

(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 104573474 A

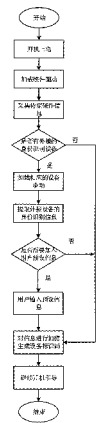
(43) 申请公布日 2015. 04. 29

(21) 申请号 201410457574. 1
(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 21/44(2013. 01)

权利要求书1页 说明书2页 附图2页

(54) 发明名称
一种基于 UEFI 的身份标识生成系统和方法

(57) 摘要
本发明公开了一种基于 UEFI 的设备身份标识生成系统和方法,属于计算机安全技术领域。系统包括设备信息采集模块、本地身份验证接口和标识生成模块;其中,所述设备信息采集模块用于采集设备的硬件信息,所述本地身份验证接口用于接入外置的身份验证设备;所述标识生成模块可以结合本地设备信息与外接设备信息,生成唯一设备标识码。本发明在更换硬盘、重新分区、重新安装操作系统的情况下,不需要安装特定的软件,可以在固件层生成相应的标识。



1. 一种基于 UEFI 的身份标识生成系统,其特征在于,所述系统包括设备信息采集模块、本地身份验证接口和标识生成模块;其中,所述设备信息采集模块用于采集设备的硬件信息,所述本地身份验证接口用于接入外置的身份验证设备;所述标识生成模块可以结合本地设备信息与外接设备信息,生成唯一设备标识码。

2. 如权利要求 1 所述的基于 UEFI 的身份标识生成系统,其特征在于,实现步骤如下:

步骤一、计算机开机上电,进入开机引导过程;

步骤二、在固件层加载相应的硬件驱动,如硬盘驱动;

步骤三、采集特定的硬件信息;

步骤四、检测是否有外接的身份识别设备;如果有外接设备转入步骤五;如果没有外接设备则跳过此步,进入步骤九;

步骤五、加载相应的设备驱动;

步骤六、提取外接设备的身份识别信息;

步骤七、检测是否需要用户输入预设信息;如果需要,则转入步骤六,否则,转入步骤九;

步骤八、用户输入预设信息,如某个特定的字符串;

步骤九、将收集到的信息进行加密,生成设备唯一标识;

步骤十、继续进行开机引导,本流程结束。

一种基于 UEFI 的身份标识生成系统和方法

技术领域

[0001] 本本发明属于计算机安全技术领域,涉及一种基于 UEFI 固件,在开机引导过程中生成唯一机器标识的方法。

背景技术

[0002] 目前,在计算机安全领域,设备唯一标识一般用于服务器或其他计算机设备能够快速进行被系统识别。设备标识一般是通过操作系统中的特定软件生成的,有着以下的不足,主要包括:

[0003] (1) 在更换硬盘、重新分区、重新安装操作系统后,需要重新安装特定的设备标识生成程序,才能生成设备标识。

[0004] (2) 在操作系统中安装的设备标识生成程序,容易受到病毒或木马的篡改和删除,导致系统无法识别原有设备。

发明内容

[0005] 有本发明的目的是为了克服已有技术的缺陷,为了解决在开机的引导过程中,操作系统启动前,能够生成设备的身份标识的问题,提出一种基于 UEFI 的设备身份标识生成系统和方法。

[0006] 一种基于 UEFI 的身份标识生成系统,所述系统包括设备信息采集模块、本地身份验证接口和标识生成模块;其中,所述设备信息采集模块用于采集设备的硬件信息,所述本地身份验证接口用于接入外置的身份验证设备,如 U-key、IC 卡等;所述标识生成模块可以结合本地设备信息与外接设备信息,生成唯一设备标识码。

[0007] 其生成的过程为:

[0008] 步骤一、计算机开机上电,进入开机引导过程;

[0009] 步骤二、在固件层加载相应的硬件驱动,如硬盘驱动;

[0010] 步骤三、采集特定的硬件信息(如主板编号、CPU 编号等);

[0011] 步骤四、检测是否有外接的身份识别设备;如果有外接设备转入步骤五;如果没有外接设备则跳过此步,进入步骤九;

[0012] 步骤五、加载相应的设备驱动;

[0013] 步骤六、提取外接设备的身份识别信息;

[0014] 步骤七、检测是否需要用户输入预设信息;如果需要,则转入步骤六,否则,转入步骤九;

[0015] 步骤八、用户输入预设信息,如某个特定的字符串;

[0016] 步骤九、将收集到的信息进行加密,生成设备唯一标识;

[0017] 步骤十、继续进行开机引导,本流程结束。

[0018] 有益效果:

[0019] 1、本发明在更换硬盘、重新分区、重新安装操作系统的情况下,不需要安装特定的

软件,可以在固件层生成相应的标识。

[0020] 2、本发明在固件层生成相应的标识,不易受到病毒或木马的篡改和删除。

附图说明

[0021] 图1为本发明的系统总体框架结构图;

[0022] 图2为本发明设备身份标识码生成的流程图。

具体实施方式

[0023] 下面结合附图并举实施例,对本发明进行详细描述。

[0024] 如附图1所示,本发明提供了一种基于UEFI的身份标识生成系统,所述系统包括设备信息采集模块、本地身份验证接口和标识生成模块;其中,所述设备信息采集模块用于采集设备的硬件信息,所述本地身份验证接口用于接入外置的身份验证设备,如U-key、IC卡等;所述标识生成模块可以结合本地设备信息与外接设备信息,生成唯一设备标识码。

