[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 说 明 书

专利号 ZL 200610039902.1

[45] 授权公告日 2009 年 2 月 4 日

[11] 授权公告号 CN 100458808C

[22] 申请日 2006.4.26

[21] 申请号 200610039902.1

[73] 专利权人 南京大学

地址 210093 江苏省南京市汉口路 22 号

共同专利权人 江苏南大苏富特软件股份有限公司

[72] 发明人 伍卫民 胡 静 谢俊元 谢 立

[56] 参考文献

CN1591329A 2005.3.9

WO01/11480A1 2001.2.15

US5677953A 1997.10.14

基于驱动层的 USB 存储设备安全增强技术. 吴宇，唐朝京，张权. 计算机应用研究，第 21 卷第 2 期. 2004

文件过滤驱动及应用. 李民，方勇，刘林超，熊帆. 信息与电子工程，第 3 卷第 4 期. 2005

审查员 徐飞兵

[74] 专利代理机构 南京天翼专利代理有限责任公司

代理人 汤志武 王鹏翔

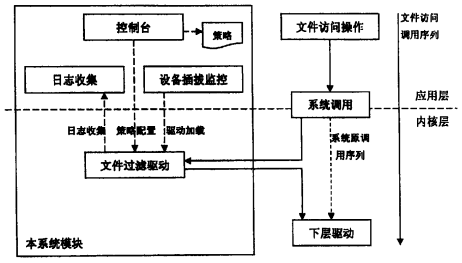
权利要求书 2 页 说明书 4 页 附图 3 页

[54] 发明名称

一种对即插即用存储设备进行读写访问控制的方法

[57] 摘要

一种对即插即用存储设备进行读写访问控制的方法，使用控制台、即插即用存储设备检测、文件系统过滤驱动部件、日志收集四个模块，其工作包含以下几个基本步骤：控制台模块配置即插即用存储设备使用安全策略；插即用存储设备检测模块实时检测即插即用存储设备的插入，并通知内核挂接过滤设备，开启监控；文件系统过滤驱动部件模块根据策略实现即插即用存储设备访问监控的具体操作；插即用存储设备检测模块实时检测即插即用存储设备的移除，并通知内核卸载过滤设备，停止监控。 系统分应用层与内核层，在应用层实时检测可移动存储设备的插拔，及时通知内核模块挂接过滤设备进行监控。



1、一种对即插即用存储设备进行读写访问控制的方法，其特征在于使用控制台、即插即用存储设备检测、文件系统过滤驱动部件、日志收集四个模块，其工作包含以下几个步骤：

步骤 1：控制台模块配置即插即用存储设备使用安全策略，具体包括如下两个步骤；

步骤 1-1：控制台加载文件系统过滤驱动部件；

步骤 1-2：控制台读取初始策略文件，并向文件系统过滤驱动部件设置监控策略；

步骤 2：即插即用存储设备检测模块实时检测即插即用存储设备的插入，并通知内核挂接文件系统过滤驱动部件，开启监控，具体步骤如下；

步骤 2-1：控制台启动即插即用存储设备检测模块，使之实时检测即插即用设备的插入，及时通知过滤驱动进行过滤设备挂接；

步骤 3：文件系统过滤驱动部件模块根据步骤 1 配置的安全策略实现即插即用存储设备访问监控的具体操作；

步骤 4：即插即用存储设备检测模块实时检测即插即用存储设备的移除，并通知内核卸载文件系统过滤驱动部件，停止监控；

步骤 5：控制台接收用户设置的新策略，并向文件系统过滤驱动部件设置监控策略；

步骤 6：控制台接收用户停止监控命令，停止并卸载所有内核部件。

2、根据权利要求 1 所述的对即插即用存储设备进行读写访问控制的方法，其特征在于其控制台、即插即用存储设备检测和日志收集模块处于操作系统应用层，其中控制台动态配置监控策略，并管理文件系统过滤驱动部件完成监控任务；文件系统过滤驱动部件则处于操作系统内核层。

3、根据权利要求 2 所述的对即插即用存储设备进行读写访问控制的方法，其特征在于文件系统过滤驱动部件工作于操作系统内核，使用 Windows 驱动层次结构中的文件系统层过滤驱动技术进行访问控制。

