(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 105830477 A
(43)申请公布日 2016.08.03

(21)申请号 201480054937.5

(22)申请日 2014.08.11

(30)优先权数据
61/864,899 2013.08.12 US
62/026,272 2014.07.18 US

(85)PCT国际申请进入国家阶段日
2016.04.05

(86)PCT国际申请的申请数据
PCT/CA2014/050761 2014.08.11

(87)PCT国际申请的公布数据
WO2015/021547 EN 2015.02.19

(71)申请人 哥莱菲特软件公司
地址 加拿大安大略

(72)发明人 亚历山大·詹姆斯·迈因
詹姆士·亨利·阿兰·普德雷尔

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 柴德海 康泉

(51)Int.Cl.
H04W 12/08(2006.01)
G06F 21/44(2006.01)
G06F 9/445(2006.01)
H04W 4/00(2006.01)

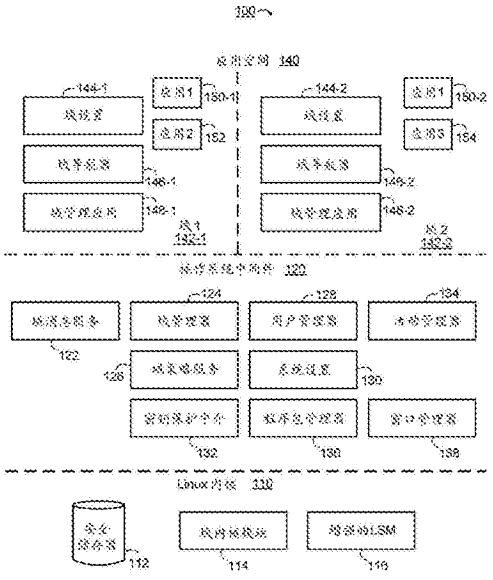
权利要求书5页 说明书20页 附图7页

(54)发明名称

集成操作系统的域管理

(57)摘要

一种提供多个安全域的计算设备操作系统。域管理器选择性地创建多个安全域，并且选择多个安全域中的一个作为当前域。域策略服务针对每个安全域存储并执行包括规则集的策略，该规则集控制与该域关联的文件和应用的访问。程序包管理器针对每个安全域执行与该域关联的应用的安装。域消息服务提供与多个安全域中的不同安全域关联的运行进程之间的通信。活动管理器选择性地切换当前域。实现了域隔离，同时启用了提供对多个域的资源的并行访问的统一用户界面。



CN 105830477 A

1.一种移动设备，所述移动设备包括处理器和存储指令的存储器，所述指令由所述处理器可执行以实现安卓操作系统，在所述移动设备中，改进包括：

用户管理器，用于选择性地创建与在所述安卓操作系统中实现的任何用户账户不同的多个域；

域管理器，用于选择所述多个域中的一个作为当前域；

域策略服务，用于针对每个域存储和执行包括规则集的策略，所述规则集控制对与该域关联的文件和应用的访问；

程序包管理器，用于针对每个域，基于该域的策略和所述当前域的策略，选择性地允许或阻止与该域关联的应用的安装或执行；

域消息服务，用于基于所述多个域中不同的域的相应策略，提供与所述多个域中所述不同的域关联的运行进程之间的通信；以及

活动管理器，用于选择性地切换所述当前域，

其中所述用户管理器、所述域管理器、所述域策略服务、所述程序包管理器、所述域消息服务以及所述活动管理器在所述安卓操作系统中在所述安卓操作系统的内核以外实现。

2.根据权利要求1所述的移动设备，其中所述改进进一步包括：

域内核模块，用于针对每个域执行与该域关联的策略，

其中所述域内核模块在所述安卓操作系统的所述内核中实现。

3.一种由计算设备的处理器实施的方法，所述方法用于在所述计算设备的操作系统中提供多个安全域，所述方法包括：

(a)针对每个安全域：

(a1)将该安全域的资源与唯一域标识符关联，该资源包括至少一个数据文件或至少一个应用；以及

(a2)与所述唯一域标识符关联地存储策略，该策略包括用于控制对该资源的访问的规则集；

(b)接收所述多个安全域中选择的一个作为当前域，其中所述多个安全域包括与所述当前域不同的目标域；以及

(c)基于与所述当前域关联的策略和/或与所述目标域关联的策略，控制对目标域资源的访问。

4.根据权利要求3所述的方法，进一步包括：

至少部分地在所述操作系统的内核之外执行所述操作系统的至少一个服务，以实施(a)、(b)和(c)中的至少一个。

5.根据权利要求3所述的方法，其中至少部分地由在所述操作系统的内核中操作的第一服务以及至少部分地由在所述操作系统的位于所述内核之外的中间件中操作的第二服务实施(c)。

6.根据权利要求5所述的方法，其中由在所述操作系统的位于所述内核之外的所述中间件中操作的其它服务实施(a)和(b)。

7.根据权利要求3所述的方法，其中所述操作系统实现多个用户账户，并且其中所述当前域和所述目标域共同地与所述多个用户账户中的一个关联。

8.根据权利要求3所述的方法，其中(c)包括：基于与所述当前域关联的策略和与所述

目标域关联的策略，控制进程对所述目标域资源的访问，其中所述进程与所述当前域关联。

9.根据权利要求8所述的方法，其中所述进程基于所述当前域的所述唯一域标识符与执行环境标识符关联，并且其中(c)包括基于所述执行环境标识符，控制所述程序对所述目标域资源的访问。

10.根据权利要求9所述的方法，其中所述当前域资源包括所述至少一个应用，并且其中所述执行环境标识符基于所述当前域的所述唯一域标识符和与为生成所述进程而执行的所述至少一个应用关联的唯一应用标识符。

11.根据权利要求10所述的方法，其中所述操作系统是安卓操作系统，所述唯一应用标识符是在安装时分配给所述应用的Unix型用户标识符(UID)，所述执行环境标识符包括所述应用的所述UID，并且所述唯一域标识符包含在所述UID的保留位中。

12.根据权利要求3所述的方法，其中所述操作系统提供用户界面，该用户界面提供对所述当前域资源的资源和所述目标域的资源的并行访问。

13.根据权利要求12所述的方法，其中所述目标域的资源包括与所述目标域关联的所述至少一个应用，并且其中所述用户界面提供用于执行所述至少一个应用的方式。

14.根据权利要求13所述的方法，其中所述用户界面实现与所述目标域的所述至少一个应用关联的图标，其中所述图标包括表示所述至少一个应用与所述目标域的关联的覆盖。

15.根据权利要求12所述的方法，其中所述目标域的资源进一步包括接收到的与所述目标域关联的消息，并且其中所述用户界面提供用于打开所述消息的方式。

16.根据权利要求3所述的方法，其中(a1)包括存储将所述资源与所述安全域的所述唯一域标识符关联的元数据。

17.根据权利要求3所述的方法，其中所述安全域中的一个是外部地控制的域，并且其中经由网络从远程域管理服务器接收与所述外部地控制的域关联的策略。

18.根据权利要求17所述的方法，其中所述当前域是所述外部地控制的域，并且其中所述远程域管理服务器将对与所述当前域关联的策略的至少一部分的修改阻挡在外。

19.根据权利要求3所述的方法，其中所述目标域资源包括以下所述至少一个应用：该至少一个应用包含公共应用的第一版本，与所述当前域关联的策略和与所述目标域关联的策略阻止对所述公共应用的所述第一版本的访问。

20.根据权利要求19所述的方法，其中所述当前域资源包括以下所述至少一个应用：该至少一个应用包含所述公共应用的与所述公共应用的第一版本不同的第二版本。

21.一种计算机可读介质，包括在所述计算机可读介质上存储的指令，该指令在由计算机执行时实施根据权利要求3所述的方法。

22.一种在计算设备的操作系统中提供多个安全域的方法，所述方法包括：

(a)针对每个安全域：

(a1)将所述安全域的资源与关联于所述安全域的唯一域标识符关联，所述资源包括至少一个数据文件或至少一个应用；以及

(a2)与所述唯一域标识符关联地存储策略，所述策略包括用于控制对所述资源的访问的规则集；

(b)生成与关联于所述多个安全域中的第一安全域的初始进程关联的事件消息；

(c)确定与所述多个安全域中的第二安全域关联的目标进程被配置为对所述事件消息做出响应;

(d)基于与所述第一域关联的策略和与所述第二域关联的策略,处理所述事件消息,以产生处理的事件消息;以及

(e)基于与所述第一域关联的策略和与所述第二域关联的策略,向所述目标进程传递所处理的事件消息或对所述目标进程组织阻止所处理的事件消息。

23.根据权利要求22所述的方法,其中所述事件消息指示由所述初始进程生成的复制并粘贴动作,与所述第一域关联的策略实现允许将剪贴板缓冲区传递至所述第一域之外的第一规则,并且与所述第二域关联的策略实现允许将所述剪贴板缓冲区传递至所述第二域内的第二规则,其中向所述目标进程传递基于所述剪贴板缓冲区的所处理的事件消息。

24.根据权利要求22所述的方法,其中所述事件消息指示由所述初始进程生成的复制并粘贴动作,与所述第一域关联的策略实现防止将剪贴板缓冲区传递至所述第一域之外的第一规则,或者与所述第二域关联的策略实现防止将所述剪贴板缓冲区传递至所述第二域内的第二规则,其中对所述目标进程阻止基于所述剪贴板缓冲区的所处理的事件消息。

25.根据权利要求22所述的方法,其中所述事件消息包括由所述初始进程生成的消息收到通知,与所述第一域关联的策略实现第一规则或者与所述第二域关联的策略实现第二规则,所述第一规则实现所述消息收到通知的过滤,所述第二规则所述消息收到通知的过滤,其中所处理的事件消息包括经过滤的消息收到通知,并且其中所述经过滤的消息收到通知被传递至所述目标进程。

26.根据权利要求22所述的方法,其中(a1)包括存储将所述资源与所述安全域的所述唯一域标识符关联的元数据。

27.根据权利要求25所述的方法,其中所述过滤至少移除或掩盖所述消息收到通知的发送者标识符或主题标识符。

28.一种计算机可读介质,包括在所述计算机可读介质上存储的指令,该指令在由计算机执行时实施根据权利要求22所述的方法。

29.一种在计算设备的操作系统中提供多个安全域的方法,所述方法包括:

(a)针对每个安全域:

(a1)将所述安全域的资源与关联于所述安全域的唯一域标识符关联,所述资源包括至少一个数据文件或至少一个应用;以及

(a2)与所述唯一域标识符关联地存储策略,该策略包括用于控制对所述资源的访问的规则集;

(b)从与所述多个安全域中的第一安全域关联的初始进程接收用于启动与所述多个安全域中的第二安全域关联的目标进程的请求;以及

(c)基于与所述第一域关联的策略和与所述第二域关联的策略,处理所述请求。

30.根据权利要求29所述的方法,其中所述初始进程生成与关联于所述第二域的接收到的消息关联的消息收到通知,所述请求用于显示所述消息,与所述第二域关联的策略实现允许在所述第二域中显示所述消息的第二规则,并且所述目标进程显示所述消息。

31.根据权利要求30所述的方法,其中与所述第一域关联的策略实现允许实施在所述第二域中显示所述消息的第一规则。

32.一种计算机可读介质，包括在所述计算机可读介质上存储的指令，该指令在由计算机执行时实施根据权利要求29所述的方法。

33.一种在数据处理系统中的方法，所述数据处理系统具有处理器和用于存储操作系统的存储机制，所述操作系统包括内核和位于所述内核之外的中间件，所述方法包括：

在所述中间件中提供第一装备，所述第一装备用于创建多个域并且将所述多个域与用于控制对所述多个域的访问的对应策略关联；

在所述中间件中提供第二装备，所述第二装备用于在所述多个域之间切换；以及

至少部分地在所述中间件中提供第三装备，所述第三装备用于执行所述多个域的对应策略。

34.根据权利要求33所述的方法，进一步包括：

在所述中间件中提供第四装备，所述第四装备用于基于所述多个域的所述对应策略来管理应用的安装。

35.根据权利要求34所述的方法，进一步包括：

在所述中间件中提供第五装备，所述第五装备用于提供所述多个域中不同域内的多个运行进程之间的通信。

36.根据权利要求35所述的方法，其中所述多个运行进程实现从所述多个域中的第一域向所述多个域中的第二域的复制并粘贴动作，其中所述第五装备提供所述第一域中的所述多个运行进程中的第一运行进程和所述第二域中的所述多个运行进程中的第二运行进程之间的信令，并且其中所述第五装备基于与所述第一域对应的策略和与所述第二域对应的策略，允许或阻止所述复制并粘贴动作。

37.根据权利要求35所述的方法，其中所述多个运行进程实现在所述多个域中的第一域中运行的消息客户端，其中所述第五装备提供所述第一域中的所述多个运行进程中的第一运行进程和所述第二域中的所述多个运行进程中的第二运行进程之间的信令，以基于与所述第一域对应的策略和与所述第二域对应的策略来选择性地允许、过滤或阻止与所述第二域相关地生成的消息收到通知。

38.根据权利要求35所述的方法，进一步包括：

在所述中间件中提供第六装备，所述第六装备用于基于所述多个域中的第一域的对应策略和所述多个域中的第二域的对应策略，启用与所述第二域关联的至少一个应用在所述第一域中的执行。

39.根据权利要求38所述的方法，其中所述第六装备从与所述第一域关联的初始进程接收请求以执行所述至少一个应用，并且基于与所述第一域关联的策略和与所述第二域关联的策略来允许或阻止所述至少一个应用的所述执行。

40.根据权利要求39所述的方法，所述请求用于显示关联于所述第二域的接收到的消息。

41.根据权利要求38所述的方法，进一步包括：

在所述中间件中执行第七装备，用户界面基于所述多个域的对应策略来提供对所述多个域中的不同域的并行访问。

42.根据权利要求33所述的方法，进一步包括：部分地在所述内核中提供所述第三装备。

43.根据权利要求33所述的方法，其中所述操作系统实现多个用户账户，并且其中所述多个用户账户中的至少一个唯一地与对应的所述多个域关联。

44.根据权利要求33所述的方法，其中所述第三装备基于与所述多个域中的第一域关联的多个策略中的第一策略和与所述多个域中的第二域关联的多个策略中的第二策略，控制与所述第一域关联的进程控制对与所述第二域关联的资源的访问。

45.根据权利要求44所述的方法，其中所述进程基于所述第一域的所述唯一域标识符与执行环境标识符关联，并且其中所述第三装备基于所述执行环境标识符，控制所述进程对所述资源的访问。

