(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111052117 B
(45)授权公告日 2023.09.19

(21)申请号 201880012082.8
(22)申请日 2018.02.14
(65)同一申请的已公布的文献号
申请公布号 CN 111052117 A
(43)申请公布日 2020.04.21
(30)优先权数据
15/436,719 2017.02.17 US
(85)PCT国际申请进入国家阶段日
2019.08.15
(86)PCT国际申请的申请数据
PCT/US2018/018081 2018.02.14
(87)PCT国际申请的公布数据
WO2018/152138 EN 2018.08.23
(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 S·R·歇尔 M·N·萨基卜
金舒曼 D·R·罗尔夫
D·E·罗宾斯 I·麦卡蒂
J·M·周 D·J·林斯利
(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 李光颖
(51)Int.Cl.
G06F 21/57(2006.01)
G06F 21/51(2006.01)
G06F 9/4401(2006.01)
(56)对比文件
US 2014331064 A1,2014.11.06
US 2004064457 A1,2004.04.01
US 2016378990 A1,2016.12.29
US 2010169633 A1,2010.07.01
审查员 李佳曦

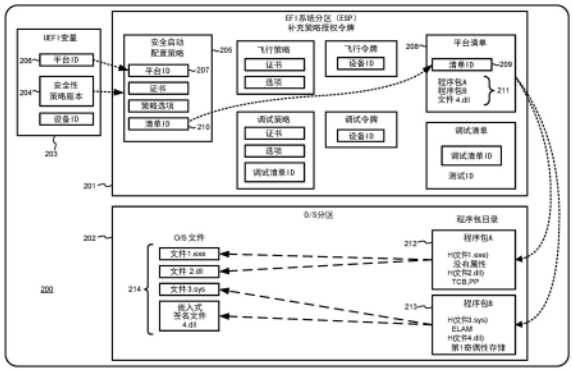
权利要求书2页 说明书10页 附图5页

(54)发明名称

在没有多元化创作的情况下安全地定义操作系统组成

(57)摘要

实施例涉及通过以下操作来管理在设备上加载的软件组件:识别具有有效证书的平台清单;确认所述平台清单被绑定到所述设备;识别在平台清单上列出的组件;确认所列出的组件具有有效证书,并且在所述设备上加载所列出的具有有效证书的组件。所述组件可以是针对操作系统的二进制文件和程序包。所述组件可以以嵌入方式或者利用分离签名进行签名。所述平台清单可以以允许识别未授权平台清单的方式被绑定到设备。



CN 111052117 B

1.一种用于管理在运行操作系统的设备上加载的软件组件的方法,包括在启动过程期间:

将安全启动配置策略加载到存储器中,所述安全启动配置策略包括与所述操作系统独有地相关联的授权平台清单识别符;

基于所述授权平台清单识别符来识别具有第一有效证书的平台清单,其中,所述平台清单包括操作系统版本所允许的组件的列表;

将所述平台清单加载到所述存储器中;

验证所述平台清单中的清单识别符与所述安全启动配置策略中的所述授权平台清单识别符相匹配;

识别在所述平台清单上列出的组件;

确认所列出的组件具有第二有效证书;以及

在所述设备上加载所列出的具有所述第二有效证书的组件。

2.根据权利要求1所述的方法,还包括:

识别具有第三有效证书的额外组件;

确定所述额外组件未在所述平台清单上列出;以及

从所述设备阻止所述额外组件。

3.根据权利要求1所述的方法,其中,所述组件包括针对操作系统的二进制文件和程序包。

4.根据权利要求1所述的方法,还包括:

在设备安全策略中识别所述清单识别符;以及

使用所述清单识别符来确认所述平台清单被绑定到所述设备。

5.根据权利要求1所述的方法,还包括:

在设备安全策略中识别多个清单识别符;

加载与所述多个清单识别符相对应的多个平台清单文件;以及

将所述多个平台清单文件合并为针对所述设备的活动平台清单。

6.根据权利要求1所述的方法,其中,所述组件以嵌入方式或者利用分离签名进行签名。

7.根据权利要求1所述的方法,其中,所述平台清单以允许识别未授权平台清单的方式被绑定到所述设备。

8.根据权利要求1所述的方法,还包括:

选择要包含在针对选定平台的操作系统中的多个文件,所述多个文件具有有效文件证书;

生成一个或多个代码签名平台清单,每个代码签名平台清单具有平台清单识别符和有效平台证书并且列出所述多个文件中的一个或多个文件;以及

通过列出设备安全策略中的可接受平台清单识别符来控制能够在设备上加载什么操作系统,其中,如果针对其他操作系统的文件没有出现在可接受平台清单上,则所述文件将不被加载在所述设备上。

9.一种用于管理在运行操作系统的设备上加载的软件组件的系统,包括:

一个或多个处理器;以及

包括指令的存储器，所述指令能由所述一个或多个处理器运行以用于在启动过程期间：

将安全启动配置策略加载到存储器中，所述安全启动配置策略包括与所述操作系统独有地相关联的授权平台清单识别符；

基于所述授权平台清单识别符来识别具有第一有效证书的平台清单，其中，所述平台清单包括操作系统版本所允许的组件的列表；

将所述平台清单加载到所述存储器中；

验证所述平台清单中的清单识别符与所述安全启动配置策略中的所述授权平台清单识别符相匹配；

识别在所述平台清单上列出的组件；

确认所列出的组件具有第二有效证书；以及

在所述设备上加载所列出的具有所述第二有效证书的组件。

10.根据权利要求9所述的系统，其中，所述组件包括针对操作系统的二进制文件和程序包。

11.根据权利要求9所述的系统，其中，所述清单识别符是在设备安全策略中识别出的并且被用于确认所述平台清单被绑定到所述设备。

12.根据权利要求9所述的系统，其中，所述指令能由所述一个或多个处理器运行以用于：

在设备安全策略中识别多个清单识别符；

加载与所述多个清单识别符相对应的多个平台清单文件；以及

将所述多个平台清单文件合并为针对所述设备的活动平台清单。

13.根据权利要求9所述的系统，其中，所述指令能由所述一个或多个处理器运行以用于：

识别具有第三有效证书的额外组件；

确定额外组件未在所述平台清单中列出；以及

从所述设备阻止所述额外组件。

14.根据权利要求9所述的系统，其中，所述组件以嵌入方式或者利用分离签名进行签名。

15.根据权利要求9所述的系统，其中，所述平台清单以允许识别未授权平台清单的方式被绑定到所述设备。

在没有多元化创作的情况下安全地定义操作系统组成

背景技术

[0001] 最初为台式计算机创建的操作系统最近已经扩展到其他设备，诸如移动电话和游戏控制器。操作系统从台式机(desktop)平台到移动电话平台的转换是复杂的，因为这些设备中的安全模式不同。个人计算机平台通常是开放式平台。另一方面，移动操作系统通常是锁定平台。移动电话没有像登录个人计算机那样的相同登录概念，因此，不具有在台式机上找到的相同的用户权限组和访问控制列表。

