(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112613011 B
(45)授权公告日 2024.01.23

(21)申请号 202011610404.4
(22)申请日 2020.12.29
(65)同一申请的已公布的文献号
申请公布号 CN 112613011 A
(43)申请公布日 2021.04.06
(73)专利权人 北京天融信网络安全技术有限公司
地址 100000 北京市海淀区上地东路1号院3号楼四层
专利权人 北京天融信科技有限公司
北京天融信软件有限公司
(72)发明人 姜新利 陈天凯 罗元
(74)专利代理机构 北京超凡宏宇知识产权代理有限公司 11463
专利代理师 唐菲
(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/46(2013.01)
G06F 21/57(2013.01)
G06F 21/79(2013.01)
(56)对比文件
CN 101123507 A,2008.02.13
CN 104580136 A,2015.04.29
CN 105354507 A,2016.02.24
CN 108965222 A,2018.12.07
CN 110659522 A,2020.01.07
US 2012185683 A1,2012.07.19
审查员 梁旭姣

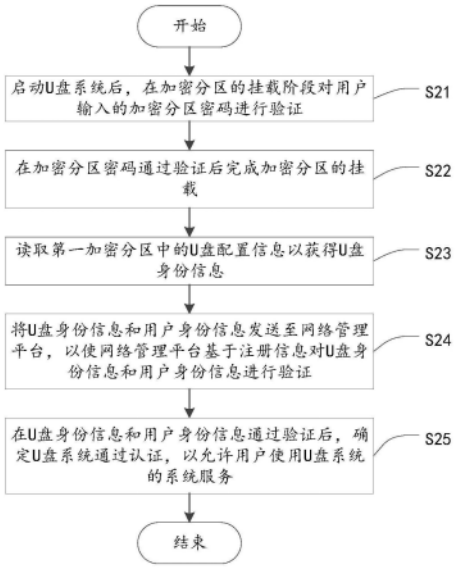
权利要求书2页 说明书9页 附图2页

(54)发明名称

U盘系统认证方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种U盘系统认证方法、装置、电子设备及存储介质，涉及信息安全技术领域。U盘包括系统分区、第一加密分区和第二加密分区，该方法包括：启动U盘系统后，在第一加密分区的挂载阶段对用户输入的加密分区密码进行验证后完成加密分区的挂载；读取第一加密分区中的U盘配置信息以获得U盘身份信息；将U盘身份信息和用户身份信息发送至网络管理平台，以使网络管理平台基于注册信息对U盘身份信息和用户身份信息进行验证；在U盘身份信息和用户身份信息通过验证后，确定U盘系统通过认证。通过对U盘使用的用户以及U盘进行身份验证，以及加密分区验证，保证了U盘系统不被替换，提高了U盘系统的使用安全性。



CN 112613011 B

1.一种U盘系统认证方法,其特征在于,应用于U盘,所述U盘包括用于内置U盘系统的系统分区和加密分区,所述加密分区包括用于存储U盘配置信息和用户身份信息的第一加密分区以及用于存储用户生产数据的第二加密分区,所述方法包括:

启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证;

在所述加密分区密码通过验证后完成所述加密分区的挂载;

读取所述第一加密分区中的U盘配置信息以获得U盘身份信息;

将所述U盘身份信息和所述用户身份信息发送至网络管理平台,以使所述网络管理平台基于注册信息对所述U盘身份信息和所述用户身份信息进行验证;

在所述U盘身份信息和所述用户身份信息通过验证后,确定所述U盘系统通过认证,以允许所述用户使用所述U盘系统的系统服务;

所述方法还包括:

在所述U盘系统启动的内核引导阶段,通过内核安全检查对所述U盘系统的启动过程进行校验;

在所述U盘系统的启动过程通过所述内核安全检查时,进入所述挂载阶段;

在所述读取所述第一加密分区中的U盘配置信息以获得U盘身份信息之前,所述方法还包括:

对所述U盘系统的引导加载程序进行验证;

在所述引导加载程序通过验证时,执行所述启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证的步骤。

2.根据权利要求1所述的方法,其特征在于,所述对所述U盘系统的引导加载程序进行验证,包括:

采用预设解密方式对所述引导加载程序中的自定义加密信息进行解密,获得解密结果;

在所述解密结果与所述引导加载程序的预设解密结果相同时,确定所述引导加载程序通过验证。

3.根据权利要求1—2中任一项所述的方法,其特征在于,在所述将所述U盘身份信息和所述用户身份信息发送至网络管理平台之前,所述方法还包括:

向所述网络管理平台发送所述U盘身份信息和所述用户身份信息,以进行所述U盘和所述用户的注册,使所述网络管理平台基于注册信息对所述U盘发送的所述U盘身份信息和所述用户身份信息进行验证。

