(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 104573499 A
(43)申请公布日 2015.04.29

(21)申请号 201410457614.2

(22)申请日 2014.09.10

(71)申请人 中电科技（北京）有限公司
地址 100083 北京市海淀区卧虎桥甲 6 号工作区（南）太极大厦 13 层北侧

(72)发明人 陈小春 孙亮 张超 朱立森

(51)Int.Cl.
G06F 21/52(2013.01)

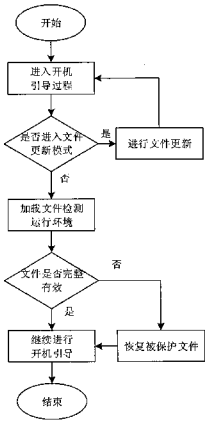
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种基于UEFI的可执行程序文件保护系统和方法

(57)摘要

本发明公开了一种基于UEFI的可执行程序文件保护系统和方法，属于计算机安全技术领域。系统包括文件守护程序驱动模块和文件守护服务端。文件守护程序驱动模块的作用是在开机过程中，对操作系统中的特定文件进行完整性度量和恢复；文件守护服务端的主要作用是提供被保护文件的分发，将被保护文件推送到客户端，由客户端进行文件保护；文件保护系统还可以对被保护文件或文件保护程序驱动程序进行更新，UEFI固件对操作系统中可执行程序文件进行可信度量、可信恢复为基础，能够在开机引导过程中，对操作系统中的文件进行完整性度量，并在发现文件异常时可以进行恢复。本发明可以应用于软件厂商、整机厂商或设备厂商对关键程序的文件进行保护。



CN 104573499 A

1. 一种基于 UEFI 的可执行程序文件保护系统，其特征在于，包括文件守护程序驱动模块和文件守护服务端；

所述文件守护程序驱动模块的作用是在开机过程中，对操作系统中的特定文件进行完整性度量和恢复；文件守护驱动模块是符合 UEFI 规范的固件模块，包括环境加载和安装器子模块、文件检测器子模块和被保护文件，其中，环境加载和安装器子模块是在开机过程中加载相应的驱动，建立文件检测器子模块的运行环境；文件检测器子模块的作用是在操作系统启动时，对计算设备的硬盘或 Flash 存储空间中的特定文件进行检测，如果发现文件被篡改或删除，将释放储存在固件中的被保护文件到硬盘或 Flash 中；

所述文件守护服务端的作用是提供被保护文件的分发，将被保护文件推送到客户端，由客户端进行文件保护；文件保护系统还可以对被保护文件或文件保护程序驱动程序进行更新，更新的方式包括用网络或外部存储设备；文件保护系统的服务端通过网络，将新的被保护文件发送到客户端设备，更新被保护文件。

2. 一种基于 UEFI 的可执行程序文件保护方法，其特征在于，实现步骤如下：

步骤一、计算设备开机上电后，开始进入 UEFI 的开机引导过程；

步骤二、检测是否进入更新模式；如果未进入更新模式，进入步骤三，反之，将在固件层对被保护文件进行更新；

步骤三、在固件层加载硬件驱动，在固件层加载文件系统，识别硬盘及相应的分区及文件系统；通过环境加载安装子模块加载文件度量检测子模块的运行环境；

步骤四、文件度量检测子模块检测硬盘的特定文件是否完整；如果文件正常，则转入步骤五，反之，恢复被保护文件，将被保护文件释放到硬盘的特定位置；

步骤五、文件保护过程结束，固件层将继续进行开机引导过程。

3. 如权利要求 2 所述的基于 UEFI 的可执行程序文件保护方法，其特征在于，在所述步骤二中，将检测是否要进行文件更新；包括以下步骤，

步骤 1、进入固件层开机引导过程；

步骤 2、检测当前开机引导过程是否需要进入固件文件更新模式；如果需要进入更新模式则转入步骤 3，如果不需要更新，则继续进行开机引导过程；

步骤 3、检测当前的更新方式是否是通过网络进行更新；如果需要网络更新则进入步骤 4；检测是否有接入本地的存储设备，且存储设备有需要更新的被保护文件；如果有需要更新的被保护文件，则从外部存储设备中读取需要更新的文件及配置文件，转入步骤 5；