[0002] 因为移动电话被直接连接到移动网络，所以重要的问题是保护这些网络。服务提供商需要确保未在移动电话上安装或运行可能威胁网络的安全性和完整性的恶意或破坏性应用。当开发移动电话操作系统时，尽管存在不同的安全模式，但是现有的台式机组件被重用在移动电话上提供相同的功能。然而，如果针对台式机设计的各种开发工具和管理工具的使用没有限制，那么将意味着破坏移动电话锁定模式。台式机上可接受的组件在移动电话上可能不安全。

[0003] 为了将移动电话维持为锁定平台，需要区分被认为在每个平台上工作的组件。这是使用两种不同集合的数字签名来完成的。存在代码签名证书的台式机集合以及代码签名证书的移动电话集合。

[0004] 要在移动电话平台上运行的组件需要利用代码签名证书的移动电话集合来签名。通常，开发过程首先产生所有台式机组件，然后开始移动构建过程。移动构建过程置入相关的台式机组件。然后，存在重新签名步骤以对所选择的台式机组件进行授权，并且利用移动代码签名证书将其与所有其他未置入台式机组件区分开来。对于专为移动设备构建的其他组件，其是利用移动代码签名证书来签名的，无需任何类型的置入。

发明内容

[0005] 提供本发明内容是为了以简化的形式介绍一些概念，这些概念将在下文的具体实施方式中进一步描述。该发明内容并非旨在识别所要求保护的主题的关键特征或必要特征，也并不旨在用于限制所要求保护的主题的范围。

[0006] 平台清单创建通过允许操作系统中的所有文件利用相同的证书集合进行签名来简化操作系统签名系统，但是仍然允许个体平台或版本，其限制操作系统的哪些部分在设备上运行。该特征防止交叉传播(cross-pollination)攻击，其中，攻击者从不同版本的操作系统获取文件并将其放置在非预期的设备上，这对该平台的安全性具有潜在的重大负面影响。平台清单自身是在操作系统构建期间根据版本的定义而自动生成的。

[0007] 平台清单特征是整个代码签名策略的一部分。平台清单的目的是将证书的授权限制为仅由该证书签名的文件的子集。具体而言，平台清单基于程序包(package)和个体文件包含在操作系统的特定版本中而对其进行授权。将不允许在操作系统版本上未授权的文件和其他程序包，即使利用有效证书对其进行了签名。

[0008] 一种用于管理在设备上加载的软件组件的方法，包括：识别具有有效证书的平台清单；确认所述平台清单被绑定到所述设备；识别在所述平台清单上列出的组件；确认所列

出的组件具有有效证书;以及在所述设备上加载所列出的具有有效证书的组件。所述组件可以是针对操作系统的二进制文件和程序包。以嵌入方式或者利用分离签名对所述组件进行签名。以允许识别未授权平台清单的方式将所述平台清单绑定到所述设备。

[0009] 所述方法还可以包括:识别具有有效代码签名证书的额外组件;确定所述额外组件未在所述平台清单上列出;以及从所述设备阻止所述额外组件。

[0010] 所述方法还可以包括:在设备安全策略中识别清单识别符;以及使用所述清单识别符来确认所述平台清单被绑定到所述设备。

[0011] 所述方法还可以包括:在设备安全策略中识别多个清单识别符;加载与所述多个清单识别符相对应的多个平台清单文件;以及将所述多个平台清单文件合并为针对所述设备的活动平台清单。

[0012] 一种设备,包括:处理器,其运行操作系统加载器和代码完整性组件;以及设备存储器,其存储安全策略和操作系统组件,其中,所述操作系统加载器被配置为使用所述安全策略中的平台清单识别符来识别平台清单并且加载在所述平台清单中列出的组件,并且其中,所述代码完整性组件被配置为在所述操作系统加载器加载所述组件之前确认所述平台清单和在所述平台清单中列出的组件具有有效证书。

[0013] 所述组件可以是针对操作系统的二进制文件和程序包。所述设备安全策略可以被用于确认所述平台清单被绑定到所述设备。所述组件以嵌入方式或者利用分离签名进行签名。所述平台清单以允许识别未授权平台清单的方式被绑定到所述设备。

[0014] 所述操作系统加载器还可以被配置为:加载与所述安全策略中的多个清单识别符相对应的多个平台清单文件,并且将所述多个平台清单文件合并为针对所述设备的活动平台清单。

[0015] 所述操作系统加载器还可以被配置为确定额外组件未在所述平台清单中列出,并且即使所述代码完整性组件将所述额外组件识别为具有有效代码签名证书也从所述设备阻止所述额外组件。

[0016] 一种强制实施操作系统组成的方法,包括:选择要包含在针对选定平台的操作系统中的多个文件,所述文件具有有效证书;以及生成一个或多个平台清单,每个平台清单具有平台清单识别符和有效证书并且列出所述多个文件中的一个或多个文件。

[0017] 所述方法还可以包括:通过列出设备安全策略中的可接受平台清单识别符来控制在设备上能够加载什么操作系统,其中,如果针对其他操作系统的文件没有出现在可接受平台清单上,则所述文件将不被加载在所述设备上。

[0018] 所述方法还可以包括:将两个或更多个平台清单合为到针对设备的活动平台清单。

附图说明

[0019] 为了进一步阐明本发明的实施例的以上以及其他优点和特征,将通过参考附图来呈现对本发明的实施例的更具体的描述。应当意识到,这些附图仅仅描绘了本发明的典型实施例,因此不应当被视为限制其范围。通过使用附图,将以额外的特征和细节来描述和解释本发明,在附图中:

[0020] 图1是图示操作系统的不同版本的常规创建的框图。

[0021] 图2是根据本文所描述的实施例的运行操作系统的设备上的数据存储装置(诸如硬盘驱动器或固态驱动器)的框图。

[0022] 图3是图示针对使用平台清单的不同平台的操作系统的不同版本的框图。

[0023] 图4是图示根据一个实施例的用于管理在设备上加载的软件组件的方法的流程图。

[0024] 图5图示了为策略驱动强制实施平台清单提供合适的计算环境的设备的示例。

具体实施方式

[0025] 通过从提供SKU(库存保持单元)所需功能要求的一些组件中进行选取来创建操作系统的版本或SKU。每个组件包括一些二进制文件(可执行文件)和配置数据。这些文件由操作系统构建来签名。每个SKU选取操作系统包含的组件。存在从操作系统的单个构建导出的许多SKU,诸如家庭版本、专业版本、服务器版本、移动版本以及嵌入式版本。另外,OEM(原始设备制造商)可以创建针对特定需求而定制的操作系统平台。OEM能够从可用组件中进行挑选并且构建仅包含他们所需的组件的平台。这种选择使得其能够减少操作系统的占用空间(footprint),这也减少了其平台的可攻击表面面积。然而,如果攻击者能够将其他二进制文件放到设备上,则所述设备将信任操作系统接受的那些二进制文件。