4、根据权利要求 1 或 2 所述的对即插即用存储设备进行读写访问控制的方法，其特征在于文件系统过滤驱动部件对文件访问操作进行访问控制，包含以下几个步骤：

步骤 1：用户的文件访问操作转换成操作系统文件访问接口调用；

步骤 2：操作系统文件访问接口调用传递到 I/O 管理器，转换成过滤驱动处理的 I/O 请求包；

步骤 3：I/O 管理器在将文件访问请求包传递给文件系统驱动前先交给文件过滤驱动；

步骤4：文件过滤驱动根据监控策略对I/O请求包进行处理，根据I/O请求包指向文件，处理如下：

1. 若策略为禁止访问，使I/O请求包失败；
2. 若策略为禁止写，只允许读请求包通过，以写方式打开文件的请求包失败；
3. 若策略为允许访问，但需审计，记录访问请求；

步骤5：将如上允许通过的I/O请求包传递给下层驱动程序，并进行日志。

5、根据权利要求1或2所述的对即插即用存储设备进行读写访问控制的方法，其特征在于所述日志收集模块工作于操作系统应用层，从内核中取出根据监控记录生成的监控日志，以供后续安全分析。

一种对即插即用存储设备进行读写访问控制的方法

技术领域

本发明涉及一种对即插即用存储设备读写访问控制的方法，尤其是在主机平台上对各种可移动存储设备的安全使用进行管理，保障主机的信息安全，属于计算机信息安全领域。

背景技术

大容量移动存储设备(如USB硬盘，磁带存储设备等)广泛使用，使信息传递更加方便快捷，若不能有效控制其使用，会使内网信息安全存在严重问题，如何对外围存储设备的使用有效控制显得越来越紧迫。针对外围存储设备的安全使用，现有 windows 系统能提供简单的对特定类型设备读写控制，如允许管理员设置网络内用户主机系统的USB闪存，磁带，软驱等不允许使用、只读等，以防止信息通过这些设备而泄露。还有一些安全产品，通过程序控制各种外围存储设备的接入，简单地允许或禁止外围存储设备的使用。

必须对即插即用存储设备的读写访问进行控制，这是保证内网信息安全的重要措施，但由于外围存储设备的下层的驱动程序复杂性，如对每一种外围设备编写过滤驱动程序则太复杂。

发明内容

本发明的目的在于：为主机上各种各样即插即用存储设备提供统一的监控方法。使用基于文件系统过滤驱动，能很好的对各种外围存储设备进行监控，一方面文件系统层屏蔽了各种外围存储设备下层的驱动程序复杂性，不需为每一种外围设备编写过滤驱动程序，另一方面通常I/O管理器将请求直接交给文件系统层的驱动处理，文件系统层则处于较高的层次，能很好的实施对文件资源访问的保护机制，根据文件的相关属性，决定读写访问是否允许，并可记录必要信息，以供后续分析。

本发明的内容是这样实现的，一种对即插即用存储设备进行读写访问控制的方法为：

整个系统包含如下四个模块：控制台、即插即用存储设备检测、文件系统过滤驱动部件、日志收集四个模块。

控制台程序也是整个监控系统的主控程序，工作于操作系统应用层，其工作为：动态配置监控策略，并管理文件系统过滤驱动部件完成监控任务；控制台对文件过滤驱动的管理，其工作步骤为：

步骤1：控制台加载文件系统过滤驱动部件；

步骤2：控制台读取初始策略文件，并向文件系统过滤驱动部件设置监控策略；

步骤3：启动即插即用存储设备检测模块，使之可以实时检测即插即用设备

的插入，及时通知过滤驱动进行过滤设备挂接；

步骤 4：控制台接收用户设置的新策略，并向文件系统过滤驱动部件设置监控策略；

步骤 5：控制台接收用户停止监控命令，停止并卸载所有内核部件。

即插即用存储设备检测部件，用轮询的方式，及时发现即插即用设备的插入或移除，并动态的挂载或卸载用于监控的过滤设备。

用于实现文件访问控制的文件系统过滤驱动部件，工作于操作系统内核，使用了 Windows 驱动层次结构中的文件系统层过滤驱动技术进行访问控制，由于其处于文件过滤驱动层，这种逻辑结构可以屏蔽底层设备类型的复杂性，文件系统过滤驱动部件进行访问控制工作的原理，其特征在于包含以下几个基本步骤：

