(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102217226 B
(45)授权公告日 2015.05.20

(21)申请号 200980145855.0
(22)申请日 2009.10.30
(30)优先权数据
12/270,920 2008.11.14 US
(85)PCT国际申请进入国家阶段日
2011.05.13
(86)PCT国际申请的申请数据
PCT/US2009/062740 2009.10.30
(87)PCT国际申请的公布数据
WO2010/056552 EN 2010.05.20
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 N·奈斯 H·菲图西
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 顾嘉运
(51)Int.Cl.
H04L 9/32(2006.01)
G06F 15/16(2006.01)
(56)对比文件
US 2007 / 0015499 A1,2007.01.18,
Scott Garriss et al.Towards Trustworthy Kiosk Computing.《Eighth IEEE Workshop on Mobile Computing Systems and Applications》.2007,41-45.
审查员 杨群

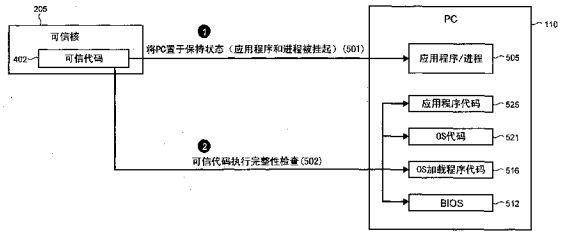
权利要求书2页 说明书6页 附图6页

(54)发明名称

合并移动设备和计算机以创建安全的个性化环境

(57)摘要

通过将移动设备(105)的CPU(中央处理器)(312)和OS(操作系统)(316)配置为不变的可信核(205),当诸如移动电话、智能电话、个人音乐播放器、手持式游戏设备等移动设备(105)可操作地与PC(110)合并时,可创建出安全且个性化的计算平台(110)。在移动设备(105)中的可信核(205)验证PC(110)的完整性,包括验证例如PC的驱动程序、应用程序和其它软件是可信的和未经修改的,从而在未对合并后的计算平台的完整性呈现威胁的情况下可安全使用。移动设备(105)还可以选择性地储存和传输用户的个性化数据(616)-包括,例如,用户的桌面、应用程序、数据、证书、设置、以及偏好-当移动设备与PC(110)相合并时,这些个性化数据可以通过PC(110)被访问,从而创建一个个性化的计算环境。



CN 102217226 B

1. 一种移动设备 (105)，适于与一计算平台 (110) 一起使用，当所述移动设备可操作地耦合至所述计算平台时，为用户 (112) 创建安全的计算环境 (100)，所述移动设备包括 ：

包括一个或多个处理器的 CPU(312) ；

包含指令的计算机可读介质，所述指令在由所述一个或多个处理器执行时为所述移动设备 (105) 实现一操作系统 (316) ；以及

采用所述移动设备的所述 CPU(312) 的一部分和所述操作系统 (316) 的一部分来实现的可信核 (205)，所述可信核 (205) 被配置成用于验证所述计算平台的完整性，并且进一步被配置为挂起所述计算平台上的操作并将对所述计算平台的功能性组件的控制交接给所述移动设备以便所述可信核能对驻留在所述计算平台上的可执行代码是可信的进行验证。

2. 如权利要求 1 所述的移动设备，其特征在于，还包括包含指令的计算机可读介质，所述指令在由所述一个或多个处理器执行时实现许可实施模块，该许可实施模块被配置成用于实施许可条款，所述许可条款可应用于在所述计算平台上执行的软件。

3. 如权利要求 1 所述的移动设备，其特征在于，还包括包含指令的计算机可读介质，所述指令在由所述一个或多个处理器执行时实现策略实施模块，所述策略实施模块被配置用于实施策略，所述策略可应用于所述用户对所述计算平台的使用。

4. 如权利要求 3 所述的移动设备，其特征在于，其中所述策略包括安全策略、应用程序使用策略、生产效率策略、或行政策略中的至少一个。

5. 如权利要求 1 所述的移动设备，其特征在于，其中所述验证包括检查在所述计算平台上的代码是未被修改并可信的。

6. 如权利要求 1 所述的移动设备，其特征在于，其中所述计算平台是台式计算机、膝上型计算机、或工作站中的一个。

7. 如权利要求 1 所述的移动设备，其特征在于，还包括包含指令的计算机可读介质，所述指令在由所述一个或多个处理器执行时实现个性化模块，所述个性化模块被配置用于向所述计算平台展现个性化数据以便为所述用户在所述计算平台上进行个性化体验。

8. 如权利要求 7 所述的移动设备，其特征在于，其中所述个性化数据包括用户简档、设置、用户偏好、证书、数据、应用程序或桌面中的至少一个。

9. 如权利要求 1 所述的移动设备，其特征在于，其中所述可信核执行不变的代码。

10. 如权利要求 1 所述的移动设备，其特征在于，还包括由下述设备中的一个或多个所提供的功能性组件 ：移动电话、个人数字助理、智能电话、个人媒体播放器、手持式游戏设备、数码相机、数码录像机、或口袋计算机。

