(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 104573491 A
(43)申请公布日 2015.04.29

(21)申请号 201410457570.3

(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 21/51(2013.01)
G06F 21/52(2013.01)
G06F 21/56(2013.01)
H04L 29/08(2006.01)

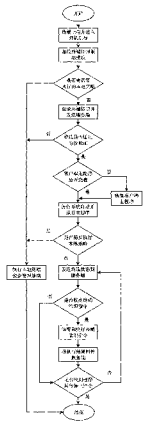
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于UEFI的终端管理系统和方法

(57)摘要

本发明公开了一种基于UEFI的终端管理系统和方法，属于计算机安全技术领域。系统包括终端管理驱动模块、终端管理客户端主程序和终端管理服务端；终端管理驱动模块能够在开机过程中生成终端标识，并将终端发送到服务端进行身份验证，能够执行在本地终端或通过网络接收的终端安全保护策略；终端管理客户端主程序通过接口与终端管理驱动模块实现实时的守护，能够保证客户端主程序的正确运行；终端管理系统服务端提供终端信息管理服务、终端策略管理服务和网络通信服务，能够对通过网络发送终端管理指令和软件更新。本发明能解决在更换硬盘、重新分区时，无法自动恢复终端管理客户端的问题。



CN 104573491 A

1. 一种基于固件的终端管理系统，其特征在于，所述系统包括终端管理驱动模块、终端管理客户端主程序和终端管理服务端；

所述终端管理驱动模块是符合 UEFI 规范的，驻守在固件层的驱动程序；该驱动模块能够在开机过程中生成终端标识，并将终端发送到服务端进行身份验证，能够执行在本地终端或通过网络接收的终端安全保护策略；同时，终端管理驱动模块可以执行对终端管理客户端主程序的实时守护，包括在开机阶段和操作系统运行阶段；当终端管理客户端主程序的程序文件被篡改或删除时，终端管理驱动模块可以执行对终端管理客户端主程序的自动恢复；

所述终端管理客户端主程序运行于操作系统中，通过接口与终端管理驱动模块实现实时的守护，能够保证客户端主程序的正确运行；终端管理客户端主程序包括指令解析子模块、指令执行子模块、通信接口子模块、加 / 解密子模块；其中，通信接口子模块用于完成终端管理指令的交互功能；加 / 解密子模块用于完成对传输信息加 / 解密；指令解析子模块用于识别服务器传输指令或本地保存的策略；指令执行子模块用于执行指令解析子模块识别的终端管理指令；

