



## (12)发明专利申请

(10)申请公布号 CN 107431621 A

(43)申请公布日 2017.12.01

(21)申请号 201580077004.2

(74)专利代理机构 中国专利代理(香港)有限公司

(22)申请日 2015.12.09

72001

(30)优先权数据

代理人 郑浩 郑冀之

14/583620 2014.12.27 US

(51)Int.Cl.

H04L 9/32(2006.01)

(85)PCT国际申请进入国家阶段日

2017.08.25

(86)PCT国际申请的申请数据

PCT/US2015/064578 2015.12.09

(87)PCT国际申请的公布数据

W02016/105935 EN 2016.06.30

(71)申请人 迈克菲有限责任公司

地址 美国德克萨斯州

(72)发明人 N.M.史密斯 D.鲁巴哈 S.沙

J.马丁 M.J.舍勒 S.查克拉巴蒂

幸滨

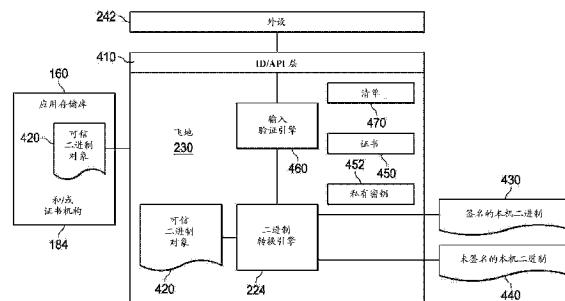
权利要求书3页 说明书19页 附图10页

(54)发明名称

采用输入标记的可信二进制的二进制转换

(57)摘要

在示例中，计算装置包含可信运行环境(TEE)(其包含飞地)。飞地可以包含二进制转换引擎(BTE)和输入验证引擎(IVE)。在一个实施例中，IVE接收可信二进制作为输入，并且分析可信二进制以识别执行输入/输出操作的函数、类和变量。为了确保这些接口的安全，可以在飞地内执行那些操作。IVE标记可信二进制，并提供二进制到BTE。BTE然后将可信二进制转换成第二格式，包含指定标记部分以供在飞地内的运行。BTE也可以对处于第二格式的新二进制文件进行签名，并将其导出离开飞地。



1. 一种计算设备,包括:

可信运行环境(TEE);

一个或多个逻辑元件,包括所述TEE内的输入验证引擎(IVE),所述IVE可操作用于:

接收可信二进制对象;

分析所述可信二进制对象以识别执行输入/输出操作的部分;

标记所述部分以创建具有标记部分的标记的可信二进制;以及

将所述部分提供到二进制转换引擎;以及

一个或多个逻辑元件,包括所述TEE内的所述二进制转换引擎(BTE),所述BTE可操作用于:

接收处于第一格式的所述标记的可信二进制;

将所述标记的可信二进制转换成处于第二格式的第二二进制对象,其中转换包括保留所述标记的部分以供在飞地内的运行。

2. 根据权利要求1所述的计算设备,其中,所述IVE还可操作用于:

在所述TEE内供应飞地;以及

在所述飞地内执行其功能的至少一些。

3. 根据权利要求2所述的计算设备,其中,所述IVE还可操作用于在所述飞地内供应所述BTE。

4. 根据权利要求3所述的计算设备,其中所述BTE包括二进制转换器,其从由运行时间引擎、解释器、即时编译器、提前编译器、虚拟机、编译器、链接器和工具链实用程序组成的组中选择。

5. 根据权利要求3所述的计算设备,其中所述BTE包括Java虚拟机,并且其中所述IVE至少部分地以Java实现并且配置成在所述BTE内操作。

6. 根据权利要求1所述的计算设备,其中,所述IVE还可操作用于执行输入验证。

7. 根据权利要求6所述的计算设备,其中,所述IVE包括从由安全网络栈、安全图形引擎、安全人性化输入装置接口引擎、安全音频引擎、安全图像处理引擎、安全遥测引擎、安全全球定位系统接收器和二进制输入分析器组成的组中选择的模块。