11. 一种用于当个人计算机 (110) 可操作地耦合至移动设备 (105) 时安排所述个人计算机以实现安全的计算环境 (100) 的方法，所述方法包括如下步骤 ：

将输入配置成可操作地耦合至位于所述移动设备 (105) 内的一个或多个功能性组件，所述一个或多个功能性组件至少包括可信核 (205) ；以及

挂起所述个人计算机 (110) 上的操作 (501) 并将对所述个人计算机的功能性组件的控制交接给所述移动设备 (105) 以便所述可信核 (205) 能对驻留在所述个人计算机 (110) 上的可执行代码 (505) 是可信的进行验证。

12. 如权利要求 11 所述的方法，其特征在于，还包括以下步骤 ：从所述移动设备处访问个性化数据以在所述个人计算机上实现个性化的用户体验，所述访问在验证了所述个人计

算机上的所述可执行代码是可信的之后执行。

13. 如权利要求 11 所述的方法，其特征在于，其中，通过采用执行从所述移动设备直接对所述个人计算机上的一个或多个存储位置访问的接口，所述输入可操作地耦合至所述移动设备。

14. 如权利要求 11 所述的方法，其特征在于，其中所述移动设备和个人计算机各自被配置成所述移动设备能够被直接对接至所述个人计算机，当如此直接对接时，所述移动设备和个人计算机可操作地相耦合。

15. 如权利要求 11 所述的方法，其特征在于，其中所述验证包括确定所述可执行代码是否被从其原始形式修改或者确定所述可执行代码不受恶意软件的影响。

合并移动设备和计算机以创建安全的个性化环境

背景技术

[0001] 针对攻击和未授权的访问，通常采用各种有效的安全性技术和产品保护在家和办公室的环境中的诸如个人计算机（“PCs”）的计算资源。然而，当今的计算机用户经常在这样一种环境中在外出差，即他们常常遇到诸如那些位于售货亭、有英特网的咖啡馆或酒店大堂内的公共可访问的计算机。为这些公共可访问的计算机提供安全经常是一个重要的挑战。它们的用户承受数据丢失、停机时间以及劳动成果丢失的风险危及计算机的完整性的安全。

[0002] 当在出差的公司用户使用公共计算资源时还经常不得不放弃他们平时在他们安全的公司环境中所享有的好处。当前，公共可访问的计算机不能够按常规的公司资产来管理，其会给出差的公司用户造成应用程序不兼容问题、所需资源的不可获得、数据完整性的丢失、以及易受恶意软件攻击的后果。如果公司用户将例如在存储介质上的不良软件（即恶意软件）带回到办公室，或者如果用户将被损害或损坏的文件从公共计算机发邮件至企业服务器，企业网络自身也变得容易受到攻击和有危及安全的风险。

[0003] 提供本背景技术来介绍以下发明内容和具体实施方式的简要上下文。本背景技术不旨在帮助确定所要求保护的主题的范围，也不旨在被看作将所要求保护的主题限于解决以上所提出的问题或缺点中的任一个或全部的实现。

发明内容

[0004] 当诸如移动电话、智能电话、个人音乐播放器、手持式游戏设备等移动设备用于与PC结合时，通过将移动设备的CPU（中央处理器）和OS（操作系统）配置作为为不变的可信核，创建出安全和个性化的计算平台。在移动设备中的可信核验证PC的完整性，包括验证例如PC的驱动程序、应用程序和其它软件是可信的和未经修改的，因此在未对合并后的计算平台的完整性呈现威胁的情况下可安全使用。移动设备可以进一步储存和传输用户的个性化数据－包括，例如，用户的桌面、应用程序、数据、证书、设置、以及偏好－当设备与PC相组合以创建一个个性化计算环境时，这些个性化数据可以通过PC被访问。PC可为合并的移动设备和PC计算平台贡献更多实质计算资源（例如，一个更强大的CPU、附加的内存等），并且还通常提供如大幅面显示器、全尺寸键盘、打印机等外围设备。

[0005] 在说明性示例中，提供可信核的移动电话可以通过电缆或直接对接布置被插入到PC以创建强大的经合并的计算平台。在可信核中的代码将通过暂时挂起PC操作来执行将PC置于保持状态。可信核提供了独立的可信平台，该可信平台将接管对PC的控制来执行对其内部外围组件的完整性检查，以确保只有未经修改的可信代码在PC上执行。通常，该建立信任的处理将涵盖PC上的包括BIOS（基本输入／输出系统）代码、OS、所有应用程序代码的所有系统，以验证PC为可信的。如果PC被验证为可信的，并从而是干净并不受恶意软件控制的，则用户的个性化数据可以有选择地从移动电话传送并加载到PC上，以完成经合并的安全和个性化计算平台的实现。如果该检查确定该PC不干净，则用户的简档和个性化数据将不被传送和加载。在某些情况下，可以通知用户PC上的问题，给予用户补救的机会，

