(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115203754 A
(43)申请公布日 2022.10.18

(21)申请号 202211112977.3

(22)申请日 2022.09.14

(71)申请人 统信软件技术有限公司
地址 100176 北京市大兴区北京经济技术开发区科谷一街10号院12号楼18层

(72)发明人 刘闻欢 闫博文 李鹤

(74)专利代理机构 北京瀚方律师事务所 11774
专利代理师 姜莹

(51)Int.Cl.
G06F 21/74(2013.01)
G06F 21/31(2013.01)
G06F 21/45(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)

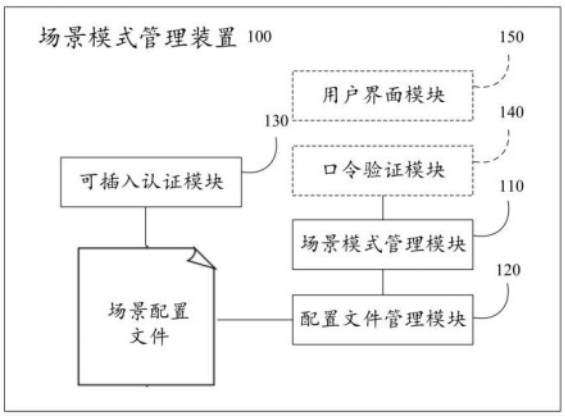
权利要求书2页 说明书13页 附图4页

(54)发明名称

场景模式管理装置、初始化方法以及场景模式切换方法

(57)摘要

本发明公开了场景模式管理装置、初始化方法以及场景模式切换方法，涉及系统安全技术领域，可以解决现有操作系统难以为不同成员提供有效隔离环境的技术问题。场景模式管理装置包括：场景模式管理模块，提供场景模式的管理接口；配置文件管理模块，对场景配置文件进行解析和修改；可插入认证模块，在用户登录操作系统时对用户密码进行认证，认证通过后，在场景模式启用时响应于用户会话的开启，从场景配置文件读取待隔离系统目录，并创建对应的命名空间，将当前场景模式对应的待隔离系统目录挂载到所创建的命名空间中以实现隔离。根据本发明技术方案，能够为操作系统的不同成员提供有效的隔离环境。



CN 115203754 A

1.一种场景模式管理装置,包括:

场景模式管理模块,用于提供场景模式的管理接口,所述场景模式包括多个预设模式;

配置文件管理模块,用于对场景配置文件进行解析和修改,所述场景配置文件用于描述所述多个预设模式各自对应的待隔离系统目录;

可插入认证模块,用于在用户登录操作系统时,基于接入的认证方式对用户密码进行密码认证,在密码认证通过后,在场景模式启用的情况下,响应于用户会话的开启,从场景配置文件读取当前场景模式对应的待隔离系统目录,并创建对应的命名空间,将当前场景模式对应的待隔离系统目录挂载到所创建的命名空间中以实现隔离。

2.根据权利要求1所述的场景模式管理装置,其中,所述待隔离系统目录包括的系统目录的数量为一个或多个。

3.根据权利要求1或2所述的场景模式管理装置,其中,所述待隔离系统目录包括以下至少一个系统目录:

家目录;已安装应用系统目录;网络配置系统目录;及防火墙系统目录。

4.根据权利要求1或2所述的场景模式管理装置,其中,所述多个预设模式包括以下至少一个:

老年模式,在该模式下,第一应用白名单之外的应用被禁止使用,应用安装和卸载功能被禁止,配置防火墙并拒绝访问恶意网站;

青少年模式,在该模式下,第二应用白名单之外的应用被禁止使用,应用安装和卸载功能被禁止,配置防火墙并拒绝访问恶意网站;

工作模式,在该模式下,默认启用VPN连接并监控VPN的连接状态,若VPN离线时长超过预设值则注销操作系统,配置防火墙并禁止访问游戏网站和恶意网站;

娱乐模式,在该模式下,默认开启显示增强和高性能模式;及

维护模式,该模式用于用户设备维护时的数据隔离。

5.根据权利要求1或2所述的场景模式管理装置,还包括:

口令验证模块,用于在所述场景模式管理装置首次启动时,请求用户设置口令,并接收用户所设置的口令作为初始口令;以及响应于用户的场景模式切换请求,提示用户输入口令,基于所述初始口令对用户输入的口令进行身份验证,以在用户输入的口令通过身份验证的情况下,允许用户使用所述管理接口进行场景模式管理。

6.根据权利要求1或2所述的场景模式管理装置,其中,所述场景模式的管理接口包括启用接口和切换接口,用于进行场景模式的启用和切换,所述切换接口仅在用户输入口令通过身份验证的情况下允许使用。

7.一种初始化方法,所述初始化方法通过如权利要求1-6中任一项所述的场景模式管理装置执行,所述初始化方法包括:

所述场景模式管理装置首次启动时,请求用户设置口令,并接收用户所设置的口令作为初始口令;

根据所述初始口令获得对应的初始口令摘要;

保存所述初始口令摘要,并开启场景模式切换功能。

8.一种场景模式切换方法,所述场景模式切换方法通过如权利要求1-6中任一项所述的场景模式管理装置执行,所述场景模式切换方法包括:

响应于用户的场景模式切换请求，提示用户输入口令，并接收用户输入的口令；

根据用户输入的口令获得对应的用户口令摘要；

根据初始口令摘要验证所述用户口令摘要；

若所述用户口令摘要与初始口令摘要一致，验证通过，允许该用户的场景模式切换请求；

若所述用户口令摘要与初始口令摘要不一致，验证失败，拒绝该用户的场景模式切换请求。

9.一种用户登录方法，所述用户登录方法通过如权利要求1-6中任一项所述的场景模式管理装置执行，所述用户登录方法包括：

响应于用户的系统登录请求，提示用户输入密码；

接收用户输入的密码，并对该密码进行摘要计算，得到对应的密码摘要；

利用所述密码摘要进行密码验证；

若密码验证未通过，拒绝用户的系统登录请求；

若密码验证通过，允许用户的系统登录请求，开启并创建会话后，读取场景配置文件以获得对应的待隔离系统目录，创建命名空间，将所述待隔离系统目录挂载到所述命名空间中以实现隔离。

10.一种计算设备，包括：

至少一个处理器和存储有程序指令的存储器；

当所述程序指令被所述处理器读取并执行时，使得所述计算设备执行如权利要求7所述的初始化方法、如权利要求8所述的场景模式切换方法以及如权利要求9所述的用户登录方法中的任一个。

11.一种存储有程序指令的可读存储介质，当所述程序指令被计算设备读取并执行时，使得所述计算设备执行如权利要求7所述的初始化方法、如权利要求8所述的场景模式切换方法以及如权利要求9所述的用户登录方法中的任一个。

场景模式管理装置、初始化方法以及场景模式切换方法

技术领域

[0001] 本发明涉及系统安全技术领域，尤其涉及一种场景模式管理装置、初始化方法以及场景模式切换方法。

背景技术

[0002] 随着智能手机的普及和功能的不断完善，原本一些需要个人计算机才能完成的功能，如今在智能手机上也能实现。换句话说，在人们的日常生活中，个人计算机的部分地位逐渐被智能手机所替代，人们对个人计算机数量的需求从原来的人手一台逐渐演变为多人共享一台。