步骤 1：用户的文件访问操作转换成操作系统文件访问接口调用；

步骤 2：操作系统调用传递到 I/O 管理器，转换成过滤驱动处理的 I/O 请求包；

步骤 3：I/O 管理器在将文件访问请求包传递给文件系统驱动前先交给文件过滤驱动；

步骤 4：文件过滤驱动根据监控策略对 I/O 请求包进行处理，并记录处理日志。

为能更好的跟踪监控对即插即用存储设备的访问，提供日志收集模块，工作于操作系统应用层，从内核中取出根据监控记录生成的监控日志，以供后续安全分析。

本发明的特点是：根据现有对即插即用存储设备使用控制方法的弱点，提出使用 Windows 驱动层次结构中的文件系统层过滤驱动技术进行控制。文件过滤驱动层，可以获得所有操作系统上层发出的文件访问操作请求，经分析并判断后决定该请求是否被真正的执行；同时，其所处的逻辑结构屏蔽了底层设备类型复杂性，可以对不同类型及不同设备驱动的存储设备进行监控。

附图说明

图 1 为本发明一个实现的系统模块结构图。

图 2 为本发明配置管理模块的工作示意图。

图 3 为本发明监控管理模块的执行逻辑示意图。

图 4 为本发明所采用的 Windows 内核文件过滤驱动技术结构图。

图 5 是系统框图

具体实施方式

以下结合附图和具体实施例对本发明做进一步说明：

参见图 1，我们实现的具体执行监控系统由六个模块组成，其中配置审计、监控管理、日志收集、内核通讯、设备插拔监控等五个模块处于应用层，过滤驱动模块则工作在内核层。

由于本实施例是更大的一个监控系统中的一个功能组成部分，配置审计和内核通讯这两个模块并非本发明的必需模块，而是为了使用上的方便、以及设计编

码时的统一化实现，所进行的抽象。

参见图 2，配置审计模块是为了系统与外界联系，如用户界面或远程管理端进行通讯，所提供的统一对外接口，在本实施例中，它用于按照预先定义好的通讯协议与远程的信息采集中心进行通讯，接受信息采集中心的管理与配置，并把本地日志发往信息采集中心保存，在整个系统中，一个信息采集中心可管理多个受监控终端；

内核通讯模块则使用 DeviceIoControl 的方式，在应用层发送 IOCTL 请求给内核驱动程序，驱动程序做相应处理，同时可以通过缓冲区传送数据、获取数据，提供一种通用的应用层与内核层的交互手段。

该监控系统的主要工作流程如下：

1. 参见图 3，监控管理模块负责整个系统的启动与管理模块，由此模块开启两个线程，负责检测即插即用存储设备插拔的设备插拔监控模块线程，以及用于收集外围存储设备使用情况的日志收集模块线程；
2. 监控管理模块通过配置审计模块的对外通讯接口，获得为本主机设置的外围存储设备使用策略，例如：是否对这些设备的读写进行监控；如需监控，那么对读操作和写操作分别采取允许、禁止、记录日志中的哪种动作；是否需要根据文件类型，进行更细粒度的控制，等等，并在获得后调用内核通讯模块设置驱动程序中策略数据；
3. 设备插拔监测模块实时监测即插即用设备的接入，及时通过内核通讯模块进行过滤设备挂接和卸载；
4. 被加载的过滤驱动模块，根据策略等信息进行访问监控，该监控过程的原理及步骤如下：

参见图 4，当操作系统在未加任何访问控制时，文件请求包 IRP 会经过文件系统层（fs，图中所示的例子为 cdfs 和 fat 两种文件系统）、存储设备驱动程序层，而到达硬件设备抽象层（hal: hardware abstraction level），最后实际在存储设备硬件上执行操作。

在文件系统层，根据不同的文件系统，如 cdfs，fat 等，它们为存储设备的每一个逻辑分区创建一个卷设备对象（vdo: volume device object），用 vdo 代表硬件盘上的卷，操作系统对文件的操作，都通过控制其所在卷对应的 vdo，以达到控制底层设备的目的。在文件系统层之下，IRP 请求通过各种存储设备驱动程序、总线驱动程序等，到达具体存储设备进行执行。