46.根据权利要求45所述的方法，其中所述执行环境标识符基于所述第一域的唯一域标识符和与为生成所述进程而执行的应用关联的唯一应用标识符。

47.根据权利要求46所述的方法，其中所述操作系统是安卓操作系统，所述唯一应用标识符是在安装时分配给所述应用的Unix型用户标识符(UID)，所述执行环境标识符包括所述应用的所述UID，并且所述唯一域标识符包含在所述UID的保留位中。

48.根据权利要求41所述的方法，其中所述用户界面基于与所述多个域中的第一域关联的策略和与所述多个域中的第二域关联的策略，提供对与所述第一域关联的至少第一应用和与所述第二域关联的至少第二应用的并行访问。

49.根据权利要求48所述的方法，其中所述用户界面实现与所述第一应用关联的第一图标和与所述第二应用关联的第二图标，并且所述第一图标包括表示所述第一应用与所述第一域的关联的覆盖。

50.根据权利要求33所述的方法，其中所述多个域中的一个是外部地控制的域，并且其中与所述外部地控制的域关联的策略是经由网络从远程域管理服务器接收的。

51.根据权利要求50所述的方法，其中所述远程域管理服务器将对与所述外部地控制的域关联的策略的至少一部分的修改阻挡在外。

52.一种计算机可读介质，包括在所述计算机可读介质上存储的指令，该指令在由处理器执行时实施根据权利要求33所述的方法。

53.一种计算设备，包括处理器和存储指令的存储器，该指令可由所述处理器执行以实施提供多个安全域的操作系统，所述操作系统包括：

域管理器，用于选择性地创建所述多个安全域，并且用于选择所述多个安全域中的一个作为当前域；

域策略服务，用于针对每个安全域，存储并执行包括规则集的策略，该规则集控制对与该域关联的文件和应用的访问；

程序包管理器，用于针对每安全域，执行与该域关联的应用的安装；

域消息服务，用于提供与所述多个安全域中的不同安全域关联的运行进程之间的通信；以及

活动管理器，用于选择性地切换所述当前域。

集成操作系统的域管理

技术领域

[0001] 本公开大体地涉及移动设备安全。更具体地，本公开涉及用于移动设备的安全域管理。

背景技术

[0002] 在诸如智能电话，平板和移动互联网设备之类的以安卓™、Linux™或任意基于Unix™的操作系统(例如，iPhone™)为基础的移动设备上需要多个隔离域，其中位于域中的应用和数据与可能由位于该域之外、位于网站上或位于同一设备的其它域中的应用产生的安全威胁隔离。这样的多个安全域通常将由单个用户、设备拥有者使用，以解决与不同移动设备使用情况关联的不同访问容易度、隐私要求和安全要求。例如，设备拥有者可能对游戏应用具有与对移动银行应用和数据不同的访问容易度、隐私要求和安全要求，或者设备拥有者可能期望暂时与家庭成员或朋友共享其设备上的特定应用，而不共享其它应用和数据，如个人电子邮件、联系人和文本消息。此外，存在由诸如设备拥有者或外部团体(如机构或公司)之类的不同实体管理不同域的要求，其中每个实体可能对他们管理的域中的应用和数据的访问和使用具有不同的安全要求。例如，对于在每个域中允许的应用以及应用可以在域中执行的条件，这些要求可能在域之间不同，每个要求可能需要是可由管理每个域的实体针对该域唯一地配置的。根据在域中包含的应用和数据的类型，还需要支持为进入不同域所需要的不同用户认证机制、不同的重认证时间范围(或可选地没有认证)(例如，设备拥有者可能不希望输入密码来玩游戏或访问谷歌™地图，但他们可能希望具有对访问移动银行应用的强认证形式)。

[0003] 移动设备安全和域隔离领域的现有技术已经使用传统个人计算机(PC)和服务器计算安全技术，如用户账户、管理程序/虚拟化、应用程序包装器和防病毒扫描。然而，移动设备的典型使用实质上与这些传统环境不同。移动设备本质上是移动的，并且总是伴随设备拥有者。他们是连接的，总是开机的并且需要对短持续时间的任务的快速访问。它们以实质上与传统工作站和大型机共享不同的方式共享。功耗对移动设备也是至关重要的，这是耗电的病毒扫描和虚拟化技术也必须在移动设备上广泛使用的一个原因。

[0004] 一种传统的域隔离方法是在设备上创建单独的用户账户，由此，每个用户必须登录已经为该用户配置的账户。根据操作系统(OS)，这可能迫使另一用户注销。此方法支持单个设备上的多个用户，并且分离或隔离每个用户的应用数据。在所有用户之间利用相同的操作系统，并且所有用户具有相同的用户界面特征。所有用户可访问已安装的应用，这是存储器和中央处理单元(CPU)资源的有效使用。这也允许用户以他们期望的外观和感觉配置他们的账户。

[0005] 虽然用户账户提供数据隔离以及在不同用户账户之间使用相同应用和OS的效率，但是此方法受以下限制。其提供对设备的全部访问或全部不访问，而没有临时访问的灵活性。“来宾”用户账户可以被设置有限的访问权，但这不能帮助对移动设备而言(例如，对家庭成员或朋友而言)常见的自发共享。用户账户在被认为是个人设备的移动设备上通常不

可用。用户仍然必须在每个用户账户之间切换，这不能反映人们期望使用他们的移动设备的方式。在切换用户账户时用户必须登录，这进一步造成该方法的不方便，因为在多用户账户情况中的第一用户和第二用户之间没有隐含关系。通常不存在不活动的计时器或类似机制，使得在切换域时不总是需要登录。用户(账户)之间的隔离位于用户空间或应用级，并且由OS执行。具有管理员或根权限的任何人或任何软件(包括恶意软件)可以访问所有用户的数据。一些系统确定能够加密一些用户数据来帮助缓解此侵害，但是用户数据通常仍极易受攻击，并且任何内核级开发或处理能够修改应用、进程，拦截数据并且访问其期望的任何文件/对象。

[0006] 此外，(在大型计算机上开发的且类似地扩展至台式机的)传统用户账户在真正的个人设备(如智能电话)上不能很好地工作。移动设备与大型计算机或台式计算机不同地共享。设备拥有者和用户日益想要具有移动设备上的传统锁屏或‘全部或全部不’访问控制机制的替代方式。例如，设备拥有者在不需要用户认证的域中具有频繁地访问的且不包含敏感信息的应用，是令人期望的；这与个人保护域或工作保护域的要求不同。这种开放的、共享的或公共的域的主要目标是在这样的应用和数据的安全被用户视为不重要时(例如，天气或导航)的使用方便和快速访问。因此，用户不想每次他们访问这样的开放域时都输入密码或PIN。此外，这样的开放域可以包括与用户或域拥有者可以在他们的保护域中允许的那些应用相比可能不那么可信的应用。例如，安卓上的许多应用已知会访问联系人数据库。最后，虽然这种权限必须在安装时被授权以能够安装应用，但是许多用户对此不严密地进行检查或不理解授予这样权限的含义。

[0007] 现在参照图1A至1D描述其它传统域隔离方法。

[0008] 如本领域已知的且在图1A中图示的，实现操作系统的计算设备(如移动设备)可以被理解为包括：硬件、包括内核和中间件的操作系统、以及应用空间(或用户空间)。内核管理软件应用并且向软件应用提供输入/输出(I/O)服务以访问硬件，并且中间件向软件应用提供除由内核提供的那些服务之外的服务。

[0009] 图1B和图1C中图示的一种传统域隔离方法使用基于管理程序的虚拟化或虚拟机。利用虚拟机来某种程度地复制操作系统，以提供不同的隔离域。根据管理程序，存在不同类型的虚拟机。图1B中图示的类型1(或裸机)管理程序直接在设备CPU上运行(‘裸机’)，且通过针对每个域支持完整的且分离的无特权的操作系统实例，提供域隔离。隔离仅依赖于管理程序。图1C中图示的类型2管理程序是另一虚拟化方法，其中第二来宾OS在主OS之上运行。还存在其它混合操作系统级虚拟化方法。

[0010] 基于管理程序的虚拟化提供域之间的隔离，但受到以下限制。OS和应用的复制意味着在设备存储器、CPU和功耗方面存在显著设备开销。管理程序方案的高资源需求使得支持多个域不现实。数据、应用共享和进程间通信(IPC)通常是不可能的，尽管提出了如果管理程序支持特殊消息服务则通过特殊消息服务进行某种跨域数据共享。每个OS被暴露给内核级恶意软件，内核级恶意软件可能破坏域之间的隔离。用户必须在域之间来回切换(例如，从个人应用切换至工作应用)，这不反映人们期望使用他们的移动设备的方式。将类型1或类型2管理程序集成到移动设备上的时间和开销是非常高的，使得此方法对于低成本的移动设备不可行。在域之间切换的性能影响高。最终，这样的方案支持由每个OS提供任何用户账户和用户认证，这是传统的全部或全部不访问。

[0011] 图1D图示的移动设备上的域隔离的第三种传统方法涉及应用级容器化(containerization)。在这样的情况中,应用容器(或域)共享相同的硬件和OS,但使用容器化或包装器技术来作为容器和OS中的应用之间的代理。这通过提供间接的一层产生多个独立域,使得较低级设备资源、存储器和文件系统可以透明地映射至仅应当由容器或域中的应用访问的更高级资源。尽管应用在容器内和容器外通常被复制(例如,在容器内可以用于工作和在容器外可以用于个人使用的电子邮件应用),但是由于仅存在一个版本的OS,所以容器化在移动设备资源的消耗方面(尤其与虚拟化相比)是相对高效的。作为应用级方案,容器方案具有非常实际的好处,因为其已经在本领域中(例如,反向兼容)被下载到设备上。

[0012] 在容器化中,所有安全和所有执行都被包装在容纳应用的容器周围。因此,下载被容纳的应用的任何人不但接收该应用,而且接收与该应用关联的所有安全信息。利用容器化,坏人仍然可能:(1)对安全策略进行反向工程;或(2)在环境中(如在可以从其中提取信息的仿真器上)执行该应用。

[0013] 但是,应用级容器化作为一种用于域隔离的方法受到以下限制。从安全角度看,具有一些基础技能的黑客或者位于设备上的恶意软件相对容易地拦截容器和OS之间的调用,从而破坏隔离并捕获数据和个人信息。容器化不是在操作系统或内核中执行的,并且暴露于可能在设备上存在的恶意软件。例如,如果操作系统是Linux或安卓且黑客获得根访问特权,那么相对简单的是从RAM中提取域数据或其它重要信息(例如,用于访问域的密码,或用于加密域中的数据的密码术密钥),或这样的内核级恶意软件在I/O驱动(如麦克风或帧缓冲器)上窃听。容器隔离由该容器"包装"的应用和数据,但不限制不在容器中的其它应用访问存储器、文件或网络等。跨域共享单个应用映像是不可能的,这样的技术不允许相同的应用既在容器内又在容器外。结果,容器通常仅支持已对该容器修改的预定应用,如邮件、消息、浏览、联系人、日历等。这不提供用户或公司IP部门期望的应用选择。公共应用必须被修改以支持容器,这成倍增加设备上的存储器和内存并且增加应用开发者的努力和参与。通常,必须为容器方案专门创建私人应用储存库,这增加了对供应商方案的锁定且需要应用开发者的参与,从而进一步限制选择。利用应用包装方法,可能需要用对如何存储、共享和发送数据进行控制的安全库对可执行的代码打补丁。这引入了许可和版权问题,因为通常不授权许可拥有者修改应用。用户必须仍在域或容器之间来回切换,这不反映人们使用其移动设备的方式。最后,域通常具有其自己预定的用户界面,该预定用户界面不同于本地OS用户体验且不能由设备用户定制。

[0014] 域隔离的又一种方法是设备操作系统中的内核级平台安全方法,如Security Enhanced Linux™(SELinux™)。SELinux提供应用和用户对对象和资源(如文件)的强制访问控制(MAC)。为每个用户或应用分配安全标签,并且可以为所有标签分配策略。SELinux可以用于与域切换机制相结合的基于角色的访问控制,但是安卓™不以这样的方式使用用户标识符。SELinux使用特殊内核模块,该特殊内核模块依赖于Linux中的Linux安全模块(LSM)接口来基于安全策略执行进程之间的隔离。在加载之前可以针对SELinux策略验证应用,并且所有进程可以局限于预定访问,使得如果策略不允许那样,那么一个应用不能启动或访问另一进程、目录或数据。利用正确的策略机制,可以防止应用、恶意软件以及甚至内核根套件(root kits)访问属于另一用户或应用的应用和数据。

[0015] 虽然与容器相比以及与虚拟化方法相比,本地OS方案从安全、性能和应用隔离角

度具有许多优点，但是其受到如下缺陷：内核对中间件级不具有用以能够执行在中间件级要求的域隔离的可见性。

[0016] 此外，内核级平台安全作为用于域隔离的方法受到以下限制。这样的内核模块方法不具有任何用户界面或域的概念，但是通常使用已有的传统用户账户，这包括允许具有跨所有域的特权的根或管理员账户。在此方法中使用的内核模块在操作系统中是非常低的，且不具有如下的细化的应用特定信息：该细化的应用特定信息用于提供为满足移动设备上的隔离域的消费者需求和共同使用所需的那类策略控制(例如，用于域的用户认证策略)以及应用控制(例如，对特定域的应用约束)。将SELinux类型策略语言和执行扩展至中间件显著提高了方案的复杂性。这样的策略通常是静态的且不是最新的。已存在用于为SELinux提供远程策略更新的计划，但策略应用于整个设备且对于每个域不是唯一的。例如，安卓上的进程间通信(IPC)难以监控，因为权限检查以及调用方/被调用方检查是安卓中间件中实施的，并且内核不能访问足够的信息来监视和控制域之间的IPC。最终，通常没有对限定域间数据共享的用户和应用访问的足够细化控制，这引起数据泄露问题，这对于特定类型的数据是不可接受的。虽然这可能对于一些共享应用(例如，摄像头和图片库)是可接受的，但是存在用内核级方案不可能实现的对文件和文件阅读器应用(例如，PDF查看器)需要的更高程度细化。

[0017] 用于提供安全的另一传统方法是加密的文件系统，如密码术的堆叠文件系统。例如，eCryptFS文件系统(http://ecryptfs.org)是用于Linux的POSIX兼容的企业密码术堆叠文件系统。但是，加密的文件系统不是提供多个域的合适方式。

[0018] 因此，期望提供用于在移动设备上创建多个域的方式，其中位于域中的应用和数据与安全威胁隔离(安全威胁可能产生自网站上的位于该域之外或相同设备上位于另一域中的应用)，且该方式缓解上述传统方法中每个传统方法的一个或多个缺陷，提供了相对于这些传统方法上的优点，或提供了这些传统方法的替代方法。