[0003] 在诸如家庭等使用场所中，不同成员对个人计算机有不同的功能需求，并且人们都不希望与他人共享诸如个人使用记录等隐私数据。因此，需要个人计算机中的操作系统提供一种机制来隔离不同成员的使用环境。

发明内容

[0004] 为此，本发明提供了一种场景模式管理装置、初始化方法以及场景模式切换方法，以力图解决或者至少缓解上面存在的至少一个问题。

[0005] 根据本发明的第一方面，提供了一种场景模式管理装置，包括：场景模式管理模块，用于提供场景模式的管理接口，所述场景模式包括多个预设模式；配置文件管理模块，用于对场景配置文件进行解析和修改，所述场景配置文件用于描述所述多个预设模式各自对应的待隔离系统目录；可插入认证模块，用于在用户登录操作系统时，基于接入的认证方式对用户密码进行密码认证，在密码认证通过后，在场景模式启用的情况下，响应于用户会话的开启，从场景配置文件读取当前场景模式对应的待隔离系统目录，并创建对应的命名空间，将当前场景模式对应的待隔离系统目录挂载到所创建的命名空间中以实现隔离。

[0006] 可选地，在根据本发明的场景模式管理装置中，所述待隔离系统目录包括的系统目录的数量为一个或多个。

[0007] 可选地，在根据本发明的场景模式管理装置中，所述待隔离系统目录包括以下至少一个系统目录：家目录；已安装应用系统目录；网络配置系统目录；及防火墙系统目录。

[0008] 可选地，在根据本发明的场景模式管理装置中，所述多个预设模式包括以下至少一个：老年模式，在该模式下，第一应用白名单之外的应用被禁止使用，应用安装和卸载功能被禁止，配置防火墙并拒绝访问恶意网站；青少年模式，在该模式下，第二应用白名单之外的应用被禁止使用，应用安装和卸载功能被禁止，配置防火墙并拒绝访问恶意网站；工作模式，在该模式下，默认启用VPN连接并监控VPN的连接状态，若VPN离线时长超过预设值则注销操作系统，配置防火墙并禁止访问游戏网站和恶意网站；娱乐模式，在该模式下，默认开启显示增强和高性能模式；及维护模式，该模式用于用户设备维护时的数据隔离。

[0009] 可选地，根据本发明的场景模式管理装置还包括：口令验证模块，用于在所述场景模式管理装置首次启动时，请求用户设置口令，并接收用户所设置的口令作为初始口令；以

及响应于用户的场景模式切换请求，提示用户输入口令，基于所述初始口令对用户输入的口令进行身份验证，以在用户输入的口令通过身份验证的情况下，允许用户使用所述管理接口进行场景模式管理。

[0010] 可选地，在根据本发明的场景模式管理装置中，所述场景模式的管理接口包括启用接口和切换接口，用于进行场景模式的启用和切换，所述切换接口仅在用户输入口令通过身份验证的情况下允许使用。

[0011] 根据本发明第二方面，提供一种初始化方法，所述初始化方法通过如上所述的场景模式管理装置执行，所述初始化方法包括：所述场景模式管理装置首次启动时，请求用户设置口令，并接收用户所设置的口令作为初始口令；根据所述初始口令获得对应的初始口令摘要；保存所述初始口令摘要，并开启场景模式切换功能。

[0012] 根据本发明第三方面，提供一种场景模式切换方法，所述场景模式切换方法通过如上所述的场景模式管理装置执行，所述场景模式切换方法包括：响应于用户的场景模式切换请求，提示用户输入口令，并接收用户输入的口令；根据用户输入的口令获得对应的用户口令摘要；根据初始口令摘要验证所述用户口令摘要；若所述用户口令摘要与初始口令摘要一致，验证通过，允许该用户的场景模式切换请求；若所述用户口令摘要与初始口令摘要不一致，验证失败，拒绝该用户的场景模式切换请求。

[0013] 根据本发明第四方面，提供一种用户登录方法，所述用户登录方法通过如上所述的场景模式管理装置执行，所述用户登录方法包括：响应于用户的系统登录请求，提示用户输入密码；接收用户输入的密码，并对该密码进行摘要计算，得到对应的密码摘要；利用所述密码摘要进行密码验证；若密码验证未通过，拒绝用户的系统登录请求；若密码验证通过，允许用户的系统登录请求，开启并创建会话后，读取场景配置文件以获得对应的待隔离系统目录，创建命名空间，将所述待隔离系统目录挂载到所述命名空间中以实现隔离。

[0014] 根据本发明的第五方面，提供一种计算设备，包括：至少一个处理器和存储有程序指令的存储器；当所述程序指令被所述处理器读取并执行时，使得所述计算设备执行如上所述的初始化方法、场景模式切换方法以及用户登录方法中的任一个。

[0015] 根据本发明的第六方面，提供一种存储有程序指令的可读存储介质，当所述程序指令被计算设备读取并执行时，使得所述计算设备执行如上所述的初始化方法、场景模式切换方法以及用户登录方法中的任一个。

[0016] 通过本发明的场景模式管理装置、初始化方法、场景模式切换方法以及用户登录方法，使得操作系统能够隔离不同用户的使用环境，上述技术通过命名空间隔离系统目录，使得即使相同的目录在不同的场景模式下也能够相互隔离，展示不同内容。

附图说明

[0017] 为了实现上述以及相关目的，本文结合下面的描述和附图来描述某些说明性方面，这些方面指示了可以实践本文所公开的原理的各种方式，并且所有方面及其等效方面旨在落入所要求保护的主题的范围内。通过结合附图阅读下面的详细描述，本公开的上述以及其它目的、特征和优势将变得更加明显。遍及本公开，相同的附图标记通常指代相同的部件或元素。

[0018] 图1示出根据本发明实施方式的场景模式管理装置100的示意性结构框图；

图2示出根据本发明实施方式的场景模式管理装置进行初始化的示例性处理示意图；

图3示出根据本发明实施方式的场景模式管理装置进行场景模式切换的示例性处理示意图；

图4示出根据本发明实施方式的场景模式管理装置进行用户登录的示例性处理示意图；

图5示出根据本发明一个实施方式的计算设备的示意图。

具体实施方式

[0019] 下面将参照附图更详细地描述本公开的示例性实施方式。虽然附图中显示了本公开的示例性实施方式，然而应当理解，可以以各种形式实现本公开，且本公开不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开，并且能够将本公开的范围完整地传达给本领域的技术人员。

[0020] 在现有的诸如Linux、Windows等操作系统中，多用户模式是一种简单的隔离方法，通过为不同的成员配置不同的账户，从而实现了不同账户拥有不同的家目录。在上述方法中，通常由操作系统的管理员为成员创建不同的账户，并以用户名为名来创建不同的家目录；此外，管理员可以为不同的家目录设置不同的访问控制策略，仅允许同名用户访问；而且，不同用户登录时，会使用同名的目录作为家目录，操作系统使用数据存储于此家目录中。以上方法由于当前用户不具备对其他用户的家目录的访问权限，因此不能窥视其他用户的隐私数据。