4.根据权利要求3所述的方法,其特征在于,所述U盘身份信息包括所述U盘的序列号、产品识别码和供应商识别码中的至少一种。

5.根据权利要求1所述的方法,其特征在于,所述方法还包括:

在所述U盘系统通过认证后,通过U盘烧录工具对所述U盘进行配置更新,所述配置更新包括所述U盘系统的更新、所述U盘配置信息的更新和/或所述用户身份信息的更新。

6.一种U盘系统认证装置,其特征在于,应用于U盘,所述U盘包括用于内置U盘系统的系统分区和加密分区,所述加密分区包括用于存储U盘配置信息和用户身份信息的第一加密分区以及用于存储用户生产数据的第二加密分区,所述装置包括:

加密分区密码验证模块,用于启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证;

挂载模块,用于在所述加密分区密码通过验证后完成所述加密分区的挂载;

U盘配置读取模块,用于读取所述第一加密分区中的U盘配置信息以获得U盘身份信息;

身份验证模块,用于将所述U盘身份信息和所述用户身份信息发送至网络管理平台,以使所述网络管理平台基于注册信息对所述U盘身份信息和所述用户身份信息进行验证;

认证使用模块,用于在所述U盘身份信息和所述用户身份信息通过验证后,确定所述U盘系统通过认证,以允许所述用户使用所述U盘系统的系统服务;

内核安全检查模块,用于在U盘系统启动的内核引导阶段,通过内核安全检查对U盘系统的启动过程进行校验;在U盘系统的启动过程通过内核安全检查时,进入挂载阶段;

引导加载程序验证模块,用于对U盘系统的引导加载程序进行验证;在引导加载程序通过验证时,执行启动U盘系统后,在加密分区的挂载阶段对用户输入的加密分区密码进行验证的步骤。

7.一种电子设备,其特征在于,所述电子设备包括存储器和处理器,所述存储器中存储有程序指令,所述处理器运行所述程序指令时,执行权利要求1—5中任一项所述方法中的步骤。

8.一种存储介质,其特征在于,所述存储介质中存储有计算机程序指令,所述计算机程序指令被一处理器运行时,执行权利要求1—5任一项所述方法中的步骤。

U盘系统认证方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及信息安全技术领域,具体而言,涉及一种U盘系统认证方法、装置、电子设备及存储介质。

背景技术

[0002] 目前,基于U盘启动的操作系统很多,但对U盘内置的操作系统的防替换保护很少,以及对U盘使用者身份的验证也没有,及U盘身份的验证也很少。面对层出不穷的针对系统的攻击,仅仅依靠U盘系统自身的保护方式,不能有效保护系统的安全。同时,U盘具有的即插即用的特点,使得U盘中的数据更容易被盗取和破坏。因此,现有的基于U盘启动的操作系统存在安全性较低的问题。

发明内容

[0003] 有鉴于此,本申请实施例的目的在于提供一种U盘系统认证方法、装置、电子设备及存储介质,以改善现有技术中存在的现有的基于U盘启动的操作系统存在安全性较低的问题。

[0004] 本申请实施例提供了一种U盘系统认证方法,应用于U盘,所述U盘包括用于内置U盘系统的系统分区和加密分区,所述加密分区包括用于存储U盘配置信息和用户身份信息的第一加密分区以及用于存储用户生产数据的第二加密分区,所述方法包括:启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证;在所述加密分区密码通过验证后完成所述加密分区的挂载;读取所述第一加密分区中的U盘配置信息以获得U盘身份信息;将所述U盘身份信息和所述用户身份信息发送至网络管理平台,以使所述网络管理平台基于注册信息对所述U盘身份信息和所述用户身份信息进行验证;在所述U盘身份信息和所述用户身份信息通过验证后,确定所述U盘系统通过认证,以允许所述用户使用所述U盘系统的系统服务。

[0005] 在上述实现方式中,通过加密分区密码验证、U盘配置验证和U盘身份信息和用户身份信息验证等多重验证方式,防止U盘内置的U盘系统被替换,同时结合网络管理平台进行U盘身份信息和用户身份信息验证以保证U盘被盗或丢失后破坏者无法使用U盘系统的系统服务,从而提高了U盘系统的安全性。

[0006] 可选地,在启动所述U盘系统时,所述方法还包括:在所述U盘系统启动的内核引导阶段,通过内核安全检查对所述U盘系统的启动过程进行校验;在所述U盘系统的启动过程通过所述内核安全检查时,进入所述挂载阶段。

[0007] 在上述实现方式中,在内核引导阶段对U盘系统进行内核安全检查,进一步保证了U盘系统的使用安全性。

[0008] 可选地,在所述读取所述第一加密分区中的U盘配置信息以获得U盘身份信息之前,所述方法还包括:对所述U盘系统的引导加载程序进行验证;在所述引导加载程序通过验证时,执行所述启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区