[0026] 为了进一步减少攻击表面,并且为了避免其他交叉传播问题,操作系统的一些SKU将对文件进行重新签名,以便其可以移除对Windows构建如何对文件进行签名的信任,并且替代地仅信任包含在该版本中的那些文件。例如,移动操作系统构建采用来自台式机构建的二进制文件的相同副本,并且利用移动证书对其进行重新签名。这种模式在若干方面是浪费的。首先,签名基础设施必须维护证书的多个集合,并且必须处理对需要签名的多个文件副本进行签名所需的工作量。其次,更新是分散的,因为必须处理多个副本,并且更新管道必须知道要将哪些位传送到特定SKU。同样地,当组件要求服务更新或临时补丁时,必须跨SKU来协调更新。

[0027] 图1是图示操作系统的不同版本的常规创建的框图。操作系统供应商可以发布多个平台,诸如操作系统的台式机版本101和移动版本102。每个版本使用大量公共组件,诸如程序包A 103a和103b和程序包B 104a和104b。不同版本也具有特定于每个平台的许多组件。例如,程序包N 105仅用在台式机版本中,而程序包M 106仅用在移动版本中。供应商在相同的公共构建系统中构建程序包103-106。

[0028] 每个平台可以具有不同的安全承诺,并且如果程序包N 105在移动设备上运行,则对于台式机版本101必要的组件(诸如程序包N 105)可能损害移动平台102的安全性。为了保护客户,移动平台通常旨在成为锁定的操作系统。合法的台式机组件(诸如支持查看、搜索和更改系统注册表中的设置的注册表编辑器)在移动设备上运行的情况下可能破坏操作系统的许多安全承诺。为了解决该问题,所有移动组件103b、104b和106都利用不同的有效证书(诸如代码签名证书)来签名。移动平台强制要求所有内容都必须由移动证书来签名。对于公共组件103a和103b、104a和104b,存在重新签名过程107,其将移动代码签名证书应用于现有的台式机签名程序包A 103a和B 104a。原始台式机代码签名程序包版本103a、104a被转换为移动代码签名程序包103b、104b,使得允许其在移动平台上运行。

[0029] 现有方案存在若干问题。首先,必须维护代码签名证书的单独列表以对每个平台

进行签名。这创建证书管理开销并且增加可靠性问题的表面面积。其次，多个代码签名证书被用于对每个平台中不同类型的组件进行有效地签名。为了获得有效的构建，除了定义哪些组件构成每个平台之外，还需要维护如何利用每个平台对组件进行签名的映射。第三，对不同平台重用的所有组件进行重新签名需要额外的时间，这增加了整体构建完成时间。

[0030] 对现有操作系统构建的问题的解决方案消除了重新签名步骤的使用，而是在常规移动映像创建过程期间生成平台清单。所述平台清单包括授权的二进制文件和程序包的列表。能够在代码执行时引用所述平台清单以确定将要执行的二进制文件是否被授权用于该平台。

[0031] 所述平台清单是签名文档，其允许系统验证没有人篡改所述平台清单。对所述平台清单进行签名还提供了一种安全的方式，以确保攻击者简单地通过将二进制文件添加到授权的二进制文件和程序包的列表中不能够损害平台的安全性。

[0032] 所述平台清单识别特定SKU所需的组件而无需对组件的重新签名。SKU或定制版本能够将操作系统中的信任定义为如在所述平台清单中定义的由操作系统构建单独签名的特定组件集合。已签名的平台清单定义操作系统的SKU。如果文件出现在所述平台清单上并且如果文件被签名，则所述文件被包含在针对该SKU的构建中。所述平台清单被绑定到设备(即，与SKU相关联的设备)。备选地，绑定到所述设备的安全策略可以允许所述平台清单。

[0033] 签名的文件包括其经认证的属性中的父组件的识别符。当对组件的目录进行签名时，该组件的识别符被包含在经认证的属性中。SKU的真实性可验证组成配置包括形成该SKU的组件识别符的列表。当对文件进行授权时，将文件的父组件的识别符与组成中的识别符的列表进行比较。

[0034] 所述平台清单列出了关于要包含在操作系统映像(image)中的程序包的信息。这些程序包可以来自现有的操作系统映像，诸如台式机版本，或者其可以是专门为该特定操作系统映像产生的。对所述平台清单进行签名，使得可以检测到更改，并且能够信任所述平台清单。所述平台清单通过阻止意图用于一个操作系统构建的有效签名的二进制文件在运行时与其他操作系统一起加载来防止交叉传播。

[0035] 能够为每个操作系统映像生成新的平台清单。当创建操作系统映像时创建所述平台清单，并且当操作系统在实际使用中时检查所述平台清单。当设备在启动过程期间加载操作系统时，所述设备检查所述平台清单是否为有效文件，并且所述系统加载为操作系统组件的所有二进制文件基于平台清单文件的内容来授权。另外，无论何时加载可执行文件，都相对于所述平台清单对其进行检查，这在没有检测的情况下不能够更改。所述系统验证二进制文件和可执行文件是否具有正确的代码签名证书。如果签名不是预期的，则所述系统能够采取一些补救动作，诸如重新加载文件或者取回文件的缓存版本。

[0036] 所述平台清单是从公共工程基础构建和锁定操作系统的可扩展方式。能够使用相同的工具，而无需重新签名过程和不同的代码签名证书。所需要的仅仅是在供应商想要制作需要锁定的新操作系统时再生成一个文件—平台清单。所述平台清单被绑定到特定的设备类型。

[0037] 所述平台清单识别预期在特定构建上的程序包。所述平台清单按名称或者其他识别符列出特定文件。二进制文件和程序包可以在平台清单中通过例如名称、目录(.cat)文件或压缩包(.cab)文件来进行识别，所述压缩包文件是包含其他分布式文件(诸如驱动器

和系统文件)的压缩文件。所述平台清单不识别每个组件所期望的签名,但是所列出的组件必须利用嵌入或分离签名进行签名。

[0038] 该技术特别地自动生成平台清单而无需创作。在生成操作系统映像时,将在映像中使用的所有组件的列表被放在允许列表中。因此,在共同工程系统中构建和签名但是未包含在该映像中的任何内容都将不会出现在允许列表中,因此,其将不会通过平台清单测试,并且也将不被加载在所述设备上。

[0039] 诸如台式机或移动设备之类的设备具有定义系统的基本安全策略的安全策略,诸如安全启动配置策略。所述安全策略正在被扩展以具有与平台清单相关的额外值。所述平台清单仅被设计用于限制签名。在现有代码完整性系统中不被信任的文件或目录将仍然不会使用平台清单特征而被信任。然而,在先前的安全系统下被信任的一些签名现在将被禁止。

[0040] 图2是在运行操作系统的设备200上的数据存储装置(诸如硬盘驱动器或固态驱动器)的框图。所述数据存储装置具有EFI系统分区201,EFI系统分区201是由遵循统一可扩展固件接口(UEFI)的设备所使用的分区。当设备被启动时,UEFI固件加载被存储在EFI系统分区(ESP)201上的文件以开始所安装的操作系统和实用程序。ESP 201包含针对所安装的操作系统的启动加载器或内核映像,其被包含在O/S分区202中。ESP 201还包含针对设备上存在的硬件的驱动程序文件、系统实用程序以及诸如错误日志的数据文件。UEFI固件使用UEFI变量203来启动设备。