8. 根据权利要求1-6中任一项所述的计算设备,其中,所述BTE还可操作用于对所述第二二进制对象进行签名。

9. 根据权利要求8所述的计算设备,其中,第一签名的对象要由密钥签名,并且其中对所述第二对象进行签名包括采用所述密钥对所述第二对象进行签名。

10. 根据权利要求8所述的计算设备,其中,第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一密钥的共同发起者签名的第二密钥对所述第二对象进行签名。

11. 根据权利要求8所述的计算设备,其中,第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一对象的供应商提供的第二密钥对所述第二对象进行签名。

12. 根据权利要求8所述的计算设备,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一密钥签名的第二密钥对所述第二对象进行签名。

13. 根据权利要求8所述的计算设备,其中所述二进制转换引擎还可操作用于在对所述第二对象进行签名之前咨询证书过期或撤销列表。

14. 一个或多个计算机可读媒介,在其上存储有指令,所述指令在执行时指令处理器用于:

在TEE内提供输入验证引擎(IVE),所述IVE可操作用于:

接收可信二进制对象;

分析所述可信二进制对象以识别执行输入/输出操作的部分;

标记所述部分以创建具有标记部分的标记的可信二进制;以及

将所述部分提供到二进制转换引擎;以及

在所述TEE内提供所述二进制转换引擎(BTE),所述BTE可操作用于:

接收处于第一格式的所述标记的可信二进制;

将所述标记的可信二进制转换成处于第二格式的第二二进制对象,其中转换包括保留所述标记的部分以供在飞地内的运行。

15. 根据权利要求14所述的一个或多个计算机可读媒介,其中所述IVE还可操作用于:

在所述TEE内供应飞地;以及

在所述飞地内执行其功能的至少一些。

16. 根据权利要求15所述的一个或多个计算机可读媒介,其中所述IVE还可操作用于在所述飞地内供应所述BTE。

17. 根据权利要求16所述的一个或多个计算机可读媒介,其中所述BTE包括Java虚拟机,并且其中所述IVE至少部分地以Java实现并且配置成在所述BTE内操作。

18. 根据权利要求14-17中任一项所述的一个或多个计算机可读媒介,其中所述IVE还可操作用于执行输入验证。

19. 根据权利要求14-17中任一项所述的一个或多个计算机可读媒介,其中所述BTE还可操作用于对所述第二二进制对象进行签名。

20. 根据权利要求19所述的一个或多个计算机可读媒介,其中第一签名的对象要由密钥签名,并且其中对所述第二对象进行签名包括采用所述密钥对所述第二对象进行签名。

21. 根据权利要求19所述的一个或多个计算机可读媒介,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一密钥的共同发起者签名的第二密钥来对所述第二对象进行签名。

22. 根据权利要求19中的任一项所述的一个或多个计算机可读媒介,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一对象的供应商提供的第二密钥来对所述第二对象进行签名。

23. 根据权利要求19所述的一个或多个计算机可读媒介,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一密钥签名的第二密钥对所述第二对象进行签名。

24. 一种用于在可信运行环境(TEE)内的运行的计算机实现的方法,包括:

接收可信二进制对象;

分析所述可信二进制对象以识别执行输入/输出操作的部分;

标记所述部分以创建具有标记部分的标记的可信二进制;以及

将所述标记的可信二进制转换成处于第二格式的第二二进制对象，其中转换包括保留所述标记的部分以供在飞地内的运行。

25. 根据权利要求24所述的方法，还包括对所述第二二进制对象进行签名。

## 采用输入标记的可信二进制的二进制转换

### [0001] 相关申请的交叉引用

本申请要求2014年12月27日提交的命名为“BINARY TRANSLATION OF A TRUSTED BINARY WITH INPUT TAGGING”的美国非临时专利申请No.14/583620的权益和优先权，其通过引用整体结合在本文中。

