(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102073815 A
(43)申请公布日 2011.05.25

(21)申请号 201010613703.3

(22)申请日 2010.12.27

(71)申请人 奇瑞汽车股份有限公司
地址 241006 安徽省芜湖市经济技术开发区长春路 8 号

(72)发明人 付明勇 裴锦

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 罗建民 张天舒

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

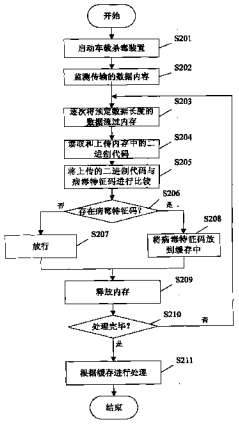
权利要求书 3 页 说明书 7 页 附图 2 页

(54)发明名称

一种车载杀毒系统及其杀毒方法

(57)摘要

本发明提供一种车载杀毒系统，包括：车载杀毒服务器，其用于保存和更新病毒库，并将更新的病毒库发送给车载杀毒装置；和车载杀毒装置，其用于实时监测通过车载信息系统的接口传输的数据内容，并将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中存在病毒特征码，则清除所述数据内容，或者提示用户对所述数据内容进行处理，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容；或者虚拟执行所述数据内容，并根据执行行为和结果进行判断和处理。通过本发明，可实时监控通过车载信息系统的接口传输的数据内容，以实现对车载信息系统进行防毒和杀毒的目的。



CN 102073815 A

1. 一种用于对车载信息系统进行杀毒的车载杀毒系统，所述车载信息系统包括用于与外界传输数据的接口，其特征在于，所述车载杀毒系统包括：

车载杀毒服务器，其用于保存和更新病毒库，并将更新的病毒库发送给车载杀毒装置；和

车载杀毒装置，其用于实时监测通过车载信息系统的接口传输的数据内容，并将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中存在病毒特征码，则清除所述数据内容，或者提示用户对所述数据内容进行处理，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容。

2. 根据权利要求 1 所述的车载杀毒系统，其特征在于，所述车载杀毒装置包括：

本地病毒库，其用于保存从车载杀毒服务器接收的病毒库；

实时监控模块，其用于实时监测通过车载信息系统的接口传输的数据内容，并逐次将监测到的数据内容中的预定数据长度的数据流过内存；

特征码比较模块，其用于将流过内存的数据内容与本地病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容；和

处理模块，其用于当特征码比较模块检测到所述数据内容中存在病毒特征码时，清除所述数据内容，或者提示用户对所述数据内容进行处理，并根据用户的处理意见进行相应处理。

3. 根据权利要求 2 所述的车载杀毒系统，其特征在于，所述车载杀毒装置还包括定时扫描模块，其包括：

定时扫描时间设定模块，其用于供用户设定定时扫描时间；和

定时扫描执行模块，其用于在用户设定的定时扫描时间自动对车载信息系统中的所有文件和应用程序进行全面扫描，

特征码比较模块将扫描的文件和应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序；对于特征码比较模块检测到其存在病毒特征码的文件和 / 或应用程序，处理模块清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序进行处理，并根据用户的处理意见进行相应处理。

4. 根据权利要求 2 所述的车载杀毒系统，其特征在于，所述车载杀毒装置还包括自定义杀毒模块：

自定义模块，其用于供用户定义扫描模式和车载信息系统中待扫描的文件和 / 或应用程序，所述扫描模式包括快速扫描和全面扫描；和

自定义扫描执行模块，其用于根据用户定义的扫描模式对用户定义的待扫描的文件和 / 或应用程序进行扫描，

特征码比较模块将扫描的文件和 / 或应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和 / 或应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序；对于特征码比较模块检测到其存在病毒特征码的文件和 / 或应用程序，处理模块清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序