[0041] UEFI变量203识别指向与ESP 201中的安全启动配置策略205相对应的安全性策略版本204。UEFI变量203还提供指向安全启动配置策略205中的平台识别符207的平台识别符206。平台清单208是从ESP 201加载的一个或多个文件。平台清单208是由具有在安全启动配置策略205中的对应值210的清单识别符209授权的签名文件。多个平台清单文件能够由安全启动配置策略205来授权,并且所有这些文件将由设备加载。当加载多个平台清单文件时,其将被合并在一起以形成针对所述系统的活动平台清单。

[0042] 在加载安全启动配置策略205之后立即由UEFI启动管理器加载平台清单208。这在系统中早期发生,然后验证任何其他签名。活动平台清单208从启动管理器传送到系统加载器和内核,以便其能够在操作系统加载期间使用所述平台清单来验证签名是否有效。

[0043] 平台清单208包括允许针对该操作系统版本的程序包和二进制文件的列表211。所列出的程序包和二进制文件211指向O/S分区202上的组件212和213,诸如程序包A和程序包B。操作系统文件214是从平台清单208中列出的程序包和二进制文件中提取和加载的。

[0044] 所述系统验证平台清单208被绑定到设备200并且所述平台清单是代码签名的。平台清单208可以被直接或间接地绑定到设备200,诸如通过绑定到设备200的安全策略。组件212和213被验证为在所述平台清单上列出,并且还必须利用有效证书进行代码签名。组件212和213不需要特定于平台的代码签名证书,这消除了现有系统的双重创作问题。此外,因为仅有在平台清单208上列出的组件被加载在O/S分区202上,所以这消除了现有系统的交叉传播问题。

[0045] 操作系统构建中的程序包可以包含对该程序包中的所有文件进行签名的目录文件。目录中的程序包名称属性引用哪个程序包负责哪个目录,使得代码完整性能够验证程序包中的文件。

[0046] 在构建文件时，不知道将包含该文件的(一个或多个)程序包的识别。利用构建文件高速缓存，预期的程序包可能在构建文件之后改变。二进制ID属性被存储在嵌入式签名文件中的嵌入式签名内。二进制ID是必需的，以便平台清单能够直接信任所述文件，而无需知道文件所属的程序包。二进制ID可以是SHA256散列(hash)，其在文件的生存期内保持相对恒定并且以合理的保真度级别来识别所述文件。使用“合理”一词是因为这在不同情况下将是不同的，诸如生产场景与开发人员场景。

[0047] 授权平台清单可以作为计数阵列被存储在安全启动配置策略中。一个条目保持授权平台清单的计数，并且针对每个授权清单都存在单独的条目。

[0048] 平台清单数据文件格式可以是由以下结构定义的二进制文件格式：

[0049] -用于识别文件格式的幻数或文件签名；

[0050] -识别文件格式的版本的文件格式版本；

[0051] -用于识别生成该平台清单文件的构建的识别和版本控制信息，诸如构建字符串；

[0052] -必须与来自安全启动配置策略的授权平台清单识别符相匹配的清单识别符或通用独有识别符；

[0053] -清单版本；

[0054] -表示清单自身中条目数量的条目计数；以及

[0055] -文件的其余部分是散列，每个散列指定授权实体的散列。

[0056] 清单自身可以是散列数组，其长度由文件格式版本来描述。为了改变散列长度，必须递增文件格式版本。在一些实施例中，操作系统供应商对平台清单数据结构进行签名，诸如通过将其装包在PKCS#7签名中。在其他实施例中，OEM可以对平台清单进行签名以在OEM的平台上使用。

[0057] 当从磁盘加载平台清单文件并且验证签名时，其将被加载并且以程序包清单数据结构被存储在存储器中。最初在启动环境中创建程序包清单数据结构，在所述启动环境中用于验证操作系统的启动组件的签名。然后，将程序包清单数据结构与存储器表示中的相同数据一起传输到内核，其中，在操作系统的执行期间对其进行保存。程序包清单数据结构包括数组，该数组包含针对已加载和贡献散列的所有平台清单文件的识别和版本控制信息。

[0058] 图3是图示根据使用平台清单的示例性实施例的针对不同平台的操作系统的不同版本的框图。操作系统供应商可以发布台式机版本301和移动版本302。每个版本使用大量公共组件，诸如程序包A 303和程序包B 304。不同版本还具有特定于每个平台的组件，诸如程序包N 305仅用在台式机版本301中，而程序包M 306仅用在移动版本302中。

[0059] 替代如在图1中所图示的要求重新签名步骤，在图3中，每个版本都包括与特定平台或设备相关联的平台清单。程序包清单307对于台式机版本301是独有的，而程序包清单308对于移动版本308是独有的。程序包清单307、308诸如通过设备上的安全策略与特定设备或设备类型相关联。在程序包清单上列出了在每个版本中所使用的个体组件，诸如程序包303-306和二进制文件。程序包清单307、308由供应商签名。组件不必专门针对版本进行签名，而是替代地能够由操作系统供应商签名以在加载时进行验证。平台消除了交叉传播的风险，因为如果由供应商签名但是意图用于其他构建的组件未在平台清单上列出，则无法加载所述组件。

[0060] 图4是图示根据一个实施例的用于管理在设备上加载的软件组件的方法的流程图。在步骤401中，识别具有有效代码签名证书的平台清单。在步骤402中，平台清单被确认为绑定到设备。在步骤403中，识别在平台清单上列出的组件。在步骤404中，针对有效的代码签名证书来评估每个列出的组件。

[0061] 如果在步骤404中组件具有有效的代码签名证书，则在步骤405中，组件被加载在设备上。否则，在步骤406中，从所述设备阻止所述组件，因为其不具有有效的代码签名证书。所述组件可以是例如针对操作系统的二进制文件和程序包。所述组件可以以嵌入方式或者利用分离签名进行签名。所述平台清单可以以允许识别未授权平台清单的方式被绑定到设备。

[0062] 可以识别具有有效代码签名证书的额外组件。如果确定额外组件未在平台清单上列出，则从设备阻止所述额外组件。

[0063] 可以在设备安全策略中识别清单识别符。所述清单识别符可以被用于确认平台清单被绑定到设备。

[0064] 可以在设备安全策略中识别多个清单识别符。然后，可以加载与多个清单识别符相对应的多个平台清单文件。所述多个平台清单文件被合并为针对设备的活动平台清单。

[0065] 图5图示了为策略驱动强制实施平台授权清单提供可以在其上实施图1-4的示例的合适计算环境的计算机500的示例，以防止甚至是可能已经在设备上实现完全管理访问的实体在系统之间的可执行文件的交叉传播。计算机500仅仅是合适的计算环境的一个示例，并不旨在对本发明的使用范围或功能提出任何限制。本发明与许多其他通用或专用计算系统环境或配置一起操作。可以适于与本发明一起使用的众所周知的计算系统、环境和/或配置的示例包括但不限于：个人计算机(PC)、服务器计算机、手持或膝上型设备、平板设备、游戏控制台、智能电话、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子件、网络PC、小型计算机、大型计算机、包括任何上述系统或设备的分布式计算环境等。