终端管理系统服务端提供终端信息管理服务、终端策略管理服务和网络通信服务，能够对通过网络发送终端管理指令和软件更新。

2. 一种基于固件的终端管理系统的实现方法，其特征在于，其实现步骤如下：

步骤一、开机上电后，在 UEFI 引导阶段中，加载相应的驱动；

步骤二、加载终端管理驱动模块；

步骤三、终端管理驱动模块检测是否有需要执行的本地策略；如果有则执行本地终端安全管理策略，该流程结束；否则，转入步骤四；

步骤四、终端管理驱动模块生成终端标识，并发送到服务端；

步骤五、检测是否该终端通过了身份验证；如果未通过身份认证，则执行本地终端安全管理策略，该流程结束；如果通过身份认证，则转入步骤六；

步骤六、终端管理驱动模块对硬盘中的终端管理客户端主程序文件进行检测，查看是否被篡改和删除，如果文件异常则进行恢复；

步骤七、操作系统启动后，终端管理客户端主程序随操作系统自启动；

步骤八、终端管理客户端主程序检测是否需要执行本地策略；如果需要，则执行本地安全管理策略；否则，转入步骤九；

步骤九、终端管理主程序将终端状态发送到服务端；

步骤十、终端管理客户端主程序与终端管理服务端进行通信，检测是否需要对终端进行控制；如果需要则转入步骤十一，否则转入步骤十四；

步骤十一、终端管理客户端主程序从服务器端下载相应的终端管理控制指令并进行解析；

步骤十二、终端管理客户端主程序执行终端管理控制指令；

步骤十三、终端管理客户端主程序将执行结果回传到服务端；

步骤十四、检测是否收到终端管理客户端主程序停止运行指令，如果收到，则终端管理流程结束，否则，转入步骤九。

一种基于 UEFI 的终端管理系统和方法

技术领域

[0001] 本发明属于计算机安全技术领域，涉及一种基于 UEFI 固件，在开机引导过程和操作系统运行的过程中，通过固件层对计算机终端进行管理的方法。

背景技术

[0002] 目前，在计算机安全领域，对计算机终端进行管理的方法主要是通过在操作系统中运行的终端管理程序执行既定策略实现对终端的管理。终端可以执行存储在本地的策略，可以执行通过网络传输的管理策略。

[0003] 通过在操作系统中运行的终端管理程序执行对终端的管理有着以下的不足，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，将不能自动地重新安装和恢复终端管理程序。

[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重新安装和恢复终端管理程序。

[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安装和恢复终端管理程序。

[0007] (4) 当被保护软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，将不能自动地重新安装和恢复终端管理程序。

[0008] (5) 不能阻止合法的终端使用用户非法地卸载本终端上运行的终端管理程序。

[0009] (6) 当终端的操作系统中的终端管理程序被病毒或木马篡改和删除后，将不能合法地启动和运行。

[0010] (7) 不能在操作系统启动前，确定终端管理程序文件是否存在。如果该程序文件不存在，则终端将无法通过终端管理程序进行管理和保护。

[0011] (8) 不能够在操作系统启动前，对终端进行身份验证。

发明内容

[0012] 本发明的目的是为了克服已有技术的缺陷，为了解决在更换硬盘、重新分区时，无法自动恢复终端管理客户端的问题，提出一种基于固件的终端管理系统和方法。

[0013] 一种基于 UEFI 的终端管理系统，所述系统包括终端管理驱动模块、终端管理客户端主程序和终端管理服务端；

[0014] 所述终端管理驱动模块是符合 UEFI 规范的，驻守在固件层的驱动程序；该驱动模块能够在开机过程中生成终端标识，并将终端发送到服务端进行身份验证，能够执行在本地终端或通过网络接收的终端安全保护策略；同时，终端管理驱动模块可以执行对终端管理客户端主程序的实时守护，包括在开机阶段和操作系统运行阶段；当终端管理客户端主程序的程序文件被篡改或删除时，终端管理驱动模块可以执行对终端管理客户端主程序的自动恢复；

[0015] 所述终端管理客户端主程序运行于操作系统中，通过接口与终端管理驱动模块实现实时的守护，能够保证客户端主程序的正确运行；终端管理客户端主程序包括指令解析子模块、指令执行子模块、通信接口子模块、加/解密子模块；其中，通信接口子模块用于完成终端管理指令的交互功能；加/解密子模块用于完成对传输信息加/解密；指令解析子模块用于识别服务器传输指令或本地保存的策略；指令执行子模块用于执行指令解析子模块识别的终端管理指令；