进行处理，并根据用户的处理意见进行相应处理。

5. 根据权利要求 3 或 4 所述的车载杀毒系统，其特征在于，所述车载杀毒装置还包括：

信息备份模块，其用于当定时扫描模块或自定义扫描模块扫描完成后，将扫描的文件进行备份；和

修复模块，其用于根据信息备份模块中备份的文件对被病毒损坏的文件进行修复。

6. 根据权利要求 2 所述的车载杀毒系统，其特征在于，所述车载杀毒装置还包括：

病毒库更新模块，其用于自动链接到车载杀毒服务器，并根据车载杀毒服务器中病毒库的更新情况及时更新本地病毒库，或者由用户手动选择更新本地病毒库。

7. 根据权利要求 2 所述的车载杀毒系统，其特征在于，在以软件实现所述车载杀毒装置的情况下，所述车载杀毒装置还包括：

自身保护模块，其用于对所述车载杀毒装置进行保护，以避免病毒杀死车载杀毒装置自身的程序进程。

8. 根据权利要求 2 所述的车载杀毒系统，其特征在于，在以软件实现所述车载杀毒装置的情况下，所述车载杀毒装置还包括：

版权保护模块，其用于保护所述车载杀毒装置的版权，以防盗版。

9. 一种用于对车载信息系统进行杀毒的车载杀毒方法，所述车载信息系统包括用于与外界传输数据的接口，其特征在于，所述车载杀毒方法包括：

实时监测通过车载信息系统的接口传输的数据内容；

将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中存在病毒特征码，则清除所述数据内容，或者提示用户对所述数据内容进行处理，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容。

10. 根据权利要求 9 所述的车载杀毒方法，其特征在于，还包括：

在用户设定的定时扫描时间自动对车载信息系统中的所有文件和应用程序进行全面扫描；

将扫描的文件和应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序；对于检测到其存在病毒特征码的文件和 / 或应用程序，清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序进行处理，并根据用户的处理意见进行相应处理。

11. 根据权利要求 9 所述的车载杀毒方法，其特征在于，还包括：

根据用户定义的扫描模式对用户定义的待扫描的文件和 / 或应用程序进行扫描；

自定义扫描执行模块，其用于根据用户定义的扫描模式对用户定义的待扫描的文件和 / 或应用程序进行扫描，

将扫描的文件和 / 或应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和 / 或应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序；对于检测到其存在病毒特征码的文件和 / 或应用程序，处理模块清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序进行处理，并根据用户的处理意见进行相应处理。

12. 根据权利要求 10 或 11 所述的车载杀毒方法，其特征在于，还包括：

当扫描完成后，将扫描的文件进行备份；和

根据备份的文件对被病毒损坏的文件进行修复。

13. 根据权利要求 9 所述的车载杀毒方法，其特征在于，还包括：

自动链接到用于保存和更新病毒库的车载杀毒服务器，并根据车载杀毒服务器中病毒库的更新情况即时更新车载信息系统本地的病毒库，或者让用户手动更新车载信息系统的本地病毒库。

14. 根据权利要求 9 所述的车载杀毒方法，其特征在于，还包括：

对实现所述车载杀毒方法的程序进行保护，以避免病毒杀死该程序自身的进程。

15. 根据权利要求 9 所述的车载杀毒方法，其特征在于，还包括：

保护实现所述车载杀毒方法的软件的版权，以防盗版。

一种车载杀毒系统及其杀毒方法

技术领域

[0001] 本发明涉及车载信息处理技术领域，尤其涉及一种用于对车载信息系统进行防毒和杀毒的车载杀毒系统及其杀毒方法。

背景技术

[0002] 随着汽车技术的发展，车载信息系统市场正在迅速升温。目前新一代车载信息系统多数集成以下主要功能：基于卫星定位技术 (GPS GIS) 的地面导航；基于 ITS 数字广播 (GPS GIS LBS CDMB) 的智能交通；基于无线移动通信技术 (2G/3G DSRC WLAN) 的远程信息服务；以及基于数字广播技术 (CDMB-T/CMMB ITS) 的车载文化娱乐，当然还包括 PC 上所拥有的商务和娱乐功能。

[0003] 车载信息系统一般都有用于与外界传输数据的接口，例如 I/O 接口（如 USB 端口、DVD 端口）和无线网络接口。然而，这些接口都是裸漏在外的，目前没有任何相关应用程序对通过这些接口传输的数据内容（例如通过 I/O 接口交互的文件和应用程序、通过无线网络接口进行网页浏览、电子邮件收发和上传、下载等通讯操作而传输的通讯内容等）进行监控。一旦这些数据内容带有病毒（即，恶意程序代码）等，这些病毒将会侵入车载信息系统，不仅车载信息系统将会面临崩溃，甚至将会影响到整车安全，给用户带来不可估量的损失。

[0004] 然而，由于车载信息系统的 CPU 处理能力较低，内存比 PC 小，因此，不能直接利用一般 PC 所使用的杀毒软件对车载信息系统进行杀毒，而是需要一种能够专门针对车载信息系统进行防毒和杀毒的方法。但是，到目前为止，还没有提出和实现这种专用的车载杀毒方法。