[0021] 然而，本发明人发现，上述多用户模式隔离方法仅能保证家目录的隔离，在该系统中其他的系统目录则是共用的，并不能实现应用的隔离，这是因为，应用不是安装在家目录中的；此外，该方法中的家目录是通过访问控制策略进行保护的，若用户具有管理员角色，则仍能绕过访问控制策略，窥视其它用户的隐私。

[0022] 由此，本发明的实施例提供了一种场景模式管理装置，包括：场景模式管理模块，用于提供场景模式的管理接口，场景模式包括多个预设模式；配置文件管理模块，用于对场景配置文件进行解析和修改，场景配置文件用于描述多个预设模式各自对应的待隔离系统目录；可插入认证模块，用于在用户登录操作系统时，基于接入的认证方式对用户密码进行密码认证，在密码认证通过后，在场景模式启用的情况下，响应于用户会话的开启，从场景配置文件读取当前场景模式对应的待隔离系统目录，并创建对应的命名空间，将当前场景模式对应的待隔离系统目录挂载到所创建的命名空间中以实现隔离。

[0023] 根据本发明实施方式，提供了一种场景模式管理装置。图1示出根据本发明实施方式的场景模式管理装置100的示意性框图。如图1所示，该场景模式管理装置100包括场景模式管理模块110、配置文件管理模块120和可插入认证模块130。

[0024] 如图1所示，场景模式管理模块110用于提供场景模式的管理接口，场景模式包括多个预设模式。

[0025] 管理接口例如包括启用接口和切换接口，用于进行场景模式的启用和切换，其中，场景模式的切换接口仅在用户输入口令通过身份验证(即，用户输入口令与管理员预先设置的初始口令一致)的情况下允许使用。此外，管理接口也可以包括其他功能接口，这里不

再赘述。

[0026] 在本发明的实施例中，配置文件管理模块120用于对场景配置文件进行解析，可选地，还可以对场景配置文件进行修改。

[0027] 场景配置文件是用于描述多个预设模式各自对应的待隔离系统目录的文件。当然，除了描述多个预设模式各自对应的待隔离系统目录之外，场景配置文件中也可以包含描述其他信息的内容。

[0028] 作为示例，场景配置文件可以是YAML格式的配置文件，用于场景模式的启用和切换。

[0029] 根据本发明的实施例，在场景配置文件中，例如可以包含当前场景配置文件的版本信息。

[0030] 此外，在场景配置文件中，例如可以包含场景模式的状态信息，例如启用或未启用。

[0031] 根据本发明的实施例，在场景配置文件中，例如可以包括当前场景模式以及对应的隔离的系统目录，即待隔离系统目录。其中，当前场景模式是多个预设模式之一。

[0032] 在一个例子中，一个场景配置文件可以包含所有的预设模式及每个预设模式对应的待隔离系统目录，这样，通过修改场景配置文件中的当前场景模式，便可以通过读取一个场景配置文件来确定当前场景模式的待隔离系统目录。

[0033] 在另一个例子中，也可以通过不同的场景配置文件来描述不同预设模式。比如，第一场景配置文件用于描述第一预设模式及其对应的待隔离系统目录，第二场景配置文件用于描述第二预设模式及其对应的待隔离系统目录，等等。这样，通过另一个用于描述当前场景模式的配置文件(例如，该文件中的当前场景模式可以被修改为上述多个预设模式中的任一个)，再结合对应预设模式的场景配置文件，便可以确定当前场景模式的待隔离系统目录。

[0034] 根据本发明的实施例，在场景配置文件中，可以通过系统目录原路径、系统目录隔离路径前缀、忽略目录隔离的用户列表以及隔离后执行的脚本这四个方面来描述待隔离系统目录。例如，对于任一待隔离系统目录A_x(以下简称目录A_x)，可以通过定义目录A_x的原路径、目录A_x的隔离路径前缀、忽略目录A_x隔离的用户列表以及隔离后执行的脚本这四个方面来描述。

[0035] 此外，根据本发明的实施例，在场景配置文件中还可以设置场景模式的个性化配置，例如，个性化配置可以包括模式名称、最大系统使用时间(即允许使用的最长时间)、防火墙设置等。

[0036] 根据本发明的实施例，待隔离系统目录中的系统目录可以是一个，也可以是多个。

[0037] 根据本发明的实施例，待隔离系统目录可以是预定系统目录中的一种或多种。预定系统目录可以包括但不限于：家目录；已安装应用的系统目录；网络配置的系统目录；及防火墙系统目录等。

[0038] 此外，根据本发明的实施例，多个预设模式可以是老年模式、青少年模式、工作模式、娱乐模式及维护模式等模式中的任一种或多种。

[0039] 在老年模式下，仅第一应用白名单上的应用可被使用，而该第一应用白名单之外的应用则被禁止使用；不允许安装应用，也不允许卸载应用(例如，可以将应用商店、应用安

装器列入黑名单),防止老人受到恶意应用的侵害;配置防火墙并拒绝访问恶意网站,恶意网站例如是预设的,或者经检测或其他方式获取的。其中,第一应用白名单是老年模式对应的应用白名单,第一应用白名单上所包含的应用名单可以根据经验或实际需求所设置。

[0040] 在青少年模式下,仅第二应用白名单上的应用可被使用,而该第二应用白名单之外的应用被禁止使用;不允许安装应用,也不允许卸载应用(例如,可以将应用商店、应用安装器列入黑名单),防止青少年受到恶意应用的侵害;配置防火墙并拒绝访问恶意网站;恶意网站例如是预设的,或者经检测或其他方式获取的。其中,第二应用白名单是青少年模式对应的应用白名单,第二应用白名单上所包含的应用名单可以根据经验或实际需求所设置。

[0041] 在工作模式下,默认启用VPN连接并监控VPN的连接状态,若VPN离线时长超过预设值则注销操作系统,防止数据泄露;配置防火墙并禁止访问游戏网站和恶意网站;游戏网站和/或恶意网站例如是预设的,或者经检测或其他方式获取的。其中,预设值例如可以根据经验设定,或者通过试验的方法确定,这里不再详述。

[0042] 在娱乐模式下,默认开启显示增强和高性能模式,提升娱乐体验。

[0043] 此外,维护模式用于用户设备维护时的数据隔离;如返厂维修时,可以切换至此模式,这样即可在不影响维修人员操作的情况下,保护用户的数据。

[0044] 除此之外,对于上述各种模式,也可以个性化设置或更改每种模式对应的待隔离系统目录以及个性化配置等。

[0045] 作为示例,不同预设模式对应的待隔离系统目录可以是相同的,也可以是不同的。

[0046] 在一个例子中,任意两个不同预设模式对应的待隔离系统目录可以是不同的,如第一预设模式对应的待隔离系统目录为A1、A2和A3,而第二预设模式对应的待隔离系统目录为A1、A2和A4;又如,第一预设模式对应的待隔离系统目录为A1、A2和A3,而第二预设模式对应的待隔离系统目录为A4、A5和A6。