[0016] 终端管理系统服务端提供终端信息管理服务、终端策略管理服务和网络通信服务，能够对通过网络发送终端管理指令和软件更新。

[0017] 一种基于 UEFI 的终端管理系统的实现方法，其实现步骤如下：

[0018] 步骤一、开机上电后，在 UEFI 引导阶段中，加载相应的驱动；

[0019] 步骤二、加载终端管理驱动模块；

[0020] 步骤三、终端管理驱动模块检测是否有需要执行的本地策略；如果有则执行本地终端安全管理策略，该流程结束；否则，转入步骤四；

[0021] 步骤四、终端管理驱动模块生成终端标识，并发送到服务端；

[0022] 步骤五、检测是否该终端通过了身份验证；如果未通过身份认证，则执行本地终端安全管理策略，该流程结束；如果通过身份认证，则转入步骤六；

[0023] 步骤六、终端管理驱动模块对硬盘中的终端管理客户端主程序文件进行检测，查看是否被篡改和删除，如果文件异常则进行恢复；

[0024] 步骤七、操作系统启动后，终端管理客户端主程序随操作系统自启动；

[0025] 步骤八、终端管理客户端主程序检测是否需要执行本地策略；如果需要，则执行本地安全管理策略；否则，转入步骤九；

[0026] 步骤九、终端管理主程序将终端状态发送到服务端；

[0027] 步骤十、终端管理客户端主程序与终端管理服务端进行通信，检测是否需要对终端进行控制；如果需要则转入步骤十一，否则转入步骤十四；

[0028] 步骤十一、终端管理客户端主程序从服务器端下载相应的终端管理控制指令并进行解析；

[0029] 步骤十二、终端管理客户端主程序执行终端管理控制指令；

[0030] 步骤十三、终端管理客户端主程序将执行结果回传到服务端；

[0031] 步骤十四、检测是否收到终端管理客户端主程序停止运行指令，如果收到，则终端管理流程结束，否则，转入步骤九。

[0032] 有益效果：

[0033] 1、在计算设备更换硬盘、Flash 等存储被保护程序的装置后，能够自动地重新安装和恢复终端管理程序。

[0034] 2、在对硬盘、Flash 等被保护程序的存储空间进行重新分区后，计算设备能够自动地重新安装和恢复终端管理程序。

[0035] 3、在对硬盘、Flash 等被保护程序的存储空间进行格式化后，计算设备能够自动地重新安装和恢复终端管理程序。

[0036] 4、当被保护软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，能够自动地重新安装和恢复终端管理程序。

[0037] 5、能够阻止合法的终端使用用户非法地卸载本终端上运行的终端管理程序。

[0038] 6、当终端的操作系统中的终端管理程序被病毒或木马篡改和删除后，能够合法地启动和运行。

[0039] 7、能够在操作系统启动前，确定终端管理程序文件是否存在。如果该程序文件不存在，则终端将无法通过终端管理程序进行管理和保护。

[0040] 8、能够在操作系统启动前，对终端进行身份验证。

附图说明

[0041] 图 1 为本发明的总体框架结构示意图；

[0042] 图 2 为本发明终端管理驱动模块和客户端主程序流程图。

具体实施方式

[0043] 下面结合附图并举实施例，对本发明进行详细描述。

[0044] 如附图 1 所示，本发明提供了一种基于固件的终端管理系统，所述系统包括终端管理驱动模块、终端管理客户端主程序和终端管理服务端；

[0045] 所述终端管理驱动模块是符合 UEFI 规范的，驻守在固件层的驱动程序；该驱动模块能够在开机过程中生成终端标识，并将终端发送到服务端进行身份验证，能够执行在本地终端或通过网络接收的终端安全保护策略；同时，终端管理驱动模块可以执行对终端管理客户端主程序的实时守护，包括在开机阶段和操作系统运行阶段；当终端管理客户端主程序的程序文件被篡改或删除时，终端管理驱动模块可以执行对终端管理客户端主程序的自动恢复；

[0046] 所述终端管理客户端主程序运行于操作系统中，通过接口与终端管理驱动模块实现实时的守护，能够保证客户端主程序的正确运行；终端管理客户端主程序包括指令解析子模块、指令执行子模块、通信接口子模块、加 / 解密子模块；其中，通信接口子模块用于完成终端管理指令的交互功能；加 / 解密子模块用于完成对传输信息加 / 解密；指令解析子模块用于识别服务器传输指令或本地保存的策略；指令执行子模块用于执行指令解析子模块识别的终端管理指令；