发明内容

[0005] 为了解决上述问题，本发明提供一种车载杀毒系统及其杀毒方 法，以实现对车载信息系统进行防毒和杀毒的目的。

[0006] 为了实现以上目的，本发明提供一种用于对车载信息系统进行杀毒的车载杀毒系统，所述车载信息系统包括用于与外界传输数据的接口，其特征在于，所述车载杀毒系统包括：车载杀毒服务器，其用于保存和更新病毒库，并将更新的病毒库发送给车载杀毒装置；和车载杀毒装置，其用于实时监测通过车载信息系统的接口传输的数据内容，并将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中存在病毒特征码，则清除所述数据内容，或者提示用户对所述数据内容进行处理，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容。

[0007] 优选地，所述车载杀毒装置包括：本地病毒库，其用于保存从车载杀毒服务器接收的病毒库；实时监控模块，其用于实时监测通过车载信息系统的接口传输的数据内容，并逐次将监测到的数据内容中的预定数据长度的数据流过内存；特征码比较模块，其用于将流

过内存的数据内容与本地病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容；和处理模块，其用于当特征码比较模块检测到所述数据内容中存在病毒特征码时，清除所述数据内容，或者提示用户对所述数据内容进行处理，并根据用户的处理意见进行相应处理。

[0008] 优选地，所述车载杀毒装置还包括定时扫描模块，其包括：定时扫描时间设定模块，其用于供用户设定定时扫描时间；和定时扫描执行模块，其用于在用户设定的定时扫描时间自动对车载信息系统中的所有文件和应用程序进行全面扫描，特征码比较模块将扫描的文件和应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和／或应用程序；对于特征码比较模块检测到其存在病毒特征码的文件和／或应用程序，处理模块清除存在该文件和／或应用程序，或者提示用户对该文件和／或应用程序进行处理，并根据用户的处理意 见进行相应处理。

[0009] 优选地，所述车载杀毒装置还包括自定义杀毒模块：自定义模块，其用于供用户定义扫描模式和车载信息系统中待扫描的文件和／或应用程序，所述扫描模式包括快速扫描和全面扫描；和自定义扫描执行模块，其用于根据用户定义的扫描模式对用户定义的待扫描的文件和／或应用程序进行扫描，特征码比较模块将扫描的文件和／或应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和／或应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和／或应用程序；对于特征码比较模块检测到其存在病毒特征码的文件和／或应用程序，处理模块清除存在该文件和／或应用程序，或者提示用户对该文件和／或应用程序进行处理，并根据用户的处理意见进行相应处理。

[0010] 优选地，所述车载杀毒装置还包括：信息备份模块，其用于当定时扫描模块或自定义扫描模块扫描完成后，将扫描的文件进行备份；和修复模块，其用于根据信息备份模块中备份的文件对被病毒损坏的文件进行修复。

[0011] 优选地，所述车载杀毒装置还包括：病毒库更新模块，其用于自动链接到车载杀毒服务器，并根据车载杀毒服务器中病毒库的更新情况及时更新本地病毒库，或者由用户手动选择更新本地病毒库。

[0012] 优选地，在以软件实现所述车载杀毒装置的情况下，所述车载杀毒装置还包括：自身保护模块，其用于对所述车载杀毒装置进行保护，以避免病毒杀死车载杀毒装置自身的程序进程。

[0013] 优选地，在以软件实现所述车载杀毒装置的情况下，所述车载杀毒装置还包括：版权保护模块，其用于保护所述车载杀毒装置的版权，以防盗版。

[0014] 相应地，本发明提供一种用于对车载信息系统进行杀毒的车载杀毒方法，所述车载信息系统包括用于与外界传输数据的接口，其特征在于，所述车载杀毒方法包括：实时监测通过车载信息系统的接口传输的数据内容；将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述 数据内容中存在病毒特征码，则清除所述数据内容，或者提示用户对所述数据内容进行处理，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容。

[0015] 优选地，所述方法还包括：在用户设定的定时扫描时间自动对车载信息系统中的所有文件和应用程序进行全面扫描；将扫描的文件和应用程序与本地病毒库中的病毒特征

码进行比较，以检测扫描的文件和应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序 ；对于检测到其存在病毒特征码的文件和 / 或应用程序，清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序进行处理，并根据用户的处理意见进行相应处理。

[0016] 优选地，所述方法还包括 ：根据用户定义的扫描模式对用户定义的待扫描的文件和 / 或应用程序进行扫描 ；自定义扫描执行模块，其用于根据用户定义的扫描模式对用户定义的待扫描的文件和 / 或应用程序进行扫描，将扫描的文件和 / 或应用程序与本地病毒库中的病毒特征码进行比较，以检测扫描的文件和 / 或应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序 ；对于检测到其存在病毒特征码的文件和 / 或应用程序，处理模块清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序进行处理，并根据用户的处理意见进行相应处理。

