[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810065371.2

[43] 公开日 2009 年 8 月 26 日

[11] 公开号 CN 101515317A

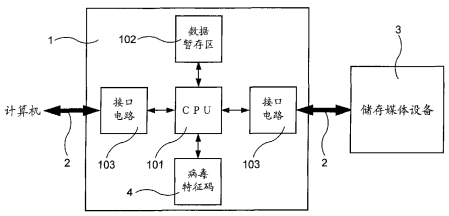
[22] 申请日 2008.2.19
[21] 申请号 200810065371.2
[71] 申请人 黄金富
地址 100032 北京市西城区金融街 27 号投资广场 B 座 19 层
[72] 发明人 黄金富
权利要求书 3 页 说明书 6 页 附图 1 页

[54] 发明名称

计算机与储存媒体设备 I/O 接口间的防病毒装置和方法

[57] 摘要

一种计算机与储存媒体设备 I/O 接口间的防病毒装置和方法，由防病毒装置(1)将所有流经计算机与储存媒体设备 I/O 接口(2)的数据暂存于数据暂存区(102)，并对数据暂存区(102)内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码(4)相符合的数据，当发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该 I/O 接口(2)传送到目的地。 本发明的防病毒装置(1)与计算机的操作系统无关，由于防病毒装置(1)是一个独立的硬体设备，即使操作系统出现漏洞被病毒攻击，防病毒装置(1)仍然能不受干扰继续对所有流经的数据进行病毒过滤。



1. 一种计算机防病毒装置，设置于计算机储存媒体设备的I/O接口之间，主要用于检测所有流经该 I/O 接口的数据是否含有病毒特征，其特征在于，所述的防病毒装置(1)内设有包括CPU(101)及数据暂存区(102)，所述的防病毒装置（1）并设有与所述的 I/O 接口（2）连接的接口电路（103）和储存有各病毒特征码（4），以及，所述的防病毒装置（1）按预定程序运作，将所有流经该I/O接口（2）的数据暂存于数据暂存区（102），并对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（4）相符合的数据，当发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该I/O接口（2）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后通过该I/O接口（2）转送到目的地。

2. 如权利要求 1 所述的计算机防病毒装置，其特征在于，所述的防病毒装置（1）上设有记忆卡接口（104）和与该记忆卡接口（104）相连接的记忆卡(5)，以及，所述的记忆卡(5)内储存有各病毒特征码(4)。

3. 如权利要求 1 所述的计算机防病毒装置，其特征在于，所述的储存媒体设备(3)包括: 硬盘 和/或 软盘 和/或 USB记忆卡 和/或 光盘驱动器 等等之类用于储存数据的储存媒体设备。

4. 如权利要求 1 所述的计算机防病毒装置，其特征在于，所述的 I/O 接口（2）包括: IDE（Integrated Drive Electronics） 和/或 EIDE（Enhanced Integrated Drive Electronics） 和/或 SCSI（Small Computer System Interface） 和/或 SATA（Serial Advanced

Technology Attachment） 和/或 USB（Universal Serial Bus） 和/或 IEEE1394 和/或 FireWire 等等之类 I/O 接口。

5. 一种计算机防病毒方法，采用如权利要求 1 至 4 任一项所述的计算机防病毒装置，其特征在于，所述的方法包括如下步骤:

1. 在计算机储存媒体设备（3）的 I/O 接口（2）之间加设防病毒装置（1）；
2. 在防病毒装置（1）内预先储存有各病毒特征码（4）；
3. 防病毒装置（1）将所有流经该 I/O 接口（2）的数据暂存于数据暂存区（102）；
4. 防病毒装置（1）对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（4）相符合的数据;
5. 当防病毒装置（1）发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该 I/O 接口（2）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后通过该 I/O 接口（2）转送到目的地。

6. 如权利要求 5 所述的计算机防病毒方法，其特征在于，当所述的防病毒装置（1）发现暂存数据中带有其中任何一病毒的特征时，向用户发出提示信号。

7. 如权利要求 6 所述的计算机防病毒方法，其特征在于，所述的方法还包括如下步骤，是防病毒装置（1）发现暂存数据中带有其中任何一病毒的特征时，向用户发出提示信号后，用户在防病毒装置（1）上作出如下的操作步骤:

用户按一次拦截键后，防病毒装置（1）拒绝让该数据流经该 I/O 接口（2）传送到目的地;

或

用户按一次通行键后，防病毒装置（1）允许该数据流经该 I/O 接口（2）传送到目的地。

8. 如权利要求 5 所述的计算机防病毒方法，其特征在于，所述的防病毒装置（1）于 I/O 接口（2）空闲时，自动读取储存媒体设备（3）内所储存的文件进行病毒扫描，当发现被扫描的文件中带有其中任何一病毒的特征时，向用户发出提示信号。

计算机与储存媒体设备I/O接口间的防病毒装置和方法

【技术领域】

本发明涉及计算机数据安全技术领域，特别是涉及一种计算机与储存媒体设备I/O接口间的防病毒装置和方法。

【背景技术】

计算机技术发展突飞猛进，计算机已经成为人们日常工作必需的工具之一，但是计算机病毒的出现，干扰了人们使用计算机的工作，现时绝大部分的计算机病毒具有传染性，病毒可以匿藏于文件或数据内，只要用户将带有病毒的文件或数据放到一台没有感染的计算机，就有机会令该计算机也感染病毒，例如用户从一台感染了病毒的计算机复制一个感染了病毒的文件到USB盘，然后将这USB盘放到另一台计算机，并将该感染了病毒的文件复制到该另一台计算机，就有可能令该另一台计算机也感染病毒，再由这被感染的计算机通过不同途径将病毒传播开去。这些感染了病毒的计算机，可以给计算机用户带来严重的影响，用户储存在计算机内的数据随时会被病毒破坏，给用户造成无法估量的损失，是一个极待解决的问题。

【发明内容】

本发明的目的，在于提供一种计算机防毒装置和方法，设置于计算机储存媒体设备的I/O接口之间，对所有流经该I/O接口的数据进行病毒过滤，使计算机病毒不能通过储存媒体设备传播。

一般的计算机病毒传播到计算机后，该病毒通常会匿藏于计算机的内存和储存媒体设备中，当用户将计算机关机后重新启动时，匿藏于计算机内存的病毒由于计算机关机后会令内存中的数据丢失，令匿藏于内存的病毒也同时消失，这样只要重新启动计算机就可以清除所有匿藏于内存的病

毒。但是大部分的计算机病毒除了匿藏于内存外，也会同时匿藏于文件或数据中，有些病毒更会直接匿藏于计算机的储存媒体设备上，病毒的主要宿主就是这些储存媒体设备，当用户重新启动计算机时，只要计算机载入了这些储存媒体设备上带有病毒的文件或数据，就有可能将该病毒也连同文件或数据载入计算机内存，使重新启动后的计算机内存中仍然感染了该病毒。本发明通过在储存媒体设备的 I/O 接口上加设过滤病毒的装置，使带有病毒的文件或数据不能从 I/O 接口传送到储存媒体设备上储存，以及储存媒体设备上带有病毒的文件或数据也不能从 I/O 接口传送到计算机的内存，这样即使计算机的内存感染了病毒，由于带有病毒的文件或数据不能从 I/O 接口传送到储存媒体设备上储存，只要将计算机重新启动，匿藏于内存的病毒也会随之消失。

本发明的目的是这样实现的，采用这样一种计算机防病毒装置，设置于计算机储存媒体设备的 I/O 接口之间，主要用于检测所有流经该 I/O 接口的数据是否含有病毒特征，其特征在于，所述的防病毒装置（1）内设有包括 CPU（101）及数据暂存区（102），所述的防病毒装置（1）并设有与所述的 I/O 接口（2）连接的接口电路（103）和储存有各病毒特征码（4），以及，所述的防病毒装置（1）按预定程序运作，将所有流经该 I/O 接口（2）的数据暂存于数据暂存区（102），并对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（4）相符合的数据，当发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该 I/O 接口（2）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后通过该 I/O 接口（2）转送到目的地。