[0066] 可以在由计算机执行的计算机可执行指令(诸如程序模块)的一般上下文中描述本发明。通常，程序模块包括执行任务或者实施抽象数据类型的例程、程序、对象、组件、数据结构等。本发明还可以在分布式计算环境中实践，其中，任务由通过通信网络链接的远程处理设备来执行。在分布式计算环境中，程序模块可以位于包括存储器存储设备的本地和/或远程计算机存储介质中。

[0067] 参考图5，用于实施本发明的各个方面的示例性系统可以包括计算机500形式的通用计算设备。组件可以包括但不限于各种硬件组件，诸如处理单元501、数据存储装置502(诸如系统存储器)以及将包括数据存储装置502的各种系统组件耦合到处理单元501的系统总线503。系统总线503可以是若干种类型的总线结构中的任意一种，包括存储器总线或存储器控制器、外围总线以及使用各种总线架构的本地总线。通过示例而非限制，这样的架构包括工业标准架构(ISA)总线、微通道架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)本地总线以及外围组件互连(PCI)总线(也被称为夹层总线)。

[0068] 计算机500通常包括各种计算机可读介质504。计算机可读介质504可以是能够由计算机500访问的任何可用介质，并且包括易失性和非易失性介质以及可移除和不可移除介质两者，但是不包括传播的信号。通过示例而非限制，计算机可读介质504可以包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、

程序模块或其他数据之类的信息的任何方法或技术实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于:RAM、ROM、EEPROM、闪存或其他存储技术、CD-ROM、数字通用盘(DVD)或其他光盘存储设备、磁带盒、磁带、磁盘存储设备或其他磁存储设备,或者能够用于存储所需信息并且能够由计算机500访问的任何其他介质。通信介质通常以诸如载波或其他传输机制的调制数据信号来体现计算机可读指令、数据结构、程序模块或其他数据,并且包括任何信息传递介质。术语"调制数据信号"意指以对信号中的信息进行编码的方式来设置或改变其一个或多个特性的信号。通过示例而非限制,通信介质包括诸如有线网络或直连线的有线介质,以及诸如声学、RF、红外和其他无线介质的无线介质。上述项的任何组合也可以被包括在计算机可读介质的范围之内。计算机可读介质可以体现为计算机程序产品,诸如被存储在计算机存储介质上的软件。

[0069] 数据存储装置或系统存储器502可以是例如易失性和/或非易失性存储器形式的计算机存储介质,诸如只读存储器(ROM)、随机存取存储器(RAM)、硬盘驱动器或固态驱动器。包含有助于诸如在启动期间在计算机500内的各元件之间转移信息的基本例程的基本输入/输出系统(BIOS)或UEFI固件通常被存储在ROM中。RAM通常包含由处理单元501可立即访问和/或当前正在操作的数据和/或程序模块。通过示例而非限制,数据存储装置502保持操作系统、应用程序以及其他程序模块和程序数据。

[0070] 数据存储装置502可以包括分区,诸如EFI系统分区和操作系统(O/S)分区,并且可以存储诸如UEFI变量和安全策略的系统数据。处理单元501上的O/S加载器和代码完整性组件可以被用于加载操作系统并且确保组件具有有效的代码签名证书。

[0071] 数据存储装置502还可以包括其他可移除/不可移除、易失性/非易失性计算机存储介质。仅作为示例,数据存储装置502可以是从不可移除的非易失性磁介质读取或向其写入的硬盘驱动器、从可移除的非易失性磁盘读取或向其写入的磁盘驱动器,以及从可移除的非易失性光盘(诸如CD ROM或其他光学介质)读取或向其写入的光盘驱动器。能够在示例性操作环境中使用的其他可移除/不可移除、易失性/非易失性计算机存储介质包括但不限于:磁带盒、闪存卡、数字通用盘、数字录像带、固态RAM、固态ROM等。如上文所述以及在图5中所图示的,驱动器以及其相关联的计算机存储介质为计算机500提供计算机可读指令、数据结构、程序模块和其他数据的存储。

[0072] 用户可以通过用户界面505或者其他输入设备输入命令和信息,所述输入设备诸如是游戏控制器、触摸屏、平板计算机、电子数字转换器、麦克风、键盘和/或定点设备(通常被称为鼠标、轨迹球或触摸板)。其他输入设备可以包括操纵杆、游戏手柄、圆盘式卫星天线、扫描仪等。另外,语音输入,使用手或手指的手势输入,或者其他自然用户界面(NUI)也可以与适当的输入设备一起使用,诸如麦克风、相机、平板计算机、触摸板、手套或其他传感器。这些和其他输入设备常常通过耦合到系统总线503的用户输入接口505被连接到处理单元501,但是可以通过其他接口和总线结构连接,诸如并行端口、游戏端口或者通用串行总线(USB)。监视器506或其他类型的显示设备也经由诸如视频接口的接口连接到系统总线503。监视器506还可以与触摸屏面板等集成。注意,监视器和/或触摸屏面板能够物理地耦合到其中包含计算机500的壳体,诸如在平板型个人计算机中。另外,诸如计算机500的计算机还可以包括其他外围输出设备,诸如扬声器和打印机,其可以通过输出外围接口等连接。

[0073] 计算机500可以使用到一个或多个远程设备(诸如远程计算机)的网络接口507在

联网或云计算环境中操作。远程计算机可以是个人计算机、服务器、路由器、网络PC、对等设备或其他公共网络节点，并且通常包括上文相对于计算机500描述的许多或所有元件。在图5中所描绘的逻辑连接包括一个或多个局域网(LAN)以及一个或多个广域网(WAN)，但是也可以包括其他网络。这样的联网环境在办公室、企业范围的计算机网络、内联网和互联网中是常见的。

[0074] 当在网络或云计算环境中使用时，计算机500可以通过网络接口或适配器507被连接到公共或专用网络。在一些实施例中，调制解调器、收发器、网络接口卡或者其他单元用于通过网络建立通信。可以是内部的或外部的网络接口507可以经由网络接口507或者其他适当的机制被连接到系统总线503。诸如包括接口和天线的无线网络组件可以通过诸如接入点或对等计算机的合适设备被耦合到网络。在联网环境中，相对于计算机500或者其部分所描述的程序模块可以存储在远程存储器存储设备中。可以意识到，所示的网络连接是示例性的，并且可以使用在计算机之间建立通信链路的其他单元。

[0075] 一种用于管理在设备上加载的软件组件的示例性方法，包括：识别具有有效证书的平台清单；确认所述平台清单被绑定到所述设备；识别在所述平台清单上列出的组件；确认所列出的组件具有有效证书；以及在所述设备上加载所列出的具有有效证书的组件。所述方法还可以包括：识别具有有效证书的额外组件；确定所述额外组件未在所述平台清单上列出；以及从设备阻止所述额外组件。所述组件可以是针对操作系统的二进制文件和程序包。

[0076] 所述方法还可以包括：在设备安全策略中识别清单识别符；以及使用所述清单识别符来确认所述平台清单被绑定到所述设备。

[0077] 所述方法还可以包括：在设备安全策略中识别多个清单识别符；加载与所述多个清单识别符相对应的多个平台清单文件；以及将所述多个平台清单文件合并为针对所述设备的活动平台清单。