[0017] 优选地，所述方法还包括 ：当扫描完成后，将扫描的文件进行备份 ；和根据备份的文件对被病毒损坏的文件进行修复。

[0018] 优选地，所述方法还包括 ：自动链接到用于保存和更新病毒库的车载杀毒服务器，并根据车载杀毒服务器中病毒库的更新情况及时更新车载信息系统本地的病毒库，或者让用户手动更新车载信息系统的本地病毒库。

[0019] 优选地，所述方法还包括 ：对实现所述车载杀毒方法的程序进行保护，以避免病毒杀死该程序自身的进程。

[0020] 优选地，所述方法还包括 ：保护实现所述车载杀毒方法的软件的版权，以防盗版。

[0021] 通过以上技术方案，本发明可获得以下技术效果 ：

[0022] (1) 可实时监控通过车载信息系统的接口 (包括 I/O 接口和无线网络接口) 传输的数据内容，防止病毒侵入车载信息系统和对侵入车载信息系统的病毒进行处理 (例如，根据用户的处理意见清除或放行病毒以及上报给车载杀毒服务器)，从而将带有病毒的可疑数据内容阻止在外，及时保障车载信息系统的安全 ；

[0023] (2) 通过定时扫描，可定时对车载信息系统进行安全检测，对不安全程序、文件等进行自动处理 (例如，清除病毒以及上报给车载杀毒服务器) ；

[0024] (3) 及时根据当前病毒情况，升级病毒库。

附图说明

[0025] 图 1 是根据本发明实施例的车载杀毒系统的框图 ；

[0026] 图 2 是根据本发明的第一实施例的由车载杀毒装置 2 执行的及时诊断流程的流程图。

具体实施方式

[0027] 以下，将参照附图和实施例对本发明进行描述。

[0028] (第一实施例)

[0029] 如上所述，病毒可通过经由车载信息系统的接口 (包括 I/O(如 USB 端口、DVD 端口) 和无线网络接口) 传输的数据内容侵入车载信息系统，也就是说，病毒侵入车载信息系统的途径主要包括 ：I/O 接口的文件交互、无线网络通讯中的网页浏览、无线网络通讯中的

电子邮件收发、无线网络通讯中的文件和应用程序下载等。

[0030] 在本实施例中，对通过车载信息系统的接口传输的数据内容（例如，通过 I/O 接口交互的文件、通过无线网络接口传输的通讯内容等）进行实时监测，并将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测监测到的数据内容中是否存在病毒特征码。一旦检测到传输的数据内容中存在病毒特征，即，发现异常情况，可立即对该数据内容进行清除，或者，可立即上报给车载杀毒系统的用户界面，提示用户发现病毒等相关信息，这些信息包括病毒特征码和其所处的物 理位置等，同时给出处理意见（例如，清除带有病毒的数据内容或放行该数据内容）供用户选择，然后根据用户的选择进行相应处理。

[0031] 图 1 是根据本发明实施例的车载杀毒系统的框图。如图 1 所示，该车载杀毒系统包括车载杀毒服务器 1 和车载杀毒装置 2，其中，车载杀毒服务器 1 用于保存和更新病毒库，并将更新的病毒库发送给车载杀毒装置 2 ；车载杀毒装置 2 用于实时监测通过车载信息系统的接口传输的数据内容，并将监测到的数据内容与病毒库中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中存在病毒特征码，则清除所述数据内容，或者提示用户对所述数据内容进行处理，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容。

[0032] 这里，车载杀毒服务器是指一台普通的 PC 端服务器，比如，瑞星公司的瑞星杀毒软件的工作服务器，此时，车载杀毒服务器中的病毒库就是瑞星的病毒库。

[0033] 本发明的车载杀毒装置 2 可用硬件（例如，单片机）或软件来实现。在用软件实现车载杀毒装置 2（即，实现为车载杀毒软件）的情况下，可将其预装在车载信息系统中，也可以后装于车载信息系统，也可将其装在专用存储器中，即插即用于车载信息系统。在即插即用的情况下，只要插上装有本发明的车载杀毒软件的存储器，就能及时监测通过车载信息系统的接口传输的数据内容，同时对车载信息系统做出安全检测，对于异常情况，给出处理措施。

