(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 104572169 A
(43)申请公布日 2015.04.29

(21)申请号 201410457629.9

(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 9/445(2006.01)

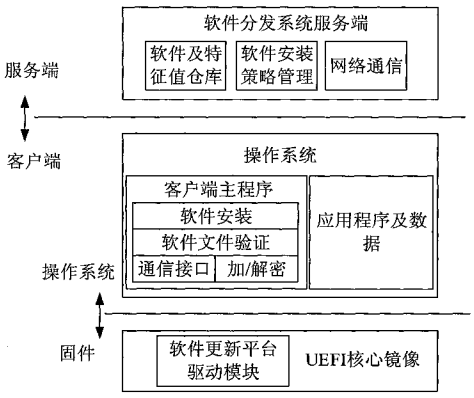
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于UEFI的软件分发和安装系统

(57)摘要

本发明公开了一种基于UEFI的软件分发和安装系统，属于计算机系统技术领域。系统包括系统包括于固件层的软件分发驱动模块、位于操作系统层的软件分发客户端主程序和服务端；软件分发驱动模块能够提供对软件分发客户端主程序的实时保护；软件分发客户端主程序运行于操作系统中，通过接口与UEFI驱动模块实现实时的守护；服务端的作用是提供被软件推送、制定软件安装策略；本发明能够解决在更换硬盘、重新分区时，无法自动进行软件更新的问题。



CN 104572169 A

1. 一种基于 UEFI 的软件分发和安装系统，其特征在于，所述系统包括位于固件层的软件分发驱动模块、位于操作系统层的软件分发客户端主程序和服务端；

所述软件分发驱动模块是符合 UEFI 规范的，驻守在固件层的驱动程序；该驱动程序的能够提供对软件分发客户端主程序的实时保护；当运行于操作系统的客户端主程序文件被篡改或删除时，驱动模块将对客户端主程序进行自动恢复；

所述软件分发客户端主程序运行于操作系统中，通过接口与 UEFI 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；软件分发客户端主程序包括软件安装子模块、软件文件验证子模块、通信接口子模块、加 / 解密子模块；其中，软件安装子模块用于安装服务端分发的软件；软件文件验证子模块用于比对要分发软件的完整性度量值；通信接口子模块用于完成文件下载和上传功能；加 / 解密子模块用于完成对传输信息和文件的加 / 解密；

所述服务端的作用是提供被软件推送、制定软件安装策略；服务端包括软件仓库服务、分发安装策略服务、网络通信服务三个部分；其中，软件仓库服务用于存储需要推送的软件，并可以提供版本管理功能；分发安装策略管理服务用于制定软件分发和安装的策略；网络通信子模块用于提供服务端与客户端主程序建立安全网络连接。

2. 根据权利要求 1 所述一种基于 UEFI 的软件分发和安装系统，其特征在于，其实现的步骤如下：

步骤 1. 开机上电后，在 UEFI 引导阶段中，加载相应的驱动；

步骤 2. 软件分发驱动模块软件被加载后，将在固件层生成终端标识，用于对终端进行身份认证；

步骤 3. 软件分发驱动模块对硬盘中的软件分发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 4. 操作系统启动后，客户端主程序随操作系统自启动；

步骤 5. 客户端主程序与服务端进行通信，检测是否需要对软件进行更新；如果需要更新则转入步骤六，如果不需要更新则流程结束；

步骤 6. 客户端主程序将终端标识发送到服务端进行身份验证；

步骤 7. 检测身份认证信息是否通过；身份验证通过后将转入步骤八；如果未能通过验证，则软件更新流程结束；

步骤 8. 身份验证通过后将接收软件文件完整性度量值；如果未能通过验证，则软件更新流程结束；

步骤 9. 客户端从服务器端下载软件更新文件和软件安装脚本；可以在硬盘或 Flash 等存储空间中，划分一块保护空间用于保存下载的安装文件；

步骤 10. 客户端根据下载的安装脚本，对软件进行自动安装；

步骤 11. 软件安装流程结束。

一种基于 UEFI 的软件分发和安装系统

技术领域

[0001] 本发明涉及计算机系统领域，具体涉及一种基于 UEFI 固件，在操作系统运行的过程中，通过被固件守护的专用程序，进行软件分发和安装的系统。

背景技术

[0002] 目前，在计算机安全领域中，软件的分发和安装的主要方法是在网络中部署软件分发服务器，在终端的操作系统中安装特定的客户端程序。当有软件更新的需要时，由服务端推送软件包到客户端，或收到更新通知的客户端将软件包下载在本地进行安装。