[0047] 终端管理系统服务端提供终端信息管理服务、终端策略管理服务和网络通信服务，能够对通过网络发送终端管理指令和软件更新。

[0048] 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：

[0049] (1) 在 UEFI 核心镜像中添加驱动模块。

[0050] (2) 在 UEFI 核心镜像中挂载 Option ROM 模块。

[0051] (3) 在可信卡等其他外围设备中挂载驱动模块。

[0052] 如附图 2 所示，本发明的一种基于固件的终端管理系统的实现方法，其实现步骤如下：

[0053] 步骤一、开机上电后，在 UEFI 引导阶段中，加载相应的驱动；

[0054] 步骤二、加载终端管理驱动模块；

[0055] 步骤三、终端管理驱动模块检测是否有需要执行的本地策略；如果有则执行本地终端安全管理策略，包括锁定终端、删除文件等，在执行完安全管理流程后，则流程结束。否

则，转入步骤四；

[0056] 步骤四、终端管理驱动模块生成终端标识，并发送到服务端；

[0057] 步骤五、检测是否该终端通过了身份验证；如果未通过身份认证，则执行本地终端安全管理策略，包括锁定终端、删除文件等，在执行完安全管理流程后，则流程结束，如果通过身份认证，则转入步骤六；

[0058] 步骤六、终端管理驱动模块对硬盘中的终端管理客户端主程序文件进行检测，查看是否被篡改和删除，如果文件异常则进行恢复；

[0059] 步骤七、操作系统启动后，终端管理客户端主程序随操作系统自启动；

[0060] 步骤八、终端管理客户端主程序检测是否需要执行本地策略；如果需要，则执行本地安全管理策略；否则，转入步骤九；