[0019] 附图图示

[0020] 现在将参照附图，仅通过示例来描述本公开的实施例。

[0021] 图1A、图1B、图1C和图1D示出图示用于域隔离的操作系统结构和传统方法的框图。

[0022] 图2示出图示用于提供隔离域的本发明的系统的框图。

[0023] 图3示出图示多个用户账户和多个域的实现方式的示意图。

[0024] 图4示出图示从第一域切换至第二域的方法的框图。

[0025] 图5示出图示域消息方法的框图。

[0026] 图6示出图示跨域执行方法的框图。

[0027] 图7示出图示域应用安装方法的框图。

[0028] 图8示出图示更新策略方法的框图。

[0029] 图9示出图示从当前域切换至另一域的方法的框图。

[0030] 图10示出图示从当前域切换至未运行的、加密的、且要求访问认证的目标域的方法的框图。

具体实施方式

[0031] 本文公开的方案向移动设备提供灵活的、有效的且安全的隔离域以及这样的域的

管理，并且减轻上面描述的传统方法中的每个传统方法的一个或多个缺陷，提供相比于这些传统方法的优点，或提供这样的传统方法的替代方法。

[0032] 下面的要素与克服上面的传统方法的缺点的方案有关。首先，近些年已经从主要将移动设备用于移动电话和SMS(短消息服务)转移至将移动设备用于网页浏览、社交网络、游戏、电子邮件、即时消息、基于定位的服务和移动商务。利用经由服务提供商和WiFi的宽互联网连接，移动计算一直是连接的，且是真正地移动的。此外，由于应用激增以及包括诸如像摄像头、GPS、加速度计、气压计等之类的传感器的设备的能力，移动设备具有更加多样的用途。它们通过IP网络或传统电话网络用于娱乐，社交网络，摄像头/视频，导航，访问用于个人(例如，照片共享)或工作(例如，公司CRM系统)或二者结合(例如，文件共享(如Drop Box))的云服务，以及来自文本、聊天、电子邮件和语音的许多形式的消息。此外，随着不断增加的这种移动设备上的应用的功率、连接和数量，用户日益在这些设备上存储和追踪更敏感的信息(例如，个人数据、凭证、密码术密钥、信用卡号、密码、联系人、过去的位置、当前位置、网页浏览历史、安装的应用以及当前设备状态(例如，未移动)等)。此敏感信息通常是恶意用户和恶意软件(电脑病毒)的目标。此外，由于移动设备随人一起携带且由于它们的可扩展能力，所以希望能够快速地访问这些设备以进行快速回复、快速网页搜索等。传统设备锁定程序的使用带来不方便。例如，为了查找词典中的词，用户可能不希望输入密码来解锁设备。此外，经常例如为了临时目的而共享移动设备(或期望共享移动设备)，如为了进行电话呼叫、让家庭成员玩游戏或在设备拥有者正在开车时在车辆导航过程中。这大大不同于传统计算或服务器环境中的传统用户账户，其中在多人之间共享一个设备或服务，但提前知道这些用户，且这样的共享使用往往是在持续不断的和规则的基础上的。此外，由于移动设备的较小形状因子以及使用频率和位置，移动设备比便携式计算机或PC大大频繁地丢失或被偷，因此可能落入黑客手中。许多用户和企业需要远程地锁定、定位和/或“擦除”(从设备上删除所有应用和数据)丢失或被偷的移动设备的方式，该方式包括一些国家的智能电话防盗条例(http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment)。此外，公司环境中的员工针对个人用途和工作用途使用单个设备是常见的。这是共享的另一形式—但仅是硬件和网络服务的共享—其中由于公司期望拥有和控制工作数据的传播(例如，尤其在员工离职时)，所以安全、隐私和数据隔离要求较高，且用户可能具有他不想要与雇主共享的隐私数据。在许多情况下，相同的应用可以用于个人使用和公司使用——因为这样提高生产率——然而，应用数据必须隔离，使得可以删除(擦除)公司数据而不影响个人数据，或者可以删除(擦除)个人数据而不影响公司数据。此外，由于设备能力、敏感信息、共享和双重使用，所以越来越需要隐私和灵活的访问控制。通知常常显示设备拥有者不总是希望每个人看到或访问的敏感个人信息(聊天消息、软件更新、广告)。用户想要借出其设备的灵活性，但期望限制访问特定能力和/或服务，如只读、仅接听电话呼叫或特定账户(例如，脸书(Facebook))。许多用户面对在全部或全部不设备锁定的不满意替代和根本不保护设备之间进行选择。最后，移动设备本质上比PC连接至更多的网络(例如，饭店、酒店和机场中的WiFi网络)，这使这些设备暴露于更多基于网络的攻击、入侵和分组捕获。此外，移动设备用户可访问第三方应用储存库，第三方应用储存库使用户能够下载可能包含恶意软件(电脑病毒)的应用。例如，基于安卓操作系统的移动设备现在占以移动设备为目标的恶意软件的90％以上。

[0033] 在本文中，‘域’可以被认为代表一组资源(例如数据文件、应用和服务)和规则集或‘策略’之间的关系，由此进程对资源的访问至少部分地受策略控制。例如，可以认为特定域包括或包含与该域关联的多个数据文件，并且对这些数据文件的访问至少部分地受与该域关联地限定的策略控制。类似地，可以安装应用或者应用可以与特定域关联，并且对该应用(包括例如执行应用的能力)的访问至少部分地受与该域关联地限定的策略控制。

[0034] 例如，在单用户设备中能够提供具有对选择的应用和其它资源提供不同访问权的不同策略的多个域，是令人期望的。在一个情况中，可能令人期望的是，提供需要认证且包含希望孩子不可访问的数据或应用的受限域，以及不需要认证且希望孩子可访问(以例如玩游戏)的儿童模式域。因此，当在开放域中操作时，受限域的数据或应用不可由与开放域关联的进程访问，是令人期望的。

[0035] 上面讨论的域的期望功能中的一些可以由通常在多用户操作系统中实现的传统用户账户提供。可以认为这样的用户账户构成一种域，因为用户账户代表一组资源(例如，用户的数据文件、应用)以及与控制对用户资源的访问的该用户账户(例如，权限、特权)关联的规则集或策略，等等。

[0036] 但是，针对在移动设备上提供不同域资源的安全隔离的益处以及方便且统一的单用户体验，传统用户账户不是恰当的方式。除上面的期望功能之外，提供期望体验还需要并行实施涉及两个域的动作的能力，例如从一个域向另一域进行复制并粘贴、提供并行访问多个域的资源的单用户界面、或从在第一域中操作的邮件客户端打开与第二域关联的邮件。传统用户账户不旨在支持这样的功能，因为用户隔离控制(通常集成在操作系统服务中的且逻辑上符合不同用户账户旨在由不同个体使用的假设)不允许或者不容易地支持不同域的多个进程和资源的现成共享和协作，该现成共享和协作是由个体并行地使用多个域以启用期望功能所需要的。

[0037] 虽然如上面讨论的那样，可能不以与用户账户相同的方式限制诸如虚拟化和容器化之类的替代隔离机制，但它们具有上面讨论的不同缺陷。因此，希望提供隔离域管理作为操作系统的集成特征。此外，虽然仍如上面讨论的那样，一些期望功能可以由位于操作系统的内核中的服务提供，但是当前操作系统内核通常不能支持或允许足够的域信令和域管理来提供为同时涉及多个域的动作所需的进程共享和协作。

[0038] 因此，所公开的方案经由对操作系统的现有组件或服务的修改或新的组件或服务的引入，来提供域感知。在一些实施例中，组件和服务中的至少一些设置在内核外的操作系统中，即在中间件中(中间件在本文中用于表示内核外部且在内核和用户应用之间的操作系统)。在一些实施例中，组件和服务中的至少一些设置在操作系统内核中。在一些实施例中，由操作系统中间件的经修改或新的组件或服务启用域创建和管理，并且域执行由操作系统内核实施，并且为此目的提供经修改或新的内核模块或内核修改。

[0039] 因此，在第一实施例中，在包括处理器和存储可由该处理器执行以实现安卓操作系统的存储器的移动设备中，改进包括：用户管理器，该用户管理器用于选择性地创建与在安卓操作系统中实现的任意用户账户不同的多个域；域管理器，该域管理器用于选择多个域中的一个作为当前域；域策略服务，该域策略服务用于针对每个域，存储和执行包括规则集的策略，该规则集控制对与该域关联的文件和应用的访问；程序包管理器，该程序包管理器用于针对每个域，基于该域的策略和当前域的策略，选择性地允许或阻止与该域关联的

应用的安装或执行;域消息服务,该域消息服务用于基于多个域中不同域的相应策略,提供与多个域中该不同域关联的运行进程之间的通信;以及活动管理器,该活动管理器用于选择性地切换当前域,其中用户管理器、域管理器、域策略服务、程序包管理器、域消息服务以及活动管理器在安卓操作系统的内核外部在该安卓操作系统中实现。改进可以进一步包括:域内核模块,该域内核模块用于针对每个域,执行与该域关联的策略,其中域内核模块在安卓操作系统的内核中实现。

[0040] 在第二实施例中,由计算设备的处理器实施的用于在该计算设备的操作系统中提供多个安全域的方法包括:(a)针对每个安全域:(a1)将该安全域的资源与唯一域标识符关联,该资源包括至少一个数据文件或至少一个应用;以及(a2)与该唯一域标识符关联地存储策略,该策略包括用于控制对该资源的访问的规则集;(b)接收该多个安全域中选择的一个作为当前域,其中该多个安全域包括与当前域不同的目标域;以及(c)基于与当前域关联的策略以及与目标域关联的策略,控制对目标域资源的访问。

[0041] 在第三实施例中,用于在计算设备的操作系统中提供多个安全域的方法包括:(a)针对每个安全域:(a1)将该安全域的资源与关联于该安全域的唯一域标识符关联,该资源包括至少一个数据文件或至少一个应用;以及(a2)与该唯一域标识符关联地存储策略,该策略包括用于控制对该资源的访问的规则集;(b)生成与关联于该多个安全域中的第一安全域的初始进程关联的事件消息;(c)确定与该多个安全域中的第二安全域关联的目标进程被配置为对该事件消息做出响应;(d)基于与该第一域关联的策略以及与该第二域关联的策略,处理该事件消息,以产生经处理的事件消息;以及(e)基于与该第一域关联的策略和与该第二域关联的策略,向该目标进程传递该经处理的事件消息或对该目标进程阻止该经处理的事件消息。

[0042] 在第四实施例中,在计算设备的操作系统中提供多个安全域的方法包括:(a)针对每个安全域:(a1)将该安全域的资源与关联于该安全域的唯一域标识符关联,该资源包括至少一个数据文件或至少一个应用;以及(a2)与该唯一域标识符关联地存储策略,该策略包括用于控制对该资源的访问的规则集;(b)从与多个安全域中的第一安全域关联的初始进程接收用于启动与多个安全域中的第二安全域关联的目标进程的请求;以及(c)基于与该第一域关联的策略和与该第二域关联的策略,处理该请求。

[0043] 在第五实施例中,在具有处理器和用于存储包括内核和位于该内核之外的中间件的操作系统的存储机制的数据处理系统中,一种方法包括:在该中间件中提供第一装备,该第一装备用于创建多个域并且将该多个域与用于控制对该多个域的访问的对应策略关联;在该中间件中提供第二装备,该第二装备用于在该多个域之间切换;以及至少部分地在该中间件中提供第三装备,该第三装备用于执行该多个域的对应策略。

[0044] 在第六实施例中,一种计算设备包括处理器和存储指令的存储器,该指令可由该处理器执行以实时提供多个安全域的操作系统,并且该操作系统包括:域管理器,该域管理器用于选择性地创建该多个安全域,并且用于选择该多个安全域中的一个作为当前域;域策略服务,该域策略服务用于针对每个安全域,存储并执行包括规则集的策略,该规则集控制对与该域关联的文件和应用的访问;程序包管理器,该程序包管理器用于针对每个安全域,执行与该域关联的应用的安装;域消息服务,该域消息服务用于提供与该多个安全域中的不同安全域关联的运行进程之间的通信;以及活动管理器,该活动管理器用于选择性地

切换当前域。

[0045] 现在参照图2描述用于提供隔离域的示例性系统100。

[0046] 该系统可以在任何计算设备中实现，该计算设备包括移动设备，如智能电话、平板、便携式计算机或台式机、或具有易失性存储器和处理器的任意其它电子设备，易失性存储器包含可由处理器执行以提供操作系统和软件应用(或者应用)的计算机代码。计算设备可以进一步包括接口，该接口可以包括用户输入设备，如键盘、指点设备、触摸屏，并且该计算设备可以进一步包括通信接口，如用于通过有线通信网络或无线通信网络通信的无线电和关联的控制电路，有线通信网络或无线通信网络可以是互联网和/或蜂窝或WiFi链路或蓝牙或近场通信(NFC)。

[0047] 操作系统的特征可以在于包括内核以及中间件，内核管理软件应用并且向软件应用提供来自设备的处理器和其它硬件组件的输入/输出(I/O)服务，中间件提供除由内核提供的那些服务之外的服务。

[0048] 一般而言，本发明的方案包括：修改操作系统级协议以使能域感知。在移动设备上创建多个域。在此后描述的实施例中，操作系统是安卓™，但是这样的选择不应被认为限制本发明的方案的期望范围。安卓仅用作示例，并且类似于其它多用户操作系统(例如，QNX、视窗)。

[0049] 因此，如图2所示，系统100包括内核，在系统100在运行安卓™操作系统的移动设备中实现时，该内核是Linux™内核110。内核100包括：安全数据储存库112、域内核模块116和Linux安全模块114，在一个实施例中，Linux安全模块114是增强的Linux安全模块，下面将进一步讨论它们各自的功能。本领域技术人员将理解，内核110可以进一步具有其它传统组件(例如，驱动)或与前述组件不同的其它组件。

[0050] 系统100进一步包括操作系统中间件120，操作系统中间件120包括：域消息服务122、域管理器124、域策略服务126、用户管理器128、系统设置模块130、密钥保护中介132、活动管理器134、程序包管理器136以及窗口管理器138。用户管理器128、系统设置模块130、密钥保护中介132、活动管理器134、程序包管理器136以及窗口管理器138对应于并且拥有安卓™的已知组件或服务的相应功能，但被修改为如下面讨论的那样是域感知的。域消息服务122、域管理器124和域策略服务126是其它组件，它们的功能在下面讨论。