[0047] 在另一个例子中,所有预设模式对应的待隔离系统目录可以是相同的,如各预设模式对应的待隔离系统目录均为A1、A2和A3。

[0048] 这样,即使是对于相同的系统目录,在不同的场景模式下也能够相互隔离,展示不同内容。

[0049] 下面给出场景配置文件的一个示例性描述,该示例的场景配置文件的定义及含义如下所示:

```
# 配置文件版本
version: 1.0
# 场景模式是否启用
enabled: true
# 当前场景模式,可用值为:娱乐模式(normal)、老年模式(oldage)、工作模式(work)、青少年模式(child)、维护模式(maintenance)
scene_mode: "normal"
# 隔离的系统目录,可配置多个
poly_dirs:
  -
```

```
    # 系统目录原路径
    poly_dir: "/usr/share/applications"
    # 系统目录隔离路径前缀
    poly_inst_dir: "/usr/share/applications.inst/"
    # 忽略目录隔离的用户列表
    ignore_user: "root,lightdm"
    # 隔离后执行的脚本
    hooks:
      -
        "app_white.sh"
  -
    poly_dir: "$HOME"
    poly_inst_dir: "$HOME/$USER.inst/"
    ignore_user: "root,lightdm"
# 模式个性化配置
mode_list:
  -
    # 模式名称
    name: "normal"
    # 最大系统使用时间
    max_usage_time: 0
    # 防火墙
    firewall:
      - "-t mangle -D OUTPUT -j SCENE"
      - "-t mangle -F SCENE"
      - "-t mangle -X SCENE"
```

根据本发明的实施例,当用户登录操作系统时,系统会请求(或提示)用户输入密码,系统接收该密码作为用户密码,可插入认证模块130能够基于接入的认证方式对上述用户密码进行密码认证;在密码认证通过后,在场景模式启用的情况下,响应于用户会话的开启,可插入认证模块130从场景配置文件读取当前场景模式对应的待隔离系统目录,并创建对应的命名空间,将当前场景模式对应的待隔离系统目录挂载到所创建的命名空间中以实现隔离。

[0050] 根据本发明的实施例,若可插入认证模块130对用户密码进行密码认证失败,则用户无法完成登录。

[0051] 在本发明的实施例中,可插入认证模块130可以是一个实现了PAM(Pluggable Authentication Modules,可插入认证模块)会话接口的PAM模块,用于在用户登录时配置多目录隔离环境;换句话说,可插入认证模块130可以采用一个具有会话接口的PAM模块来实现。用户会话开启时,可插入认证模块130可以从场景配置文件读取待隔离的系统目录,在场景模式开启的情况下,创建命名空间(namespace),并将配置的目录挂载(mount)到此

命名空间中,实现目录隔离。

[0052] 其中,PAM是一种认证框架,其可通过提供的API接入任意的认证方式。而命名空间是一种内核级别环境隔离的方法,提供了对UTS、IPC、mount、PID、network、User等系统目录的隔离机制。

[0053] 这样,在场景模式启用、且已选取多个预设模式之一作为当前场景模式的情况下,可插入认证模块130能够根据场景配置文件来为用户配置当前场景模式对应的隔离环境。

[0054] 作为示例,可以使用unshare(CLONE_NEWNS)函数来创建命名空间,或者可以采用其他方式来创建,这里不再赘述。

[0055] 需要说明的是,在诸如Linux等操作系统中,可以使用命名空间来表示从不同进程角度所见的视图。不同的命名空间的进程所看到的资源或进程表是不同的;而相同命名空间中的不同进程看到的则是同样的资源。

[0056] 例如,mnt namespace(mnt 命名空间)可为进程提供独立的文件系统视图。当clone 函数或 unshare 函数中带有 CLONE_NEWNS 标志时,新的 mount namespace(mount命名空间)在子进程中被创建。新的 mount namespace 是一份父 mount namespace 的拷贝,但是在子进程中调用mount安装的文件系统,将独立于父进程的 mount namespace ,只出现在新的 mount namespace 上。

[0057] 基于上述原理,当用户会话开启时,使用带 CLONE_NEWNS 的 unshare 函数创建用户会话进程,则用户会话进程就会拥有独立的 mount namespace ,即独立的文件系统。随后在用户会话进程中执行待隔离目录的 mount 操作,即让用户会话拥有隔离的文件系统。

[0058] 根据本发明的实施例,场景模式管理装置100还可以包括口令验证模块140和用户界面模块150中的至少一个。

[0059] 需要说明的是,图1中虚线框表示对应的模块是可选的,而非必须的。

[0060] 作为示例,在场景模式管理装置首次启动时,口令验证模块140请求用户设置口令,并接收用户所设置的口令作为初始口令。

[0061] 此外,响应于用户的场景模式切换请求(作为场景模式管理的示例),口令验证模块140提示用户输入一个口令,基于初始口令对用户输入的口令进行身份验证,在用户输入的口令通过身份验证的情况下,允许用户使用管理接口进行场景模式切换(作为场景模式管理的示例)。

[0062] 例如,当用户输入的口令与初始口令一致时,判定用户输入的口令通过身份验证;而当用户输入的口令与初始口令不一致时,判定用户输入的口令未通过身份验证。

[0063] 其中,初始口令例如可以是预存在口令验证模块140中的。或者,初始口令也可以是场景模式管理装置进行场景切换功能初始化时,由管理员设置的。

[0064] 用户界面模块150是一个图形界面,用于提供不同预设模式供用户(如管理员)选择。

[0065] 图2示出了根据本发明实施例的场景模式管理装置进行场景切换功能初始化的处理流程。

[0066] 如图2所示,场景模式管理装置首次启动时,需要配置口令,用于场景模式管理(例如场景模式切换)时的身份验证。

[0067] 进行场景切换功能初始化的用户作为管理员用户(以下简称为管理员),其开启场景模式切换功能时,场景模式切换界面(相当于下文中的用户界面模块)请求管理员设置口令,管理员设置的口令作为初始口令;对该初始口令进行摘要计算,以获得相应的口令摘要,作为初始口令摘要,其中,摘要计算的过程例如可以采用现有的任一种摘要计算方法实现,这里不再赘述。场景模式切换界面将得到的初始口令摘要发送至场景模式切换服务进行保存,以完成场景模式切换功能的开启;场景模式切换服务将开启结果通过场景模式切换界面返回给管理员。

[0068] 需要说明的是,图2所示的场景模式切换服务例如是指根据本发明实施例的场景模式管理装置中除去下文描述的用户界面模块之外的其他组成部分;换句话说,若将根据本发明实施例的用户界面模块看作两部分组成,一部分是用户界面模块,另一部分则是除了用户界面模块之外的所有其他模块。

[0069] 这样,初始口令摘要可以由口令验证模块来保存,或者也可由场景模式管理装置中诸如场景模式管理模块等的其他模块保存。

[0070] 上述开启结果例如为开启成功或开启失败。例如,可预设一些限制条件(字符限制、字数限制等)来判定是否开启成功;换句话说,符合预设限制条件的口令所得到的口令摘要能够成功开启场景模式切换功能,而不符合上述预设限制条件的口令所得到的口令摘要则不能开启该功能。此外,也可以采用其他方式来判定是否开启成功,这里不再赘述。

[0071] 这样,在管理员设置好初始口令后(或者初始口令已预存),当用户想要切换当前场景模式时,需要输入口令来验证其身份,也即,验证其是否为管理员或管理员授权的用户;若其口令与初始口令(如初始化时管理员设置的口令)一致,则通过验证,否则验证失败。若验证失败,则不允许切换场景模式,只有验证通过才允许切换场景模式,以此保证场景模式仅授权通过后才可修改。

