

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
25 November 2010 (25.11.2010)

PCT

(10) International Publication Number
WO 2010/133254 A1

(51) International Patent Classification:
G06F 3/06 (2006.01)

(21) International Application Number:
PCT/EP2009/056163

(22) International Filing Date:
20 May 2009 (20.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **NEC EUROPE LTD.** [DE/DE]; NEC Laboratories Europe, Rathausallee 10, 53757 Sankt Augustin (DE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **RIPKE, Andreas** [DE/DE]; c/o NEC Europe Ltd., NEC Laboratories Europe, IT Division, Rathausallee 10, 53757 Sankt Augustin (DE). **KLAAS, Jens** [DE/DE]; c/o NEC Europe Ltd., NEC Laboratories Europe, IT Division, Rathausallee 10, 53757 Sankt Augustin (DE).

(74) Agent: **DR. DIETER HEUNEMANN, VOSSIUS & PARTNER**; Siebertstraße 4, 81675 München (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, 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 (Art. 21(3))

(54) Title: MASQUERADING A STORAGE MEDIA IN A COMPUTER SYSTEM

(57) Abstract: The invention provides for a method for influencing the result of an inquiry of a computer system. A storage media is attached to the computer system, and the method comprises the method step of masquerading the storage media during the inquiry. Further, the invention provides for a computer program product comprising one or more computer readable media having computer executable instructions for performing the steps of the above method. Furthermore, the invention provides for an adapter for a computer system to which a storage media is attached. The adapter is configured to masquerade the storage media during an inquiry of the computer system.



WO 2010/133254 A1

Masquerading a storage media in a computer system

5 The invention relates to a method for influencing the result of an inquiry of a computer system to which a storage media is attached and to an adapter for carrying out the method. In one embodiment, the storage media is a removable storage media, more particularly a removable USB storage media.

10 Storage media may appear as local media or local drive and as removable media, like floppy or flash card readers. For example, USB memory sticks are classified as removable storage media, since the sticks may be attached and detached from a personal computer.

Particular applications useful in connection with the storage media, e.g. partitioning the
15 storage media to have several partitions on the media, may sometimes not easily run and/or may, for example, depend on the operating system of the computer system.

However, partitioning a storage media, particularly a removable storage media, may be advantageous if the capacity of the storage media exceeds the maximum size of the
20 computer file system architecture (for example, FAT32) and/or if customary (for example, NTFS) or newer file systems are not applicable or available.

A further need may exist to enhance data organization in the storage media, for example in order to store particular programs and data on separate partitions in the storage media. For
25 instance, an encryption tool resides on one partition that is to be used to access the other, encrypted, partition. Further, it may be advantageous to have a movie on one partition and the respective movie player on another partition, for example, since the partitions may be formatted separately from each other.

Therefore, a need exists to provide a method for allowing particular applications of a computer system to easily run in connection with a storage media.

The above objects may be achieved with the features of the claims.

5

In particular, the present invention is directed to a method for masquerading a storage media attached to a computer system. In case the computer system makes an inquiry, the masquerading of the storage media may influence the computer system's determination as to the question whether the storage media is a particular storage media, for example whether the storage media is a local or a removable storage media. In doing so, it may be possible to let run any application useful for working with the storage media.

15 According to the present invention, a method for influencing the result of an inquiry of a computer system is provided. A storage media is attached to the computer system, and the method comprises the method step of masquerading the storage media during the inquiry.

The storage media may be any media for storing and/or processing data, for example, digital cameras, printers, scanners, modems, telephones, video phones, and/or network connections. In normal system operation, when the storage media is attached to the computer system, the computer system may be configured to automatically detect that the storage media is attached and may be configured to determine the type of storage media by carrying out an inquiry. If the result of the determination meets predetermined conditions communications from the computer system to the storage media may be established.

25

In order to influence the result of the inquiry, the storage media is masqueraded during the inquiry. In doing so, it may be possible to simulate the presence of a different media than the storage media actually attached.

30

The masquerading may be achieved by using a particular adapter configured to masquerade the storage media, in particular by having a particular firmware in the adapter for hiding and/or virtually substituting the storage media.

- 5 Firmware is a program to internally control the functionality of electronic devices, for example, of an adapter. The expression “firmware” is contrasted with “hardware” and “software” which are well-known terms in this technical field. Firmware may be a microcode which cannot be manipulated or changed by a user. For example, in general terms, firmware denotes anything ROM-resident.

