systems of the computer 10 (513) and/or network 12. However, the device 16 may still remain inserted in the port 14.

The lookup table may be maintained in the host computer 10 and may be maintained by the administrator. If the computer 10 is connected to the network 12, the lookup table is preferably maintained in a server of the network 12 and again is maintained by the administrator. However, application 32 will reside in the computer 10 whether or not it is connected to the network 12.

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 concerned that many variations in details of design, construction and/or operation may be made without departing from the present invention.

The Claims

1. A method for authentication of an external storage device operatively connected to a port of a host computer, the method comprising:

the host computer conducting a handshake with the external storage device seeking an authentication key from the external storage device;

electrically disconnecting the external storage device from the host computer if the authentication key is at least one selected from the group consisting of: incorrect, and not provided within a predetermined period; and

allowing access to the host computer by the external storage device if the authentication key is correct and provided within the predetermined period.

2. A method as claimed in claim 1, wherein correct authentication keys are maintained in a lookup table.

3. A method as claimed in claim 2, wherein the lookup table is maintained in one of: the host computer, and a server of a network to which the host computer is connected.

4. A method as claimed in claim 2, wherein the authentication key is restricted by at least one selected from the group consisting of: a particular user, a particular host computer, a particular terminal of a network to which the host computer is connected.

5. A method as claimed in claim 4, wherein the particular user is determined by user login code, the particular host computer is determined by host computer identity, and the particular terminal of the network is determined by network terminal identity.

6. A method as claimed in claim 5, wherein the user login code, the host computer identity, and the network terminal identity are stored in the lookup table.

7. A method as claimed in any one of claims 2 to 6, wherein access to the host computer is restricted to certain applications or certain data of the host computer, the restrictions being maintained in the lookup table.

8. A method as claimed in any one of claims 3 to 6, wherein access to the network is restricted to certain applications or certain data, the restrictions being maintained in the lookup table.

9. A method as claimed in any one of claims 1 to 8 further comprising allocating the authentication key to the external storage device that does not have the authentication key by querying if the authentication key is required and, upon a positive response within the predetermined period, checking the external storage device and, if the external storage device is clear, allocating the authentication key to the external storage device.

10. A method as claimed in claim 9, wherein the checking of the external storage device includes at least one selected from the group consisting of: external storage device identity, user identity, host computer identity, network terminal identity, and scans for viruses or other malignant applications or data.

11. A method as claimed in claim 9 or claim 10, wherein an authentication module is downloaded to the external storage device before the authentication key is sent to the external storage device.

12. A method as claimed in any one of claims 9 to 11 further comprising electrically disconnecting the external storage device from the host computer if the response is negative or if the response is not provided within the predetermined period.

13. A method as claimed in any one of claims 9 to 12, wherein allocation of the authentication key is by an administrator.

14. An external storage device able to be operatively connected to a port of a host computer by use of a connector of the external storage device, the external storage device comprising an authentication module configured to communicate with an authentication application of the host computer; the authentication module being configured to comprise an authentication key for sending to the authentication application for authentication of the external storage device.

15. An external storage device as claimed in claim 15, wherein at least one of the authentication module and the authentication key is able to be downloaded from the authentication application.

16. An external storage device as claimed in claim 14 or claim 15, wherein the authentication key is restricted by at least one selected from the group consisting of: a particular user, a particular host computer, and a particular terminal of a network to which the host computer is connected.

17. An external storage device as claimed in claim 16, wherein the particular user is determined by user login code, the particular host computer is determined by host computer identity, and the particular terminal of the network is determined by network terminal identity.

18. A system for authentication of an external storage device operatively connected to a port of a host computer by use of a connector of the external storage device, the external storage device comprising an authentication module to communicate with an authentication application of the host computer; the authentication module comprising

an authentication key for sending to the authentication application for authentication of the external storage device.

19. A system as claimed in claim 18, wherein the host computer conducts a handshake with the external storage device seeking the authentication key from the external storage device.

20. A system as claimed in claim 18 or claim 19, wherein correct authentication keys are maintained in a lookup table maintained in one of: the host computer, and a server of a network to which the host computer is connected.

21. A system as claimed in claim 20, wherein the authentication key is restricted by at least one selected from the group consisting of: a particular user, a particular host computer, a particular terminal of a network to which the host computer is connected.

22. A system as claimed in claim 21, wherein the particular user is determined by user login code, the particular host computer is determined by host computer identity, and particular terminal of the network is determined by network terminal identity.

23. A system as claimed in claim 22, wherein the user login code, the host computer identity, and the network terminal identity are stored in the lookup table.

24. A system as claimed in any one of claims 20 to 23, wherein access to the host computer is restricted to certain applications or certain data of the host computer, the restrictions being maintained in the lookup table.

25. A system as claimed in any one of claims 20 to 24, wherein access to the network is restricted to certain applications or certain data, the restrictions being maintained in the lookup table.

26. A system as claimed in any one of claims 20 to 25, where the authentication key is allocated by an administrator.