[0072] 应当理解的是,在其他示例中,用户界面模块所执行的处理也可由场景模式管理装置中诸如场景模式管理模块等的其他模块来执行,并能够达到相同的功能和效果。例如,用户界面模块请求用户设置口令的处理,也可以通过场景模式管理模块或其他模块来实现,比如场景模式管理模块或其他模块可设有诸如键盘(可以是电脑键盘或其他实体键盘)以供用户输入(或设置)口令,可选地,该键盘可以设有提示灯来提示用户何时输入(或设置),等等。

[0073] 图3给出了切换场景模式的一个示例性处理流程。

[0074] 如图3所示,某用户(如图3所示的管理员,或者也可能是其他用户)想要切换当前场景模式,场景模式切换界面请求该用户输入口令以进行验证。例如,可以通过上文所述的摘要计算方法来对本次用户输入的口令进行计算,将本次得到的口令摘要与初始口令所对应的口令摘要(即初始口令摘要)进行验证比对,若一致,验证成功;否则,验证失败。

[0075] 当验证失败时,切换失败,即不允许该用户进行场景模式的切换。

[0076] 当验证成功时,允许该用户进行场景模式切换。

[0077] 图4示出了用户登录操作系统的一个示例性处理流程。

[0078] 如图4所示,当用户登录操作系统时,PAM认证模块对用户输入的密码进行验证。例如,利用接入的认证方式对应算法对该密码进行摘要计算,得到对应的密码摘要,再对该密码摘要进行验证:若密码验证未通过,认证失败,无法登录;若密码验证通过,认证成功(即

认证通过),PAM认证模块开启会话,PAM会话模块创建会话,并通过场景模式PAM会话模块来读取场景配置文件,以得到对应的目录列表(即对应的待隔离系统目录)。

[0079] 在得到上述目录列表后,例如通过unshare命令(或其他命令或系统调用)来创建命名空间,以将上述目录列表中的所有目录挂载到新创建的上述命名空间中,实现对这些目录的隔离,从而完成用户登录。

[0080] 需要说明的是,在图4所示例子中,PAM认证模块、PAM会话模块和场景模式PAM会话模块这三个模块的功能可由上文所述的可插入认证模块来实现。例如,可以在可插入认证模块中设置三个子模块,即第一子模块、第二子模块和第三子模块,这样,将PAM认证模块的功能和处理通过第一子模块实现,将PAM会话模块的功能和处理通过第二子模块实现,将场景模式PAM会话模块的功能和处理通过第三子模块实现。

[0081] 上述根据本发明实施例的场景模式管理装置,其利用命名空间特性,将对应的待隔离系统目录挂载到创建的命名空间中,实现目录的隔离;此外,通过实现的钩子(hooks)机制,可自定义在不同场景模式下待隔离系统目录的内容,满足个性化和安全管理要求。

[0082] 本发明的实施例还提供了一种场景模式管理方法,上述场景模式包括多个预设模式,场景模式管理方法包括:当用户登录操作系统时,在场景模式启用并已选取多个预设模式之一作为当前场景模式的情况下,通过解析场景配置文件来确定当前场景模式对应的待隔离系统目录,以配置当前场景模式对应的隔离环境;其中,场景模式的管理接口包括启用接口和切换接口,用于进行场景模式的启用和切换,切换接口仅在用户输入口令通过身份验证的情况下允许使用;场景配置文件用于描述多个预设模式各自对应的待隔离系统目录。

[0083] 在该方法中,当用户登录操作系统时,在场景模式启用并已选取多个预设模式之一作为当前场景模式的情况下,通过解析场景配置文件来确定当前场景模式对应的待隔离系统目录,以配置当前场景模式对应的隔离环境。

[0084] 其中,场景模式的管理接口包括启用接口和切换接口,用于进行场景模式的启用和切换,切换接口仅在用户输入口令通过身份验证的情况下允许使用;场景配置文件用于描述多个预设模式各自对应的待隔离系统目录。

[0085] 作为示例,在通过解析场景配置文件来确定当前场景模式对应的待隔离系统目录之前,还可以包括:基于可插入认证模块所接入的认证方式,对用户密码进行认证。

[0086] 作为示例,可以通过如下方式来配置当前场景模式对应的隔离环境:在对用户密码认证通过的情况下,响应于用户会话的开启,从场景配置文件读取当前场景模式对应的待隔离系统目录,创建对应的命名空间,将当前场景模式对应的待隔离系统目录挂载到所创建的命名空间中以实现隔离。

[0087] 作为示例,待隔离系统目录可以包括一个或多个系统目录。

[0088] 作为示例,待隔离系统目录可以包括以下至少一个:家目录;已安装应用系统目录;网络配置系统目录;及防火墙系统目录。

[0089] 作为示例,多个预设模式可以包括以下至少一个:老年模式,在该模式下,第一应用白名单之外的应用被禁止使用,应用安装和卸载功能被禁止,配置防火墙并拒绝访问恶意网站;青少年模式,在该模式下,第二应用白名单之外的应用被禁止使用,应用安装和卸载功能被禁止,配置防火墙并拒绝访问恶意网站;工作模式,在该模式下,默认启用VPN连接

并监控VPN的连接状态，若VPN离线时长超过预设值则注销操作系统，配置防火墙并禁止访问游戏网站和恶意网站；娱乐模式，在该模式下，默认开启显示增强和高性能模式；及维护模式，该模式用于用户设备维护时的数据隔离。

[0090] 作为示例，上述场景模式管理方法还可以包括：首次启动时，提示用户设置口令，并将所设置的口令用于所述身份验证。

[0091] 根据本发明实施方式的场景模式管理方法的未详述部分，还请参考以上关于装置实施方式的具体描述。

[0092] 根据本发明实施例的一种场景模式管理装置及场景模式管理方法，其提供了一种基于命名空间的场景模式切换技术，预设不同的场景模式，如老年模式、工作模式、娱乐模式、青少年模式、维护模式等，通过命名空间隔离系统目录，使得相同的目录在不同的模式下相互隔离，展示不同的内容。

[0093] 本发明的上述技术可配置多个系统目录作为待隔离系统目录，能够为不同模式提供完整的隔离环境，包括但不限于家目录、已安装应用、网络配置、防火墙等。

[0094] 本发明的上述技术使用命名空间隔离系统目录，确保了不同场景模式下系统目录的隔离，即使拥有管理员权限也无法查看其它模式下的数据。

[0095] 本发明的上述技术可配置多种场景模式，能满足不同成员以及返厂维修的需求。

[0096] 此外，本发明的上述技术使用的是单用户，能够避免多用户的管理问题。

[0097] 本发明的实施例还提供了一种初始化方法，初始化方法通过如上所述的场景模式管理装置执行。该初始化方法与上文结合图2描述的场景模式管理装置进行初始化的示例性处理相类似，并能够达到相似的技术效果。

[0098] 参见图2，在该初始化方法中，当场景模式管理装置首次启动时，请求用户设置口令，并接收用户所设置的口令作为初始口令。

[0099] 接着，根据初始口令获得对应的初始口令摘要。

[0100] 保存初始口令摘要，并开启场景模式切换功能。

[0101] 此外，本发明的实施例还提供了一种场景模式切换方法，场景模式切换方法通过如上所述的场景模式管理装置执行。该场景模式切换方法与上文结合图3描述的场景模式管理装置进行场景模式切换的示例性处理相类似，并能够达到相似的技术效果。