密码进行验证的步骤。

[0009] 在上述实现方式中,在U盘系统启动阶段验证加密分区,如果验证失败,将导致U盘系统启动失败,从而提高了U盘系统的认证安全性。

[0010] 可选地,所述对所述U盘系统的引导加载程序进行验证,包括:采用预设解密方式对所述引导加载程序中的自定义加密信息进行解密,获得解密结果;在所述解密结果与所述引导加载程序的预设解密结果相同时,确定所述引导加载程序通过验证。

[0011] 在上述实现方式中,基于自定义加密信息对引导加载程序进行验证,确定引导加载程序是否遭到攻击或恶意修改,从而提高了U盘系统的完整性和安全性。

[0012] 可选地,在所述将所述U盘身份信息和所述用户身份信息发送至网络管理平台之前,所述方法还包括:向所述网络管理平台发送所述U盘身份信息和所述用户身份信息,以进行所述U盘和所述用户的注册,使所述网络管理平台基于注册信息对所述U盘发送的所述U盘身份信息和所述用户身份信息进行验证。

[0013] 在上述实现方式中,通过网络管理平台对U盘身份信息和用户身份信息进行验证,可以避免U盘丢失后被冒用或破坏,提高了U盘系统的使用安全性。

[0014] 可选地,所述U盘身份信息包括所述U盘的序列号、产品识别码和供应商识别码中的至少一种。

[0015] 在上述实现方式中,U盘身份信息包括U盘的序列号、产品识别码和供应商识别码中的至少一种时,能够在U盘身份信息验证时提高验证灵活度和安全性。

[0016] 可选地,在所述U盘系统通过认证后,通过U盘烧录工具对所述U盘进行配置更新,所述配置更新包括所述U盘系统的更新、所述U盘配置信息的更新和/或所述用户身份信息的更新。

[0017] 在上述实现方式中,为U盘提供了配置更新功能,能够根据需求对U盘进行配置或验证信息的更新,进一步提高了U盘系统的使用安全性。

[0018] 本申请实施例还提供了一种U盘系统认证装置,应用于U盘,所述U盘包括用于内置U盘系统的系统分区和加密分区,所述加密分区包括用于存储U盘配置信息和用户身份信息的第一加密分区以及用于存储用户生产数据的第二加密分区,所述装置包括:加密分区密码验证模块,用于启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证;挂载模块,用于在所述加密分区密码通过验证后完成所述加密分区的挂载;U盘配置读取模块,用于读取所述第一加密分区中的U盘配置信息以获得U盘身份信息;身份验证模块,用于将所述U盘身份信息和所述用户身份信息发送至网络管理平台,以使所述网络管理平台基于注册信息对所述U盘身份信息和所述用户身份信息进行验证;认证使用模块,用于在所述U盘身份信息和所述用户身份信息通过验证后,确定所述U盘系统通过认证,以允许所述用户使用所述U盘系统的系统服务。

[0019] 在上述实现方式中,通过加密分区密码验证、U盘配置验证和U盘身份信息和用户身份信息验证等多重验证方式,防止U盘内置的U盘系统被替换,同时结合网络管理平台进行U盘身份信息和用户身份信息验证以保证U盘被盗或丢失后破坏者无法使用U盘系统的系统服务,从而提高了U盘系统的安全性。

[0020] 可选地,所述U盘系统认证装置还包括:内核安全检查模块,用于在所述U盘系统启动的内核引导阶段,通过内核安全检查对所述U盘系统的启动过程进行校验;在所述U盘系

统的启动过程通过所述内核安全检查时,进入所述挂载阶段。

[0021] 在上述实现方式中,在内核引导阶段对U盘系统进行内核安全检查,进一步保证了U盘系统的使用安全性。

[0022] 可选地,所述U盘系统认证装置还包括:引导加载程序验证模块,用于对所述U盘系统的引导加载程序进行验证;在所述引导加载程序通过验证时,执行所述启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证的步骤。

[0023] 在上述实现方式中,在U盘系统启动阶段验证加密分区,如果验证失败,将导致U盘系统启动失败,从而提高了U盘系统的认证安全性。

[0024] 可选地,所述引导加载程序验证模块具体用于:采用预设解密方式对所述引导加载程序中的自定义加密信息进行解密,获得解密结果;在所述解密结果与所述引导加载程序的预设解密结果相同时,确定所述引导加载程序通过验证。

[0025] 在上述实现方式中,基于自定义加密信息对引导加载程序进行验证,确定引导加载程序是否遭到攻击或恶意修改,从而提高了U盘系统的完整性和安全性。

[0026] 可选地,所述U盘系统认证装置还包括:注册发送模块,用于向所述网络管理平台发送所述U盘身份信息和所述用户身份信息,以进行所述U盘和所述用户的注册,使所述网络管理平台基于注册信息对所述U盘发送的所述U盘身份信息和所述用户身份信息进行验证。