然后再次尝试创建合并的计算平台。

[0006] 合并的移动设备和 PC 平台上的最终的安全使用环境能够进一步显示为用户所熟悉，并且对任何可用 PC 将在外观和操作上一致。有利的是，移动设备的存储功能可以为用户提供个性化的使用环境，同时其可信核功能性确保该环境受到保护。可信核用于独立地验证平台的完整性，从而避免了一些与自我评估时产生的固有矛盾。合并后的移动设备和 PC 平台进一步允许针对漫游的公司用户的企业策略的实施。此外，根据许可条款的软件使用可为所有用户确认。

[0007] 提供本发明内容是为了以简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述不旨在标识出所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。

附图说明

[0008] 图 1 显示了可以被合并以创建一个安全的个性化环境的示例性的移动设备和 PC ；

[0009] 图 2 显示了移动设备上的一组示例性的功能性组件，包括可信核、个性化模块以及策略和许可实施模块 ；

[0010] 图 3 和图 4 显示可信核的示例性实现细节 ；

[0011] 图 5 是显示合并的移动设备和 PC 平台的功能性组件之间的交互的简化的示例性框图 ；

[0012] 图 6 显示示例性的个性化数据从移动设备向 PC 的传送 ；以及

[0013] 图 7 是显示公司策略和 / 或软件许可条款如何在合并的移动设备和 PC 平台上实施的示例性图示。

[0014] 各附图中相同的附图标记指示相同的元素。

具体实施方式

[0015] 图 1 显示包括移动设备 105 和 PC 110 的示例性计算环境 100。移动设备 105 可以选自多个不同设备中的一个，该多个不同设备包括例如移动电话、智能电话、口袋 PC、PDA（个人数字助理）、诸如 MP3（运动图像专家组，MPEG-1，音频层 3）播放器的个人媒体播放器、数码相机、数码录像机、手持式游戏设备，结合上述功能中的一个或多个的设备，等等。通常，移动设备 105 将是紧凑且重量轻的，使其能够由用户 112 从一个地方方便地携带到另一个地方。还通常提供诸如移动设备 105 中的电池的板载电源，以进一步提高设备的实用性和功能性。

[0016] PC 110 代表诸如台式 PC、膝上型 PC、工作站等的计算平台。在这个具体的例子中，计算环境 100 和 PC 110 为公共可访问的，它们可能遇上位于酒店大堂、有英特网的咖啡馆、公共图书馆、电脑亭等内的计算机。公共可访问的计算机在经常提供非常方便和有用的服务的同时，由于这种计算机通常不提供与家或办公室等更可控的环境的安全级别一样的安全级别，会将用户 112 暴露于恶意软件或其它恶意活动。

[0017] 如图 1 所示，移动设备 105 采用诸如电缆 116 等连接可操作地耦合至 PC 110。电缆 116 支持 DMA（直接存储器存取）连接或支持被配置成允许将数据从与 PC 内的 CPU 独立的 PC 内存中传送出去或传送至该 PC 内存的类似连接。不需要电缆的直接对接布置也可以

在某些情况下使用，即移动设备 105 被配置成与 PC 110 中的对应的槽或插座可操作地相接合的情况。位于移动设备 105 和 PC110 中的相应的连接器被配置成用于当移动设备被对接时的可配对的接合，以允许信号路径从中建立。然而，需要强调的是，此处描述的 DMA 连接是示例性的，并且其它类型的可操作的耦合机制、方法和协议可以被用来允许移动设备 105 与 PC 110 之间的期望的互用性，以满足给定实现的需要。

[0018] 图 2 显示了移动设备 105 上的一组示例性的功能性组件，包括可信核 205、个性化模块 210 以及策略和许可实施模块 216；需要强调的是，虽然显示了分离的功能性组件，在替换实现中，各组件提供的功能性可以按不同方式分布。例如，功能性可合并到一给定的组件或分割成不同的组件。正如在下面详细描述的，在该说明性的示例中，可信核 205 是采用硬件和软件的结合来实现的。通常，个性化模块 210 以及策略和许可实施模块 216 采用软件来实现。然而，硬件、固件和 / 或软件的各种组合可被用来实现需要满足特定应用的需要的功能模块。

[0019] 图 3 和图 4 显示移动设备 105 的可信核 205 的示例性实现细节。如图 3 所示，在本特定实例中的可信核 205 采用由移动设备 CPU（中央处理单元）312 提供的硬件和由移动设备 OS（操作系统）316 提供的软件的组合来实现。如图 4 所示，该硬件和软件的组合允许可信核 205 存储并随后执行可信代码 402，以便将 PC 110 置于保持状态，然后进行如下所述的完整性检查。可信代码 402 是不变的（意味着其状态可以永远无法被修改），从而提供了一个基础的可信平台以用来当设备 105 被操作耦合至 PC 110 时验证合并后的移动设备 /PC 平台的可信度。