[0051] 系统100进一步包括用于实现一个或多个域的应用空间140(或用户空间)。为了图示，示出第一域142-1和第二域142-2，但是将理解，可以实现任意数量的域。每个域可以包括域设置模块的实例化，如域设置模块144-1、144-2的第一实例化和第二实例化，并且通常将包括域导航器模块146-1、146-2和域管理应用148-1、148-2的第一实例化和第二实例化。每个域还可以具有第一应用的分离实例化150-1、150-2，而第一域142-1可以实例化与在第二域142-2中实例化的第三应用154不同的第二应用152。

[0052] 域

[0053] 诸如第一域142-1和第二域142-2这样的域是将任何应用和与那些应用关联的数据保持分离的隔离区域。可以远程地(例如，由企业信息技术(IT)管理者)或本地(例如，由设备拥有者)控制域，以针对特定域规定应用、数据、配置、连接和安全策略。例如，可以控制来自特定域的网络访问。可以控制密码重认证时间(例如，使得当在指定时间段内切换域时用户不需要重新认证)。域的管理员通常具有这样的控制。管理员可以是个人用户、或公司

IT管理者或其它远程实体。

[0054] 由于域的隔离和分隔性质，本文讨论的域可以被认为是受保护的域。例如，一个域可以由企业外部地管理，该企业不希望在设备丢失或被偷时或者在由另一域中的设备拥有者下载的恶意软件危害该设备时该企业的信息或私有业务应用被泄露。设备拥有者不希望企业追踪其偏好、网络浏览习惯或个人通信，因此他也希望有他自己的受保护的域。此外，设备拥有者不希望对设备上的所有应用和服务施加相同级别的认证，但保证受保护的域中的数据仍然是安全的。

[0055] 提供多个域使设备拥有者具备传统的“全部或全部不”的设备访问控制的替代方案。利用支持安全域和开放域的能力，访问可以由用户根据需要来配置，具有可变的注销时间和访问控制(例如，PIN、密码、面部识别或什么也没有)。这样的灵活性降低了由于不方便而在设备上根本不使用任何密码的可能性，同时仍赋予拥有者独立于远程管理员的设备选择。

[0056] 仅通过示例，图3示出示意图300，其中实现系统100的设备305配置有两个用户：用户A 310和用户B 315，其中三个域A1 320、A2 325、A3 330是与用户A关联地创建的，并且两个域B1 335和B2 340是与用户B关联地创建的。如图示出的，域A1的策略可以允许访问选择的电子邮件账户345，域A2的策略允许访问Gmail™账户和脸书™ 350。

[0057] 为了清晰，实现系统100的设备还可以配置有仅一个用户，且还可以创建本文描述的多个域，并且本文描述的方法和协议与这样的多个域关联地实现。

[0058] 域感知

[0059] 可以基于在Unix™操作系统和Linux™操作系统中实现的用户标识符(UID)概念和组标识符(GID)概念来提供域感知。UID和GID在Unix和Linux中用来向进程和文件分配权限。超级用户或根通常被分配UID 0，而其它范围通常为系统进程保留。

[0060] 但是，在安卓™中，UID不用于表示用户；相反，每个应用在安装时被分配唯一的UID和GID，并且此(UID,GID)对(可以认为是应用标识符)被分配给与该应用关联的进程和数据文件。在最近版本的安卓™(安卓4.2)中，引入多用户能力，该多用户能力在整个操作系统各处中增加信令来表示哪个用户账户是活跃的。UID中的特定位被保留用于表示用户账户，因此构成用户标识符。当启动进程时，此用户标识符与在安装时分配给该应用的应用标识符结合，以产生执行环境标识符来表示正在运行的进程和关联的私人数据文件的环境。利用这样的信令，可以基于用户独立地创建并存储应用数据。

[0061] 与之前的版本相比，安卓™4.2的服务已被修改成是用户账户感知的。例如且参照图2，安卓程序包管理器136被修改为控制每个用户可利用哪些应用。类似地，窗口管理器138被修改为控制向每个用户显示什么，并且活动管理器134被修改为控制每个用户的应用启动和权限执行。此外，称为用户管理器128的新服务被增加到安卓4.2中，并且处理创建、认证、删除以及用户之间的切换。

[0062] 在本方案的一个实施例中，通过将现有服务修改成域感知的，向操作系统增加与在安卓™4.2中增加的多用户能力类似的域感知信令机制。特别地，通过对UID的扩展或作为新字段的添加，增加构成域标识符或“DID”的域信令。UID中的预定位被保留以表示域，并且与在安装时向应用分配的应用标识符结合，以创建执行环境标识符，执行环境标识符表示与该域相关的正在运行的进程和关联的私有数据文件的环境。在一个实施例中，将程序包

管理器136配置为维护每个安装的应用的应用标识符和每个域之间的关联的列表。随后，基于应用的应用标识符以及该应用在其中执行的域的域标识符，为进程创建执行环境标识符。在一个实施例中，UID还具有与特定用户账户关联的保留位。这样的保留或将UID字段扩展为还表示域的方法降低了操作系统改变的程度，简化了实现方式，并且缩短了部署时间。

[0063] 在一个实施例中，实现被称为域管理器124的新服务以管理下面描述的域的创建、认证和删除。

[0064] 使系统成为域感知的可选方法是使用安全标记，如SELinux如何识别不同的资源和对象。在一些实施例中，SELinux安全标记用于这样的目的。在其它实施例中，增加识别域的其它标记或参数。

[0065] 域创建

[0066] 在一个实施例中，将用户管理器128的功能修改为能够增加新用户和还能够增加新域，这可以认为类似于单个用户的子账户。这样做使多个域能够与每个用户账户关联。修改用户管理器128的功能提供特定优势。例如，在具有多个用户的实现方式中(例如，如图3所示)，将域创建与用户管理器128中的用户创建集成在一起是有利的。在(例如，在不支持多个用户账户的智能电话上)仅具有单个用户的替代实施例中，可以在域管理器124中实现这样的功能。

[0067] 因此，在一个实施例中，对用户管理器128进行修改，以便提供以下一个或多个：(i)允许在单个用户下在域之间容易切换，而不用提示典型的登录屏幕；(ii)当在针对这样的域的策略中规定的时间段内切换至另一域时，保持登录一个或多个域；以及(iii)保持域活跃，以有助于域之间的快速切换。利用其它域信令，用户管理器128可以被配置为在存在一个以上的用户账户时仅询问用户名。

[0068] 在创建新域的情况下，用户管理器128可以调用域管理器服务124。创建新域可以类似于创建新用户，同时施加域特有的区别，如将跳过新用户欢迎屏幕。在域创建期间，可以自动地调用程序包管理器136，以安装预先存在的应用或将新应用下载至新域。域策略服务126可以设置默认策略，并且可以执行向导以帮助用户如期望的那样调整新域的策略。

[0069] 如果创建工作域(或其策略是至少部分地由除设备拥有者之外的实体外部地控制的任何其它域)，那么向用于该特定工作域的远程域管理服务器注册该域。这可能要求使用用户的工作凭证进行注册。服务器将批准这样工作域的创建，并且随后下载用户组、设备和工作域专用的策略，图标，凭证，文件，壁纸和应用。

[0070] 域策略

[0071] 在创建域时，与其关联地存储包括策略规定或策略数据的相应安全策略。在一些实施例中，在应用级和/或中间件级执行至少某种域特有的和跨域的策略(例如，认证超时)。在一些实施例中，至少部分地在内核级且依照多个域的相应安全策略来执行与每个域关联的进程和实体的隔离。在一些实施例中，至少部分地在中间件级执行隔离，即由在内核之外操作的操作系统服务和装备执行隔离。与每个域关联的相应策略可以依据该域的期望角色或其与其它实体(如，公司企业服务)的关系或关联而不同。

[0072] 例如，在不同实施例中，一个或多个策略可以是：(i)预定的且静态的；(ii)预定的，但具有一些运行时配置或选择；(iii)在管理服务器上配置之后下载的；或(iv)用户可在设备上配置的。相应策略的特定参数可以考虑任何有关的条件或变量，任何有关的条件

或变量再次与关联的域的特定角色及其与其它实体的关系有关。例如，不同策略的特征可以在于：(i)特定OS服务之间的隔离可以是静态的且预定的；(ii)可以提供可以基于布尔值设置的预定低/中/高安全级别；(iii)可以下载GPS地理围栏(geo-fencing)参数或应用白名单；或(iv)可以在设备上本地配置用于调试对个人域的访问的能力。还可以实现任意结合。

[0073] 在一些情况下，可以在设备上(例如，经由域设置应用144-1、144-2)修改策略，而在其它情况下，可以从远程服务器(例如，用于工作域的远程服务器)下载策略。在一个实施例中，域消息服务122管理策略的下载、验证、认证和更新，并且域策略服务126管理每个域的策略应用。随后，可以将策略分配至施加该策略的系统组件，该系统组件可以在应用级、中间件级或内核级。

[0074] 应用管理

[0075] 上面讨论的提供域信令使得能够跨不同的域进行应用的域专属安装和管理。通常，程序包管理器136可以被配置为基于当前的域或选择的域的DID，或基于与其关联的策略，允许或禁止程序的安装或执行。

[0076] 跨不同的域进行应用的域专属安装和管理能够具有特定优点。例如，域信令使得能够跨多个域进行不同应用版本的安装和管理。安卓™当前的情况是：当一个用户更新应用时，也为所有用户更新该应用。这样的结果不总是期望的。例如，对应用的更新可能需要其它权限，或者包括未由企业测试或支持的特征，因此不是在工作域中期望的。此外，企业可能想要关联的工作域，以仅允许以白名单列出的应用或专门将特定应用列为黑名单。

[0077] 在不同的域中提供不同的应用访问权和控制还提供改善的安全选项，即使在域总是仅由特定个人访问时。例如，安卓™设备拥有者可能更希望不在通常无限制的开放的域中设置谷歌™ Play™商店账户；如果设备被窃，那么账户将在该开放域中可获得，并且通过窃贼使用设备拥有者的账户，该偷窃可能对设备拥有者带来损失。因此，设备拥有者可能期望不在开放域中而作为替代仅在具有更加约束的安全策略的另一域中启用Play™商店应用，例如通常需要访问密码的安全策略，安全密码可能被认为对应用于该开放域是恼人地不方便的。

[0078] 因此，本方案可以包括对安卓™程序包管理器136的一个或多个修改，以使其是域感知的，使得能够根据域策略安装和更新应用。在一个实施例中，对程序包管理器136进行配置，以便维护每个安装的应用的应用标识符和每个域的域标识符之间的关联的列表。当启动进程时，为该进程创建的执行环境标识符基于该应用的应用标识符以及应用在其中执行的域的域标识符。通过这样的方式，程序包管理器136可以被配置为：(i)允许在选择的域中实现应用白名单和/或黑名单，使得在该域中仅可以安装批准的应用；(ii)使应用能够从一个域复制或移动至另一域；(iii)在下载应用时，提示用户应当将应用安装到哪个或哪些域中，而不管账户凭证位于哪个域；(iv)在设置新域时，使现有应用和现有应用的配置和数据能够被复制或移动至该新域；(v)在下载应用更新时，考虑任意应用白名单或黑名单上的软件版本，以使在不同的域中具有应用的多个不同版本(因此，使企业能够选择性地控制例如测试的和批准的应用版本的安装和更新，由此提供与管理程序方案相似程度的应用版本控制)；以及(vi)使能够基于用户输入或基于下载的策略(关于涉及该策略的域)从一个域或多个域(但可能不从其它域)选择性地删除应用。

[0079] 窗口管理

[0080] 在一个实施例中，用于窗口管理器138的默认配置与现有技术类似地为不同域提供不同屏幕。可以使用通知区(notification shade)、导航器应用(例如，域导航器146-1、146-2)或经由按钮、图标、姿势或这些的某种组合等来切换域。

[0081] 本方案还使窗口管理器138能够提供具有混合UI的更具创新性的用户界面，其中与不同域关联的应用在单个屏幕上显示。例如，在一个实施例中，窗口管理器138对表示应用与哪个域关联的一个或多个应用图标提供覆盖。与一个以上的域关联的应用可以提供多个图标，每个图标具有不同的覆盖(例如，不同的颜色、不同的符号、不同的轮廓等)，以表示应用与哪个域关联。这样的方法将消除在域之间进行切换的需要，其中由图标表示域访问，并且在访问与不同于当前域的域关联的应用时，如由被访问的应用的域策略要求的，可能要求用户进行认证。与显示机制无关地维护和执行每个域的策略和数据隔离。本方案的性能不受具有多个图标影响。此方法的优势是在域之间没有可见的切换。不足是设备主屏幕可能变得充斥图标，并且用户在其中操作的域具有较少可视表示。

[0082] 跨域通信

[0083] 系统100可以包括域管理器服务124，域管理器服务124用于管理跨域通信，如用于剪切和粘贴数据、启动电话呼叫、通知、数据共享、发送数据和应用安装等功能。域策略服务126可以用作用于在域之间执行策略的单个点。

[0084] 例如，用户可能希望在域之间移动或复制应用。工作域策略可以实现应用白名单方法，以确保恶意软件不能进入工作域来窃取公司信息(例如，工作联系人或工作文件)。作为进一步的示例，除了当在对应的受保护的域中时以外，可以使一个域中的通知在另一域中显示时变得不透明，或者可能根本不显示。作为另一示例，工作域可以限制数据(如联系人)离开工作域，以防止数据泄露。虽然用户将其个人联系人导入工作域中可能是可接受的，但是工作域策略可能不允许相反的情况。这是由将由域策略服务126管理的策略配置的域之间的单向数据共享的示例。

[0085] 外部通信

[0086] 系统100还可以管理设备内的入站(in-bound)和出站(out-bound)通信。为此，在一个实施例中，域管理器服务124管理可能需要通知或以多个域为目的的网络连接和入站事件。简单的示例是双号码的(例如，双SIM卡)智能电话的情况，在这样的情况下，策略规定对一个号码的呼叫应当被转发至特定域，对第二号码的呼叫应被注册至不同的域。这样的通信在接听入站电话呼叫的单电话号码设备的情况中要复杂得多。策略可以指示针对主叫方id的目的可以访问哪些联系人，以及应当注册呼叫日志信息。在一些实施例中，域策略服务126可以是至少某一策略执行的点，这包括对诸如VPN、蓝牙和WiFi网络资源之类的硬件资源的访问。例如，一些受保护的域的策略可以仅在指定网络上时才允许通信。