[0034] 如图 1 中实线框所示，根据本发明的车载杀毒装置 2 包括本地病毒库 201、实时监控模块 202、特征码比较模块 203 和处理模块 204，其中，本地病毒库 201 用于保存从车载杀毒服务器 1 接收的病毒库 ；实时监控模块 202 用于实时监测通过车载信息系统的接口传输的数据内容，并逐次将监测到的数据内容中的预定数据长度的数据流过内存 ；特征码比较模块 203 用于将流过内存的数据内容与本地病毒库 201 中的病毒特征码进行比较，以检测所述数据内容中是否存在病毒特征码，如果检测到所述数据内容中不存在病毒特征码，则放行所述数据内容 ；处理模块 204 用于当特征码比较模块 203 检测到所述数据 内容中存在病毒特征码时，清除所述数据内容，或者提示用户对所述数据内容进行处理，并根据用户的处理意见进行相应处理，当特征码比较模块 203 检测到所述数据内容中不存在病毒特征码时，可不进行任何处理，或者可提示用户安全。

[0035] 此外，车载杀毒装置 2 还可包括病毒库更新模块，其用于自动链接到车载杀毒服务器 1，并根据车载杀毒服务器 1 中病毒库的更新情况及时更新本地病毒库 201，或者由用户手动选择更新本地病毒库 201，从而实现病毒库的即时升级。手动更新即是指 ：当用户关闭车载杀毒自动更新功能（即，前述自动根据车载杀毒服务器 1 中病毒库的更新情况及时更新本地病毒库 201）时，车载杀毒系统可以根据用户的指令链接到车载杀毒服务器上，从车载杀毒服务器上下载最新的病毒库。

[0036] 在本发明中，需要考虑的是车载信息系统的 CPU 处理能力较低、内存比 PC 小内存较小，为了适应车载杀毒软件的 CPU 处理能力和内存，需要将即将流过内存的数据（即，通过车载信息系统的接口传输的数据内容）进行分割处理。这里，关键问题在于如何对即将流过内存的数据进行分解，即，如何确定每次流过内存的数据的长度。

[0037] 可按照如下思路解决这个问题：假设本地病毒库中最大的病毒特征码大小为 15k，则每次外界流过内存的数据不能超过 15K*n，15K*n 不能超过限定值。限定值的取值可如下设定：假设内存大小为 512M，用于车载杀毒的部分为 128MB，则 n 最大取值为 8000，即同时流进内存的数据大小不能大于 120M，由于车载信息系统 CPU 处理能力低，内存比 PC 小，所以 120M 的数据存储能力是够用的。

[0038] 具体还可以用最小公倍数的原则进行取值 n。n ＝所有病毒特征码大小的最小公倍数。但是 15k*n ＜ 120Mb，否则 15k*n ＝ 120mb。当然 120MB 这么大的数据量是不能同时流过内存的。这些就不是车载杀毒系统考虑的因素。

[0039] 这样可以尽量保证每次流过内存的数据能包含所有的病毒特征码 .

[0040] 在具体实现时，首先，在车载信息系统的硬盘中划分出一部分 空间作为一个暂时存放文件的缓存，并在车载信息系统的内存里划分一部分空间（即，从内存总量中减去车载信息系统自处理占用内存部分所剩的内存部分）用于逐次处理通过车载信息系统的接口传输的预定数据长度的数据内容。划分好内存和缓存之后，逐次将监测到的数据内容中的预定数据长度的数据流过内存。

[0041] 例如，假设在硬盘中划分出 10G 作为缓存，通过车载信息系统的 I/O 接口接收到一个 100M 大的文件，将该文件 1M、1M 地转换为二进制代码，流过内存。然后，将流过内存的二进制代码与病毒库中的病毒特征码进行比较，以判断是否存在病毒，如果存在病毒，则将当前内存中流过的包含病毒特征码的 1M（或者可能小于 1M）数据作为一个文件存入 10G 缓存中。当流过内存的数据大小为 0 时，表示通过车载信息系统的接口传输的数据内容全部传递完毕。当对这些数据内容全部处理完毕之后，处理模块 204 对这 10G 缓存中的数据进行处理。此时，便可释放大量的内存用于处理数据。

[0042] 图 2 是由车载杀毒装置 2 按照以上方法执行的及时诊断流程的流程图。

[0043] 首先，在步骤 S201 中，启动车载杀毒装置 2。然后在步骤 S202 中，实时监控模块 202 对通过车载信息系统的接口传输的数据内容进行实时监测，并在步骤 S203 中，逐次将监测到的数据内容中的预定数据长度（例如，1M）的数据转换为二进制代码，流过内存。然后，在步骤 S204 中，实时监控模块 202 读取内存中的二进制代码，上传到特征码比较模块 203。