[0020] 图 5 是显示合并的移动设备和 PC 平台的功能性组件之间的交互的简化的示例性框图；根据本布置的原理，当移动设备 105 可操作地耦合到 PC 110 时，在可信核 205 中的可信代码 402 将首先在移动设备 105 上执行以指示 PC110 挂起其应用程序和进程 505，从而进入一个保持状态（如附图标记 501 所示）。通常，在许多实现中，可信代码 402 的执行将包括软件和硬件操作的组合。一旦 PC 110 被保持，可信代码 402 将接着在移动设备 105 上执行，以对 PC 的代码 (502) 进行完整性检查。可信核 205 将接管对诸如驱动器和存储器等 PC 的内部外围组件的控制，以便获得对 PC 的软件代码的访问以进行完整性检查。

[0021] 在这个示例中，接受可信代码 402 的完整性检查的代码包括在固件中实现的 BIOS 512（基本输入 / 输出系统）、OS 加载程序代码 516、OS 代码 521、和应用程序代码 525。然而，需要强调的是，图 5 所示的具体类型的代码是示例性的，并且在 PC 110 上的受完整性检查的具体代码可按实施而不同。在大多数应用程序中，在 PC 被视为可信赖之前，在 PC 110 上的所有代码都将被进行完整性检查。

[0022] 每个完整性检查 502 将通常包括验证 PC 110 上的代码是未从原始形式修改过的并没有被改变成例如包括恶意软件。可采用各种已知完整性检测来满足特定实现的需要。例如，在 PC 110 上的代码可以经受一个散列算法，并且与已知的善意代码的散列进行比较。

[0023] 值得注意的是，在许多实现中，存储在 PC 110 上的代码一般将不会在可信核 205 上执行。此限制并不是对所有实现都必须的，但当实施后，可有助于保持移动设备 105 隔离于 PC 110 上的任何恶意软件，从而确保了在任何时候都保持可信核 205 的完整性。然而，在某些应用中，可周期性地检查可信核自身的完整性，以确保其没有受到威胁。例如，在用

户 112(图 1)可能会在该用户的日常工作地点与其进行交互的企业网络中的可信实体可被配置成对移动设备 105 进行完整性检查,以确保它是不受恶意软件控制并且遵循适用的企业策略,从而确保它是健康的。此外,移动设备 105 可被配置成周期性地发起对可信代码的执行来进行自我测试,以验证其自身的健康。

[0024] 在某些情况下,如果移动设备 105 在某给定的时间间隔内没有被检查和验证为健康的,移动设备 105 可配置为限定或限制完整性检查特性的使用。也就是说,如果移动设备 105 的完整性最近没有得到验证,它在 PC 110 上执行完整性检查的能力可被暂时失效。这有助于防止用户错误地信任 PC 是安全的,而实际上该 PC 是不安全的。

[0025] 对移动设备 105 的隔离进一步使其能够作为一个独立的代理器,来验证 PC110 的可信度。当一个软件组件本质上在对自身进行检查时,这种独立可避免与自我评估(或"自我认证")相关联的一些固有冲突。实现可信的自我评估,往往被证明是有问题的,因为软件的易受修改性可危害信任。

[0026] 移动设备 105 可被配置为在各个时间将 PC 110 置于保持状态并接管操作的控制以进行完整性检查。一般来说,当移动设备 105 第一次可操作地耦合至 PC 时,移动设备将 PC 110 置于保持状态并进行完整性检查。这可能在例如当用户 112 位于一个公共可访问的 PC 并希望在安全的环境中开始一个计算会话的情况下发生。然而,移动设备 105 可在给定的计算会话中周期性地将 PC110 置于保持状态并进行完整性检查。例如,可在任意时间间隔进行保持和检查,或者通过事件的发生触发保持和检查,例如检测到安全事件(如,在 PC 中接收到电子邮件附件中的病毒)、检测到一个至用户的家或企业网络的试图远程连接,或者通过用户 112 的手动启动来触发保持和检查。

[0027] 当可信核 205 已检查了 PC 110 上的代码的完整性并视 PC 110 是可信的之后,则可选择性地提供用户 112 的个性化数据以创造一个安全的个性化环境。然而,如果 PC 110 不被视为可信任的,则,在某些情况下,可通过显示在移动设备 105 上的指示存在需要解决的问题的警告来通知用户 112。例如,完整性检查可表明 PC 110 错过了应用程序或 OS 中需要的安全补丁。如果用户 112 能够补救该问题(例如,通过成功地对 PC 110 打补丁),以及随后通过了对问题代码的完整性检查,则用户将获得在 PC 110 上使用个性化数据的另一次机会。

[0028] 如图 6 所示,一旦 PC 110 被验证为可信的或者通过补救成为可信的,个性化模块 210 可配置为向 PC 110 提供各种类型的个性化数据 616。需要强调的是,个性化模块 210 的使用以及个性化数据的提供是可选的。在某些情况下,通过上述完整性检查简单地在 PC 110 上提供一个安全的环境,而不通过传送个性化数据为用户实现一个个性化环境,是合乎需要的。

[0029] 在这个特定示例中,个性化数据 616 可包括用户简档 621、设置 625(例如,包括系统设置和应用程序设置)、用户偏好 630、安全证书 634、用户数据 639、应用程序 645、以及用户的桌面 648。然而,这些数据类型是示例性的,根据给定的实现要求,还可采用其它类型的数据以及数据组合。