[0003] 通过在终端操作系统中的客户端程序接收软件分发和安装软件有着以下的不足，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软件分发客户端程序。

[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软件分发客户端程序。

[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软件分发客户端程序。

[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软件分发客户端程序。

[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特定软件分发客户端程序。

[0009] (6) 当终端的操作系统中的软件分发客户端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。

发明内容

[0010] 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，无法自动进行软件更新的问题，提出一种基于固件的软件分发和安装方法。

[0011] 一种基于 UEFI 的软件分发和安装系统，系统包括于固件层的软件分发驱动模块、位于操作系统层的软件分发客户端主程序和服务端；

[0012] 所述软件分发驱动模块是符合 UEFI 规范的，驻守在固件层的驱动程序；该驱动程序的能够提供对软件分发客户端主程序的实时保护；当运行于操作系统的客户端主程序文件被篡改或删除时，驱动模块将对客户端主程序进行自动恢复；

[0013] 所述软件分发客户端主程序运行于操作系统中，通过接口与 UEFI 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；软件分发客户端主程序包括软件安装子模块、软件文件验证子模块、通信接口子模块、加 / 解密子模块；其中，软件安装子模块用于安装服务端分发的软件；软件文件验证子模块用于比对要分发软件的完整性度量值；通信接口子模块用于完成文件下载和上传功能；加 / 解密子模块用于完成对传输信息和文件的

加 / 解密 ;

[0014] 所述服务端的作用是提供被软件推送、制定软件安装策略 ;服务端包括软件仓库服务、分发安装策略服务、网络通信服务三个部分 ;其中,软件仓库服务用于存储需要推送的软件,并可以提供版本管理功能 ;分发安装策略管理服务用于制定软件分发和安装的策略,如是否提供软件度量验证、补丁更新等功能 ;网络通信子模块用于提供服务端与客户端主程序建立安全网络连接。

[0015] 本发明实现的步骤如下 :

[0016] 步骤 1. 开机上电后,在 UEFI 引导阶段中,加载相应的驱动 ;

[0017] 步骤 2. 软件分发驱动模块软件被加载后,将在固件层生成终端标识,用于对终端进行身份认证 ;

[0018] 步骤 3. 软件分发驱动模块对硬盘中的软件分发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 ;

[0019] 步骤 4. 操作系统启动后,客户端主程序随操作系统自启动 ;

[0020] 步骤 5. 客户端主程序与服务端进行通信,检测是否需要对软件进行更新 ;如果需要更新则转入步骤六,如果不需要更新则流程结束 ;

[0021] 步骤 6. 客户端主程序将终端标识发送到服务端进行身份验证 ;

[0022] 步骤 7. 检测身份认证信息是否通过 ;身份验证通过后将转入步骤八 ;如果未能通过验证,则软件更新流程结束 ;

[0023] 步骤 8. 身份验证通过后将接收软件文件完整性度量值 ;如果未能通过验证,则软件更新流程结束 ;

[0024] 步骤 9. 客户端从服务器端下载软件更新文件和软件安装脚本 ;可以在硬盘或 Flash 等存储空间中,划分一块保护空间用于保存下载的安装文件 ;

[0025] 步骤 10. 客户端根据下载的安装脚本,对软件进行自动安装 ;

[0026] 步骤 11. 软件安装流程结束。

[0027] 有益效果 :

[0028] (1) 本发明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软件分发客户端程序。

[0029] (2) 本发明在对硬盘、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重新安装和恢复软件分发客户端程序。

[0030] (3) 本发明在对硬盘、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安装和恢复软件分发客户端程序。

[0031] (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软件分发客户端程序。

[0032] (5) 本发明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特定软件分发客户端程序。

[0033] (6) 终端的操作系统中的软件分发客户端程序被病毒或木马篡改和删除后,能够合法地启动和运行。

附图说明

[0034] 图 1 为本发明软件分发和安装系统总体框架图；

[0035] 图 2 为本发明终端软件安装更新流程图。

具体实施方式

[0036] 下面结合附图并举实施例，对本发明进行详细描述。

[0037] 如图 1 所示，本发明的一种基于 UEFI 的软件分发和安装系统，系统包括于固件层的软件分发驱动模块、位于操作系统层的软件分发客户端主程序和服务端；