步骤 4、向文件保护系统服务端发送下载请求，希望能够下载相应的被保护文件，及配置文件；在配置文件中将包含了该文件的名称、安装路径等配置信息；

步骤 5、根据配置文件，对存储被保护文件的固件部分进行更新；

步骤 6、重启，进入开机引导过程；固件更新过程结束。

4. 如权利要求 2 所述的基于 UEFI 的可执行程序文件保护方法，其特征在于，在所述步骤四中，将在固件层对操作系统中的文件进行完整性度量；当文件异常时，将进行文件恢复，包括以下步骤：

步骤 1、检测硬盘是否存在；若不存在，则流程结束；

步骤 2、在固件层加载读取硬盘或 Flash 等存储空间的驱动模块；

步骤 3、识别硬盘的相应分区；

步骤 4、对每个分区进行检测，查看分区的文件系统；

步骤 5、针对不同的文件系统，加载相应的驱动模块；

步骤 6、读取被保护文件的配置文件；

步骤 7、在识别分区的文件系统后，将会根据配置文件，检测相应路径的文件是否存在；如果文件存在，则转入步骤 8；若文件不存在，则根据配置文件，将固件中保存的被保护文件写到硬盘的分区上；

步骤 8、对文件进行完整性度量；

步骤 9、根据检测结果判断文件是否完整，是否被篡改；如果未发现文件异常，转入步骤 10；若文件不存在，则根据配置文件，将固件中保存的被保护文件写到硬盘的分区上；

步骤 10、继续进行开机引导流程。

一种基于 UEFI 的可执行程序文件保护系统和方法

技术领域

[0001] 本发明属于计算机安全领域，具体涉及一种基于 UEFI 固件，在开机过程中，对计算机设备操作系统内的文件，特别是可执行程序的文件进行保护的方法。

背景技术

[0002] 目前，在计算机安全领域，操作系统中的文件主要通过特定的软件方法进行保护，如在本地硬盘建立文件保护分区，或操作系统层的文件加密等。或将文件备份到外部存储设备，需要使用时进行恢复。也有建立互补备份区，相互检查彼此分区文件是否完整，如果不完整，将会对文件进行同步。

[0003] 在操作系统层对文件进行保护，特别是对关键可执行程序的文件进行保护，有着以下的不足，主要包括：

[0004] (1) 在计算设备更换硬盘、Flash 等存储被保护程序的装置后，将不能自动地重新恢复被保护文件，特别是关键可执行程序的文件。

[0005] (2) 在对硬盘、Flash 等被保护程序的存储空间进行重新分区后，计算设备将不能自动地恢复被保护文件，特别是关键可执行程序的文件。

[0006] (3) 在对硬盘、Flash 等被保护程序的存储空间进行格式化后，计算设备将不能自动地重新恢复被保护文件，特别是关键可执行程序的文件。

[0007] (4) 当被保护可执行程序文件不属于操作系统自带软件的情况下，在计算设备重新安装操作系统后，将不能自动地重新恢复被保护程序文件。

[0008] (5) 不能阻止合法的终端使用用户非法地删除本地终端上的关键文件。

[0009] (6) 当终端的操作系统中的特定软件文件被病毒或木马篡改和删除后，将不能自动地进行恢复。

[0010] (7) 不能在操作系统启动前，确定操作系统中特定的关键文件，特别是可执行程序文件是否存在。

发明内容

[0011] 本发明的目的是为了克服已有技术的缺陷，提出一种基于 UEFI 的可执行程序文件保护系统和方法，能解决在更换硬盘、Flash 等存储空间的情况下，在开机过程中，无法恢复被保护文件、特别是关键程序文件的问题。