[0087] 域执行

[0088] 系统100还提供域和每个域策略的执行，这是对创建和管理域的软件功能的附加要求。在没有域和域策略的执行的情况中，恶意软件或根套件可以静态地或动态地修改系统或内核代码，以防止执行被执行或以更新该策略。

[0089] 在一个实施例中，系统100使用SELinux™和Linux™安全模块(LSM)，以实现强制访问控制(MAC)。MAC确保主题(例如，应用)仅访问由策略允许的对象(例如，应用、文件和资

源)。这通过在安装每个应用时唯一地创建的UID/GID组合执行。如上面讨论的,在系统100的一个实施例中,UID还被扩展或被分配来表示域。

[0090] 但是,SELinux™通常对所有用户下载的应用施加相同类型(因此施加相同策略),这意味着其不执行域。因此,SELinux还可以被修改,以变成域感知的。在一个实施例中,这是通过以下方式实现的:经由策略中基于角色的访问控制字段,或通过针对不同域创建不同策略并且动态地使用域管理器124来在运行时期间调整策略,或者在安卓™的情况下通过在创建进程时通过修改Zygote和/或SEAndroid™的中间件强制访问控制特征来向进程分配域专属SELinux™安全标记以变成域感知的。

[0091] 严格地限制对系统级资源的应用访问仅是可以在内核级实现的多个安全增强中的一个。域内核模块114可以实施其它域感知安全,如控制调试访问、检查策略更新(认证和完整性验证)、加密域数据、检查加载时间应用签名、访问安全硬件和安全操作系统组件(如果可用)并且控制对诸如网络、摄像头和GPS之类的硬件资源的访问。域内核模块114还可以提供整个设备的安全设置,如在启动时内核完整性验证、策略的安全存储、其本身和其它系统级资源(例如,域策略引擎)的完整性验证、确保SEAndroid™被开启、以及远程证明。

[0092] 应注意,域与用户和管理员账户不同。虽然设备拥有者可以具有准许用于创建和删除账户的特定特权的特殊账户,但是这样的特权不等同于根访问且可能对由第三方管理员(例如,工作IT管理员)管理的域是受限的。通过使用SELinux™和SEAndroid™以及本文描述的细化域信令,应用和应用数据保持隔离,即使在不同域之间存在不同的策略和访问控制时。一个域中的恶意软件不能访问另一域中的数据或应用。

[0093] 域切换

[0094] 图4示出框图400,框图400图示从第一域142-1至第二域142-2的域切换方法的一个实施例。用户使用域导航器146-1输入请求切换至第二域的输入。域导航器146-1向活动管理器134发送信号(动作405),以切换至第二域142-2。如果第二域142-2关联于与关联于第一域142-1的用户不同的用户,(例如,从图3中的域A1至域B1),那么活动管理器134向用户管理器服务128发信号(动作410),以注销该用户,但或者不这样做。响应于来自用户管理器服务128的调用(动作412),域管理器服务124向系统设置模块130询问与第二域142-2关联的登录策略(动作415),以及向域策略服务126询问用于使这样的切换能发生的任何其它策略(例如,GPS地理围栏、网络访问要求、内核完整性)(动作420)。活动管理器134向密钥保护中介132通知第一域142-1的任何超时(这可以是立即的或延迟预定的时间段)(动作425)。密钥保护中介132实现与第二域142-2关联的策略。如果满足该策略检查,那么向密钥保护中介132通知切换至第二域142-2,并且基于策略(例如为访问所需要的认证)决定访问(动作430),或直接访问域(例如,如果不要求认证)(动作435),或可选地,可以拒绝切换。在切换之后,活动管理器134在第二域142-2中执行应用启动器424。

[0095] 在另一实施例中,如上所述的,在选择应用时可以暗示域切换,并且将不需要域导航器。

[0096] 在一些实施例中,可以配置域切换方法,以使能够进行向加密域的安全切换。可以加密与一个或多个域关联的数据文件,如使用密码术堆栈文件系统进行加密。例如,eCryptFS文件系统(http://ecryptfs.org)是用于Linux的兼容POSIX的企业密码术堆栈文件系统。在这样加密与域关联的数据文件的情况下,可以认为域可是加密的域。对称密钥可

以用于加密和解密被加密的域的数据，并且可以存储在Linux内核密钥环(内核存储器中的安全储存器)中，但还可以存储在任意安全储存器中。在密码术堆栈文件系统中，使用多个对称密钥是典型的，但是将理解，在一些实施例中，可以使用单个密钥。

[0097] 如上所述的，具有多个域的设备可以包括需要访问认证的一个或多个域。例如，在设备操作系统是安卓的情况下，内建的安卓锁屏认证(图案、pin、密码等)可以用于控制对域的访问。如果域也是加密的，那么此锁屏认证还可以用于加密和解密由密码术文件系统使用的密钥，以访问加密的域数据。

[0098] 由于设备可以具有多个域，所以多个域中的一个或多个可以是加密的，并且多个域中的一个或多个可能需要认证，在从当前域(当前拥有用户界面(UI)焦点的域)向不同目标域切换时存在四种可能的场景：域已经运行；域未运行，且不是加密的；域未运行，是加密的，但不要求认证；以及域未运行，是加密的，且要求认证。(如果与域关联的进程正在运行，那么该域被认为正在运行)。

[0099] 鉴于这些可能性，图9图示从当前域向目标域切换的方法900。如所图示，可立即切换至正在运行的域。在接收到向目标域切换的输入(开始902)时，确定该域是否正在运行(决策904)，且如果“是”(分支906)，则在UI中示出目标域(步骤908)且切换完成(结束910)。如果该域未运行(分支912)，那么确定该域是否被加密(决策914)；如果“否”(分支916)，则启动该域(步骤918)，在UI中示出该域(步骤908)，并且切换完成(结束910)。如果该域被加密(分支920)，那么确定该域是否要求认证(决策922)；如果“否”(分支924)，那么可以加载解密密钥并且装载文件系统(步骤926)，启动该域(步骤918)，在UI中显示该域(步骤908)，并且切换完成(结束910)。如果要求认证(分支928)，那么接收认证信息(步骤930)，基于该认证信息解密文件系统密钥(步骤932)，加载解密密钥并且装载文件系统(步骤926)，启动该域(步骤918)，在UI中显示该域(步骤908)，并且切换完成(结束910)。

[0100] 因此，如图9中可以看到的，可以启动并立即切换至当前未运行的未加密的域。但是，如果尝试切换至加密的域，则在可以使用该域以前必须将将密码术文件系统密钥加载到Linux内核密钥环内。如果加密的域不要求认证，则可以加载密码术文件系统密钥，且在没有用户干预的情况下装载文件系统。但是，如果加密的域要求认证，那么在可以加载密码术文件系统密钥以前必须首先解密密码术文件系统密钥本身，并且装载文件系统。因此，在最后的启动需要认证的加密域的情况中，在可以访问(装载)目标域的数据之前，需要一种机制来收集目标域的认证数据。

[0101] 但是，在许多设备操作系统中，认证过程必须在当前域中操作或与当前域关联。例如，在安卓中内置的已有锁屏认证机制对当前用户或域进行认证。在切换至目标域时，安卓锁屏从锁屏(如锁屏小工具、实时壁纸以及输入方法编辑器(IME))起运行针对目标域的进程。为了保留传统的安卓用户体验，认证需要在域切换之后发生。

[0102] 存在提供此功能的几种替代方法，如下。

[0103] 在第一替代中，提供定制用户界面(UI)以在切换至目标域之前获取认证信息。虽然此方法拥有可以使其在一些情况下适宜的多个好处，但是其还忍受如下特定缺陷。例如，此方法需要有效地努力以复制已在安卓中内置的认证机制，并且将要求更新以维持与对内置的安卓机制的更新的互操作性。此外，此方法引入安全隐患，因为定制认证UI进程将在用户正从其切换的域中运行。老练的攻击者可能替换可能不可信的域中的重要应用程序包

(如,输入方法编辑器(IME)),以捕获可信加密域的域认证信息。

[0104] 在第二替代中,方法首先切换至目标域,但不装载目标域的数据。随后,在装载目标域的数据之前,该方法仅运行使锁屏起作用需要的那些进程,然后完成切换至目标域。虽然此方法拥有可以使其在一些情况中适宜的多个好处,但是其还受到如下特定缺陷。例如,从锁屏起正常地运行的应用组件(锁屏小工具、实时壁纸以及输入方法编辑器(IME))可能要求访问加密的文件系统。事先确定什么程序包将运行通常是不可能的,因为用户和原始设备制造商(OEM)都可能改变、更新或移除这些组件,因此这些问题不能被预料到和被补偿。此外,域切换操作直至已提供域认证信息才完成。这使设备处于安卓未被设计处理的中间的未限定的状态。这在整个安卓中间件中形成了在安卓发布之间必须正确地处理、测试以及维护的许多其它边缘情况。

[0105] 在第三替代中,方法切换至在设备上有目的地创建的中间域,以有助于认证信息的安全收集以及使在域之间能够进行安全转变。中间域在切换至未运行的加密域时启动,并且要求认证。此方法克服了由上面描述的前两个替代拥有的许多缺点。

[0106] 因此,图10示出从第一正在运行的域切换至不同的目标域的方法1000,其中目标域是加密域(与在加密的文件系统包含的数据文件关联或具有在加密的文件系统中包含的数据文件)且未正运行。发起至目标域的域切换(开始1002)。目标域未在运行,被加密,且要求认证。中间域成为当前域(向安卓中间件报告的)(步骤1004),并且在中间域中开始锁屏进程(步骤1006)。修改锁屏组件或另外提供锁屏组件,使得锁屏组件在被调用时将示出用于目标域的认证盘问,并且显示识别目标域的某种指示。

[0107] 如果与目标域关联的一些UI要素未存储在加密的文件系统中,而是作为替代存储在另一位置(例如,未加密的文件或数据库中的元数据),那么可以与认证盘问一起显示这样的UI要素。例如,在这样的情况下可以显示与目标域关联的壁纸。可选地,可以显示某一其它壁纸或可视物,以指示正发生向目标域的切换。类似地,如果在与加密的文件系统不同的其它位置存储与目标域关联的IME,那么其可以用于接收认证信息。可选地,可以接收用户对用于输入认证信息的IME的选择(步骤1008)。(这可以包括例如中间域中的语言不同于目标域的语言的情况)

[0108] 然后,使用所选择的IME接收认证信息(步骤1010)。如果用户提供目标域的正确认证信息,则解密目标域的密码术文件系统密钥(步骤1012),加载这些密钥,并且装载文件系统(步骤1014)。解除通常在目标域中显示的锁屏(步骤1016)。(这与用户已经直接在该域中认证完全相同,并且提供对锁屏认证将如何对未加密的域起作用的无缝用户体验)目标域启动,成为当前域(步骤1018)。新域在UI中显示(步骤1020),并且域切换完成(结束1022)。

[0109] 如所提到的,此方法克服了切换至未运行的加密域的其它方法的至少一些缺陷,并且进一步提供了如下多个优点。

[0110] 例如,优点是:认证进程在任意用户可控的域之外发生,以使认证信息的收集更安全。从锁屏起运行的进程在不易受到从其它用户可访问的域的改变中产生的干扰影响的受控环境中运行。安卓中间件中需要的改变更容易维持,并且更容易与安卓中内置的多用户状态机兼容。这引起更少缺陷、更少维护以及更好的前向兼容性。与上面提到的其它选项相比,对IME的攻击(例如,替换、或特权提升)或用于密钥保护的用户界面更难以实施,并且将使受益最小化(例如,对中间域的访问)。需要的附加性能和存储最低。

[0111] 多个实现方式选项是可获得的。中间域可以在操作系统的最早启动时创建，或可选地可以在创建第一加密域之前的任意其它时间创建。可以锁定中间域，以防止用户进行除认证之外的其它操作。表述“锁定”可以被理解为表示禁用不需要的任意应用、服务或其它特征，或作为替代地选择性地仅启用需要的那些特定应用、服务或其它特征。例如，可以包括禁用锁屏小工具和谷歌搜索。可以使用策略机制(包括SELinux和SEAndorid)进一步锁定中间域，以进一步最小化安全风险。与其它域不同，中间域仅简单地在域之间进行切换时运行。在运行时，其相对于由安卓维护的三个活跃运行域的最大限制不被当做运行域。因此，移动至中间域不引起其它域关闭。在启动和停止中间域时，安卓不发送在启动域时通常发送的广播中的许多广播。这产生显著的性能改善，因为其防止启动不必要的进程和应用。使用白名单、禁用列表、黑名单等，中间域可以具有在域中安装的最少应用，以减少这些应用可能存在的安全风险。

[0112] 中间域可以被预配置为具有允许的应用、服务等的特定选择，或可以使用与由所有域使用的机制相同或相似的执行机制以类似于其它域的方式(例如通过使用专用于中间域的策略)来动态地设置中间域。

[0113] 域消息服务协议

[0114] 图5示出框图500，框图500示出域消息方法。与第一域142-1关联的第一进程505生成事件消息(例如，消息接收通知(其中，消息可以是电子邮件)、剪切并粘贴动作、文件复制)。生成该事件的第一进程505发送关于该事件的消息(可以采用广播的形式)，并且该消息由域管理器服务124接收(动作510)。在一个实施例中，在第二域142-2中操作的第二进程515可以是侦听进程，但将理解可选地可以使用API。域消息服务122检查在其它域中的侦听进程(如第二域142-2中的第二进程515)被配置为对接收到的事件消息做出响应。

[0115] 在确定第二域142-2中的第二进程515是这样配置的以后，域管理器服务124向域策略服务126发送关于事件消息类型(例如，通知、剪贴板缓冲区、文件)的信号(动作520)。域策略服务126实现相关策略，这样可以引起多个不同动作。例如，所请求的事件可以被允许(例如，可以通过不超过100个字符的缓冲)，或不被允许(例如，策略可以允许将文件转移至域，但阻止从该域进行这样文件转移)。可选地，策略可以引起消息被过滤(例如，可以使特定字段不透明，或者仅提供标志通知，如没有像发送方、主题等之类的细节的电子邮件接收通知)。依照该策略，将事件消息传递给第二域142-2中的第二进程515(动作525)。

[0116] 跨域执行协议

[0117] 图6中示出框图600，框图600图示跨域执行方法。

[0118] 在该方法中，第一域142-1中的第一进程605生成动作，其中该动作请求实施与第二域142-2相关的某一动作。例如，可以在第一域中选择新电子邮件的通知，并且输入请求以在第二域中查看该电子邮件。可选地，使用第一域142-1中的域设置144-1服务，可以输入删除第二域142-2的请求。或者，当在第一域142-1中操作时，可以输入请求，以实施从第二域142-2向特定电话号码的电话呼叫。