[0038] 所述软件分发驱动模块是符合 UEFI 规范的，驻守在固件层的驱动程序；该驱动程序的能够提供对软件分发客户端主程序的实时保护；当运行于操作系统的客户端主程序文件被篡改或删除时，驱动模块将对客户端主程序进行自动恢复；

[0039] 所述软件分发客户端主程序运行于操作系统中，通过接口与 UEFI 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；软件分发客户端主程序包括软件安装子模块、软件文件验证子模块、通信接口子模块、加 / 解密子模块；其中，软件安装子模块用于安装服务端分发的软件；软件文件验证子模块用于比对要分发软件的完整性度量值；通信接口子模块用于完成文件下载和上传功能；加 / 解密子模块用于完成对传输信息和文件的加 / 解密；

[0040] 所述服务端的作用是提供被软件推送、制定软件安装策略；服务端包括软件仓库服务、分发安装策略服务、网络通信服务三个部分；其中，软件仓库服务用于存储需要推送的软件，并可以提供版本管理功能；分发安装策略管理服务用于制定软件分发和安装的策略，如是否提供软件度量验证、补丁更新等功能；网络通信子模块用于提供服务端与客户端主程序建立安全网络连接。

[0041] 如附图 2 所示，本发明实现的步骤如下：

[0042] 步骤一、开机上电后，在 UEFI 引导阶段中，加载相应的驱动。

[0043] 步骤二、软件分发驱动模块软件被加载后，将在固件层生成终端标识，用于对终端进行身份认证。

[0044] 步骤三、软件分发驱动模块对硬盘中指定分区和路径的软件分发客户端主程序文件进行检测，查看是否被篡改和删除，如果文件异常则从固件层对软件文件进行恢复。

[0045] 步骤四、操作系统启动后，客户端主程序随操作系统自启动。

[0046] 步骤五、客户端主程序与服务端进行通信，检测是否需要对软件进行更新。如果需要更新则转入步骤六，如果不需要更新则流程结束。

[0047] 步骤六、客户端主程序将终端标识发送到服务端进行身份验证。服务端将对客户端发送的终端标识进行验证。

[0048] 步骤七、检测身份认证信息是否通过。身份验证通过后将转入步骤八。如果未能通过验证，则软件更新流程结束。

[0049] 步骤八、身份验证通过后将接收软件文件完整性度量值。客户端主程序将对接收的软件文件进行完整性度量，并与收到的预期完整性度量值进行比对。如果文件完整性预期值与检测值不符，则重新下载。如果未能通过验证，则软件更新流程结束。