[0012] 一种基于 UEFI 的可执行程序文件保护系统，系统包括文件守护程序驱动模块和文件守护服务端。

[0013] 所述文件守护程序驱动模块的作用是在开机过程中，对操作系统中的特定文件进行完整性度量和恢复；文件守护驱动模块是符合 UEFI 规范的固件模块，包括环境加载和安装器子模块、文件检测器子模块和被保护文件。其中，环境加载和安装器子模块是在开机过程中加载相应的驱动，建立文件检测器子模块的运行环境；文件检测器子模块的作用是在操作系统启动时，对计算设备的硬盘或 Flash 等存储空间中的特定文件进行检测，如果发

现文件被篡改或删除，将释放储存在固件中的被保护文件到硬盘或 Flash 中。

[0014] 所述文件守护服务端的作用是提供被保护文件的分发，将被保护文件推送到客户端，由客户端进行文件保护；文件保护系统还可以对被保护文件或文件保护程序驱动程序进行更新，更新的方式包括用网络或外部存储设备（如 U 盘、CD-ROM）。文件保护系统的服务端可以通过网络，将新的被保护文件发送到客户端设备，更新被保护文件。

[0015] 一种基于 UEFI 的可执行程序文件保护方法，其实现步骤如下：

[0016] 步骤一、计算设备开机上电后，开始进入 UEFI 的开机引导过程；

[0017] 步骤二、检测是否进入更新模式；如果未进入更新模式，进入步骤三，反之，将在固件层对被保护文件进行更新；

[0018] 步骤三、在固件层加载硬件驱动，在固件层加载文件系统，识别硬盘及相应的分区及文件系统；通过环境加载安装子模块加载文件度量检测子模块的运行环境；

[0019] 步骤四、文件度量检测子模块检测硬盘的特定文件是否完整；如果文件正常，则转入步骤五，反之，恢复被保护文件，将被保护文件释放到硬盘的特定位置；

[0020] 步骤五、文件保护过程结束，固件层将继续进行开机引导过程。

[0021] 在所述步骤二中，将检测是否要进行文件更新；包括以下步骤；

[0022] 步骤 1、进入固件层开机引导过程；

[0023] 步骤 2、检测当前开机引导过程是否需要进入固件文件更新模式；如果需要进入更新模式则转入步骤 3，如果不需要更新，则继续进行开机引导过程；

[0024] 步骤 3、检测当前的更新方式是否是通过网络进行更新；如果需要网络更新则进入步骤 4；检测是否有接入本地的存储设备，且存储设备有需要更新的被保护文件；如果有需要更新的被保护文件，则从外部存储设备中读取需要更新的文件及配置文件，转入步骤 5；

[0025] 步骤 4、向文件保护系统服务端发送下载请求，希望能够下载相应的被保护文件，及配置文件；在配置文件中将包含了该文件的名称、安装路径等配置信息；

[0026] 步骤 5、根据配置文件，对存储被保护文件的固件部分进行更新；

[0027] 步骤 6、重启，进入开机引导过程；固件更新过程结束。

[0028] 在步骤四中，将在固件层对操作系统中的文件进行完整性度量；当文件异常时，将进行文件恢复，包括以下步骤：

[0029] 步骤 1、检测硬盘是否存在；若不存在，则流程结束；

[0030] 步骤 2、在固件层加载读取硬盘或 Flash 等存储空间的驱动模块；

[0031] 步骤 3、识别硬盘的相应分区；

[0032] 步骤 4、对每个分区进行检测，查看分区的文件系统；

[0033] 步骤 5、针对不同的文件系统，加载相应的驱动模块；

[0034] 步骤 6、读取被保护文件的配置文件；

[0035] 步骤 7、在识别分区的文件系统后，将会根据配置文件，检测相应路径的文件是否存在；如果文件存在，则转入步骤 8；若文件不存在，则根据配置文件，将固件中保存的被保护文件写到硬盘的分区上；