以及，采用这样一种计算机防病毒方法，采用如前面所述的计算机防病毒装置，其特征在于，所述的方法包括如下步骤：

1. 在计算机储存媒体设备（3）的 I/O 接口（2）之间加设防病毒装置（1）；
2. 在防病毒装置（1）内预先储存有各病毒特征码（4）；
3. 防病毒装置（1）将所有流经该 I/O 接口（2）的数据暂存于数据暂存区（102）；
4. 防病毒装置（1）对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（4）相符合的数据；
5. 当防病毒装置（1）发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该 I/O 接口（2）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后通过该 I/O 接口（2）转送到目的地。

这样就实现了本发明的目的。

只要在计算机的所有储存媒体设备（3）的 I/O 接口之间设置了本发明的防病毒装置（1），就可以切断传播病毒的其中一条最主要的途径，令病毒无法匿藏于储存媒体设备（3）上，这样只要重新启动计算机就可确保计算机的内存没有感染病毒。这种对病毒的传播途径进行过滤拦截的方法，比一般采用软件扫描内存的防病毒方法更有效，由于防病毒装置（1）是一个独立的硬体设备，所以不会出现扫毒软件被病毒骑劫的情况。

【附图说明】

图 1 是本发明的防病毒装置（1）的结构示意说明图；

图 2 是增设了记忆卡（5）的防病毒装置（1）的结构示意说明图。

图中，相同的数字代表相同的装置、部件器件，附图是示意性的，用以说明本发明的构成和主要特征。

【具体实施方式】

下面结合附图，对本发明的计算机防病毒装置和方法作进一步详细说明。

参阅图 1，图 1 是本发明的防病毒装置（1）的结构示意说明图，图中示出的防病毒装置（1）内设有包括 CPU（101）及数据暂存区（102），所述的防病毒装置（1）并设有与所述的 I/O 接口（2）连接的接口电路（103）和储存有各病毒特征码（4），以及，所述的防病毒装置（1）按预定程序运作，将所有流经该 I/O 接口（2）的数据暂存于数据暂存区（102），并对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（4）相符合的数据，当发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该 I/O 接口（2）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后通过该 I/O 接口（2）转送到目的地。

其中，所述的储存媒体设备（3）包括：硬盘 和/或 软盘 和/或 USB 记忆卡 和/或 光盘驱动器 等等之类用于储存数据的储存媒体设备。所述的 I/O 接口（2）包括：IDE（Integrated Drive Electronics） 和/或 EIDE（Enhanced Integrated Drive Electronics） 和/或 SCSI（Small Computer System Interface） 和/或 SATA（Serial Advanced Technology Attachment） 和/或 USB（Universal Serial Bus） 和/或 IEEE1394 和/或 FireWire 等等之类 I/O 接口。

在设置方面，病毒特征码（4）是预先储存到防病毒装置（1）内，防病毒装置（1）可以通过不同的途径更新所储存的病毒特征码（4），例如通过计算机连线到指定的防病毒网站，从防病毒网站下载包含病毒特征码（4）的文件，然后由计算机将该文件储存于防病毒装置（1）内，而该文件可以采用数字证书等的加密方法，以确保文件的完整性和不被窜改。在防病毒网站方面，防病毒网站预先将文件以指定的密钥加密，然后由计算

机下载该文件并储存到防病毒装置（1）内，再由防病毒装置（1）将文件以对应的密钥进行解密，这样可保证该文件不会被病毒或其他程式窜改。

参阅图 2，图 2 是增设了记忆卡（5）的防病毒装置（1）的结构示意说明图，图 2 的实施例是本发明的更进一步改进，图中示出的防病毒装置（1）上设有记忆卡接口（104）和与该记忆卡接口（104）相连接的记忆卡（5），以及，所述的记忆卡（5）内储存有各病毒特征码（4）。与图 1 的实施例相比，不同之处在于图 2 的实施例中，将病毒特征码（4）储存到记忆卡（5）上，然后通过记忆卡接口（104）与 CPU（101）相连接，这样就可以随时为防病毒装置（1）更换储存有最新的病毒特征码（4）的记忆卡（5），方便随时更新病毒特征码（4）。例如使用另一台计算机连线到指定的防病毒网站下载包含最新的病毒特征码（4）的文件到记忆卡（5）上，然后将该记忆卡（5）插到防病毒装置（1）的记忆卡接口（104），而该文件可以采用数字证书等的加密方法，在防病毒网站预先将文件以指定的密钥加密，然后由计算机下载该文件并储存到记忆卡（5）上，再由防病毒装置（1）将该记忆卡（5）上的该文件以对应的密钥进行解密。