[0119] 在由第一域142-1中的第一进程505产生动作之后，活动管理器134接收来自第一进程505的域切换请求(动作610)。如果该切换需要认证，那么如果认证失败，则拒绝该请求。活动管理器134向域策略服务126发送信号，以检查与第一域142-1和第二域142-2关联的相应策略(动作615)，以便确定两个策略允许做出请求的第一域142-1向第二域142-2发

起所请求的动作。

[0120] 如果这两个策略允许这样，那么活动管理器134启动与第二域142-2关联的所请求的第二进程620(动作625)。关于上面介绍的示例，可以启动电子邮件服务，或者可以启动域设置144-1服务，并且提示用户确认第二域142-2的删除，或者可以通过显示要呼叫的期望号码来启动电话服务。

[0121] 域应用安装协议

[0122] 图7示出框图700，框图700图示域应用安装方法，其中在第一域中安装的应用被移动或被复制至第二域。

[0123] 如上面讨论的，可以与选择的安全域关联地安装应用，在这样的情况下与所安装的应用的应用标识符关联地存储域的DID。

[0124] 使用域设置144-1服务，用户可以选择将应用移动或复制至不同的域，如从第一域142-1移动或复制至第二域142-2。域设置144-1服务向程序包管理器136发送信号，以在第二域142-2中安装该应用(动作705)。程序包管理器136向域管理器124发送信号，以确定第二域142-2的安全标记(动作710)。随后，程序包管理器136利用从域管理器124接收的正确安全标记在第二域142-2中安装该应用。如果所选择的动作是移动而不是复制，那么域设置144-1服务向程序包管理器136发送信号，以从第一域142-1卸载应用(动作715)且还向新域发送应用用户数据。

[0125] 更新策略协议

[0126] 图8示出框图800，框图800图示更新策略方法。

[0127] 域消息服务122接收来自远程管理服务器805的策略(动作810)，或可选地，经由设备上的设置屏或经由API接收该策略，随后域消息服务122将该策略传递给域策略服务126(动作815)，随后根据情况传递给域内核模块114(动作820)，域内核模块114可以将策略存储在安全储存库112中(动作825)。由域内核模块116验证策略的起源的完整性和真实性。可以在域内核模块116或安全储存库112中施加防回滚(anti-rollback)机制，以确保不能重新使用或重演较旧的策略。域策略服务126随后加载策略和之前的策略，以便智能地仅施加所更新的策略中已改变的那些策略。域策略服务126可以向增强的Linux安全模块116发送信号，以加载策略的更新的SELinux部分(动作830)。域策略服务126向系统设置模块130服务发送信号，以更新在系统设置模块130中施加且由系统设置模块130执行的策略，如密码强度、壁纸和启动器(动作835)。域策略服务126随后更新专属于的域的其自身的策略，如域加密、域调试访问、跨域策略和域名。

[0128] 优点

[0129] 本发明的方案提供一种方式来安全地建立、维护和管理独立的受保护的域并且限定和隔离这样的独立的受保护的域中的应用和数据。与现有技术相比，本发明的方案在存储器、空间和计算功耗方面是有效的。其保持本地操作系统特征(包括应用的后向兼容性)。其在一些域中保持本地、直观的设备用户界面，还使能其它域中许多不同的用户界面选项和策略，而不是传统的“全部或全部不”设备锁定和/或用户账户访问。其利用不同域拥有者使能一个设备上的两个人、多个人、多个人之间的多个域使用、多个工作和“开放”域。其使能这样的多个域的远程管理和策略更新。其允许每个域的不同访问控制和策略。其允许策略确定是否能在域之间转移数据。其使新的使用模式(包括临时共享)更适于移动设备。其

使与其它方案相比能进行每个域中可用的应用的更细化控制。本方案可以显著地简化或甚至消除与基于管理程序的虚拟化关联的域之间的操作系统级“硬切换”，其中每个域与可以由每个对应的管理程序复制的独立的一组操作系统进程关联地操作。其在域之间隔离应用和应用数据，而没有当前方案的弱点。其将域中的应用和数据与该域外部的恶意应用隔离。最后，其解决隐私顾虑和移动设备用户的选择自由。

[0130] 独立于实现细节，存在通过域信令、域管理和域执行引入的显著优势和特征。这些如下。本方案保持原始本地操作系统特征(包括应用的后向兼容性)。所有本地操作系统权限检查和IPC机制将共同存在，并且仍将有效。操作系统不变地操作，并且本方案与之前的操作系统后向兼容。与现有技术相比，本方案在存储器、空间和计算能力方面是有效的。与像虚拟化这样的可选方法相比，设备性能和存储以及存储器利用是非常有效的，虚拟化对操作系统堆栈进行复制，这引发大量CPU和RAM开销。由于本地OS实现，所以与现有技术相比，域之间的切换非常快且有效。

[0131] 本方案利用不同域拥有者使在一个设备上的多人域、多个工作和“开放”域之间能够有两个人、多个人、多个域使用。能够以可忽略的存储器和性能影响增加和执行多个受保护的域。在单个设备上可以存在多个受保护的工作域。例如，如果用户具有多个客户，那么在相同的设备上可以存在公司X域和公司Y域。可选地，设备可以被配置为具有公司机密域和公司分类域，每个域具有不同的策略(例如，位于公司分类域中的应用的安全策略可能更受限制，如它们可以仅在正常工作期间或在设备连接至公司WiFi网络时访问)。设备可以被配置为具有用于方便访问的开放共享域，且被配置为使能设备和开放域中的应用与家庭成员或同事的自组织(ad-hoc)共享。用户可以具有用于私人目的的保护域，如以便隔离针对秘密关系或用于移动银行和商业目的的消息和联系人信息。不是设备拥有者的雇主的服务提供商(如银行)可能期望在设备上具有受保护的域，该受保护的域包含用于访问他们的服务的各种应用，如账户访问、信用卡或借记卡服务、资本交易、服务(如保险、贷款等)报价。服务提供商将具有以下信息：他们的应用和与这样的应用关联的用户的个人信息是安全的且可以在设备丢失时被擦除或被锁定。

[0132] 本方案针对不同的域、在多个域之间以及针对单个设备上受保护的域的进站通信和出站通信，允许不同的访问控制和策略。域策略可以在本地(例如，经由设备设置)管理或(例如，经由云服务)远程地管理。策略还可以由设备拥有者或第三方管理，如雇主或服务提供商。跨域通信和数据共享可以是限定和执行的策略。数据加密可以是域感知的。电话功能、主叫方通知和紧急呼叫等可以是域感知的和基于策略。例如，可以阻止特定域的向外呼叫。网络连通性可以是域感知的和策略执行的。任务选择器和进程显示可以是域感知的。例如，可以仅在登录域时显示进程。通知可以是域感知的和基于策略。例如，工作域通知可以仅从特定页面可见，以避免共享期间的数据泄露。或者，通知可以指示提供该通知的应用，但具有精简的信息(例如，不公开接收到的电子邮件的标题，或接收到的SMS的发送方，等等)。云备份和同步机制也可以是域感知的。例如，开放域可以被备份，即使没有与该域关联的特定账户。

[0133] 本方案保持原始本地的且直观的用户界面，还启用不同域之间的许多不同用户界面选项和策略，而不是传统的“全部或全部不”设备锁定和/或传统的多用户账户访问。用户界面和域之间的切换现在可以被定制为域转移的类型。可以保持传统的用户账户型界面，

并且每个域可以仍然被个性化并且针对每个域配置有所有标准本地OS能力，如每个域有不同的背景和/或不同的启动屏幕。每个域可以配置用户认证机制(例如，密码、生物特征、模式、无认证)。域登录策略可以用于减少或消除当在域之间切换时重复地认证用户的需要。可以依照针对每个受保护的域设置的策略(例如，在设备不活动15分钟后自动注销，或在域不活动5分钟之后自动域注销，或当在特定域中时每10分钟重新认证，等)，对每个受保护的域执行访问控制和认证技术。本方案使新使用模式更适于移动设备(包括应用的自组织共享，如经由开放域的自组织共享)。这是移动设备中的最近特征的扩展，其中一些设备能力从设备锁屏起可用，而不要求认证(例如，用户可以仍然拍摄照片或接听呼入)。不是限制功能，利用域信令和域隔离执行，开放区域可以提供对应用的全部特征访问，尽管可能具有其它特殊策略，如受限的互联网访问(例如，没有或仅通过WiFi)以及受限的电话访问(例如，仅呼入、或仅本地呼叫等)。可以通过使用其它用于显示域的方式(例如，图标上的覆盖)来消除域之间的切换。设备拥有者可以保持域在文件夹、标签(tab)或由操作系统支持的任意其它机制中单独地分组(可能出于隐私原因或个人偏好)。在访问标签或特定应用时仍将施加每个域的认证策略，但可以不需要切换和不同的域“主屏”和壁纸等。

[0134] 与其它方案相比，可以以更细的粒度控制和显示每个域中可用的应用，而在设备上仅存储一个副本，因此提供存储器和CPU的非常有效使用。程序包管理器可以管理每个域中的应用的安装——它已在用户账户之间进行的——但以更简洁的域专属机制。可以由策略控制每个域的应用的可用性、显示和访问。可以每个域(除每个用户账户以外)地隔离应用数据，并且(例如，如果设备丢失或终止雇佣等)可以针对每个域容易地删除和管理应用数据。可以以更直观的且更具创造性的方式移动或擦除应用，该方式类似于在主页和标签之间移动应用，而不是如安卓4.2那样针对每个域实施应用安装。

[0135] 本方案可以利用SELinux的域感知版本来执行由域规定的应用和应用数据隔离。其可以确保由一个域上的应用进行的访问不能访问另一域。其确保跨域呼叫仅可能通过执行策略的域管理器服务。其确保一个域上的恶意软件不能影响另一域中的应用和数据。其确保没有认证的域的使用不影响其它域的安全。

[0136] 本发明的方案不影响其它安全技术的使用，如虚拟化和容器，因为本方案与那些方案后向兼容。特别地，修改的类型2管理程序可以利用域信息作为不同操作系统之间的切换的一部分。应用容器方案也可以部署在本发明的方案中。

[0137] 虽然已具体地关于安卓和Linux操作系统描述上面的实施例，但是应理解，本文公开的原理适用于拥有由本公开提到的相关特性的任意操作系统。

[0138] 虽然上面已将操作该操作系统的设备称为移动设备(其可以包括智能电话、平板、个人数字助理(PDA)、智能手表、或任意类似设备)，但是将理解，本文公开的原理适用于拥有由本公开提到的相关特性的任意设备，并且在一些实施例中包括通用计算机。

[0139] 在前述描述中，为了解释而陈述许多细节，以提供对本发明的实施例的透彻理解。但是，本领域技术人员将明白，为了实施本发明，不需要这些特定细节。在其它实例中，为了不模糊本发明，以框图的形式示出了众所周知的电子结构和电路。例如，不提供关于本文描述的本发明的实施例是否被实现为软件例程、硬件电路、固件、或它们的组合的特定细节。

[0140] 本发明的实施例可以被表示为存储在机器可读介质(也称为计算机可读介质、处理器可读介质、或具有在其中包含的计算机可读程序代码的计算机可用介质)中的软件产

品。机器可读介质可以是任意合适的有形介质，任意合适的有形介质包括磁存储介质、光存储介质或电存储介质(包括磁盘、光盘只读存储器(CD-ROM)、存储设备(易失性的或非易失性的)或类似的存储机制)。机器可读介质可以包含多组指令、代码序列、配置信息或其它数据，它们在执行时引起处理器实施根据本发明的实施例的方法中的步骤。本领域技术人员将理解，实现所描述的发明所需要的其它指令和操作也可以存储在机器可读介质上。从机器可读介质运行的软件可以与电路交互，以实施所描述的任务。

[0141] 本发明的上述实施例的目的仅在于作为示例。本领域技术人员可以对特定实施例进行改变、修改和变形，而不脱离本发明的范围，本发明的范围仅由本文所附的权利要求限定。

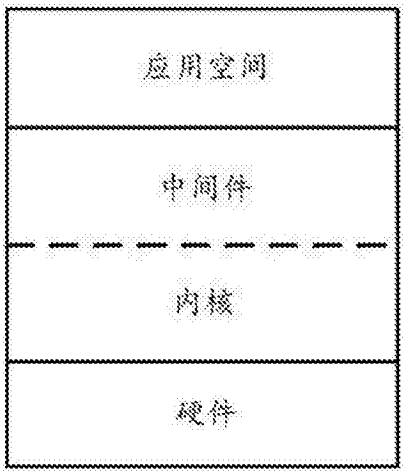


图1A(现有技术)

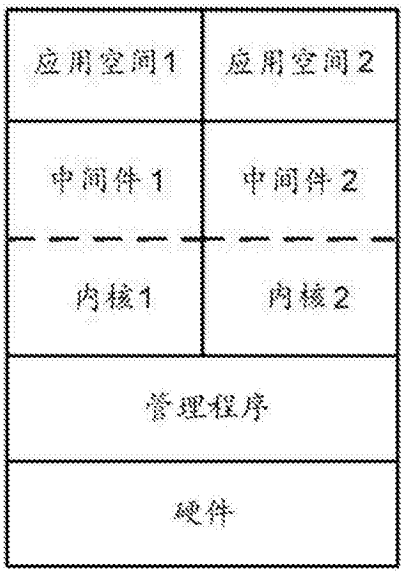


图1B(现有技术)

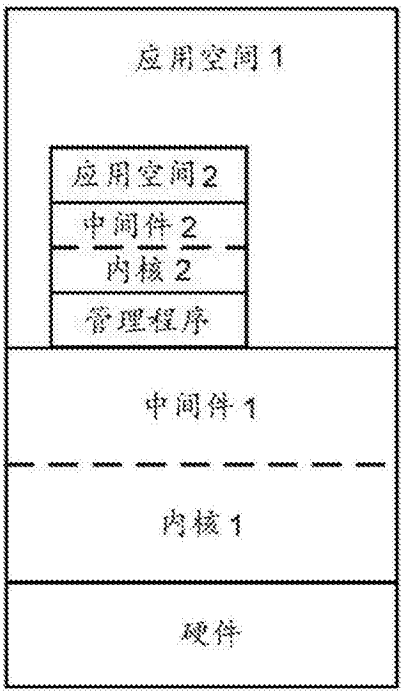


图1C(现有技术)