10

In a particular embodiment, the functionality of an adapter cannot be manipulated or changed by a user.

- 15 In a particular embodiment, the masquerading step is carried out by means of an adapter attached to the computer system and/or the storage media.

- For example, the adapter may be configured to hide the actual presence and/or to change the identification of the storage media. This may be achieved by interconnecting the adapter with the computer system and the storage media, wherein the adapter may be configured to
20 simulate particular properties of the storage media. In particular, the masquerading may be a hiding of properties and/or may retain them and/or may modify them, for example, to simulate different properties of the storage media. The properties of the storage media may, for example, be the type of the storage media, its capacity, its producer, or its compatibility.

- 25 The hiding and/or substituting as taught above may be achieved by a firmware provided by the adapter and wherein the firmware is configured to influence the properties of the storage media to be detected by the inquiry of the computer system. For example, any data to be sent from the storage media in response to the inquiry of the computer system to determine the type of the storage media connected to the computer system may be modified
30 and/or retained and/or substituted by pre-determined data. In doing so, the result of the

inquiry may simulate the presence of a different type of storage media attached to the computer system.

Using an adapter to masquerade the storage media may be advantageous, since the adapter
5 may be used in connection with different operating systems without requiring any administrator rights.

In a particular embodiment, the storage media is a removable storage media, preferably a removable USB storage media.

10

In particular, the storage media may be connected/attached to the computer via a particular port, for example, via an external port (provided at the casing of the computer, and not provided inside the casing), for example, a USB port. A USB port in a computer system is usually applied to connect peripheral devices to the computer system as discussed above.

15

For example, Universal Serial Bus (USB) storage media may be used as storage media and may also be referred to as "USB stick" or "USB drive". Storage media may be removable storage media, in particular, removable USB storage media. Removable media are meant herein to be configured for being attached/connected to an external port of the computer
20 system.

In a particular embodiment, the storage media, for example a removable storage media, is recognized by the computer system after the inquiry to be a local storage media of the computer system due to the masquerading.

25

For example, the masquerading of the storage media may lead to a substitution of data to be transmitted in response to the inquiry of the computer system. In particular, the inquiry of the computer system may be meant to detect the type of storage media attached to the computer system, but the masquerading may result in a replacement and/or modification of
30 the data to be sent as a response thereto or in a hiding of these data. In a particular

embodiment, these data are characteristic for the type of the storage media, so that changing/modifying and/or hiding and/or retaining and/or substituting/replacing them influences the result of the inquiry of the computer system and may thus simulate the presence of a different type of storage media.

5

In particular, the data to be transmitted from a removable storage media may be substituted and/or modified to simulate that the actual removable storage medium is a local storage medium. In doing so, it may be possible to partition the actual removable storage media in the same way as it would be possible for local storage media, independently from the
10 operation system used for the computer system.

In a particular embodiment, the masquerading step comprises a controlling of commands from the storage media to the computer system and/or a controlling of commands from the computer system to the storage media.

15

For example, commands from the storage media to the computer system may contain the data to be transmitted in response to the inquiry of the computer system. In particular, the original commands of a storage media may contain any information allowing the identification of the type of the storage media.

20

Thus, it may be advantageous to control the commands in order to avoid the transmission of any commands counteracting the masquerading of the storage media.

In a particular embodiment, the controlling step comprises a determining of the contents of
25 the commands.

For example, the contents of a command may be characterized by the structure of the data in the command. A particular data structure determined may be compared to a list of pre-determined and pre-stored data structures (for example, stored as "reference data
30 structures" in the adapter carrying out the method or included in the firmware carrying out

the method) and may thus be identified as being associated with a particular content.

In doing so, it may be possible to reliably identify those commands to be sent from the storage media to the computer system, which might counteract the masquerading. Hence,
5 those commands may be modified and/or substituted in response to the inquiry.

In a particular embodiment, the controlling step further comprises an intercepting of commands from the storage media if the contents are based on the fact that the storage media is actually not a local storage media.

10

In particular, the commands identified as including contents counteracting the masquerading may be retained/hindered from being transmitted to the computer system. For example, the transmission itself may be stopped by deleting these commands or by replacing their transmission by a transmission of different data structures in line with the
15 masquerading.