[0027] 在上述实现方式中,通过网络管理平台对U盘身份信息和用户身份信息进行验证,可以避免U盘丢失后被冒用或破坏,提高了U盘系统的使用安全性。

[0028] 可选地,所述U盘身份信息包括所述U盘的序列号、产品识别码和供应商识别码中的至少一种。

[0029] 在上述实现方式中,U盘身份信息包括U盘的序列号、产品识别码和供应商识别码中的至少一种时,能够在U盘身份信息验证时提高验证灵活度和安全性。

[0030] 可选地,所述U盘系统认证装置还包括:更新模块,用于在所述U盘系统通过认证后,通过U盘烧录工具对所述U盘进行配置更新,所述配置更新包括所述U盘系统的更新、所述U盘配置信息的更新和/或所述用户身份信息的更新。

[0031] 在上述实现方式中,为U盘提供了配置更新功能,能够根据需求对U盘进行配置或验证信息的更新,进一步提高了U盘系统的使用安全性。

[0032] 本申请实施例还提供了一种电子设备,所述电子设备包括存储器和处理器,所述存储器中存储有程序指令,所述处理器读取并运行所述程序指令时,执行上述任一实现方式中的步骤。

[0033] 本申请实施例还提供了一种可读取存储介质,所述可读取存储介质中存储有计算机程序指令,所述计算机程序指令被一处理器读取并运行时,执行上述任一实现方式中的步骤。

附图说明

[0034] 为了更清楚地说明本申请实施例的技术方案,下面将对本申请实施例中所需要使用的附图作简单地介绍,应当理解,以下附图仅示出了本申请的某些实施例,因此不应被看作是对范围的限定,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以

根据这些附图获得其他相关的附图。

[0035] 图1为本申请实施例提供的一种U盘制作步骤的流程示意图。

[0036] 图2为本申请实施例提供的一种U盘系统认证方法的流程示意图。

[0037] 图3为本申请实施例提供的一种U盘系统认证装置的模块示意图。

[0038] 图标:30—U盘系统认证装置;31—加密分区密码验证模块;32—挂载模块;33—U盘配置读取模块;34—身份验证模块;35—认证使用模块。

具体实施方式

[0039] 下面将结合本申请实施例中附图,对本申请实施例中的技术方案进行描述。

[0040] 经本申请人研究发现,现有技术通常采用以下两种U盘系统保护方式保证U盘系统使用的安全性:(1)通过U盘的写保护程序来控制外部对操作系统及U盘的写入的方法;(2)通过在U盘内隔离出一个加密的安全空间存放数据的方法。

[0041] 针对上述现有方法(1),该方法通过Windows XP Embedded操作系统本身的Enhanced Write Filter覆盖写保护和U盘的写保护程序来控制外部对操作系统及U盘的写入的基于U盘Windows XP Embedded随身操作系统的保护方法,若需要对U盘写入数据或更改U盘中的数据,需通过U盘写保护程序,发送打开命令,关闭写保护程序进行写入操作,反之,则U盘默认处于只读状态。

[0042] 针对上述现有方法(2),该方法首先对普通U盘进行加工处理,在U盘内预装含操作系统和办公软件的工作环境,并在U盘内隔离出一个加密的安全空间存放数据,在移动办公过程中,所借助的普通计算机的原有硬盘被设置为只读,无法写入数据,所有办公过程中编辑的数据只能保存在所述U盘的所述加密存储区域,并且,所述U盘办公环境的数据只进不出。

[0043] 由上述两种现有技术可以分析得出,现有技术中U盘中的操作系统有被其他系统替代的安全隐患,U盘系统使用者身份的合法性没做验证,如果U盘被盗或者丢失,进入U盘系统是件很容易的事情,U盘中的数据也不被保护,且U盘设备的身份没做验证,如果U盘被盗或者丢失,没有安全机制去禁用该U盘,仍然可以进入U盘系统,给用户带来安全隐患。

[0044] 为了解决现有技术存在的上述问题,本申请实施例提供了一种应用于U盘的U盘系统认证方法,首先对U盘系统进行说明,U盘系统是指U盘内的操作系统,U盘插在电脑等设备的U盘对应接口,设置设备从U盘启动,借助设备的硬件环境运行。

[0045] 对该U盘的制作方法进行说明。

[0046] 请参考图1,图1为本申请实施例提供的一种U盘制作步骤的流程示意图。该U盘制作步骤具体可以如下:

[0047] 步骤S11:定制U盘系统。

[0048] 可选地,本实施例中的U盘系统可以为Linux系统,例如麒麟桌面操作系统、统一操作系统(Unity Operating System)以及开源的Ubuntu桌面操作系统等。

[0049] 具体地,对U盘系统的定制可以是但不限于是系统加固、桌面图形化界面的改造和预装应用软件等。

[0050] 可选地,上述系统加固可以是但不限于是更新安全补丁、禁用SSH(Secure Shell,安全外壳协议)远程登录服务、用户密码复杂性要求、登录失败处理以及关闭无用端口等。

[0051] 可选地,上述桌面图像化界面改造包括但不限于是系统标识(Loge)的定制、系统版本的定制、桌面图片的定制以及系统资源浏览器的定制等。

[0052] 可选地,上述预装应用软件包括但不限于以下:系统检测服务、基本办公软件以及其他应用软件等。其中,系统检测服务用于根据特定的检查规则定时做系统检测,检测通过,正常使用系统,检测不通过,禁止使用系统。

[0053] 步骤S12:通过U盘烧录工具将U盘系统烧录到U盘。

[0054] 具体地,本实施例中的U盘烧录工具可以是但不限于是Win32DiskImager、USB Image Tool和rufus等。

[0055] 本实施例中将U盘划分三个分区:系统用于内置定制的Linux系统,第一加密分区用于U盘配置信息和用户身份信息等,第二加密分区用于存储U盘使用者生产的数据。

[0056] 步骤S13:通过U盘系统烧录工具更新U盘配置。

[0057] 可选地,U盘配置更新可以但不限于是U盘系统的更新、U盘配置信息的更新和用户身份信息的更新等。

[0058] 具体地,本实施例中的U盘配置信息包括U盘身份信息,U盘身份信息包括但不限于以下:U盘的序列号、产品识别码PID(Product Identity Document)和供应商识别码VID(Vender Identity Document)。本实施例中的用户身份信息包括但不限于用户名称和用户密码等。

[0059] 步骤S14:将U盘身份信息和用户身份信息注册到网络管理平台。

[0060] 由于U盘系统的认证需要通过网络管理平台对U盘配置信息和用户身份信息进行验证,因此需要将U盘身份信息和用户身份信息发送至网络管理平台进行注册。

[0061] 接下来对本申请实施例提供的U盘系统认证方法进行说明,请参考图2,图2为本申请实施例提供的一种U盘系统认证方法的流程示意图。该U盘系统认证方法的具体步骤可以如下:

[0062] 步骤S21:启动U盘系统后,在加密分区的挂载阶段对用户输入的加密分区密码进行验证。

[0063] 本实例中的U盘系统不存储加密分区密码,U盘系统启动过程中默认进行加密分区挂载,需要用户输入加密分区密码,如果加密分区密码验证失败,将导致U盘系统启动失败。

[0064] 由于内核是一个操作系统的核心。是基于硬件的第一层软件扩充,提供操作系统的最基本的功能,是操作系统工作的基础,它负责管理系统的进程、内存、设备驱动程序、文件和网路O系统,决定系统的稳定性和性能,且内核是否被修改等问题也很大程度上影响着系统安全性。

[0065] 因此在执行步骤S21之前,本实施例还可以对内核引导阶段进行校验,采用增加了内核安全检查的内核引导,在内核引导阶段采用自定义规则对系统启动过程做校验,在校验失败时将导致系统启动失败。

[0066] 具体地,内核引导阶段的内核安全检查步骤具体可以包括:在U盘系统启动的内核引导阶段,通过内核安全检查对U盘系统的启动过程进行校验;在U盘系统的启动过程通过内核安全检查时,进入挂载阶段。

[0067] 上述内核安全检查可以包括但不限于磁盘分区个数检查、分区大小检查以及磁盘分区中的配置文件检查等。

[0068] 本实施中的挂载表示U盘连接设备以及U盘系统可以发现U盘,使文件系统可以识别U盘并读写其中的文件。

[0069] 步骤S22:在加密分区密码通过验证后完成加密分区的挂载。

[0070] 由于引导加载程序(Bootloader)是U盘系统等嵌入式系统在加电后执行的第一段代码,在它完成CPU(Central Processing Unit,中央处理器)和相关硬件的初始化之后,再将操作系统映像或固化的嵌入式应用程序装在到内存中然后跳转到操作系统所在的空间,启动操作系统运行,因此引导加载程序是否被解锁或修改也可以表示U盘系统是否被修改,本实施例中还可以对引导加载程序进行校验,在校验通过后再执行后续步骤,在校验未通过时U盘连接设备无法进入U盘系统。

[0071] 可选地,本实施中可以通过加解密方式实现引导加载程序的校验,例如采用预设解密方式对引导加载程序中的自定义加密信息进行解密,获得解密结果,在解密结果与引导加载程序的预设解密结果相同时,确定引导加载程序通过验证。