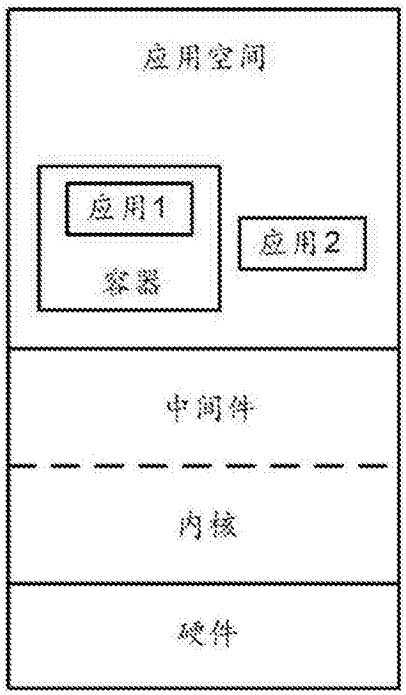


图1D(现有技术)

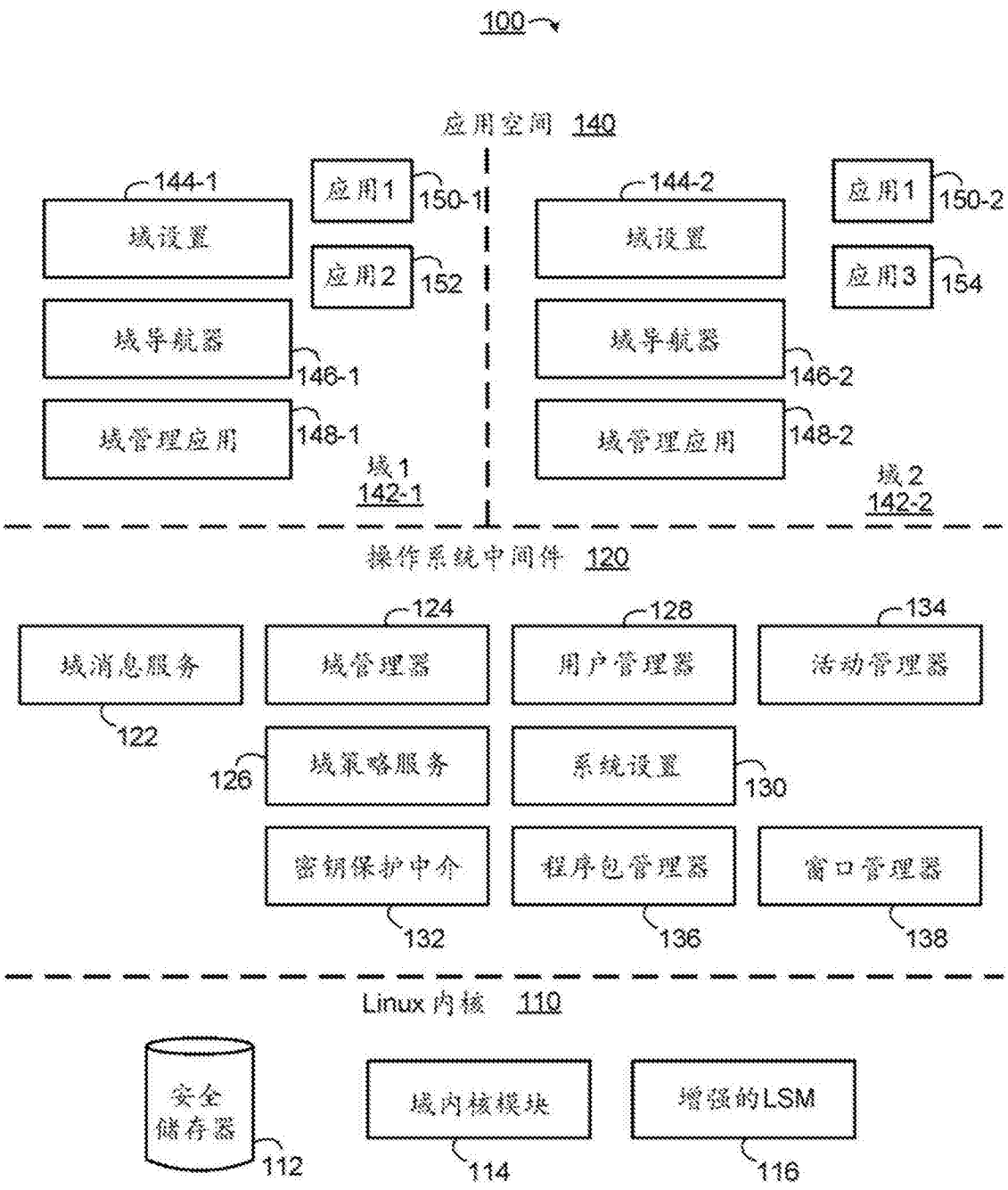

100
应用空间 140
144-1
域设置
应用1
150-1
应用2
152
域导航器
146-1
域管理应用
148-1
域1
142-1
144-2
域设置
应用1
150-2
应用3
154
域导航器
146-2
域管理应用
148-2
域2
142-2
操作系统中间件 120
域消息服务
122
124
域管理器
126
域策略服务
128
用户管理器
系统设置
130
134
活动管理器
密钥保护中介
132
程序包管理器
136
窗口管理器
138
Linux 内核 110
安全
储存器
112
域内核模块
114
增强的LSM
116

图2

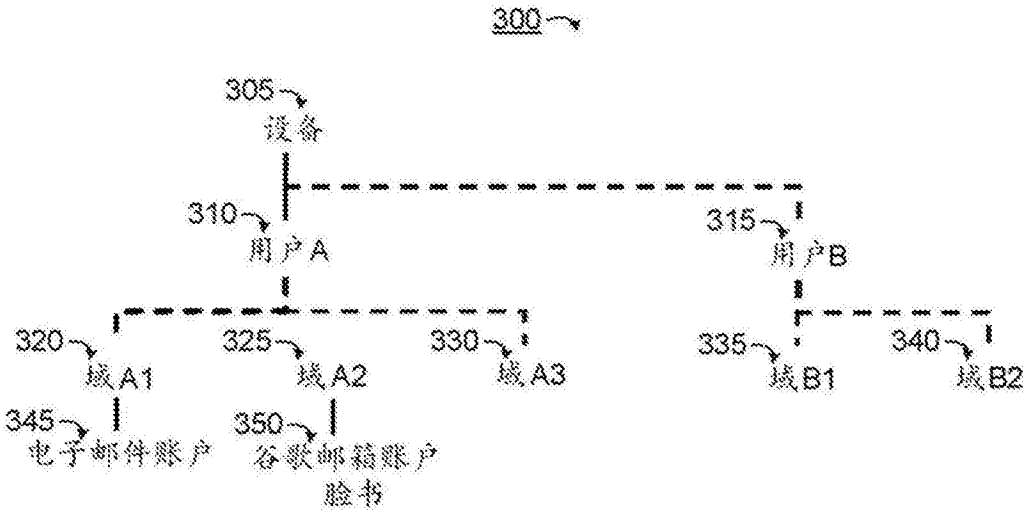

300
305
设备
310
用户A
315
用户B
320
域A1
325
域A2
330
域A3
335
域B1
340
域B2
345
电子邮件账户
350
谷歌邮箱账户
脸书

图3

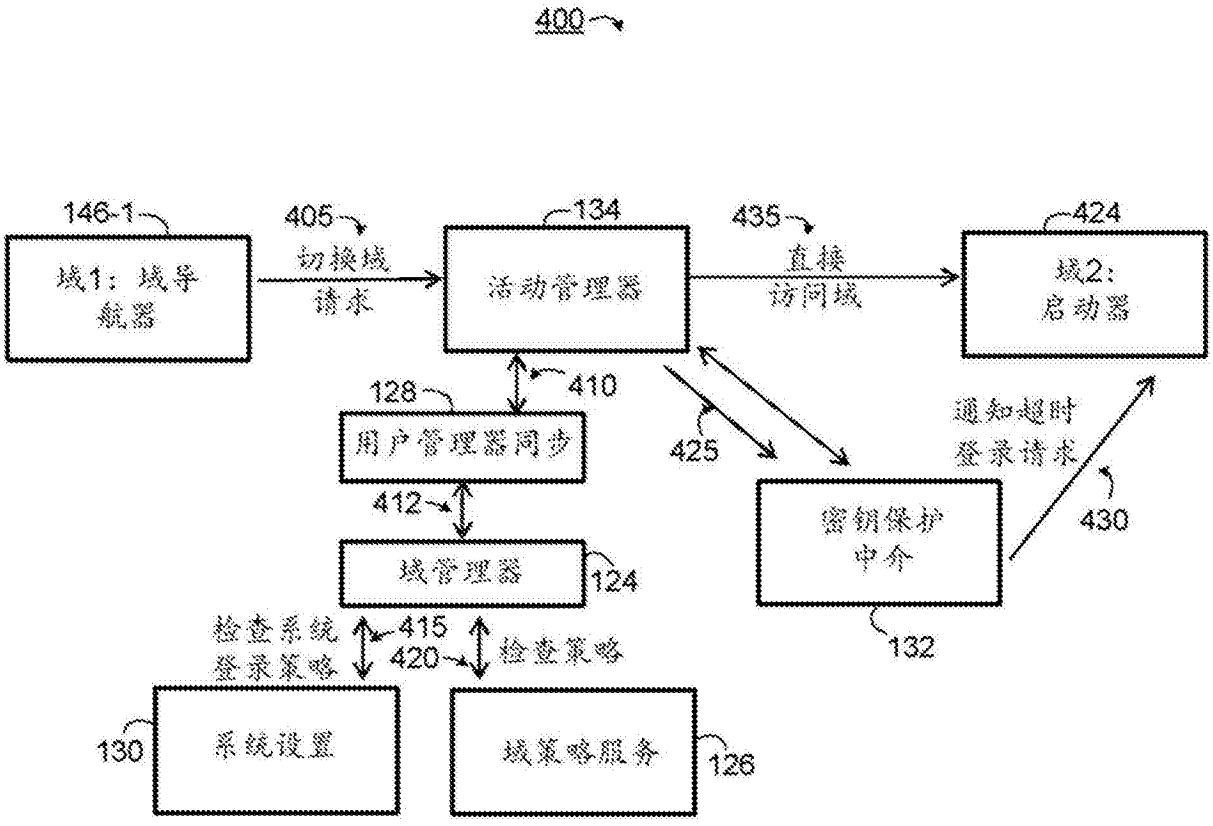

400
146-1
域1：域导航器
405
切换域请求
134
活动管理器
435
直接访问域
424
域2：启动器
410
128
用户管理器同步
412
域管理器
124
425
通知超时登录请求
430
密钥保护中介
132
检查系统登录策略
415
420
检查策略
130
系统设置
域策略服务
126