[0030] 在某些实现中,个性化数据 616 可以通过连接 116(图 1)传送到 PC 110(图 1)并被存储在本地。然而,在这种情况下,一旦用户 112 完成了所需任务并结束了他的计算会话,个性化数据 616 通常将需要从 PC 110 中删除,以维护用户 112 的隐私。之后,更典型的

是，个性化数据 616 可继续驻留在移动设备 105 并根据需要在 PC 110 上创建个性化环境时仅通过 PC110 从移动设备被访问。在这种情况下，由于个性化数据 616 不会保存在 PC 110 上，简化了对用户 112 的隐私的维护。

[0031] 从个性化模块 210 处使用个性化数据 616 可为用户 112 创建一个能方便地复制由用户经常使用的计算机提供的体验的强大而个性化的平台。用户 112 只需要拥有紧凑而便携的移动设备 105，以便能够在任何公共可访问的计算机上建立一个复制具有用户的所有数据和时常使用的应用程序的用户熟悉的桌面环境的个性化计算平台。PC 110 可为合并的移动设备和 PC 计算平台贡献更多实质计算资源（例如，一个更强大的 CPU、附加的存储器等），并且还通常提供如大幅面显示器、全尺寸键盘、打印机等外围设备。但是，不同于传统的个性化或虚拟化解决方案，本发明使得经个性化的环境在通过仅支持未被修改的应用程序和其它代码来被验证为可信的平台上实现。

[0032] 图 7 显示了本合并的移动设备和 PC 平台的另一个被可选使用的特征。此处，移动设备 105 上的策略和许可实施模块 216 被配置为监视 PC 110（如附图标记 710 所示）、实施适用的软件许可 (720)、和 / 或实施适用的公司策略 (730)。虽然单个模块在图 7 被示为结合了执行策略和许可实施两者的功能，在替换实现中，可以使用对应的策略和许可功能被分开地在其中执行的各独立模块。此外，策略实施或者许可实施可在任何给定的使用场景下使用，或者适当地根据场景的需要，两者可一起使用，或者两者都不使用

[0033] 监视 710 可包括如图 5 的文字描述所述的完整性检查，执行该完整性检查以验证 PC 110 的完整性。此外，PC 110 在被验证为可信并且用户 112 在合并的移动设备和 PC 计算平台上执行任务之后，可被连续或周期地监视。

[0034] 由于对 PC 110 上的代码进行完整性检查，可通过策略和许可实施模块 216 来验证受许可影响的应用程序为经合法授权并适当地安装在计算机上。被发现为不符合许可条款的 PC 110 上的应用程序，例如盗版或者以其它方式违反适用的许可条款，可以被暂时失效或者对用户 112 不可用。按这种方式，用户 112 将不会由于使用非遵守 (non-compliant) 软件而违反许可条款。在替换实现中，如果用户 112 被许可使用驻留在 PC 110 上的应用程序，则该被授权的状态的证书或者其它证据可以被存储在移动设备 105。当移动设备 105 耦合到 PC 110 时，检查经存储的证书，以允许合法的、经许可的对应用程序的使用，否则该应用程序的使用是不遵守适用的许可条款的。

[0035] 当 PC110 被验证为可信并且用户 112 在使用由合并的移动设备 105 和 PC110 形成的安全的个性化计算平台之后，策略和许可实施模块 216 可出于许可实施的目的监视活动。例如，当应用程序被启动和使用，策略和许可实施模块 216 可监视该活动，以确保只有合法且可信代码在 PC 110 上执行。如果不受信任的代码试图被执行，则策略和实施模块 216 可着手努力阻止此类执行。

[0036] 如果用户 112 是受公司的策略影响的雇员，则策略和许可实施模块可被配置成：当用户在使用合并的移动设备和 PC 计算平台时，实施该策略。对任何给定使用场景均使用的企业策略是可变的。它们可通常包括那些旨在改善企业网络安全性、提高员工工作效率、降低管理成本的策略。

[0037] 例如，安全策略可指示 IT（信息技术）资产（包括在企业网络的受保护的区域边界之外的那些 IT 资产）遵循各种要求，例如要求对所有网络连接均启用防火墙、要求安装

针对最新的签名的更新过的反病毒和间谍软件应用程序，并要求存在于所有安全补丁中。通常情况下，策略和许可实施模块 216 将启动针对 PC 110 的网络访问的限制，例如，防止恶意软件从 PC 扩散回到公司网络（例如，通过用户发送电子邮件返回公司网络的受感染的文件）。

[0038] 例如通过应用程序使用策略的实施、网站过滤的实施、以及其它常采用的手段，员工在 PC 110（当作为一个安全的个性化计算平台操作时）的工作效率可提高。虽然这种技术根据实现而不同，策略和许可实施模块 216 可被安排为监视 PC 110 上的应用程序使用，以执行对适用的策略的遵守。按这种方式，即使用户 112 在公司边界之外工作，对 PC 110 的操作就像在企业网络中的任何其它受管 IT 资产一样。