根据 windows 文件系统的结构，我们可以在文件系统层之上插入一个文件过滤驱动层，引入一个检查点。在文件过滤驱动层，可以为每一个 vdo 创建一个对应的过滤设备对象（fdo: filter device object），将其挂接到 vdo 之上之后，IRP 就会先经过 fdo 所在的文件过滤驱动程序，再向下传递。因而，我们只要分辨出哪些设备是即插即用设备，并为其挂载对应的 fdo，就可以对即插即用存储设备

进行访问控制了。

文件过滤驱动模块作为 I/O 子系统的一部分运行在内核。它的主要任务是设备读写访问监控，设备使用及留出信息流日志。在驱动程序 DriverEntry 例程中为通过驱动程序的 I/O 请求包 IRP 制定处理例程如下：

```
DriverObject→MajorFunction[IRP_MJ_CRETE]=
        MyFilterCreate;
DriverObject→MajorFunction[IRP_MJ_READ]=
        MyFilterRead;
DriverObject→MajorFunction[IRP_MJ_WRITE]=
        MyFilterWrite;
        ……
```

这样便可以在设置的例程中对相应的 IRP 包进行处理。根据设置的驱动策略，I/O 请求包 IRP 经过过滤驱动程序时，检查请求包以实现对特定资源的访问监控。对类型为 IRP_MJ_CREATE 的请求包（在 MyFilterCreate 例程中），检查要操作的类型（读、写等），与访问的信息体的相关属性是否符合策略，决定对 IRP 的处理：允许、禁止、还是记录详细的访问日志。其中，对资源信息体的保护可以专门部署信息资源数据库，设置相关访问属性，根据 IRP 所指向对象查找数据库中相关项的设置，以决定对其的控制。另外，可以将文件过滤驱动容易扩展到整个系统存储设备，通过文件过滤驱动程序，可以对重要系统资源在文件属性中设置访问属性的标识，以作为处理 I/O 请求包的依据。

5. 记录外围设备访问信息日志，根据策略记录下审计所需的针对外围存储设备的相关操作信息，将日志暂时保存在内核中，由内核通讯模块轮询获取并交给日志收集模块，由日志收集模块将日志及流出文件进行本地留存，或发送到远程服务器存入数据库，以供管理员检查本主机外围设备使用状况。

在本系统中，提供了更细粒度的设备访问控制，不只是简单的在 I/O 路径上对用户 I/O 操作作相应处理，且要根据获得的使用信息，整理选择出有用的操作日志，访问文件信息，以提供外围存储设备使用状况视图和事后分析审计的信息依据。操作审计模块过滤出从过滤驱动中获取的外围存储设备有用操作数据，分析并整理过滤后的信息，参照外围存储设备使用策略，生成各种违反策略操作的安全报警日志发送给网络管理员。另外根据需要留存一些用户访问流出的文件信息，以作为事后分析与检查是否信息泄露的依据。

图 5 在系统工作图中，在主机平台上对即插即用存储设备中的文件读写访问进行控制，在主流桌面系统 windows 平台下，使用文件过滤驱动技术实现即插即用存储设备读写访问控制。系统分应用层与内核层，在应用层实时检测可移动存储设备的插拔，及时通知内核模块挂接过滤设备进行监控，文件过滤驱动根据策略对文件访问操作进行监控处理，并提供监控日志供后续分析。