继续参阅图 1 和图 2，图 1 和图 2 所示的防病毒装置（1）所采用的防病毒方法，可以概括为如下步骤：

1. 在计算机储存媒体设备（3）的 I/O 接口（2）之间加设防病毒装置（1）；
2. 在防病毒装置（1）内预先储存有各病毒特征码（4）；
3. 防病毒装置（1）将所有流经该 I/O 接口（2）的数据暂存于数据暂存区（102）；
4. 防病毒装置（1）对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（4）相符合的数据；

5. 当防病毒装置（1）发现暂存数据带有其中任何一病毒的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能流经该 I/O 接口（2）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后通过该 I/O 接口（2）转送到目的地。

本发明的更进一步改进是在防病毒装置（1）上增设提示装置，当防病毒装置（1）发现暂存数据中带有其中任何一病毒的特征时，通过提示装置向用户发出提示信号，用户从提示信号就可知道有病毒出现，就可立即提高警觉，找出病毒来源，避免计算机感染病毒。此外，更可在防病毒装置（1）上增设按键，包括：通行键和拦截键，当防病毒装置（1）发现暂存数据中带有其中任何一病毒的特征时，通过提示装置向用户发出提示信号后，用户可在防病毒装置（1）上作出如下的操作步骤：

用户按一次拦截键后，防病毒装置（1）拒绝让该数据流经该 I/O 接口（2）传送到目的地；

或

用户按一次通行键后，防病毒装置（1）允许该数据流经该 I/O 接口（2）传送到目的地。

本发明的更进一步改进是在防病毒装置（1）上增设自动扫描病毒功能，是由防病毒装置（1）于 I/O 接口（2）空闲时，自动读取储存媒体设备（3）内所储存的文件进行病毒扫描，当发现被扫描的文件中带有其中任何一病毒的特征时，通过提示装置向用户发出提示信号。

以上已经详细说明了本发明的计算机防病毒装置和方法，本发明的防病毒装置（1）与计算机的操作系统无关，由于防病毒装置（1）是一个独立的硬体设备，即使操作系统出现漏洞被病毒攻击或骑劫，防病毒装置（1）仍然能不受干扰继续运作，继续对所有流经的数据进行病毒过滤。即使计算机更新或更换操作系统软件，防病毒装置（1）也无需作任何改变，仍然能继续有效运作。