[0078] 所述组件以嵌入方式或者利用分离签名进行签名。

[0079] 所述平台清单以允许识别未授权平台清单的方式被绑定到所述设备。

[0080] 一种示例性设备，包括：处理器，其运行操作系统加载器和代码完整性组件；以及设备存储器，其存储安全策略和操作系统组件，其中，所述操作系统加载器被配置为使用所述安全策略中的平台清单识别符来识别平台清单，并且加载在所述平台清单中列出的组件，并且其中，所述代码完整性组件被配置为在所述操作系统加载器加载组件之前确认所述平台清单和在所述平台清单中列出的组件具有有效证书。所述组件可以是针对操作系统的二进制文件和程序包。

[0081] 所述设备安全策略可以被用于确认所述平台清单被绑定到所述设备。

[0082] 所述操作系统加载器还被配置为：加载与所述安全策略中的多个清单识别符相对应的多个平台清单文件，并且将所述多个平台清单文件合并为所述设备的活动平台清单。

[0083] 所述操作系统加载器还可以被配置为确定额外组件未在所述平台清单中列出，并且即使所述代码完整性组件将所述额外组件识别为具有有效证书也从所述设备阻止所述额外组件。

[0084] 所述组件以嵌入方式或者利用分离签名进行签名。

[0085] 所述平台清单以允许识别未授权平台清单的方式被绑定到所述设备。

[0086] 一种强制实施操作系统组成的方法，包括：选择要包含在针对选定平台的操作系统中的多个文件，所述多个文件具有有效文件证书；以及生成一个或多个代码签名平台清单，每个代码签名平台清单具有平台清单识别符和有效平台证书并且列出多个文件中的一个或多个。

[0087] 该示例性方法还可以包括：通过列出设备安全策略中的可接受平台清单识别符来控制能够在设备上加载什么操作系统，其中，如果针对其他操作系统的文件没有出现在可接受平台清单上，则所述文件将不被加载到所述设备上。

[0088] 该示例性方法还可以包括：将两个或更多个平台清单合并为针对设备的活动平台清单。

[0089] 尽管利用特定于结构特征和/或方法动作的语言描述了本主题，但是应当理解，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。而是，公开了上述具体特征和动作作为实施权利要求的示例性形式。

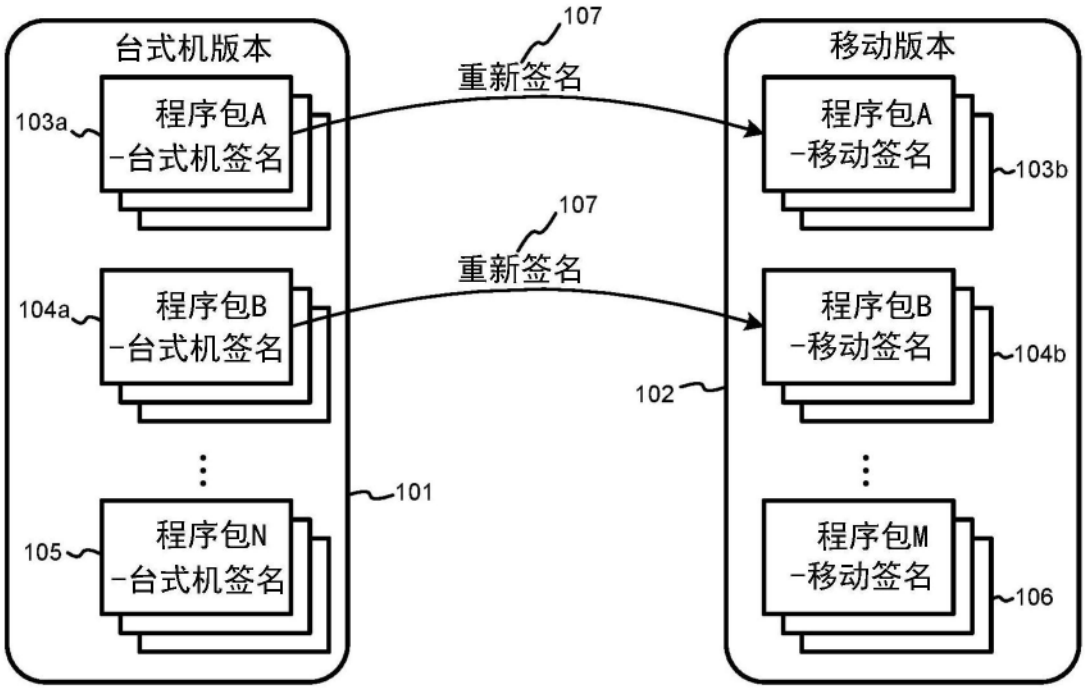

台式机版本
程序包A
-台式机签名
103a
程序包B
-台式机签名
104a
程序包N
-台式机签名
105
101
107
重新签名
107
重新签名
移动版本
程序包A
-移动签名
103b
程序包B
-移动签名
104b
102
程序包M
-移动签名
106

图1(现有技术)