[0039] 尽管用结构特征和 / 或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述具体特征或动作。相反，上述具体特征和动作是作为实现权利要求的示例形式公开的。

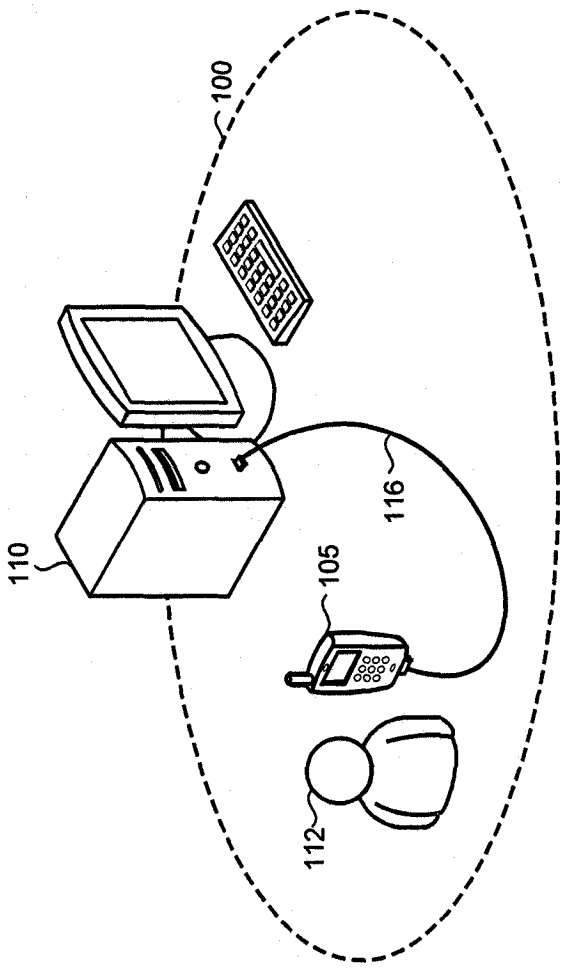


图 1

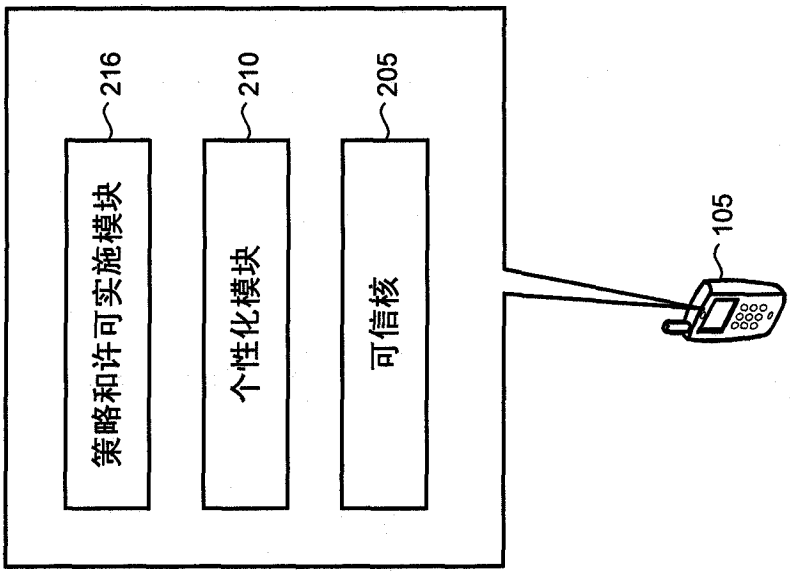


图 2