### 技术领域

[0002] 本申请涉及计算机安全领域，并且更具体地，涉及用于采用输入标记的可信二进制的二进制转换的系统和方法。

### 背景技术

[0003] 计算机安全是一方面在恶意行为者之间以及另一方面在计算机安全公司和用户之间的不断演进的军备竞赛(arms race)。有关这竞赛的安全方面的一个有用的工具是“可信运行环境”(TEE)。TEE是硬件、软件和固件的组合，其提供环境以用于运行签名和验证的二进制或其它可运行对象。TEE可以包含具有适合的扩展指令(例如英特尔®安全防护扩展(SGX)指令)的处理器、安全协处理器、适当的固件和驱动器和/或特殊存储器“飞地(enclave)”。飞地包含特殊存储器页或分区，其只能经由特殊的TEE指令访问和引用。具体地，程序可以向飞地内的存储器位置写或从飞地内的存储器位置读，或者运行飞地内的指令(仅作为特殊指令，像英特尔®SGX指令)。采用其它(非安全)指令进入飞地的任何尝试可能会导致诸如页面故障的错误。

[0004] 在一个示例中，TEE配置成仅运行被验证和签名(例如通过证书机构)的对象。这帮助确保恶意软件和其它恶意对象不在TEE内运行。在一些示例中，TEE被给予对某些敏感或重要资源(例如重要的操作系统文件、敏感数据或其它被保护的资源)的排它性访问。可以使用飞地来将对机密数据操作的可信代码与可能运行不可信代码的剩余的计算设备隔离。

### 附图说明

[0005] 当与附图一起阅读时，根据下面的详细描述最好地理解本公开。强调的是，根据行业中的标准实践，各种特征并没有按比例绘制，并且仅用于说明的目的。事实上，为了讨论的清楚，各种特征的尺寸可以任意增加或减少。

[0006] 图1是根据本说明书的一个或多个示例的安全使能网络的框图。

[0007] 图2是根据本说明书的一个或多个示例的计算装置的框图。

[0008] 图3是根据本说明书的一个或多个示例的服务器的框图。

[0009] 图4A和4B是根据本说明书的一个或多个示例的飞地的功能框图。

[0010] 图5是根据本说明书的一个或多个示例的通过一对飞地互换签名(sign)的二进制的功能框图。

[0011] 图6是根据本说明书的一个或多个示例的飞地的功能框图。

[0012] 图7是根据本说明书的一个或多个示例的输入验证引擎的功能框图。

- [0013] 图8是根据本说明书的一个或多个示例执行二进制转换的方法的流程图。
- [0014] 图9是根据本说明书的一个或多个示例执行输入验证的方法的流程图。
- [0015] 图10是根据本说明书的一个或多个示例的IVE 460和BTE 224之间的交互方法的框图。

## 具体实施方式

- [0016] 概览

在示例中，计算装置包含可信运行环境(TEE)，其包含飞地。飞地可以包含二进制转换引擎(BTE)和输入验证引擎(IVE)。在一个实施例中，IVE接收可信二进制作为输入，并且分析可信二进制以识别执行输入/输出操作的函数(function)、类和变量。为了确保这些接口的安全，可以在飞地内执行那些操作。IVE标记可信二进制，并提供二进制到BTE。BTE然后将可信二进制转换成第二格式，包含指定标记的部分以供在飞地内的运行。BTE也可以对处于第二种格式的新二进制进行签名，并将其导出离开飞地。

- [0017] 本公开的示例实施例

下面公开提供了用于实现本公开的不同特征的许多不同实施例或示例。以下描述组件和布置的特定示例以简化本公开。当然，这些仅仅是示例，而不意图是限制性的。此外，本公开可以在各种示例中重复参考数字和/或字母。此重复是为了简单和清楚的目的，并且本身并不表明所讨论的各种实施例和/或配置之间的关系。不同的实施例可具有不同的优点，并且对于任何实施例不一定要求具体的优点。

[0018] 代码签名和验证是某些安全计算架构中的基本构建块。它们帮助验证由开发人员或独立软件供应商(ISV)构建的代码或二进制在其到其消费者的途中未被篡改，因此保证软件完整性并在它们之间构建可信通道。然而，此通道通常只延伸直到软件安装时间。繁杂的TEE可能进行另外一步并验证软件的完整性直到运行点。然而，它们可能不会扩展到当代码/二进制不得不被合法修改时(像二进制转换、即时编译)或当管理的运行时间开始起作用时的用例。