图4

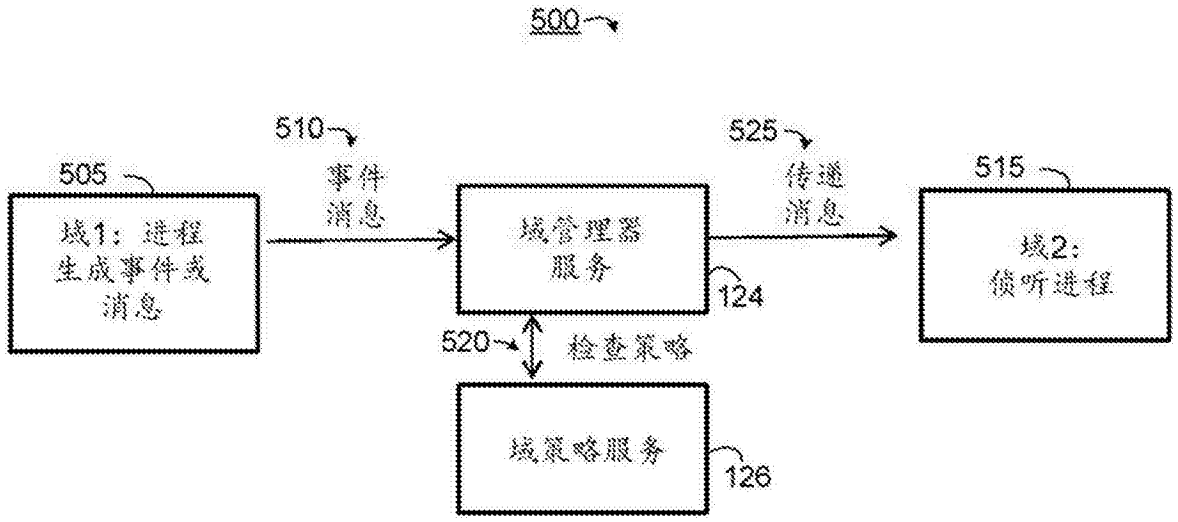

500
505
域1：进程生成事件或消息
510
事件消息
域管理器服务
124
520
检查策略
域策略服务
126
525
传递消息
515
域2：侦听进程

图5

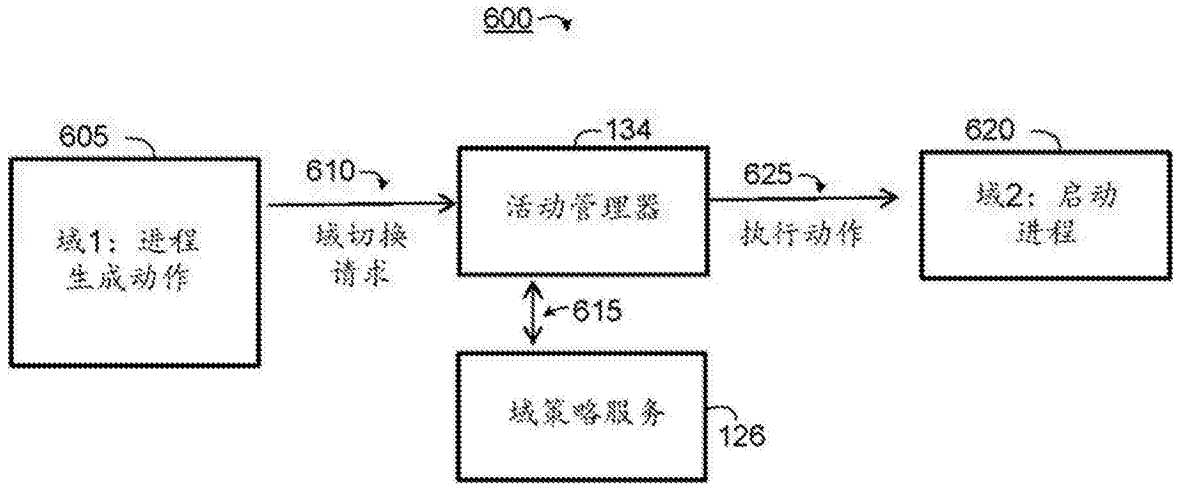

600
605
域1：进程生成动作
610
域切换请求
134
活动管理器
615
域策略服务
126
625
执行动作
620
域2：启动进程

图6

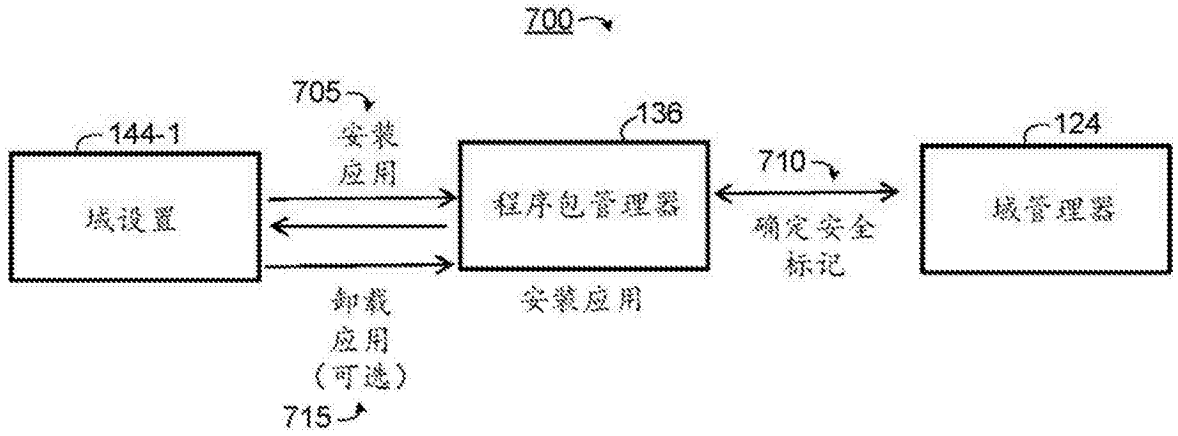

700
705
安装应用
144-1
域设置
136
程序包管理器
卸载应用（可选）
715
安装应用
710
确定安全标记
124
域管理器

图7

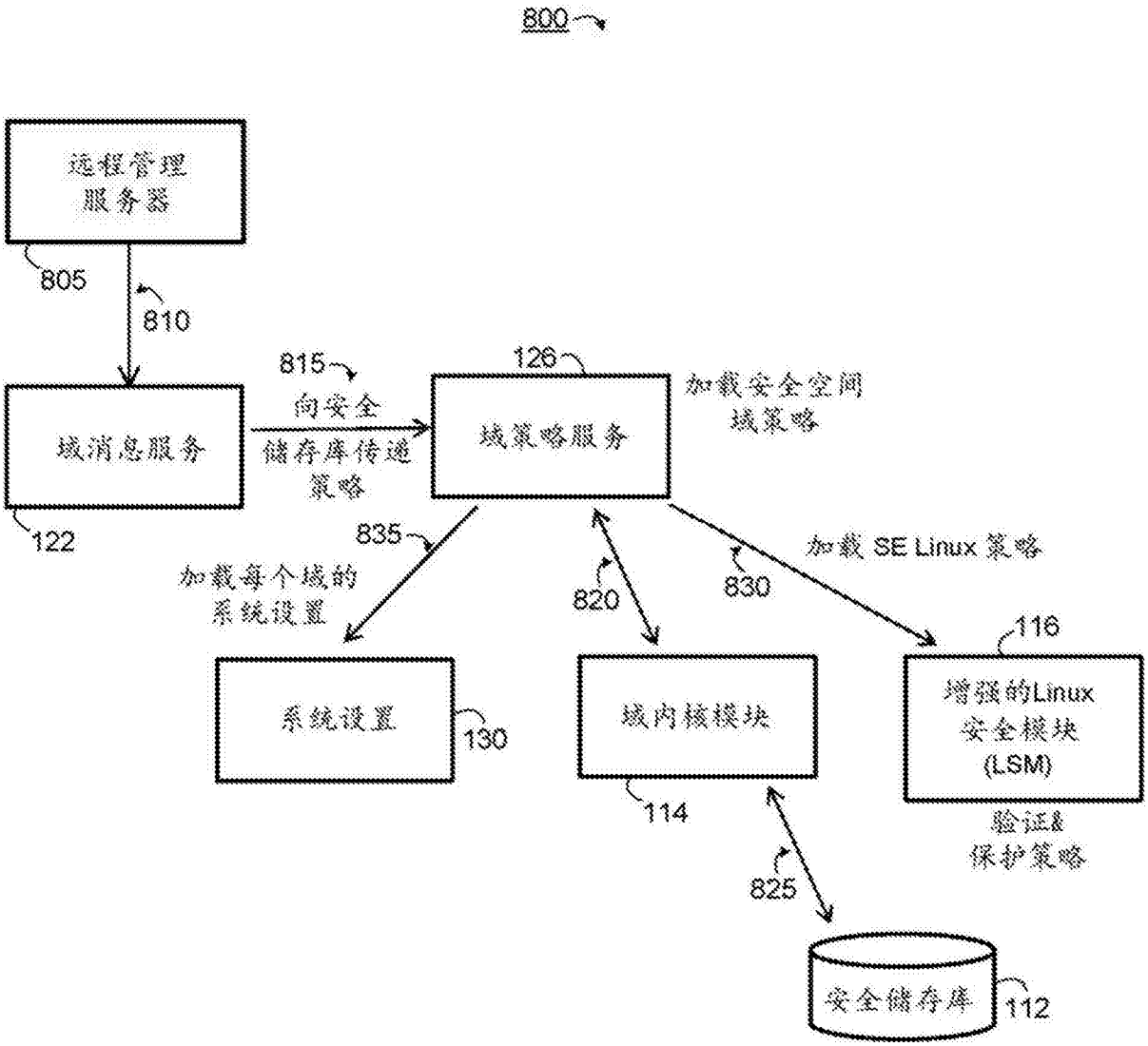

800
远程管理
服务器
805
810
815
向安全
储存库传递
策略
126
加载安全空间
域策略
域消息服务
122
域策略服务
835
加载每个域的
系统设置
820
830
加载 SE Linux 策略
116
系统设置
130
域内核模块
114
增强的Linux
安全模块
(LSM)
验证&
保护策略
825
安全储存库
112

图8

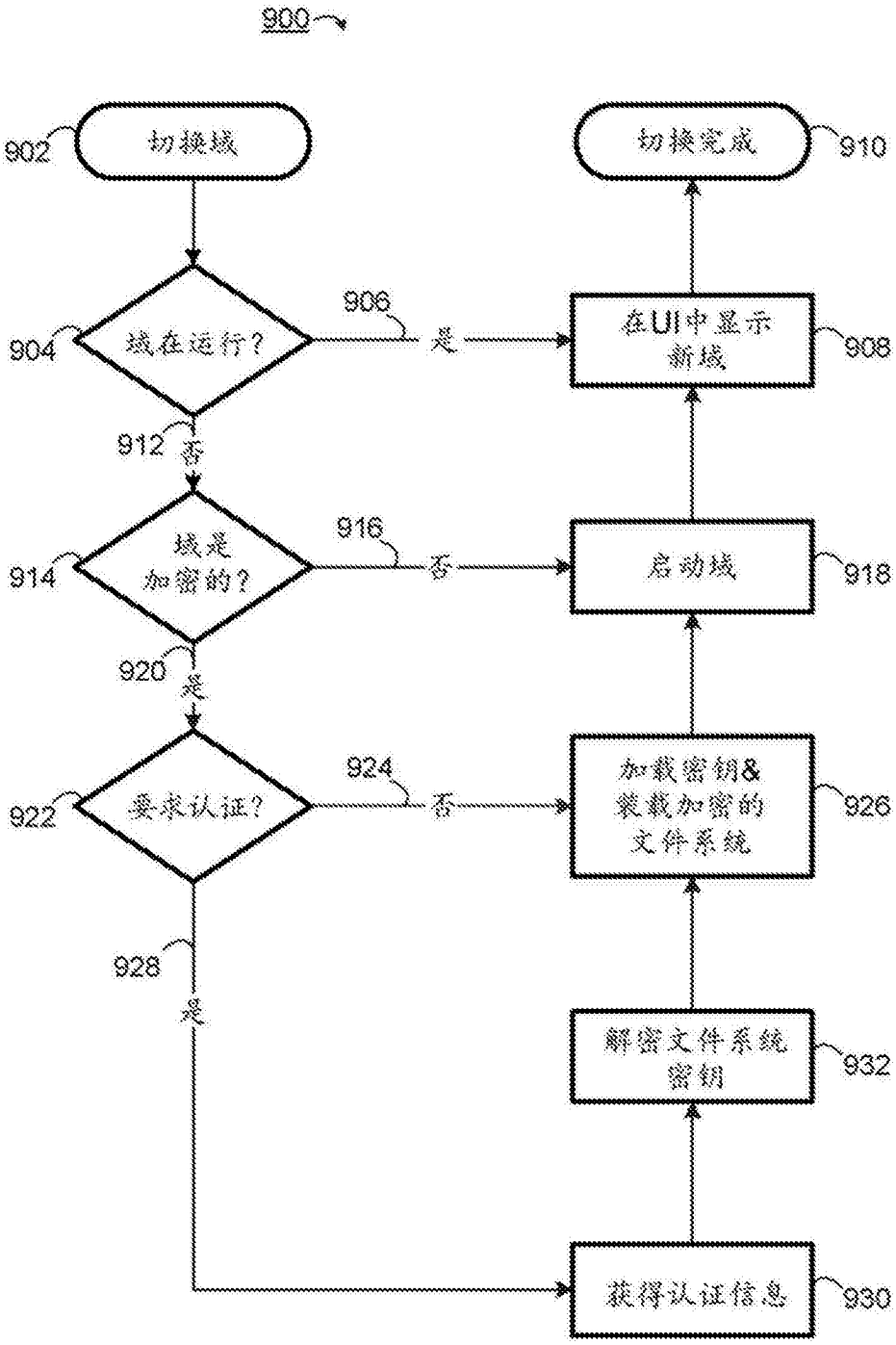

900
902
切换域
904
域在运行?
906
是
908
在UI中显示新域
910
切换完成
912
否
914
域是加密的?
916
否
918
启动域
920
是
922
要求认证?
924
否
926
加载密钥&装载加密的文件系统
928
是
930
获得认证信息
932
解密文件系统密钥

图9

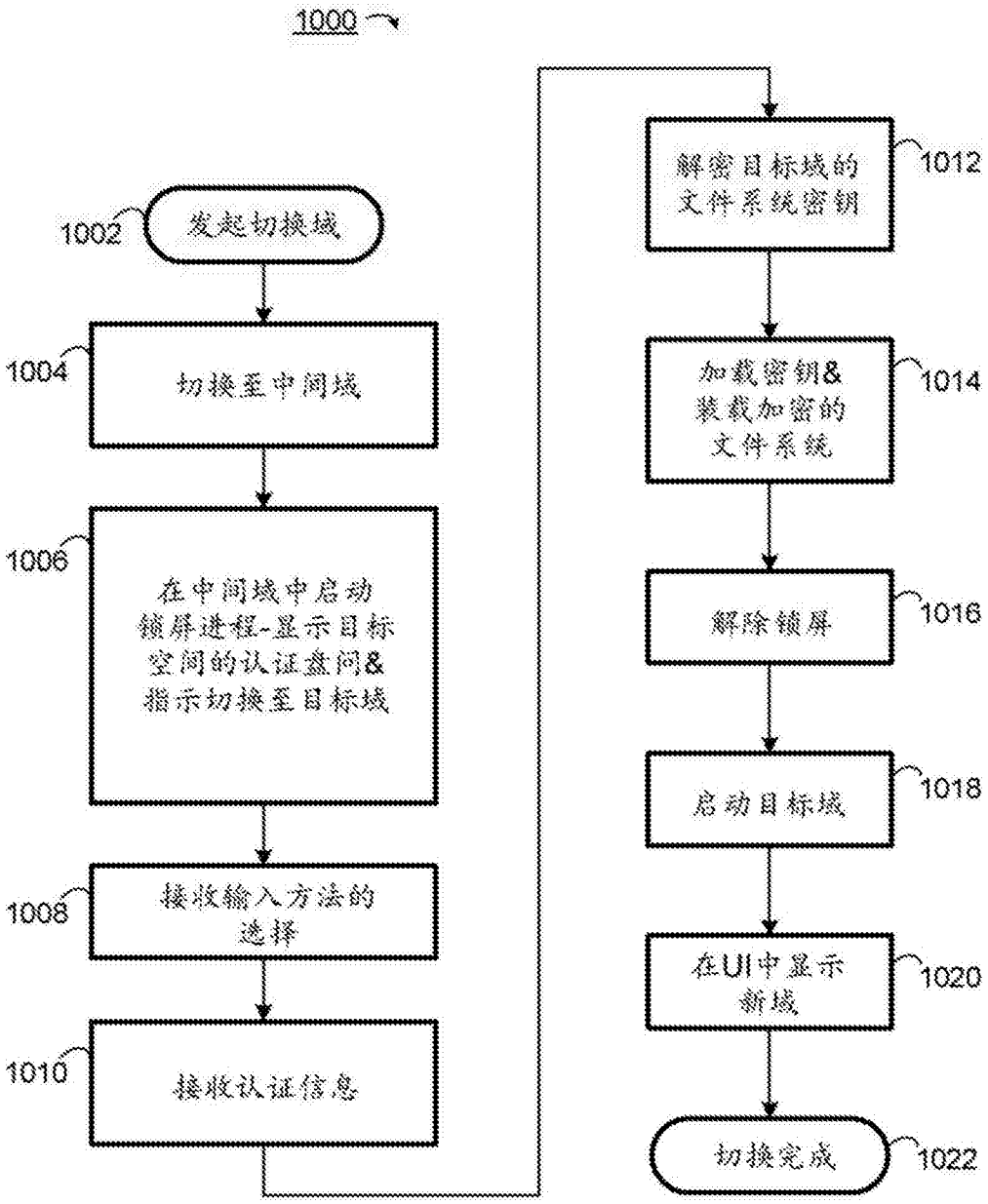

1000
1002
发起切换域
1004
切换至中间域
1006
在中间域中启动
锁屏进程-显示目标
空间的认证盘问&
指示切换至目标域
1008
接收输入方法的
选择
1010
接收认证信息
1012
解密目标域的
文件系统密钥
1014
加载密钥&
装载加密的
文件系统
1016
解除锁屏
1018
启动目标域
1020
在UI中显示
新域
1022
切换完成

图10