[0036] 步骤 8、对文件进行完整性度量；

[0037] 步骤 9、根据检测结果判断文件是否完整，是否被篡改；如果未发现文件异常，转

入步骤 10；若文件不存在，则根据配置文件，将固件中保存的被保护文件写到硬盘的分区上；

[0038] 步骤 10、继续进行开机引导流程。

[0039] 有益效果：

[0040] (1) 在计算设备更换硬盘、Flash 等存储被保护程序的装置后，能够自动地重新恢复被保护文件，特别是关键可执行程序的文件。

[0041] (2) 在对硬盘、Flash 等被保护程序的存储空间进行重新分区后，计算设备将能够自动地恢复被保护文件，特别是关键可执行程序的文件。

[0042] (3) 在对硬盘、Flash 等被保护程序的存储空间进行格式化后，计算设备将能够自动地重新恢复被保护文件，特别是关键可执行程序的文件。

[0043] (4) 在计算设备重新安装操作系统后，能够自动地重新恢复被保护程序文件。

[0044] (5) 终端用户删除本地终端上的被保护文件后，将会在开机过程中重新恢复被保护文件。

[0045] (6) 当终端的操作系统中的特定软件文件被病毒或木马篡改和删除后，能够自动地进行恢复。

[0046] (7) 在操作系统启动前，能够确定操作系统中特定的关键文件，特别是可执行程序文件存在，且文件正常。

附图说明

[0047] 图 1 为基于 UEFI 的文件保护总体框架图。

[0048] 图 2 为文件安全守护平台驱动模块框架图。

[0049] 图 3 为固件层安装和检测文件流程图。

[0050] 图 4 为被保护文件更新流程图。

[0051] 图 5 开机引导过程恢复文件流程图

具体实施方式

[0052] 下面结合附图并举实施例，对本发明进行详细描述。

[0053] 如附图 1 所示，本发明的一种基于 UEFI 的可执行程序文件保护系统包括文件守护程序驱动模块和文件守护服务端。

[0054] 所述文件守护程序驱动模块的作用是在开机过程中，对操作系统中的特定文件进行完整性度量和恢复；文件守护驱动模块是符合 UEFI 规范的固件模块，包括环境加载和安装器子模块、文件检测器子模块和被保护文件。其中，环境加载和安装器子模块是在开机过程中加载相应的驱动，建立文件检测器子模块的运行环境；文件检测器子模块的作用是在操作系统启动时，对计算设备的硬盘或 Flash 等存储空间中的特定文件进行检测，如果发现文件被篡改或删除，将释放储存在固件中的被保护文件到硬盘或 Flash 中，如图 2 所示。

[0055] 所述文件守护服务端的作用是提供被保护文件的分发，将被保护文件推送到客户端，由客户端进行文件保护；文件保护系统还可以对被保护文件或文件保护程序驱动程序进行更新，更新的方式包括用网络或外部存储设备（如 U 盘、CD-ROM）。文件保护系统的服务端可以通过网络，将新的被保护文件发送到客户端设备，更新被保护文件。

[0056] 本发明在应用前，需要在计算机终端先行部署，可以选用的方法包括：

[0057] a) 在 UEFI 核心镜像中添加驱动模块。

[0058] b) 在 UEFI 核心镜像中挂载 Option ROM 模块。

[0059] c) 在可信卡等其他外围设备中挂载驱动模块。

[0060] 一种基于 UEFI 的可执行程序文件保护方法，包括以下步骤：

[0061] 步骤一、计算设备开机上电后，开始进入 UEFI 的开机引导过程。

[0062] 步骤二、检测是否进入更新模式。如果未进入更新模式，进入步骤三，反之，将在固件层对被保护文件进行更新。如果需要进入网络更新模式则向文件保护系统服务端发送下载请求，希望能够下载并更新相应的被保护文件，及配置文件。在配置文件中将包含了该文件的名称、安装路径等配置信息。

[0063] 步骤三、在固件层加载硬件驱动，在固件层加载文件系统，识别硬盘及相应的分区及文件系统。通过环境加载安装子模块加载文件度量检测子模块的运行环境。

[0064] 步骤四、文件度量检测子模块根据配置文件，检测相应路径的文件是否存在，文件是否完整，是否被篡改。如果文件正常，则转入步骤五，反之，如果发现文件异常，将固件中保存的被保护文件写到硬盘的分区上。恢复被保护文件，将被保护文件释放到硬盘的特定位置。