[0019] 在本说明书的示例中，TEE可以包含二进制转换引擎(BTE)和输入验证引擎(IVE)中的一个或两者。BTE和IVE可以彼此独立地操作以执行其特定功能，或者可以协同工作以提供联合功能。

[0020] BTE可以配置成接收称为可信二进制的第一对象，其可以是例如二进制对象、文本文件、脚本、宏或先前已经分析和确认(validated)的任何其它适合的对象。可信二进制可能出现在TEE的白名单上，意味着可信二进制被允许在TEE内运行。可信二进制可能具有由证书机构签名的证书，包含能够通过私有密钥验证的公共密钥。然而，可信二进制可能不适合于以其原始形式在目标系统上使用。在一个非限制性示例中，可信二进制是Java字节代码二进制，其只能由Java虚拟机运行。

[0021] 移动装置和移动操作系统的增加的使用使此类可信二进制的安全态势复杂。例如，Java字节代码可能不适合于在具体架构上使用，或者可能期望将Java字节代码转变成适合于在移动装置上使用的新形式。在一个实施例中，Java字节代码将被编译为用于适合的移动装置的本机指令。然而，编译可能包含不同架构上的若干目标装置，例如基于Intel x86的架构、ARM架构或其它架构。在移动装置上使用这些二进制可能要求将字节代码编译

成每个单独的本机格式，并且然后个别对每个编译的输出进行签名。虽然这是可能的，但这可能很麻烦。

[0022] 在另一示例中，直到第一对象到达目标装置之后二进制转换才发生。例如，BTE可能是一个即时 (JIT) 编译器，其将Java字节代码实时编译成本机二进制格式。在那个情况下，二进制不能由证书机构 (authority) 事先签名。在其中TEE将只运行签名和验证的二进制的实施例中，这意味着JIT编译器的输出必须在TEE之外运行。这可能使TEE的安全目的落空，或使得二进制完全无用。

[0023] 在本说明书的一个示例中，描述了一种系统和方法，其中BTE本身是能够在TEE内全部或部分运行的可信二进制。当TEE接收处于第一格式的第一签名的对象时，BTE可以将第一签名的对象转换成处于第二格式的第二对象。例如，第二格式可以是用于主机平台的本机二进制格式。因为第一签名的对象和BTE都被签名和验证，因此假设BTE的输出（处理第一签名的对象作为输入）也能够被视为可信二进制是合理的。因此，TEE本身可以对第二对象进行签名，其为BTE的输出。对第二对象进行签名可以包含采用用来对第一签名的对象进行签名的相同密钥或采用与第一密钥不同但具有与第一个密钥相同的出处的第二密钥对其进行签名。第二二进制则适合于在主机系统上的TEE内运行。

[0024] 此外，BTE可以配置成将处于签名和加密的形式的第二对象从TEE导出。由于第二对象现在已由第一密钥或由具有与第一密钥相同出处的第二密钥签名，所以能够将其提供到以TEE的另一个机器，并且另一个机器能够将第二个对象的证书辨别为有效。在一个示例中，这可以包含在第一机器和第二机器之间执行认证。

[0025] 这在物联网 (IoT) 上下文中可以是特别有用的，其中个别的 IoT 装置不具有足够的处理能力来执行实时二进制转换。在一些情况下，装置可能甚至不能够提供其自己的TEE。相反，它们可以位于提供TEE并且只有在指令是签名和可信二进制才允许其穿过到装置的网关之后。因此，在那个上下文下，装置本身可以被视为TEE。这可以由可信引导机制或其它现有的安全装置进一步促进。

[0026] 在移动装置的上下文中，在输入验证领域中可能会遇到附加的复杂性。在许多情况下，应用或其它二进制对象的安全仅与其输入的安全一样好。因此，如果不执行正确的输入验证，即使在TEE内运行的应用也可能受到损害。此外，在一些情况下，不需要在TEE内提供整个应用。在一个示例中，流行的Android操作系统使用Java作为app的主编程语言和平台。在一些情况下，可能无需在移动装置上在TEE内运行整个app，但可以期望的是，在TEE内运行可信的、验证的和签名的输入验证引擎 (IVE) 以确保到app的输入是有效和适合的。输入验证可能阻止例如诸如缓冲区溢出和无效输入的普通问题。