[0050] 步骤九、客户端从服务器端下载软件更新文件和软件安装脚本。可以在硬盘或 Flash 等存储空间中，划分一块保护空间用于保存下载的安装文件。

[0051] 步骤十、客户端根据下载的安装脚本，对软件进行自动安装。

[0052] 步骤十一、软件安装流程结束。

[0053] 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。

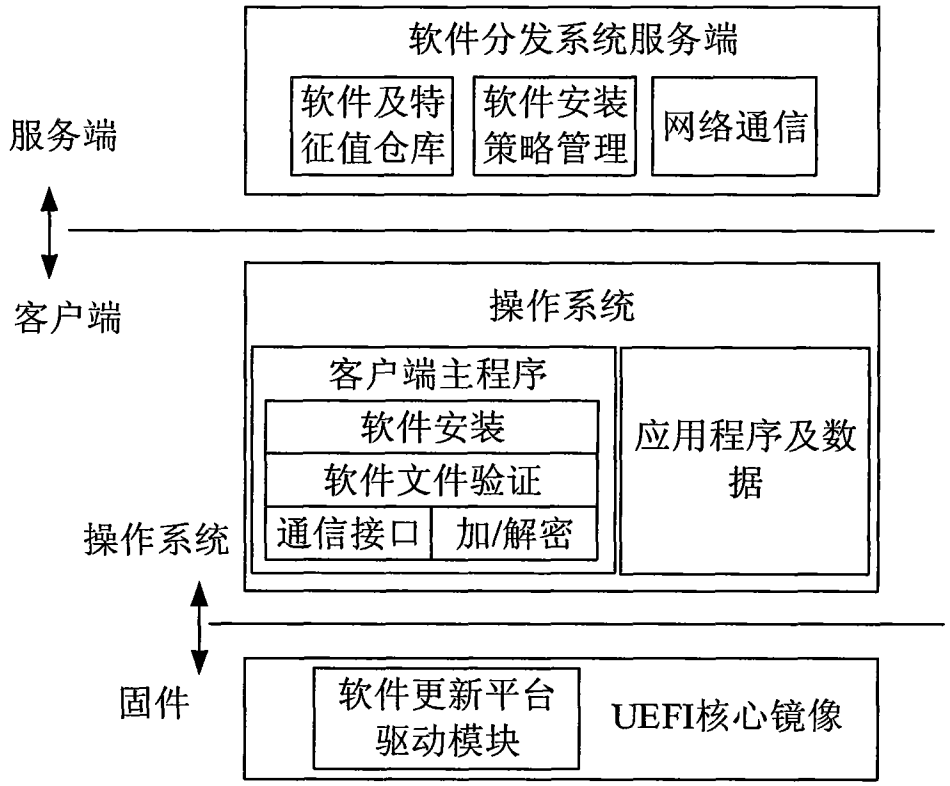

软件分发系统服务端
软件及特征值仓库
软件安装策略管理
网络通信
服务端
客户端
操作系统
客户端主程序
软件安装
软件文件验证
通信接口
加/解密
应用程序及数据
操作系统
固件
软件更新平台驱动模块
UEFI核心镜像

图 1

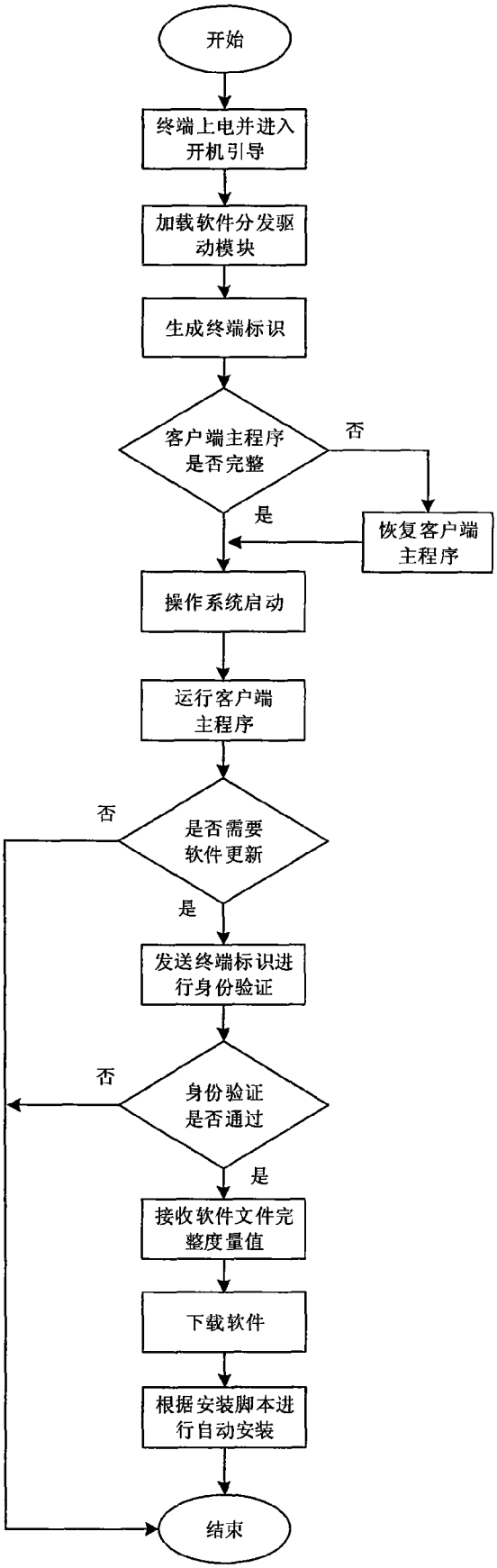

开始
终端上电并进入开机引导
加载软件分发驱动模块
生成终端标识
客户端主程序是否完整
否
是
恢复客户端主程序
操作系统启动
运行客户端主程序
是否需要软件更新
否
是
发送终端标识进行身份验证
身份验证是否通过
否
是
接收软件文件完整度量值
下载软件
根据安装脚本进行自动安装
结束

图 2