In a particular embodiment, the controlling step further comprises a step of allowing the transmission of commands from the storage media if the contents are not based on the fact that the storage media is actually not a local storage media.

20

For example, a determination of the contents of a command to be transmitted from the storage media to the computer system may result in the finding that the data structures are not identified as counteracting the masquerading. In this case, the command may be transmitted to the computer system without any modification.

25

In doing so, the intended function and use of the storage media may be guaranteed without negatively affecting the masquerading of the storage media.

In a particular embodiment, the controlling step further comprises a generating of
30 commands which are mandatory for a local storage media and are sent to the computer

system.

For example, if the determination of the contents of the commands to be sent/transmitted to the computer system finds that the data structures counteract the masquerading of the removable storage media, one or more commands may be generated to replace the original commands by the new ones. The new commands may be based on the original commands, for example, the new commands may contain data structures of the original commands combined with new data structures or may contain the original data structures modified by a particular data annex, in order to fulfil the requirements of the masquerading. Further, the newly generated command or commands may be transmitted to the computer system, for example, in response to the inquiry.

In doing so, the result of the inquiry of the computer system is influenced. For example, the generated command may simulate the presence of a different storage media than the actual storage media, e.g. of a local storage media instead of the actual removable storage media, by containing contents mandatory for a local storage media.

In a particular embodiment, the operating system of the computer system is WINDOWS®.

For example, the operating system may be any version of WINDOWS®. Further, the operating system may be Linux or MacOS. In particular, any operating system may be used for the computer system.

Further, the present invention provides a computer program product comprising one or more computer readable media having computer executable instructions for performing the steps of one of the methods as described above.

Furthermore, the present invention provides an adapter for a computer system to which a storage media is attached. The adapter is configured to masquerade the storage media during an inquiry of the computer system.

In particular, the adapter may be configured to carry out each of the method steps above. For example, the adapter may contain a firmware enabling the adapter to perform the above method.

5

Particularly, the adapter may be connectable/attachable to an external port (provided at the casing of the computer, and not provided inside the casing), for example, to a USB port. Furthermore, the adapter may be connectable/attachable to a storage media .

- 10 In a particular embodiment, the adapter is configured to control commands from the storage media to the computer system and/or to control commands from the computer system to the storage media.

- For example, the adapter may be configured to identify particular commands to be
15 transmitted to the computer system. In particular, the adapter may be configured to stop the transmission of commands if these commands counteract the masquerading of the storage media.

- Hence, the adapter may advantageously guarantee that the inquiry of the computer system
20 is responded in a preferred way, for example, to simulate the presence of a different storage media than the actual one. In doing so, it may be possible to, for example, partition a removable storage device, independently from the operating system of the computer system.

- 25 In a particular embodiment, the control of the commands comprises a determination of the contents of the commands.

- For example, the contents of a command may be characterized by the data structure as discussed above. A particular data structure already determined by the adapter may be
30 compared to a list of pre-determined and pre-stored data structures (stored in the adapter as

“reference data structures”) and may thus be identified as being associated with a particular content.

In doing so, it may be possible to reliably identify those commands which might counteract
5 the masquerading. Hence, those commands may be modified and/or substituted in response to the inquiry and may, for example, then be transmitted to the computer system.

In a particular embodiment, the adapter is configured to intercept and/or let pass the commands from the storage media, dependent on the commands' contents determined,
10 and/or generate commands mandatory of a local storage media and to be sent to the computer system.

In particular, the commands identified as including contents counteracting the masquerading may be intercepted/retained/hindered from being transmitted to the computer
15 system. For example, the transmission itself may be stopped by deleting these commands or by replacing their transmission by a transmission of different data structures in line with the masquerading.

If, for example, a determination of the contents of a command to be transmitted from the
20 storage media to the computer system result in the finding that the data structures are not identified as counteracting the masquerading, the command may be transmitted to the computer system.

In this case, the intended function and use of the storage media may be guaranteed without
25 negatively affecting the masquerading of the storage media.

If, for example, the determination of the contents of the commands to be sent/transmitted to the computer system finds that the data structures counteract the masquerading of the removable storage media, one or more commands may be generated to replace the original
30 commands as discussed above. Further, the newly generated command or commands may

be transmitted to the computer system, for example, in response to the inquiry.