[0044] 接着，在步骤 S205 中，特征码比较模块 203 将上传的二进制代码与本地病毒库 201 中的病毒特征码进行比较。然后，在步骤 S206 中，根据步骤 S205 的比较结果来检测这些二进制代码中是否存在病毒特征码。如果检测到这些二进制代码中不存在病毒特征码，则在步骤 S207 中，放行这些二进制代码，并将其编译成可执行文件。如果检测到这些二进制代码中存在病毒特征码，则在步骤 S208 中，将内存中包含该病毒特征码的数据作为一个文件放到缓存中。

[0045] 执行完步骤 S207 或 S208 后，在步骤 S209 中，释放内存。接着， 在步骤 S210 中判断通过接口传输的数据是否处理完毕，如果处理完毕，则执行步骤 S211，否则跳转到步骤

S203，继续对流过内存的数据进行处理。

[0046] 在步骤 S211 中，处理模块 204 根据缓存中的数据进行处理。具体地讲，当缓存中存在病毒特征码时，清除包含该病毒特征码的文件，或者提示用户对该文件进行处理，例如，提示用户是清除带有病毒的文件还是放行该文件，然后根据用户的处理意见进行相应处理。当缓存中不存在病毒特征码时，可提示用户当前通过车载信息系统的接口传输的数据内容安全。

[0047] 通过以上流程，根据本发明的车载杀毒与普通 PC 上的杀毒相比具有以下优点：

[0048] (1) 利用车载信息系统的硬盘空间划分缓存，将内存中的检测为存在病毒特征码的数据存放到缓存中，然后释放内存，进入下一循环处理，这样，可不占用大量内存；在利用内存处理完通过车载信息系统的接口传输的所有数据之后，由于处理的是车载信息系统硬盘上的数据（即，缓存中的数据），所以处理速度比处理外接端口的速度要快；

[0049] (2) 由于车载信息系统的上层对象为网络或存储介质（如 DVD 或 USB 接口的存储介质），所以只要服务器病毒库能及时根据 PC 病毒情况更新，就可保障车载信息系统本地的病毒库的更新速度，因此，升级速度快；

[0050] (3) 车载信息系统与外界交互的接口比 PC 少，可对应不同接口实时启动不同的监控装置，以节约资源。例如，在用软件实现车载杀毒装置（即，实现为车载杀毒软件）的情况下，将实时监控模块分成分别针对 USB 接口、DVD 接口和无线网络接口的监控模块 2021、2022 和 2023，当 USB 传输时，只启动监控模块 2021，监控模块 2022 和 2023 休眠，从而节约系统内存。

[0051] （第二实施例）

[0052] 本实施例在第一实施例的基础之上增加了定时扫描功能，即，由用户设定定时扫描时间，在到达设定的定时扫描时间时，车载杀毒装置 2 自动对整个车载信息系统进行全面扫描，一旦发现异常情况，立即上报和处理。

[0053] 为了实现以上目的，根据本发明的第二实施例的车载杀毒装置 2 还可包括定时扫描模块 206。如图 1 所示，定时扫描模块 206 进一步包括定时扫描时间设定模块 2061 和定时扫描执行模块 2062，其中，定时扫描时间设定模块 2061 例如为一个用户交互界面，用于供用户设定定时扫描时间；定时扫描执行模块 2062 用于在用户设定的定时扫描时间自动对车载信息系统中的所有文件和应用程序进行全面扫描。

[0054] 此时，特征码比较模块 203 将扫描的文件和应用程序与本地病毒库 201 中的病毒特征码进行比较，以检测扫描的文件和应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和 / 或应用程序。对于特征码比较模块 203 检测到其存在病毒特征码的文件和 / 或应用程序，处理模块 204 清除存在该文件和 / 或应用程序，或者提示用户对该文件和 / 或应用程序进行处理，并根据用户的处理意见进行相应处理。

[0055] 在具体实现时，首先，判断车载系统时间是否与设定时间相符，如果相符，则启动车载杀毒装置 2，否则不启动车载杀毒装置 2。在启动车载杀毒装置 2 之后，定时扫描执行模块 2062 自动对车载信息系统中的所有文件和应用程序进行全面扫描，例如，按照所有文件和应用程序的名称的字母顺序逐一扫描。后续步骤与图 2 中的步骤 S203 至 S211 相同。