[0102] 参见图3，响应于用户的场景模式切换请求，提示用户输入口令，并接收用户输入的口令。

[0103] 接着，根据用户输入的口令获得对应的用户口令摘要。

[0104] 然后，根据初始口令摘要验证用户口令摘要。

[0105] 若用户口令摘要与初始口令摘要一致，验证通过，允许该用户的场景模式切换请求。

[0106] 若用户口令摘要与初始口令摘要不一致，验证失败，拒绝该用户的场景模式切换请求(如图3中alt标签对应项)。

[0107] 此外，本发明的实施例还提供了一种用户登录方法，用户登录方法通过如上所述的场景模式管理装置执行。该用户登录方法与上文结合图4描述的场景模式管理装置进行用户登录的示例性处理相类似，并能够达到相似的技术效果。

[0108] 参见图4，响应于用户的系统登录请求，提示用户输入密码。

[0109] 接收用户输入的密码，并对该密码进行摘要计算，得到对应的密码摘要。

[0110] 然后，利用密码摘要进行密码验证。

[0111] 若密码验证未通过，拒绝用户的系统登录请求(如图4中alt标签对应项)。

[0112] 若密码验证通过，允许用户的系统登录请求，开启并创建会话后，读取场景配置文件以获得对应的待隔离系统目录，创建命名空间，将待隔离系统目录挂载到命名空间中以实现隔离。

[0113] 需要说明的是，图3和图4中的alt标签表示对应的替换项，也即表示备选项。

[0114] 在根据本发明实施例的上述场景模式管理装置和上述各方法中，操作系统例如可以是Linux操作系统，或者可以是能够应用上述场景模式管理装置和各方法的其他任意操作系统。

[0115] 本发明的各方法可以在计算设备中执行。计算设备可以是具有存储和计算能力的任意设备，其例如可以实现为服务器、工作站等，也可以实现为桌面计算机、笔记本计算机等个人配置的计算机，或者实现为手机、平板电脑、智能可穿戴设备、物联网设备等终端设备，但不限于此。

[0116] 图5示出了根据本发明一个实施方式的计算设备的示意图。需要说明的是，图5所示的计算设备仅为一个示例，在实践中，用于实施本发明的方法的计算设备可以是任意型号的设备，其硬件配置情况可以与图5所示的计算设备相同，也可以与图5所示的计算设备不同。相对于图5所示的计算设备的硬件组件，实践中用于实施本发明的方法的计算设备的硬件组件可以有所增加或删减。本发明对计算设备的具体硬件配置情况不做限制。

[0117] 如图5所示，该设备可以包括：处理器510、存储器520、输入/输出接口530、通信接口540和总线550。其中处理器510、存储器520、输入/输出接口530和通信接口540通过总线550实现彼此之间在设备内部的通信连接。

[0118] 处理器510可以采用通用的CPU(Central Processing Unit，中央处理器)、微处理器、应用专用集成电路(Application Specific Integrated Circuit，ASIC)、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[0119] 存储器520可以采用ROM(Read Only Memory，只读存储器)、RAM(Random Access Memory，随机存取存储器)、静态存储设备，动态存储设备等形式实现。存储器520可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器520中，并由处理器510来调用执行。

[0120] 输入/输出接口530用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中(图中未示出)，也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[0121] 通信接口540用于连接通信模块(图中未示出)，以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式(例如USB、网线等)实现通信，也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信。

[0122] 总线550包括一通路，在设备的各个组件(例如处理器510、存储器520、输入/输出接口530和通信接口540)之间传输信息。

[0123] 需要说明的是，尽管上述设备仅示出了处理器510、存储器520、输入/输出接口

530、通信接口540以及总线550，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[0124] 本发明实施方式还提供一种非暂态可读存储介质，其存储有指令，该指令用于使计算设备执行根据本发明实施方式的方法。本实施例的可读介质包括永久性和非永久性、可移动和非可移动介质，可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。可读存储介质的例子包括但不限于：相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带、磁带磁盘存储等。

[0125] 在此处所提供的说明书中，算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与本发明的示例一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的优选实施方式。

[0126] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施方式可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0127] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施方式的描述中，本发明的各个特征有时被一起分组到单个实施方式、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。本领域技术人员应当理解在本文所公开的示例中的设备的模块或单元或组件可以布置在如该实施方式中所描述的设备中，或者可替换地可以定位在与该示例中的设备不同的一个或多个设备中。前述示例中的模块可以组合为一个模块或者此外可以分成多个子模块。

[0128] 本领域技术人员可以理解，可以对实施方式中的设备中的模块进行自适应性地改变并且把它们设置在与该实施方式不同的一个或多个设备中。可以把实施方式中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除非这样的特征和/或过程或者单元中的至少一些相互排斥，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的替代特征来代替。

[0129] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施方式包括其它实施方式中所包括的某些特征而不是其它特征，但是不同实施方式的特征的组合意味着处于本发明的范围之内并且形成不同的实施方式。此外，所述实施方式中的一些在此被描述成可以由计算机系统的处理器或者由执行所述功能的其它装置实施的方法或方法元素的组合。因此，具有用于实施所述方法或方法元素的必要指令的处理器形成用于实施该方法或方法元素的装置。

[0130] 如在此所使用的那样，除非另行规定，使用序数词“第一”、“第二”、“第三”等等来描述普通对象仅仅表示涉及类似对象的不同实例，并且并不意图暗示这样被描述的对象必须具有时间上、空间上、排序方面或者以任意其它方式的给定顺序。

[0131] 尽管根据有限数量的实施方式描述了本发明，但是受益于上面的描述，本技术领域内的技术人员明白，在由此描述的本发明的范围内，可以设想其它实施方式。此外，应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。