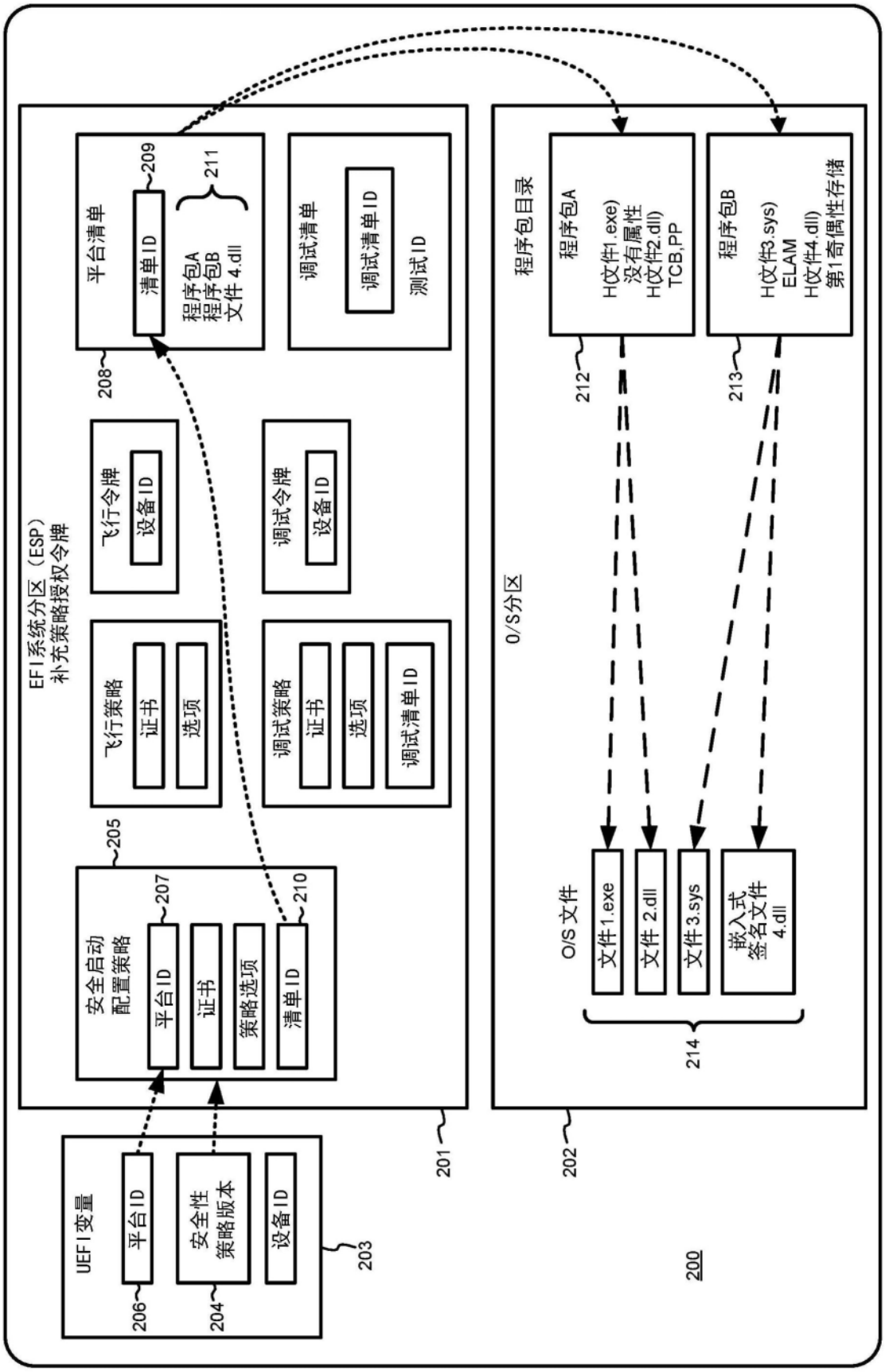

EFI系统分区（ESP）
补充策略授权令牌
平台清单
清单ID
209
211
程序包A
程序包B
文件 4.dll
208
调试清单
调试清单ID
测试ID
飞行令牌
设备ID
调试令牌
设备ID
飞行策略
证书
选项
调试策略
证书
选项
调试清单ID
205
安全启动
配置策略
207
平台ID
证书
策略选项
210
清单ID
UEFI变量
平台ID
206
安全性
策略版本
204
设备ID
203
201
程序包目录
程序包A
H(文件1.exe)
没有属性
H(文件2.dll)
TCB,PP
212
程序包B
H(文件3.sys)
ELAM
H(文件4.dll)
第1奇偶性存储
213
O/S分区
O/S文件
文件1.exe
文件 2.dll
文件3.sys
嵌入式
签名文件
4.dll
214
202
200

图2

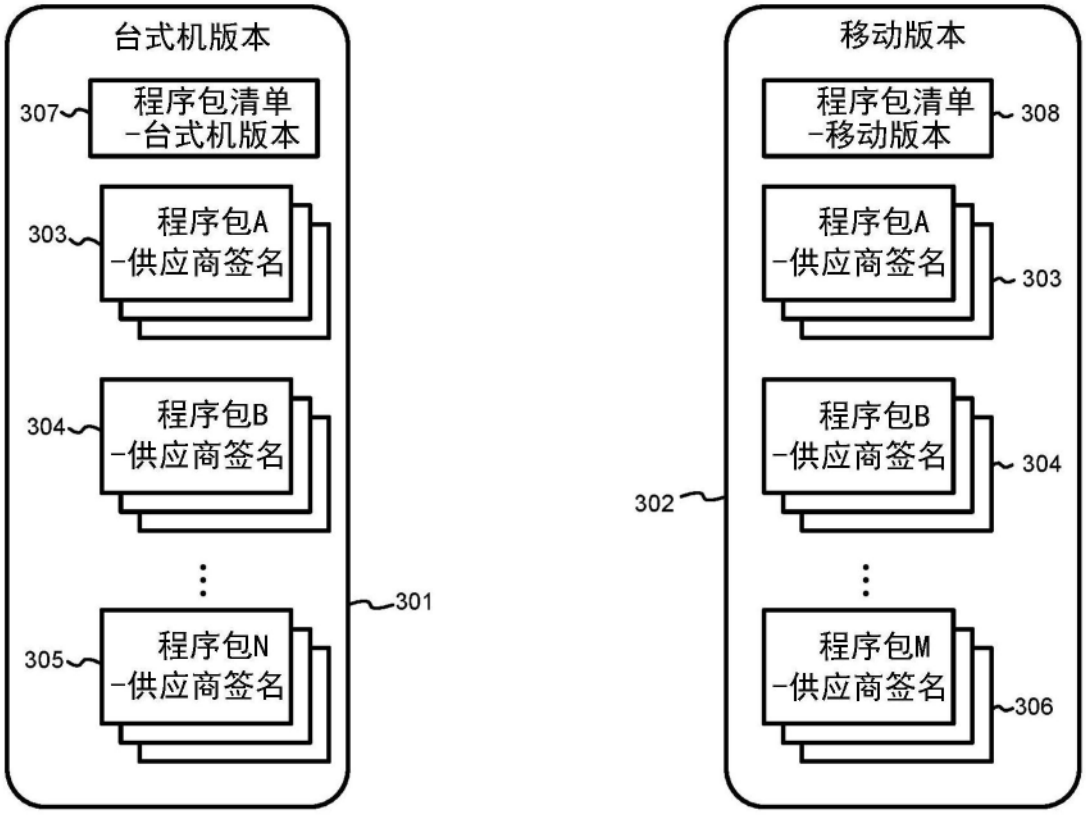

台式机版本
307
程序包清单
-台式机版本
303
程序包A
-供应商签名
304
程序包B
-供应商签名
305
程序包N
-供应商签名
301
移动版本
程序包清单
-移动版本
308
程序包A
-供应商签名
303
程序包B
-供应商签名
304
302
程序包M
-供应商签名
306