[0027] 因此，在本说明书的一个实施例中，提供了IVE，并且其可以在TEE内运行。IVE可以包含如安全网络栈、安全图形引擎、安全人性化接口装置 (HID) 引擎、安全音频输出引擎、安全图像处理引擎、安全遥测引擎和安全GPS接收器的这类功能块。

[0028] 可以提供IVE的各种功能块以验证、清理以及以其它方式调节来自用户、来自网络、来自传感器和装置或来自其它二进制对象的输入。一旦输入被正确验证和/或清理，它们就可以被编译成验证的输入分组。验证的输入分组可以在TEE内加密，并由TEE签名。验证的输入分组然后从TEE中导出，并提供到适合的接口，例如Java本机接口 (JNI) 包装器。然后，JNI包装器可以提供加密、签名和验证的输入到普通的Java应用。因为输入是加密的，所

以它们将不被恶意软件或其它恶意对象拦截，并且由于它们已由IVE验证，所以它们能够被应用信任。

[0029] 在一个示例中，IVE还可以包含到BTE的接口，使得在一些情况下，可信二进制可以在被传递到BTE之前由IVE审查。

[0030] 有利地，虽然IVE本身可能需要提供本机或较低级指令（例如以C、C++或汇编语言的），但是应用ISV可能不需要熟悉那些语言来使用IVE（一旦功能块例如由安全公司已构建）。相反，功能块能够被提供为“黑箱”实现，使得程序员仅需要知道用于从他的应用（例如Java应用）调用功能的适当原型和接口。

[0031] 在一个实施例中，程序员可以使用普通Java属性来通知TEE如何验证输入。因此，程序员可以具有配置输入验证而不需要自己写输入验证例程的灵活性。还有利地，输入验证例程本身是能够在TEE内运行的签名和验证的二进制，因此输入验证能够在可信的基础上执行。

[0032] 现在将更具体地参考附图来描述本说明书的系统和方法

图1是根据本说明书的一个或多个示例的受保护的企业100的网络级图。在图1的示例中，多个用户120操作多个客户端装置110。具体地，用户120-1操作桌上型计算机110-1。用户120-2操作膝上型计算机110-2。并且用户120-3操作移动装置110-3。

[0033] 每个计算装置可以包含适当的操作系统，例如Microsoft Window、Linux、Android、Mac OSX、Apple iOS、Unix或类似。前述中的一些可能更经常用在一种类型的装置而不是另一种类型的装置上。例如，在一个实施例中可以是工程工作站的桌上型计算机110-1可能更可能使用Microsoft Window、Linux、Unix或Mac OSX中的一个。膝上型计算机110-2（其通常是具有较少定制选项的便携式现成装置）可能更可能运行Microsoft Window或Mac OSX。移动装置110-3可能更可能运行Android或iOS。然而，这些示例并不意图是限制性的。

[0034] 客户端装置110可以经由企业网络170通信地耦合到其它网络资源或彼此通信地耦合。企业网络170可以是在一个或多个适合的联网协议上操作的任何适合的网络或一个或多个网络的组合，作为非限制性示例包含例如，局域网、内联网、虚拟网络、广域网、无线网络、蜂窝网络或因特网（可选地经由代理、虚拟机或其它类似的安全机制访问）。企业网络170还可以包含一个或多个服务器、防火墙、路由器、交换机、安全器具、防病毒服务器或其他有用的网络装置。在此说明中，为了简单起见，企业网络170被示为单个网络，但是在一些实施例中，企业网络170可以包含大量网络，例如连接到因特网的一个或多个企业内联网。企业网络170还可以经由外部网络172提供对外部网络（例如因特网）的访问。外部网络172可以类似地是任何适合类型的网络。

[0035] 配置为企业安全控制器（ESC）140的一个或多个计算装置还可以在企业网络170上操作。ESC 140可以为安全管理员150提供用户界面来定义企业安全策略，ESC 140可以将其在企业网络170上并跨客户端装置120实施。