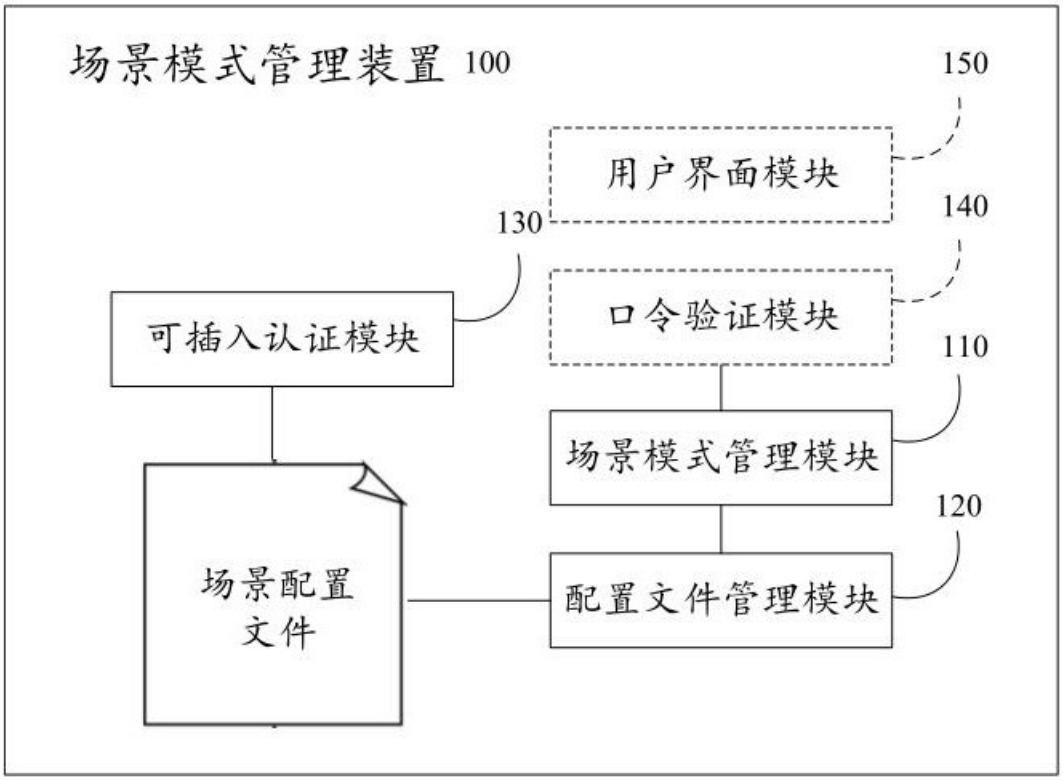

场景模式管理装置 100
150
用户界面模块
140
130
口令验证模块
可插入认证模块
110
场景模式管理模块
120
场景配置
文件
配置文件管理模块

图1

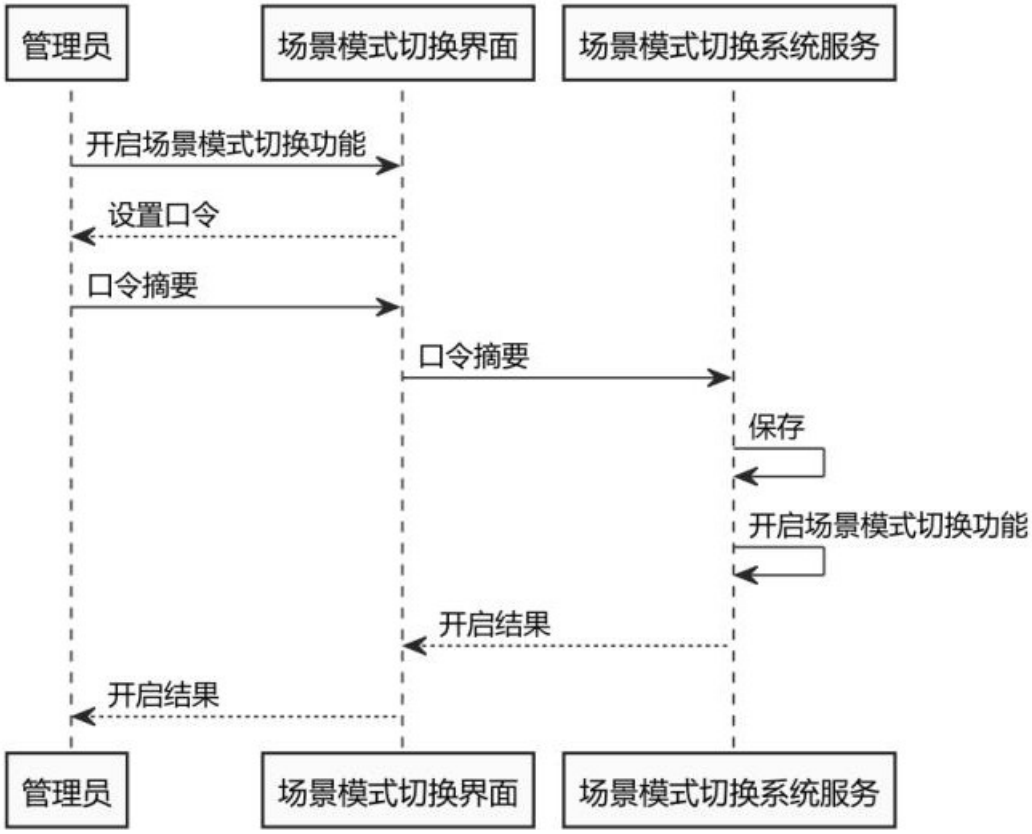

管理员
场景模式切换界面
场景模式切换系统服务
开启场景模式切换功能
设置口令
口令摘要
口令摘要
保存
开启场景模式切换功能
开启结果
开启结果
管理员
场景模式切换界面
场景模式切换系统服务