In doing so, the result of the inquiry of the computer system is influenced. For example, the generated command may simulate the presence of a local storage media instead of the
5 actual removable storage media by providing contents mandatory for local storage media.

Further explanations and features mentioned in connection with the method of the present invention and its embodiments may also be applied for the above discussed adapter and its
10 embodiments.

Due to the above discussed invention, it may be possible to start particular applications of the computer system in connection with the storage media provided with simulated properties, wherein these applications, as for example the partitioning, are not possible to be carried out without the simulated properties of the storage media.

15 While the invention has been illustrated and described in detail in the foregoing description, such illustration and description are to be considered illustrative or exemplary and non-restrictive; the invention is thus not limited to the disclosed embodiments. Features mentioned in connection with one embodiment described herein may also be advantageous
20 as features of another embodiment described herein without explicitly showing these features. Variations to the disclosed embodiments can be understood and effected by those skilled in the art and practicing the claimed invention, from a study of the disclosure and the appended claims. In the claims, the word “comprising” does not exclude other elements or steps, and the indefinite article “a” or “an” does not exclude a plurality. A single
25 processor or other unit may fulfill some functions of several items recited in the claims. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures can not be used to advantage.

CLAIMS

1. Method for influencing the result of an inquiry of a computer system to which a storage media is attached, comprising:

5 - masquerading the storage media during the inquiry.

2. Method of claim 1, wherein the masquerading step is carried out by means of an adapter attached to the computer system and/or the storage media.

10

3. Method of claim 1 or 2, wherein the storage media is a removable storage media, preferably a removable USB storage media.

15

4. Method of claim 1, 2 or 3, wherein the storage media is recognized by the computer system after the inquiry to be a local storage media of the computer system due to the masquerading.

20

5. Method of one of the preceding claims, wherein the masquerading step comprises:

- controlling commands from the storage media to the computer system and/or controlling commands from the computer system to the storage medium.

25

6. Method of claim 5, wherein the controlling step comprises:

- determining the contents of the commands.

7. Method of claim 6, wherein the controlling step further comprises:

- 5 - intercepting commands from the storage media if the contents are based on the fact that the storage media is actually not a local storage media.

8. Method of claim 6 or 7, wherein the controlling step further comprises:

10

- allowing the transmission of commands from the storage media if the contents are not based on the fact that the storage media is actually not a local storage media

15 9. Method of one of claim 5 – 8, wherein the controlling step further comprises:

- generating commands which are mandatory for a local storage media and are sent to the computer system.

20

10. Method of one of the preceding claims, wherein the operating system of the computer system is WINDOWS®.

25 11. Computer program product comprising one or more computer readable media having computer executable instructions for performing the steps of the method of one of the preceding claims.

12. Adapter for a computer system to which a storage media is attached, wherein the adapter is configured to masquerade the storage media during an inquiry of the computer system.

5

13. Adapter of claim 12, wherein the adapter is configured to control commands from the storage media to the computer system and/or to control commands from the computer system to the storage media.

10

14. Adapter of claim 13, wherein the control of the commands comprises a determination of the contents of the commands.

15

15. Adapter of claim 14, wherein the adapter is configured to intercept and/or let pass the commands from the storage media, dependent on the commands' contents determined, and/or generate commands mandatory of a local storage media and to be sent to the computer system.

20

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/056163

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F3/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

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 practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/147375 A1 (SIREN JANNE [FI] ET AL) 19 June 2008 (2008-06-19) abstract paragraphs [0027], [0028] figure 2 paragraphs [0029] - [0036] figure 3	1-15
X	US 7 383 386 B1 (IYER SREE MAMBAKKAM [US] ET AL) 3 June 2008 (2008-06-03) the whole document	1-15
X	US 6 970 954 B1 (GUY GIDEON [US] ET AL) 29 November 2005 (2005-11-29) column 7, line 14 - column 8, line 41 figure 6	1-15

☐ Further documents are listed in the continuation of Box C.

☒ 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 document 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.

8 document member of the same patent family

Date of the actual completion of the international search

30 November 2009

Date of mailing of the international search report

04/12/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

De Ceulaer, Bart

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/056163

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008147375 A1	19-06-2008	WO 2008132547 A2	06-11-2008
US 7383386 B1	03-06-2008	US 2008229005 A1	18-09-2008
US 6970954 B1	29-11-2005	NONE	