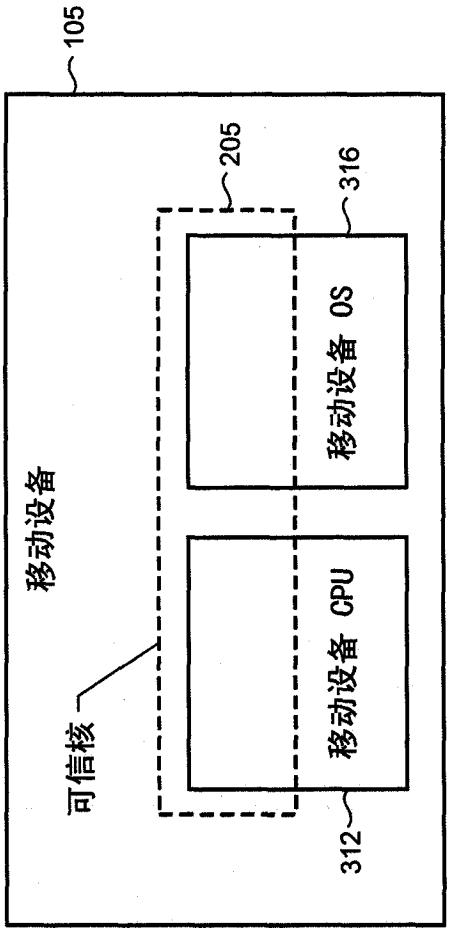


图 3

图 4

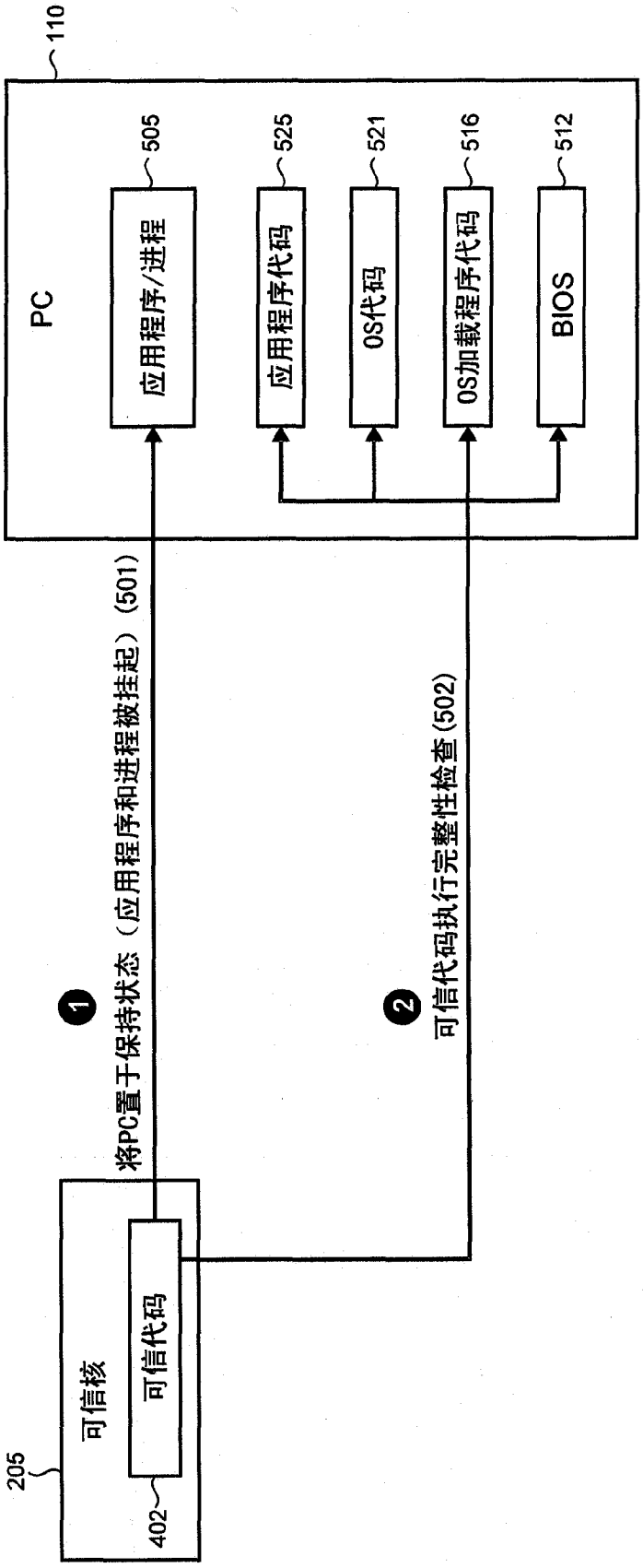

110
PC
505
应用程序/进程
525
应用程序代码
521
OS代码
516
OS加载程序代码
512
BIOS
1
将PC置于保持状态（应用程序和进程被挂起）(501)
2
可信代码执行完整性检查(502)
205
可信核
可信代码
402