图3

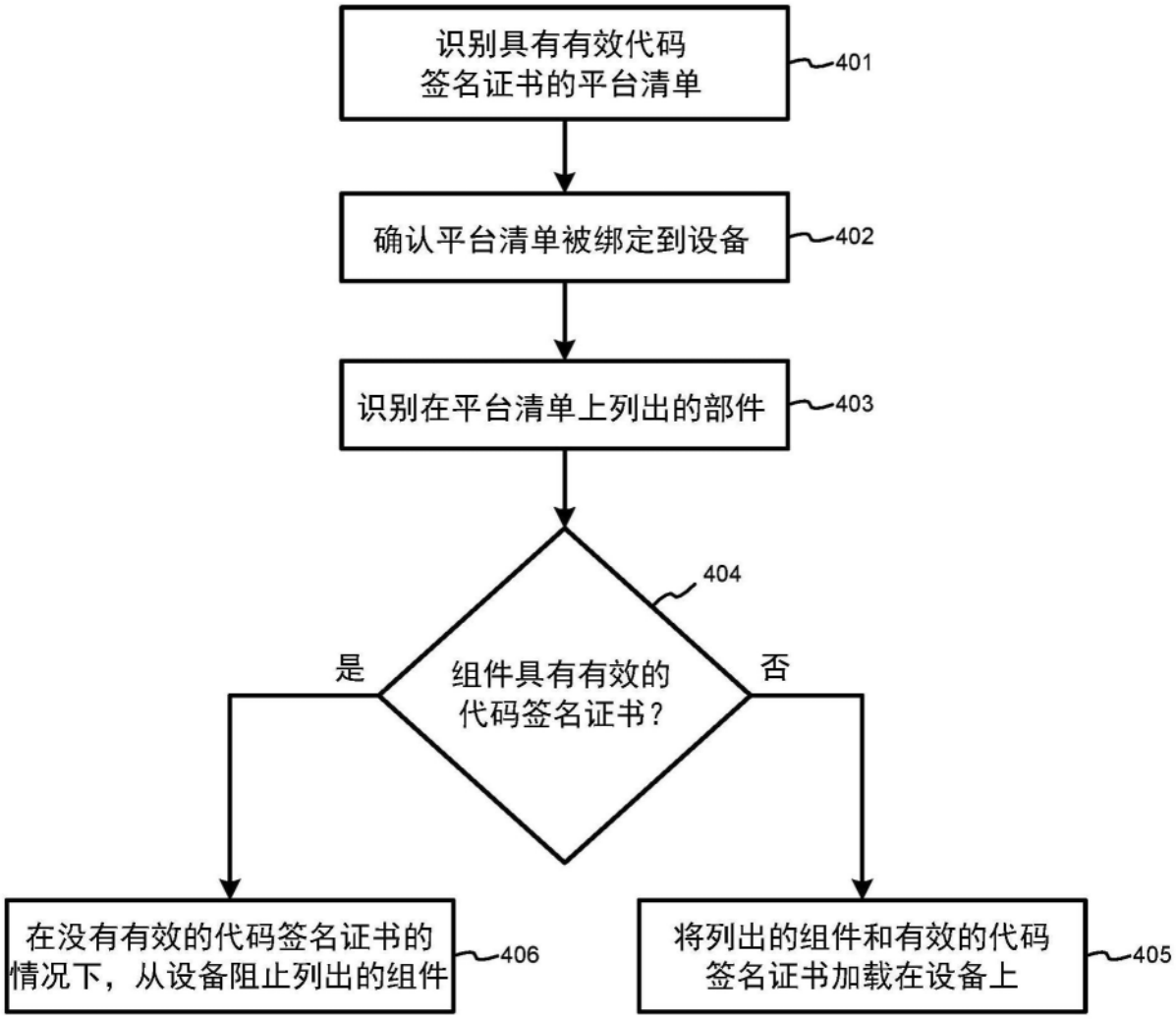

识别具有有效代码签名证书的平台清单
401
确认平台清单被绑定到设备
402
识别在平台清单上列出的部件
403
404
组件具有有效的代码签名证书？
是
否
在没有有效的代码签名证书的情况下，从设备阻止列出的组件
406
将列出的组件和有效的代码签名证书加载在设备上
405

图4

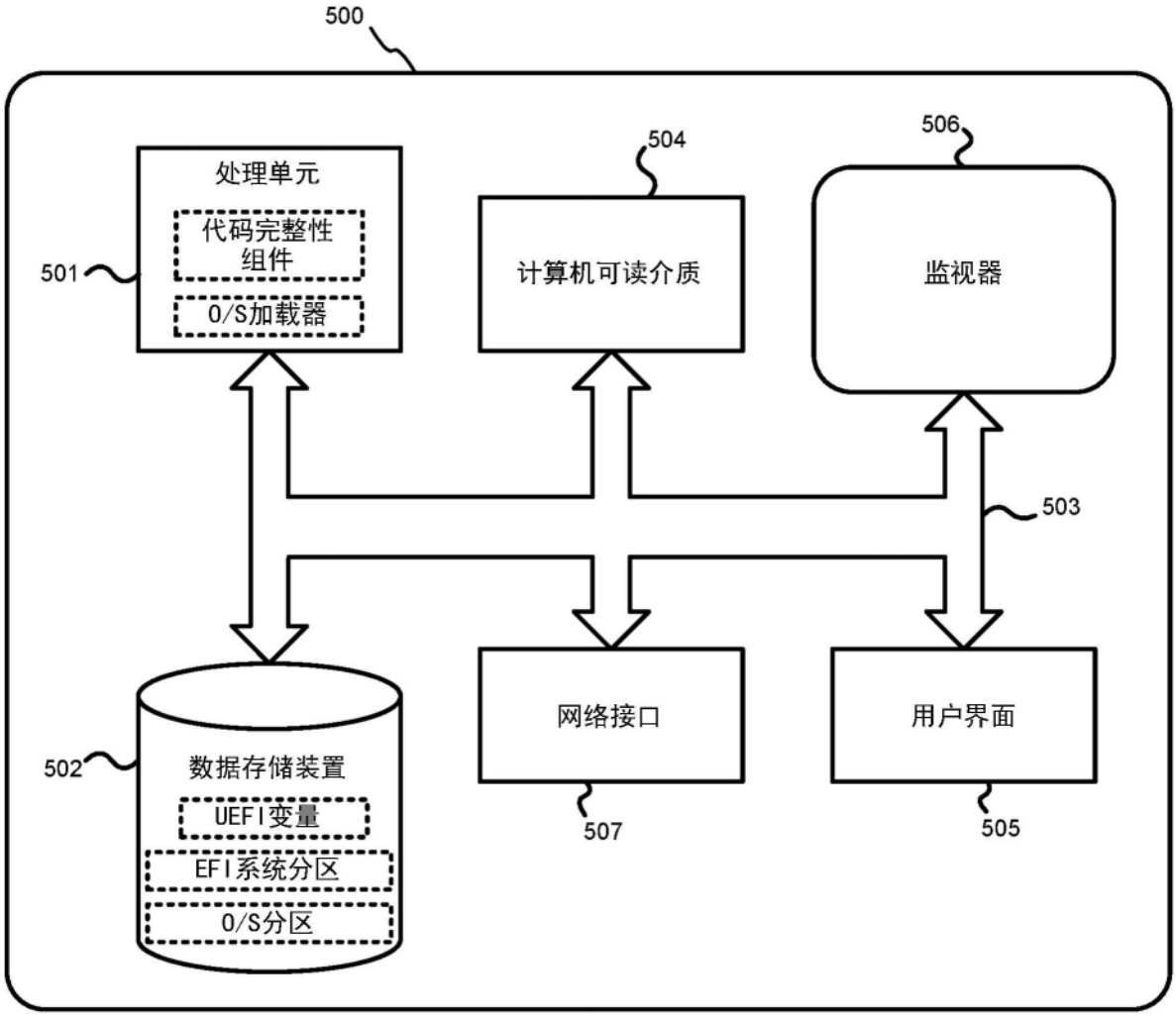

500
处理单元
代码完整性组件
O/S加载器
501
504
计算机可读介质
506
监视器
503
502
数据存储装置
UEFI变量
EFI系统分区
O/S分区
网络接口
507
用户界面
505

图5