[0072] 可选地,上述自定义加密信息可以是但不限于是一串随机字符串。

[0073] 步骤S23:读取第一加密分区中的U盘配置信息以获得U盘身份信息。

[0074] 步骤S24:将U盘身份信息和用户身份信息发送至网络管理平台,以使网络管理平台基于注册信息对U盘身份信息和用户身份信息进行验证。

[0075] 可选地,本实施例中在验证时发送至网络管理平台用户身份信息可以是U盘系统在确定第一加密分区中存储的用户身份信息与用户登录时输入的用户身份信息匹配时,发送至网络管理平台的用户身份信息。

[0076] 应当理解的是,在执行步骤S24通过网络管理平台对U盘身份信息和用户身份信息进行验证之前,需要执行上述步骤S14完成U盘和用户在网络管理平台的注册。

[0077] 步骤S25:在U盘身份信息和用户身份信息通过验证后,确定U盘系统通过认证,以允许用户使用U盘系统的系统服务。

[0078] 综合上述U盘制作步骤和U盘系统认证方法,该U盘系统的架构可以包括应用层、服务层和系统层。

[0079] 其中,应用层提供U盘系统的用户注册、用户登录和U盘注册等功能,用户注册和U盘注册通过网络管理平台完成,用户登录用于U盘系统中内置的安全服务基于第一加密分区中存储的用户身份信息验证用户身份。

[0080] 服务层提供设备校验、用户激活、用户校验和引导加载程序校验等功能。U盘系统中的安全服务会从第一加密分区中读取U盘配置信息以获得U盘身份信息,安全服务将用户身份信息和U盘身份信息加密后发给网络管理平台,网络管理平台对用户身份信息和U盘身份信息做验证,验证失败,U盘系统不能正常使用。U盘系统内置的系统检测服务会对引导加载程序做验证,防止破坏者修改引导加载程序。

[0081] 系统层提供U盘系统的校验,组成的模块包括但不限于以下:系统加固、安全检查服务、引导加载程序校验和加密分区密码校验等,其作用是为了防止U盘系统被替换和被获取系统root权限。

[0082] 可选地,本实施例中U盘系统连接的设备可以通过接入层的任一接入点与网络管理平台进行通信,网络管理平台可以包括用户认证服务节点、U盘认证服务节点、管理节点和服务节点等,此时网络管理平台也可以视为包含多种功能的安全认证服务器。

[0083] 为了配合本申请实施例提供的上述U盘系统认证方法,本申请实施例还提供了一种应用于U盘的U盘系统认证装置30。

[0084] 请参考图3,图3为本申请实施例提供的一种U盘系统认证装置的模块示意图。

[0085] U盘系统认证装置30包括:

[0086] 加密分区密码验证模块31,用于启动U盘系统后,在加密分区的挂载阶段对用户输入的加密分区密码进行验证;

[0087] 挂载模块32,用于在加密分区密码通过验证后完成加密分区的挂载;

[0088] U盘配置读取模块33,用于读取第一加密分区中的U盘配置信息以获得U盘身份信息;

[0089] 身份验证模块34,用于将U盘身份信息和用户身份信息发送至网络管理平台,以使网络管理平台基于注册信息对U盘身份信息和用户身份信息进行验证;

[0090] 认证使用模块35,用于在U盘身份信息和用户身份信息通过验证后,确定U盘系统通过认证,以允许用户使用U盘系统的系统服务。

[0091] 可选地,U盘系统认证装置30还包括:内核安全检查模块,用于在U盘系统启动的内核引导阶段,通过内核安全检查对U盘系统的启动过程进行校验;在U盘系统的启动过程通过内核安全检查时,进入挂载阶段。

[0092] 可选地,U盘系统认证装置30还包括:引导加载程序验证模块,用于对U盘系统的引导加载程序进行验证;在引导加载程序通过验证时,执行启动U盘系统后,在加密分区的挂载阶段对用户输入的加密分区密码进行验证的步骤。

[0093] 可选地,引导加载程序验证模块具体用于:采用预设解密方式对引导加载程序中的自定义加密信息进行解密,获得解密结果;在解密结果与引导加载程序的预设解密结果相同时,确定引导加载程序通过验证。

[0094] 可选地,U盘系统认证装置30还包括:注册发送模块,用于向网络管理平台发送U盘身份信息和用户身份信息,以进行U盘和用户的注册,使网络管理平台基于注册信息对U盘发送的U盘身份信息和用户身份信息进行验证。

[0095] 可选地,U盘身份信息包括U盘的序列号、产品识别码和供应商识别码中的至少一种。

[0096] 可选地,U盘系统认证装置30还包括:更新模块,用于在U盘系统通过认证后,通过U盘烧录工具对U盘进行配置更新,配置更新包括U盘系统的更新、U盘配置信息的更新和/或用户身份信息的更新。