[0065] 步骤五、文件保护过程结束，固件层将继续进行开机引导过程。

[0066] 在所述步骤二中，将检测是否要进行文件更新；包括以下步骤，如图 4 所示；

[0067] 步骤 1、进入固件层开机引导过程；

[0068] 步骤 2、检测当前开机引导过程是否需要进入固件文件更新模式；如果需要进入更新模式则转入步骤 3，如果不需要更新，则继续进行开机引导过程；

[0069] 步骤 3、检测当前的更新方式是否是通过网络进行更新；如果需要网络更新则进入步骤 4；检测是否有接入本地的存储设备，且存储设备有需要更新的被保护文件；如果有需要更新的被保护文件，则从外部存储设备中读取需要更新的文件及配置文件，转入步骤 5；

[0070] 步骤 4、向文件保护系统服务端发送下载请求，希望能够下载相应的被保护文件，及配置文件；在配置文件中将包含了该文件的名称、安装路径等配置信息；

[0071] 步骤 5、根据配置文件，对存储被保护文件的固件部分进行更新；

[0072] 步骤 6、重启，进入开机引导过程；固件更新过程结束。

[0073] 在步骤四中，将在固件层对操作系统中的文件进行完整性度量；当文件异常时，将进行文件恢复，包括以下步骤：

[0074] 步骤 1、检测硬盘是否存在；若不存在，则流程结束；

[0075] 步骤 2、在固件层加载读取硬盘或 Flash 等存储空间的驱动模块；

[0076] 步骤 3、识别硬盘的相应分区；

[0077] 步骤 4、对每个分区进行检测，查看分区的文件系统；

[0078] 步骤 5、针对不同的文件系统，加载相应的驱动模块；

[0079] 步骤 6、读取被保护文件的配置文件；

[0080] 步骤 7、在识别分区的文件系统后，将会根据配置文件，检测相应路径的文件是否存在；如果文件存在，则转入步骤 8；若文件不存在，则根据配置文件，将固件中保存的被保

护文件写到硬盘的分区上；

[0081] 步骤 8、对文件进行完整性度量；

[0082] 步骤 9、根据检测结果判断文件是否完整，是否被篡改；如果未发现文件异常，转入步骤 10；若文件不存在，则根据配置文件，将固件中保存的被保护文件写到硬盘的分区上；