[0025] 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:

[0026] a) 在UEFI核心镜像中添加驱动模块。

[0027] b) 在UEFI核心镜像中挂载Option ROM模块。

[0028] c) 在可信卡等其他外围设备中挂载驱动模块。

[0029] 如附图2所示,本发明基于UEFI的软件全过程保护方法的具体实施方法主要步骤如下:

[0030] 步骤一、在计算机上插入USB KEY,里面包含了身份识别信息。计算机开机上电,进入开机引导过程。

[0031] 步骤二、在固件层加载相应的硬件驱动,如硬盘驱动。

[0032] 步骤三、采集特定的硬件信息(如主板编号、CPU编号等)。

[0033] 步骤四、检测到外接的身份识别设备USB KEY。

[0034] 步骤五、加载身份识别设备USB KEY的驱动。

[0035] 步骤六、提取外接设备的身份识别信息。

[0036] 步骤七、弹出输入预设信息的界面。

[0037] 步骤八、用户可以输入与预设信息相通的特定字符串。

[0038] 步骤九、将收集到的硬件信息和身份认证信息进行加密,生成设备唯一标识。

[0039] 步骤十、继续进行开机引导,本流程结束。

[0040] 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。

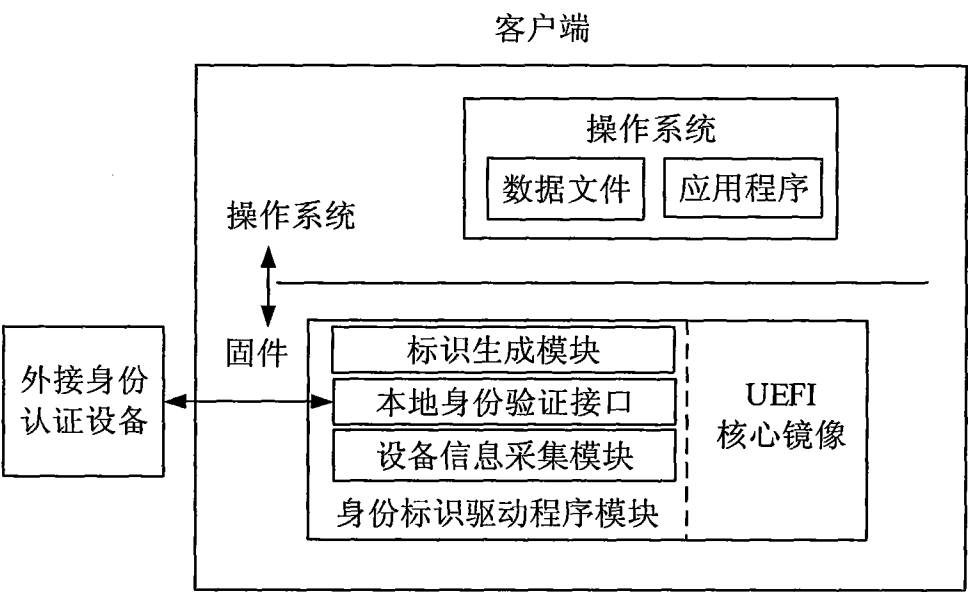


图 1

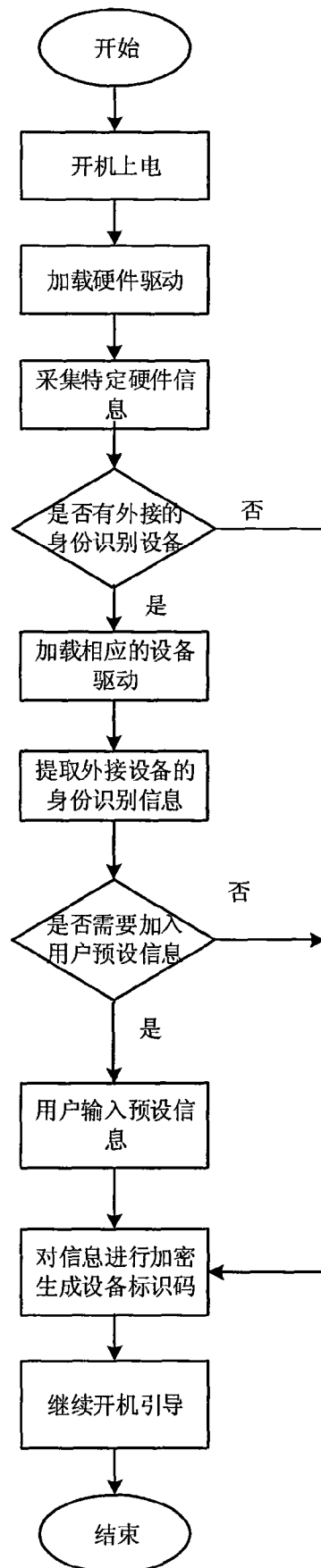


图 2