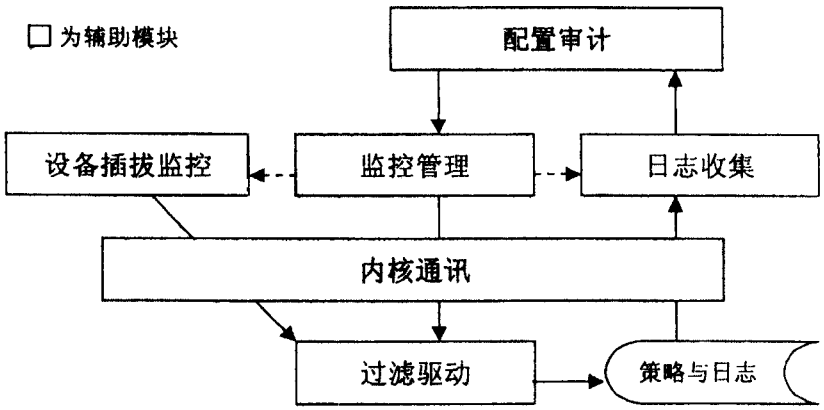

为辅助模块
配置审计
设备插拔监控
监控管理
日志收集
内核通讯
过滤驱动
策略与日志

图 1

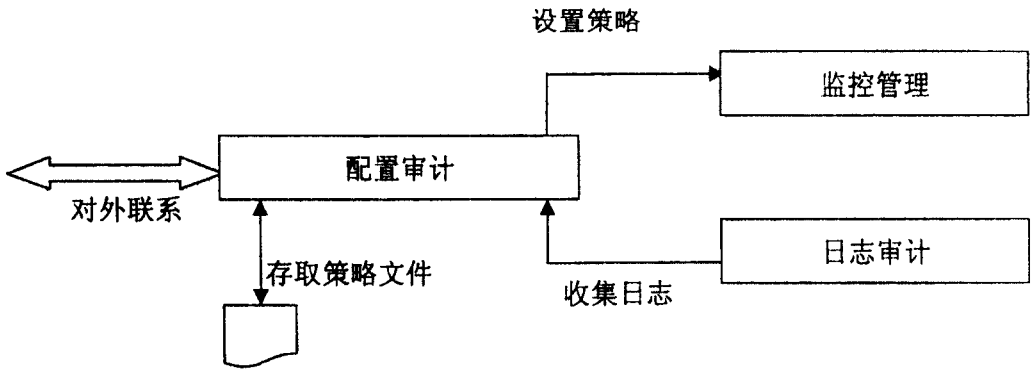

设置策略
监控管理
配置审计
对外联系
存取策略文件
日志审计
收集日志

图 2

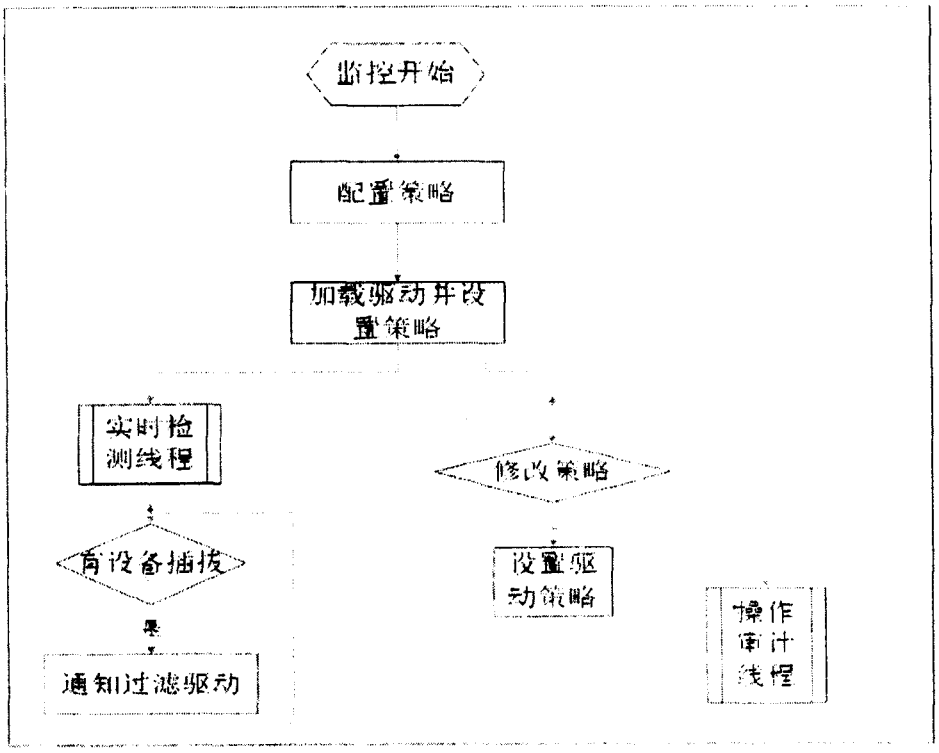

监控开始
配置策略
加载驱动并设置策略
实时检测线程
有设备插拔
是
通知过滤驱动
修改策略
设置驱动策略
操作审计线程