[0083] 步骤 10、继续进行开机引导流程，如附图 5 所示。

[0084] 综上所述，以上仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

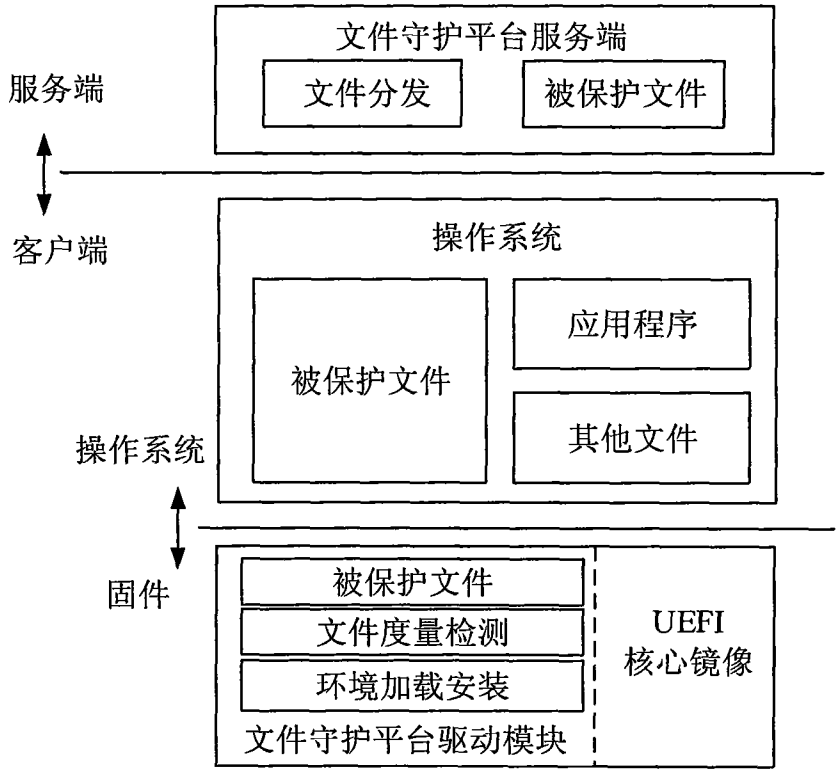

文件守护平台服务端
文件分发
被保护文件
服务端
客户端
操作系统
被保护文件
应用程序
其他文件
操作系统
固件
被保护文件
文件度量检测
环境加载安装
文件守护平台驱动模块
UEFI
核心镜像

图 1

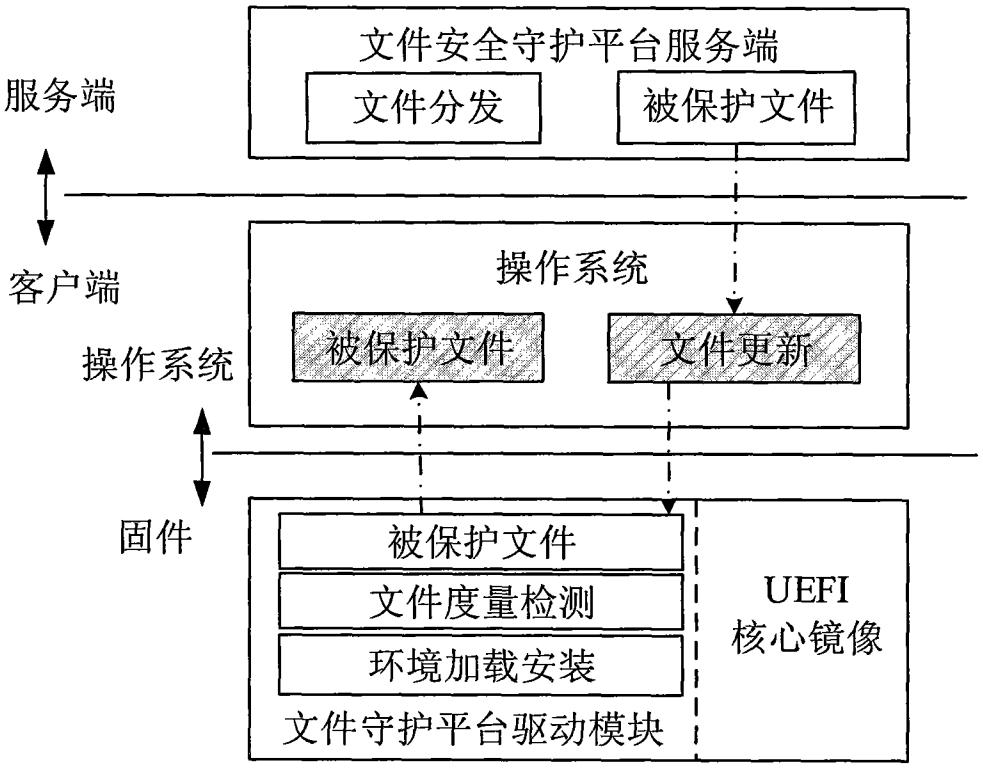

文件安全守护平台服务端
文件分发
被保护文件
服务端
客户端
操作系统
被保护文件
文件更新
操作系统
固件
被保护文件
文件度量检测
环境加载安装
文件守护平台驱动模块
UEFI
核心镜像