图2

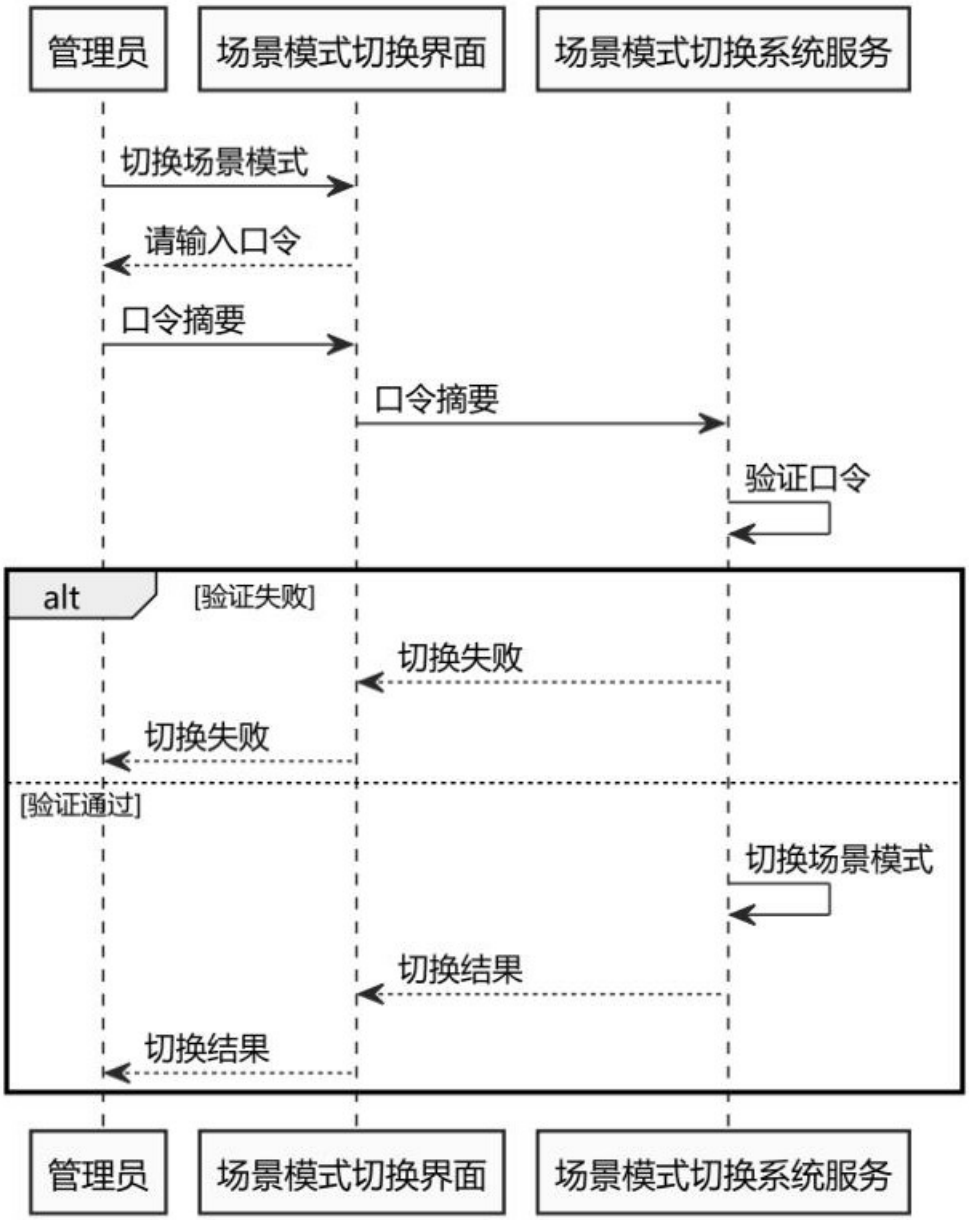

管理员
场景模式切换界面
场景模式切换系统服务
切换场景模式
请输入口令
口令摘要
口令摘要
验证口令
alt
[验证失败]
切换失败
切换失败
[验证通过]
切换场景模式
切换结果
切换结果
管理员
场景模式切换界面
场景模式切换系统服务

图3

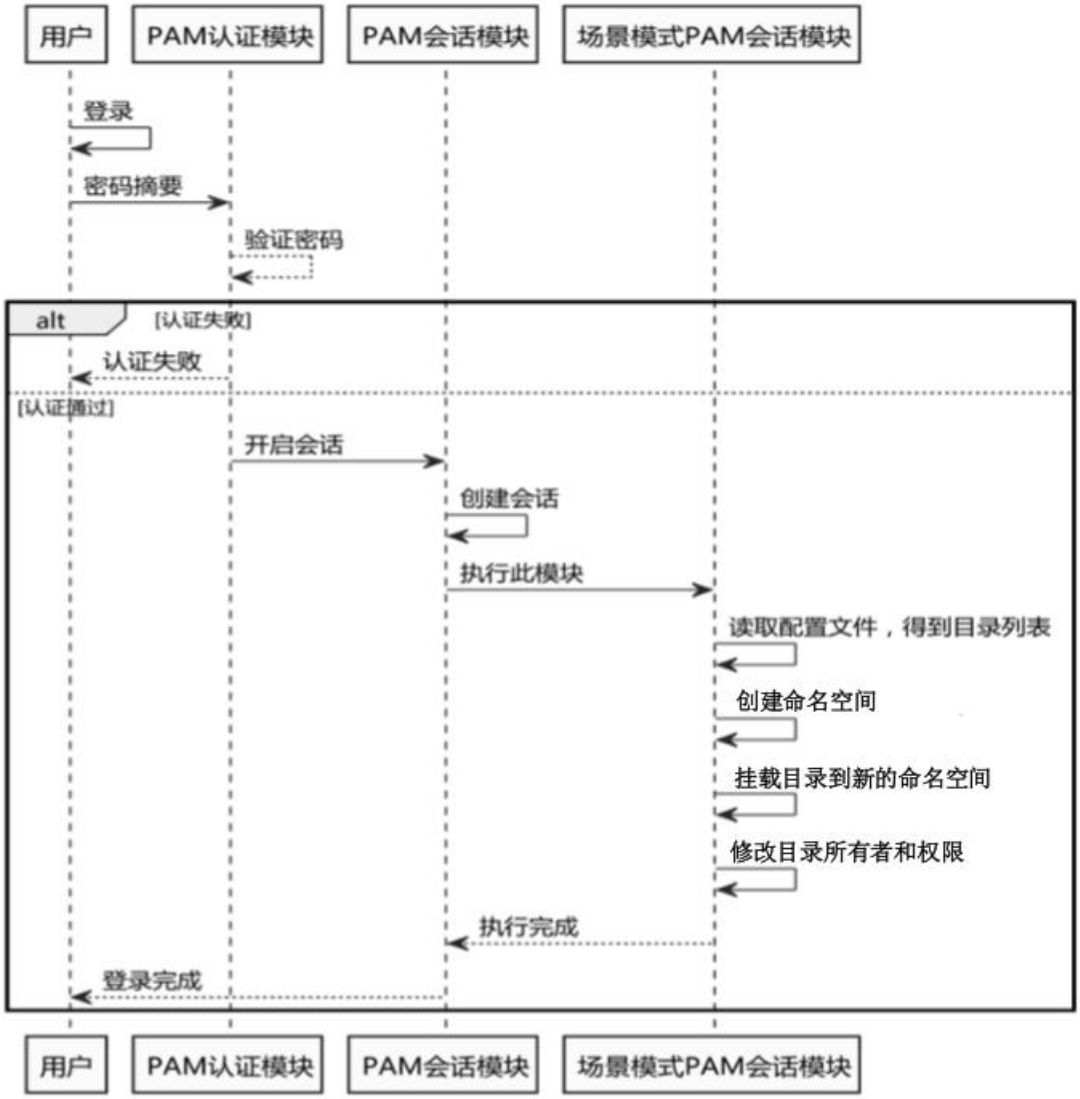

用户
PAM认证模块
PAM会话模块
场景模式PAM会话模块
登录
密码摘要
验证密码
alt
[认证失败]
认证失败
[认证通过]
开启会话
创建会话
执行此模块
读取配置文件，得到目录列表
创建命名空间
挂载目录到新的命名空间
修改目录所有者和权限
执行完成
登录完成
用户
PAM认证模块
PAM会话模块
场景模式PAM会话模块

图4

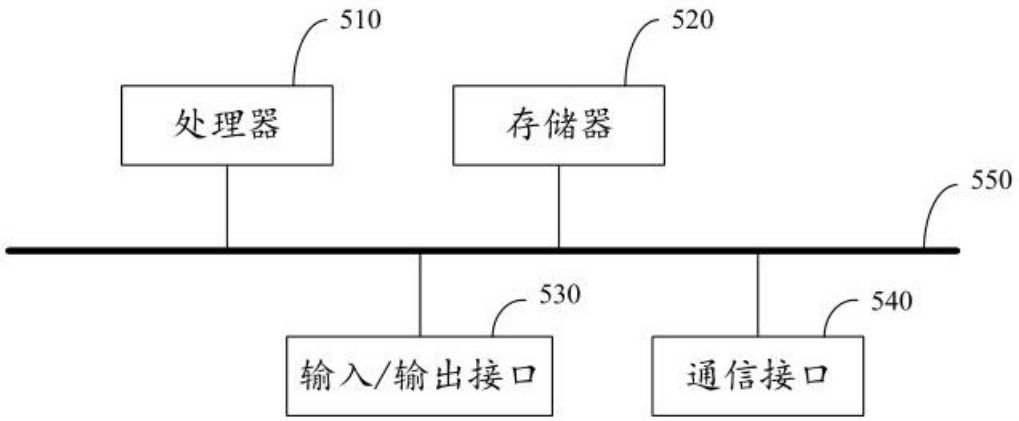

510
520
处理器
存储器
550
530
540
输入/输出接口
通信接口

图5