[0097] 本申请实施例还提供了一种电子设备,该电子设备包括存储器和处理器,所述存储器中存储有程序指令,所述处理器读取并运行所述程序指令时,基于上述U盘执行本实施例提供的U盘系统认证方法中任一项所述方法中的步骤。

[0098] 应当理解是,该电子设备可以是个人电脑(Personal Computer,PC)、平板电脑、智能手机、个人数字助理(Personal Digital Assistant,PDA)等具有逻辑计算功能的电子设备。

[0099] 本申请实施例还提供了一种可读取存储介质,所述可读取存储介质中存储有计算机程序指令,所述计算机程序指令被一处理器读取并运行时,执行U盘系统认证方法中的步骤。

[0100] 综上所述,本申请实施例提供了一种U盘系统认证方法、装置、电子设备及存储介质,应用于U盘,所述U盘包括用于内置U盘系统的系统分区和加密分区,所述加密分区包括用于存储U盘配置信息和用户身份信息的第一加密分区以及用于存储用户生产数据的第二加密分区,所述方法包括:启动所述U盘系统后,在所述加密分区的挂载阶段对用户输入的加密分区密码进行验证;在所述加密分区密码通过验证后完成所述加密分区的挂载;读取所述第一加密分区中的U盘配置信息以获得U盘身份信息;将所述U盘身份信息和所述用户身份信息发送至网络管理平台,以使所述网络管理平台基于注册信息对所述U盘身份信息和所述用户身份信息进行验证;在所述U盘身份信息和所述用户身份信息通过验证后,确定所述U盘系统通过认证,以允许所述用户使用所述U盘系统的系统服务。

[0101] 在上述实现方式中,通过加密分区密码验证、U盘配置验证和U盘身份信息和用户身份信息验证等多重验证方式,防止U盘内置的U盘系统被替换,同时结合网络管理平台进行U盘身份信息和用户身份信息验证以保证U盘被盗或丢失后破坏者无法使用U盘系统的系统服务,从而提高了U盘系统的安全性。

[0102] 在本申请所提供的几个实施例中,应该理解到,所揭露的设备,也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的,例如,附图中的框图显示了根据本申请的多个实施例的设备的可能实现的体系架构、功能和操作。在这点上,框图中的每个方框可以代表一个模块、程序段或代码的一部分,所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现方式中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图中的每个方框、以及框图的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0103] 另外,在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分,也可以是各个模块单独存在,也可以两个或两个以上模块集成形成一个独立的部分。

[0104] 所述功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。因此本实施例还提供了一种可读取存储介质中存储有计算机程序指令,所述计算机程序指令被一处理器读取并运行时,执行区块数据存储方法中任一项所述方法中的步骤。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read—Only Memory)、随机存取存储器(RAM,RanDom Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0105] 以上所述仅为本申请的实施例而已,并不用于限制本申请的保护范围,对于本领域的技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步定义和解释。

[0106] 以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何

熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。

[0107] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

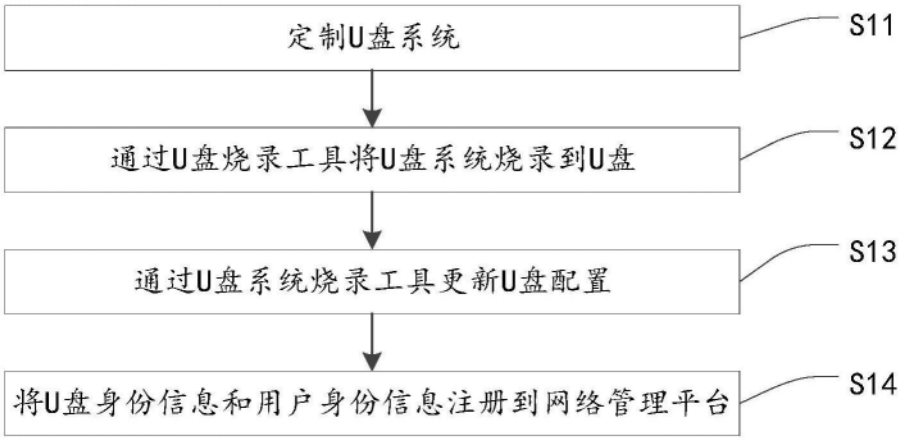

定制U盘系统
S11
通过U盘烧录工具将U盘系统烧录到U盘
S12
通过U盘系统烧录工具更新U盘配置
S13
将U盘身份信息和用户身份信息注册到网络管理平台
S14