图 2

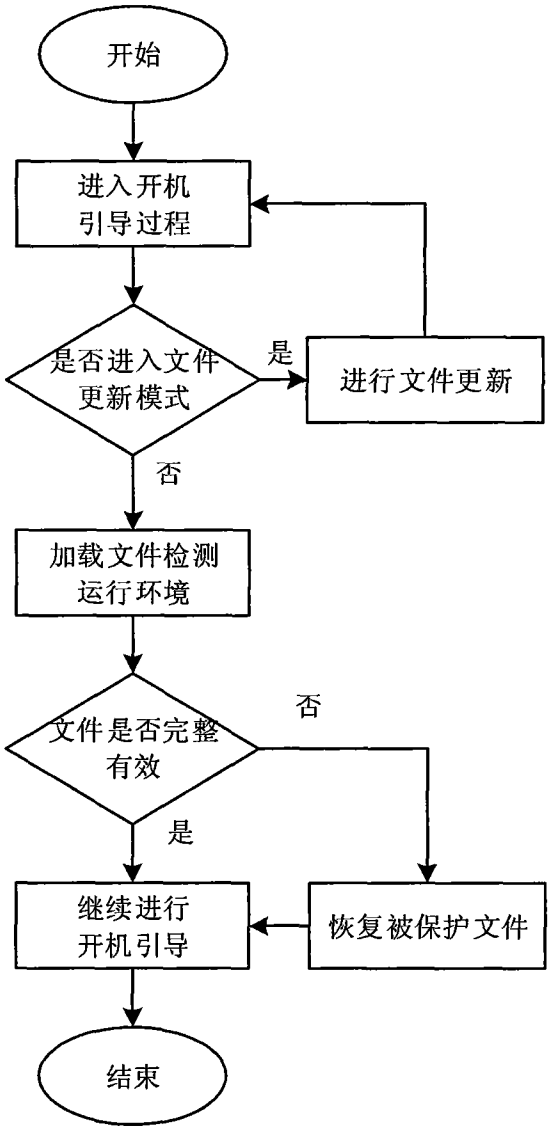

开始
进入开机
引导过程
是否进入文件
更新模式
是
进行文件更新
否
加载文件检测
运行环境
文件是否完整
有效
否
是
继续进行
开机引导
恢复被保护文件
结束