图 5

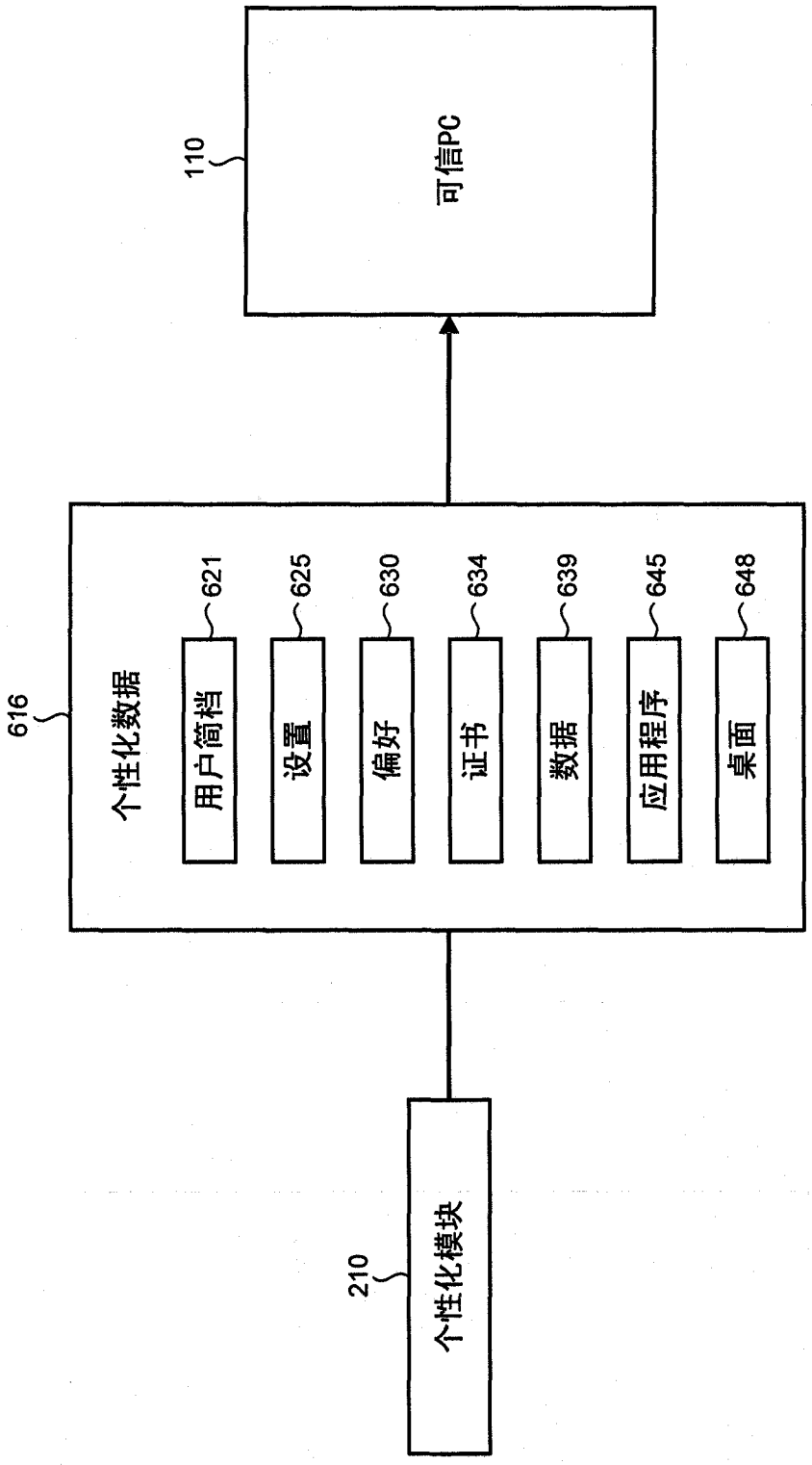

110
可信PC
616
个性化数据
621
用户简档
625
设置
630
偏好
634
证书
639
数据
645
应用程序
648
桌面
210
个性化模块

图 6

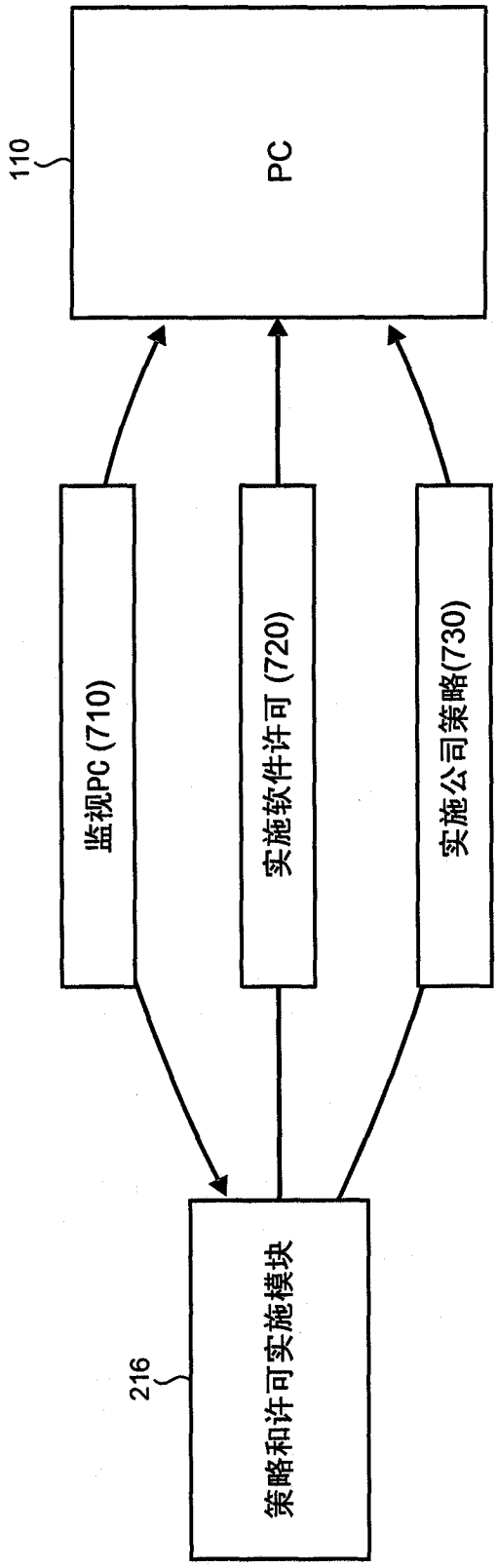


图 7