[0056] （第三实施例）

[0057] 本实施例在第一实施例或第二实施例的基础上增加了自定义杀毒功能，即，用户

可以自己定义扫描模式和车载信息系统中待扫描的文件和/或应用程序，可选的扫描模式包括全面扫描和快速扫描。一旦发现异常情况，立即上报和处理。

[0058] 为了实现以上目的，根据本发明的第三实施例的车载杀毒装置 2 还包括自定义杀毒模块 207。如图 1 所示，自定义杀毒模块 207 进一步包括自定义模块 2071 和自定义扫描执行模块 2072，其中，自定义模块 2071 例如为一个用户交互界面，用于供用户定义扫描模式和车载信息系统中待扫描的文件和/或应用程序；自定义扫描执行模块 2072 用于根据用户定义的扫描模式对用户定义的待扫描的文件和/或应用程序进行扫描。

[0059] 此时，特征码比较模块 203 将扫描的文件和/或应用程序与本地病毒库 201 中的病毒特征码进行比较，以检测扫描的文件和/或应用程序中是否存在病毒特征码，并放行未检测到病毒特征码的文件和/或应用程序。对于特征码比较模块 203 检测到其存在病毒特征码的文件和/或应用程序，处理模块 204 清除存在该文件和/或应用程序，或者提示用户对该文件和/或应用程序进行处理，并根据用户的处理意见进行相应处理。

[0060] （第四实施例）

[0061]

[0062] 本实施例在第二实施例和第三实施例的基础上增加了修复功能，即，可对被病毒损坏的文件进行修复。

[0063] 为了实现这个目的，根据本发明的车载杀毒装置 2 还包括信息备份模块和修复模块，其中，信息备份模块用于当定时扫描模块 206 或自定义扫描模块 207 扫描完成后，将扫描的文件进行备份；修复模块用于根据信息备份模块中备份的文件对被病毒损坏的文件进行修复。

[0064] （第五实施例）

[0065] 本实施例在以上实施例的基础上增加了对实现本发明的车载杀毒装置 2 的车载杀毒软件进行保护的功能。

[0066] 为了实现这个目的，根据本发明的车载杀毒装置 2 还包括自身保护模块，其用于对本发明的车载杀毒软件进行保护，以避免病毒杀死车载杀毒软件自身的程序进程，具体地讲，即，自动备份车载杀毒软件自身的应用程序，在病毒被杀掉之后，可利用自身备份的应用程序来修复损坏的应用程序。

[0067] （第六实施例）

[0068] 本实施例在以上实施例的基础上增加了对实现本发明的车载杀毒装置 2 的车载杀毒软件的版权进行保护的功能。

[0069] 为了实现这个目的，根据本发明的车载杀毒装置 2 还包括版权保护模块，其用于保护本发明的车载杀毒软件的版权，以防盗版。版权保护方法可采用任何已知的版权保护方法，例如，在车载杀毒软件中添加反编译程序上报等。

[0070] 以上已参照附图和实施例对本发明进行了详细描述，但是，应该理解，本发明并不限于以上所公开的具体实施例，任何基于本发明的变型都应包括在本发明的保护范围内。