[0061] 步骤九、终端管理客户端主程序将终端状态发送到服务端；终端信息包括终端中的软／硬件信息，如当前 CPU、内存、硬盘信息等；

[0062] 步骤十、终端管理客户端主程序与终端管理服务端进行通信，检测是否需要对终端进行控制；如果需要则转入步骤十一，否则转入步骤十四；

[0063] 步骤十一、终端管理客户端主程序从服务器端下载相应的终端管理控制指令并进行解析；控制指令包括锁定终端、删除文件、回传文件、地理追踪等；

[0064] 步骤十二、终端管理客户端主程序执行终端管理控制指令；

[0065] 步骤十三、终端管理客户端主程序将执行结果回传到服务端；

[0066] 步骤十四、检测是否收到终端管理客户端主程序停止运行指令，如果收到，则终端管理流程结束，否则，转入步骤九。

[0067] 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。

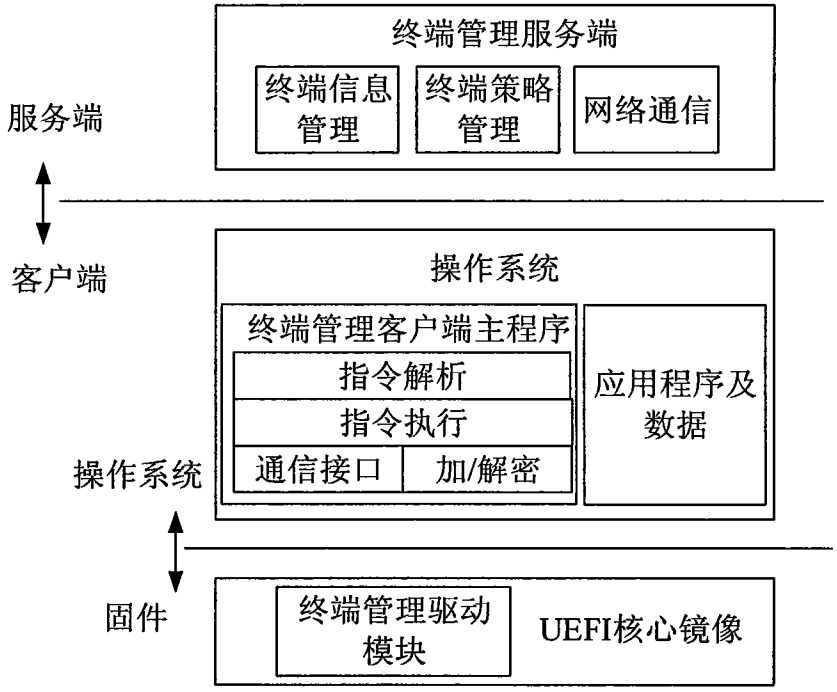

终端管理服务端
终端信息管理
终端策略管理
网络通信
服务端
客户端
操作系统
终端管理客户端主程序
指令解析
指令执行
通信接口
加/解密
应用程序及数据
操作系统
固件
终端管理驱动模块
UEFI核心镜像

图 1

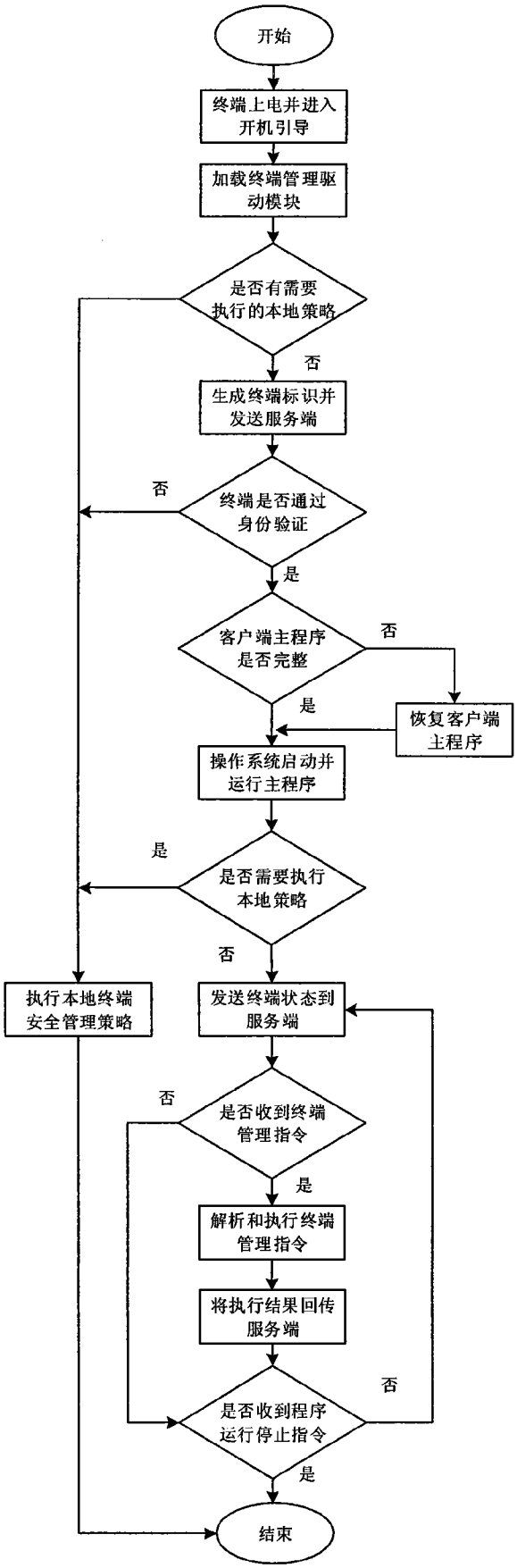

开始
终端上电并进入开机引导
加载终端管理驱动模块
是否有需要执行的本地策略
否
生成终端标识并发送服务端
否
终端是否通过身份验证
是
客户端主程序是否完整
否
是
恢复客户端主程序
操作系统启动并运行主程序
是
是否需要执行本地策略
否
执行本地终端安全管理策略
发送终端状态到服务端
否
是否收到终端管理指令
是
解析和执行终端管理指令
将执行结果回传服务端
否
是否收到程序运行停止指令
是
结束

图 2