图 3

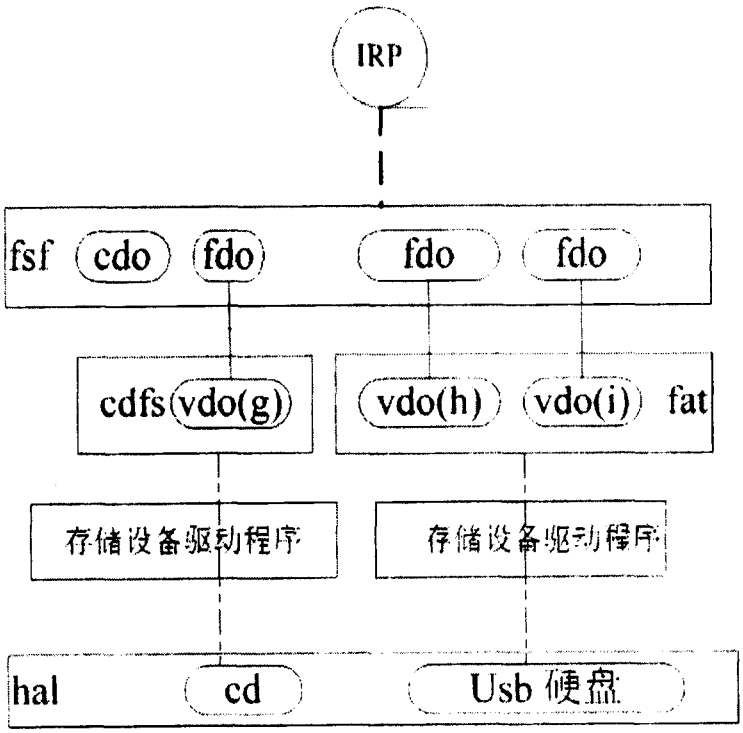

IRP
fsf
cdo
fdo
fdo
fdo
cdfs
vdo(g)
vdo(h)
vdo(i)
fat
存储设备驱动程序
存储设备驱动程序
hal
cd
Usb 硬盘

图 4

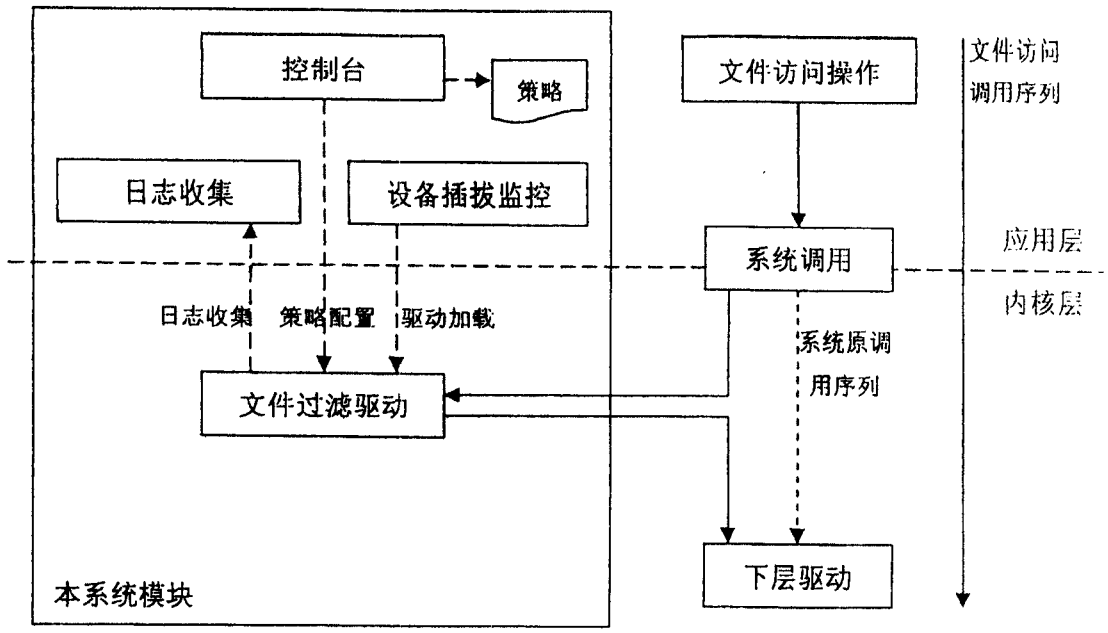

控制台
策略
日志收集
设备插拔监控
日志收集
策略配置
驱动加载
文件过滤驱动
本系统模块
文件访问操作
文件访问
调用序列
系统调用
应用层
内核层
系统原调
用序列
下层驱动

图 5