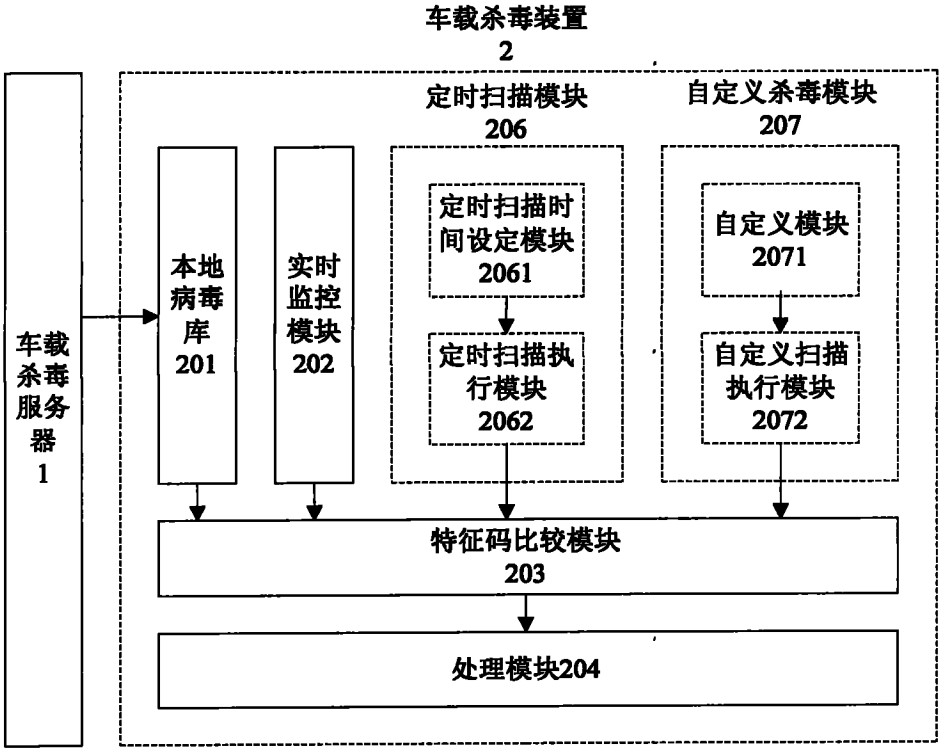

车载杀毒装置
2
定时扫描模块
206
自定义杀毒模块
207
车载杀毒服务器
1
本地病毒库
201
实时监控模块
202
定时扫描时间设定模块
2061
定时扫描执行模块
2062
自定义模块
2071
自定义扫描执行模块
2072
特征码比较模块
203
处理模块204

图 1

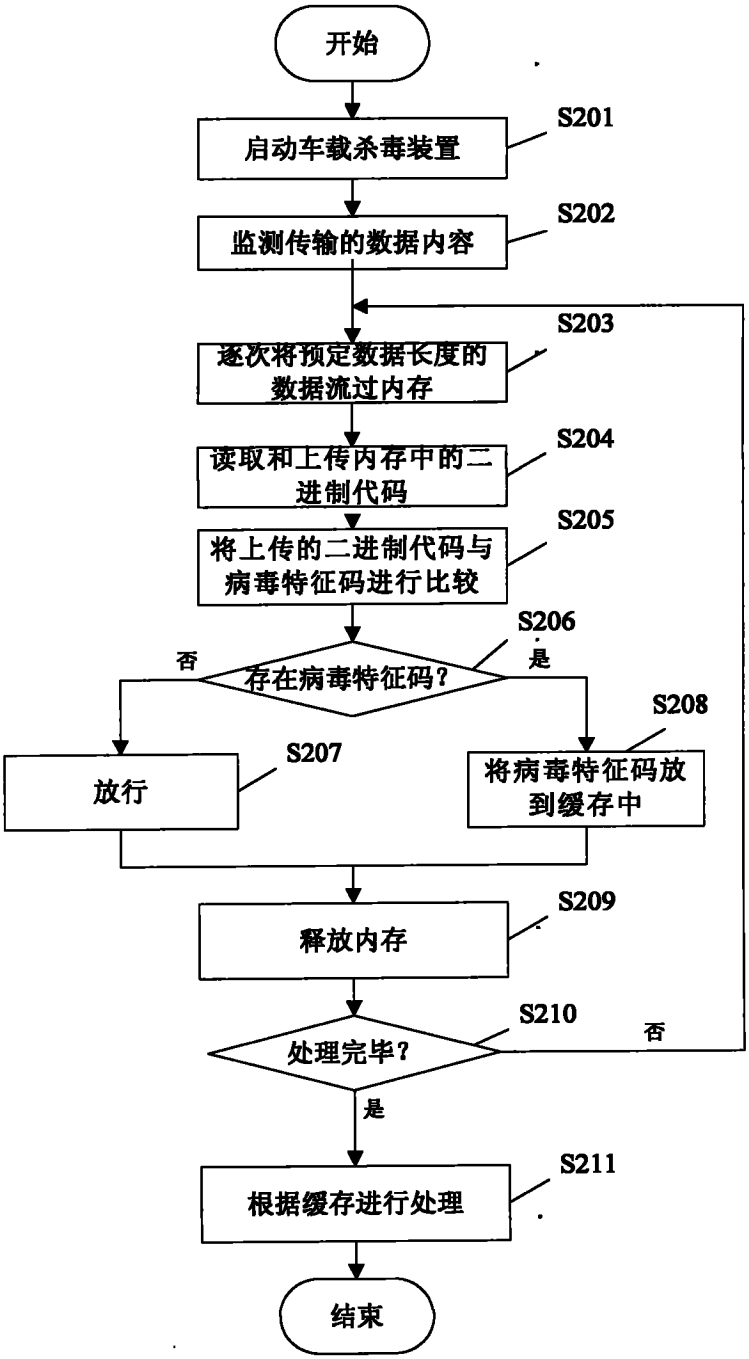

开始
S201
启动车载杀毒装置
S202
监测传输的数据内容
S203
逐次将预定数据长度的数据流过内存
S204
读取和上传内存中的二进制代码
S205
将上传的二进制代码与病毒特征码进行比较
S206
存在病毒特征码?
否
是
S207
放行
S208
将病毒特征码放到缓存中
S209
释放内存
S210
处理完毕?
否
是
S211
根据缓存进行处理
结束

图 2