图1

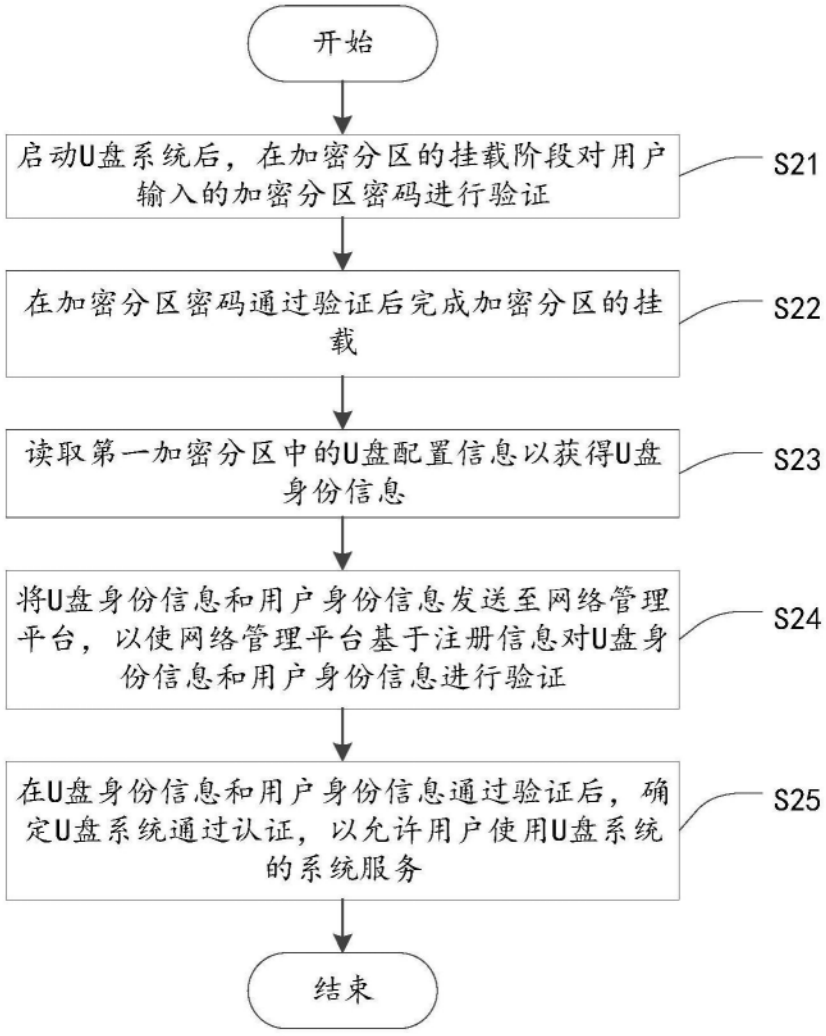

开始
启动U盘系统后，在加密分区的挂载阶段对用户输入的加密分区密码进行验证
S21
在加密分区密码通过验证后完成加密分区的挂载
S22
读取第一加密分区中的U盘配置信息以获得U盘身份信息
S23
将U盘身份信息和用户身份信息发送至网络管理平台，以使网络管理平台基于注册信息对U盘身份信息和用户身份信息进行验证
S24
在U盘身份信息和用户身份信息通过验证后，确定U盘系统通过认证，以允许用户使用U盘系统的系统服务
S25
结束

图2

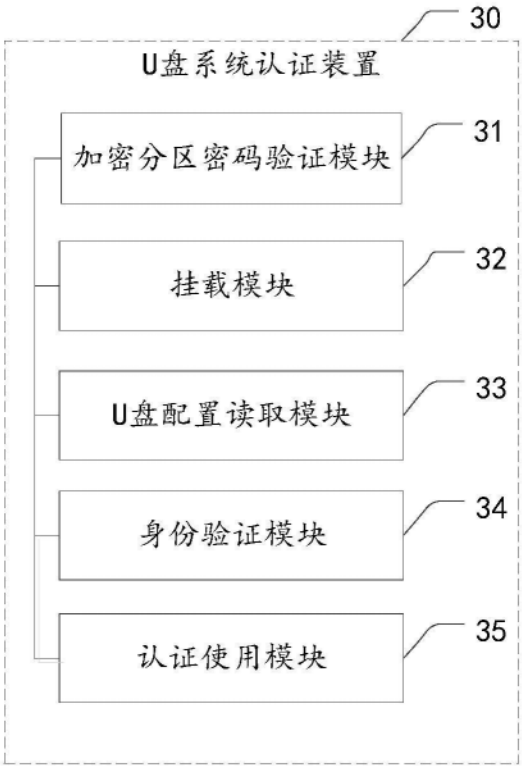

30
U盘系统认证装置
加密分区密码验证模块
31
挂载模块
32
U盘配置读取模块
33
身份验证模块
34
认证使用模块
35

图3