图 3

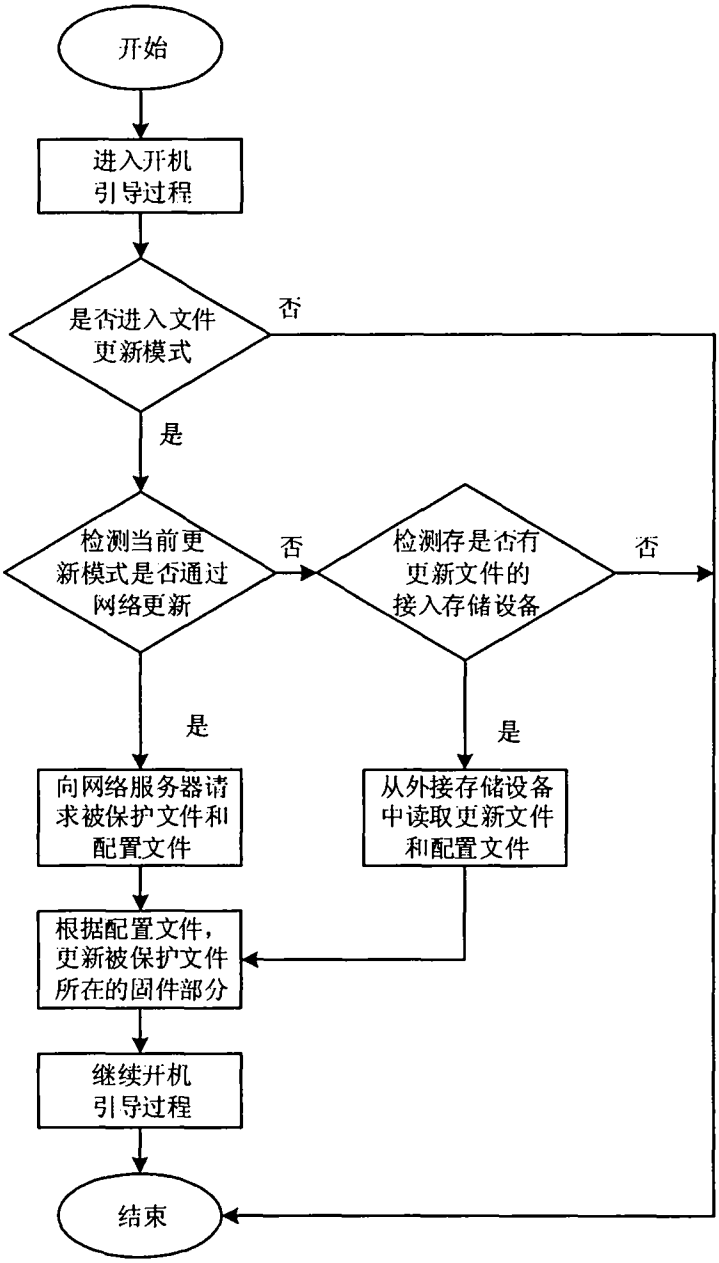

开始
进入开机引导过程
是否进入文件更新模式
否
是
检测当前更新模式是否通过网络更新
否
检测存是否有更新文件的接入存储设备
否
是
是
向网络服务器请求被保护文件和配置文件
从外接存储设备中读取更新文件和配置文件
根据配置文件，更新被保护文件所在的固件部分
继续开机引导过程
结束

图 4

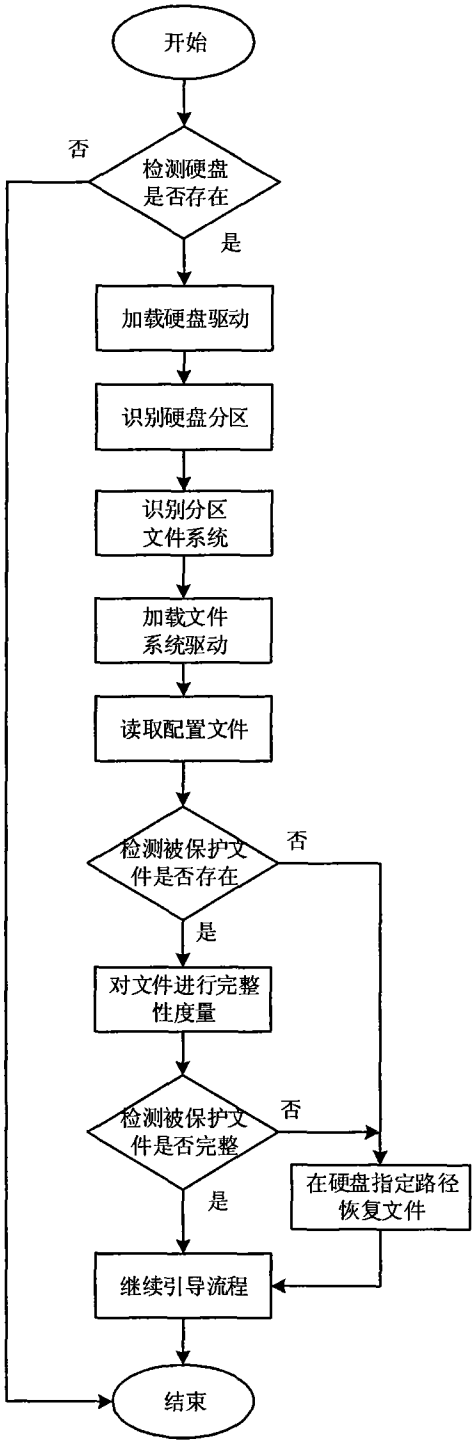

开始
否
检测硬盘是否存在
是
加载硬盘驱动
识别硬盘分区
识别分区文件系统
加载文件系统驱动
读取配置文件
检测被保护文件是否存在
否
是
对文件进行完整性度量
检测被保护文件是否完整
否
是
在硬盘指定路径恢复文件
继续引导流程
结束

图 5