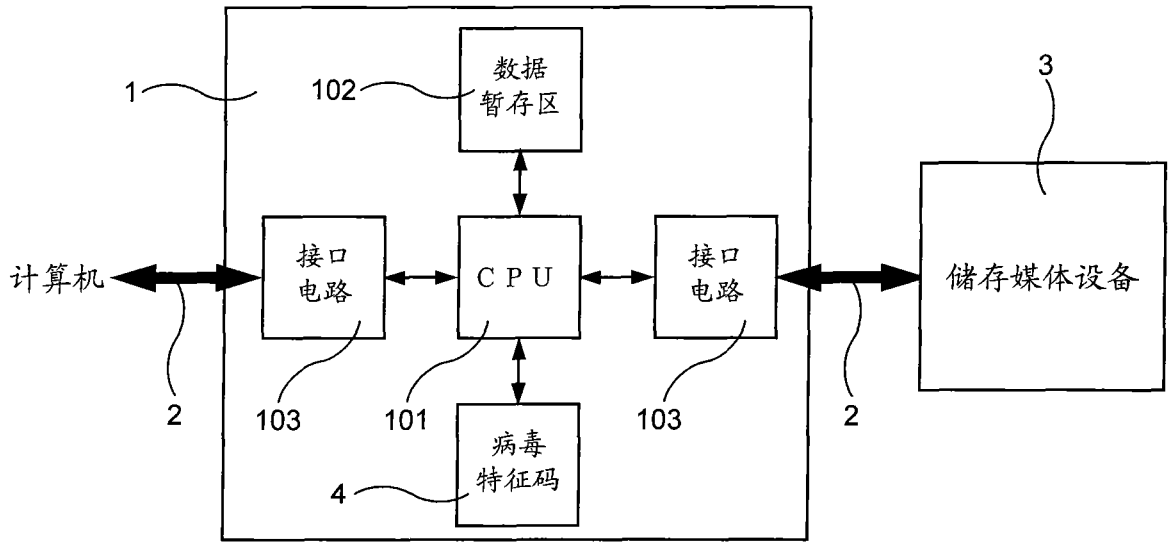

1
102
数据
暂存区
3
计算机
接口
电路
CPU
接口
电路
储存媒体设备
2
103
101
103
2
病毒
特征码
4

图 1

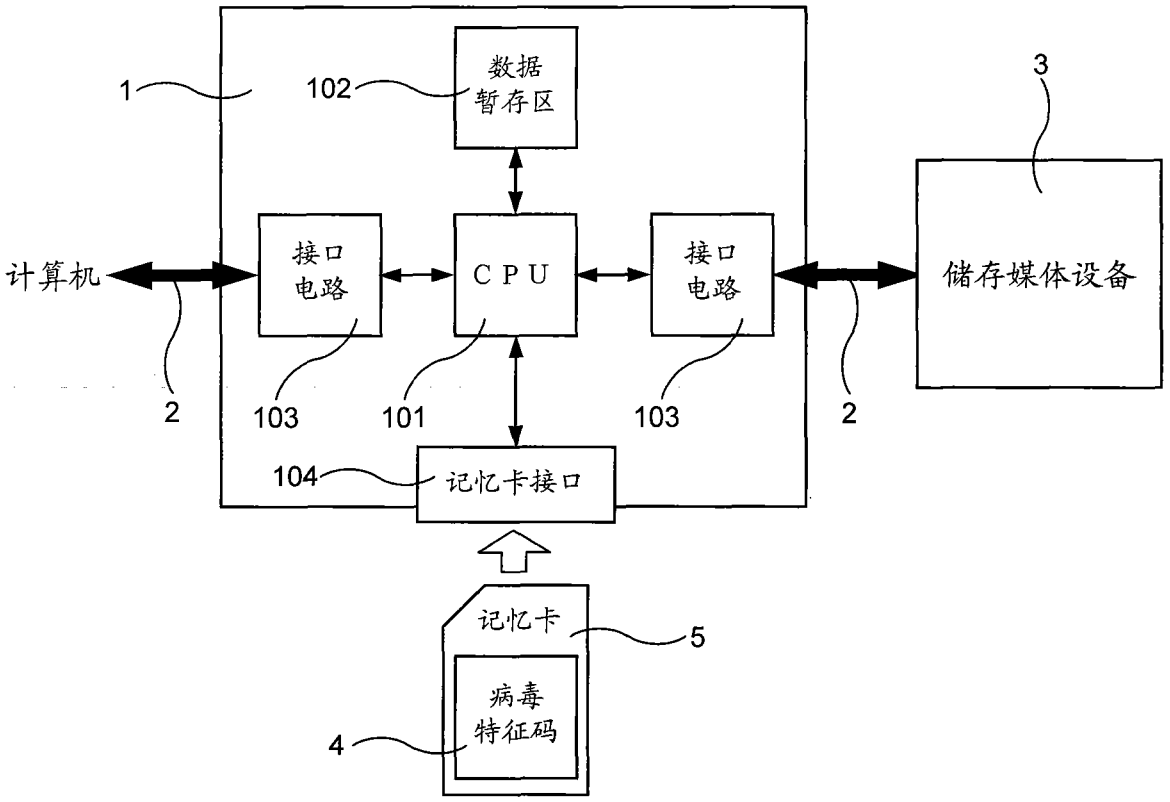

1
102
数据
暂存区
3
计算机
接口
电路
CPU
接口
电路
储存媒体设备
2
103
101
103
2
104
记忆卡接口
记忆卡
5
病毒
特征码
4

图 2