[0036] 受保护的企业100可以在网络上遇到各种“安全对象”。安全对象可以是在企业网络170上操作或与企业网络170交互并且具有实际或潜在安全暗示（implication）的任何对象。在一个示例中，对象可以宽泛地划分为硬件对象（包含与网络通信或经由网络操作的任何物理装置）以及软件对象。软件对象可以进一步细分为“可运行对象”和“静态对象”。可运

行对象包含能够主动运行代码或自主操作的任何对象,作为非限制性示例例如,应用、驱动器、程序、可运行、库、进程、运行时间、脚本、宏、二进制、解释器、解释语言文件、具有内联代码的配置文件、嵌入式代码和固件指令。静态对象可以被宽泛地指定为不是可运行对象或者不能运行的任何对象,作为非限制性示例例如,文档、图片、音乐文件、文本文件、不具有内联代码的配置文件、视频以及图形。在一些情况下,还可以提供混合软件对象,例如比如具有内建宏的文字处理文档或具有内联代码的动画。为了安全目的,这些可以被考虑为单独的软件对象类,或者可以被简单地视为可运行对象。

[0037] 企业安全策略作为非限制性示例可以包含鉴证策略、网络使用策略、网络资源配置、防病毒策略和对在客户端装置110上的可运行对象的限制。各种网络服务器可以提供诸如路由选择、联网、企业数据服务和企业应用的实质性服务。

[0038] 安全企业100可以跨企业边界104与外部网络172通信。企业边界104可以表示物理、逻辑或其它边界。外部网络172可以包含例如网站、服务器、网络协议以及其它基于网络的服务。在一个示例中,应用存储库160经由外部网络172可用,并且攻击者180(或其它类似的恶意或疏忽的行为者)也连接到外部网络172。

[0039] 用户120和安全企业100的目标可能是成功地操作客户端装置110而不受攻击者180或不想要的安全对象的干扰。在一个示例中,攻击者180是恶意软件作者,其目标或目的是要引起恶意的伤害或损坏。恶意的伤害或损坏可能采取在客户端装置110上安装根包或其它恶意软件来篡改系统、安装间谍软件或广告软件来收集个人和商业数据、损伤网站、操作诸如垃圾邮件服务器的僵尸网络或简单地惹怒并骚扰用户120的形式。因此,攻击者180的一个目的可能是将其恶意软件安装在一个或多个客户端装置110上。如本说明书通篇所使用的,恶意软件(“malware”)包含配置成提供不想要的结果或做不想要的工作的任何安全对象。在许多情况下,恶意软件对象将是可运行对象,作为非限制性示例包含病毒、特洛伊木马、僵尸、根包、后门、蠕虫、间谍软件、广告软件、勒索软件、拨号器、有效载荷、恶意浏览器帮助对象、跟踪cookie、记录器或设计成采取潜在不想要的动作的类似的对象,所述不想要的动作作为非限制性示例包含数据销毁、隐蔽数据收集、浏览器劫持、网络代理或重定向、隐蔽跟踪、数据记录、键盘记录、要去除的过度或故意的障碍、接触收获以及未经授权的自我传播。

[0040] 攻击者180还可能想要针对受保护企业100进行工业或其它间谍活动,例如窃取机密数据或专用数据、窃取身份或获得对企业资源的未经授权的访问。因此,攻击者180的策略还可以包含尝试获得对一个或多个客户端装置110的物理访问并且在没有授权的情况下操作它们,使得有效的安全策略还可以包含用于防止这样的访问的供应。

[0041] 在另一示例中,软件开发人员可能不明确地具有恶意意图,但是可能开发造成安全风险的软件。例如,众所周知且经常被利用的安全缺陷是所谓的缓冲区溢出,其中恶意用户能够将使超长的字符串进入到输入形式中,并且因此获得运行任意指令的能力或者通过提升的特权在客户端装置110上操作。缓冲区溢出可能是例如不良输入确认或使用不安全库的结果,并且在许多情况下出现在非显而易见的上下文中。因此,虽然本身不是恶意的,但是向应用存储库160贡献软件的开发人员可能无意地为攻击者180提供攻击向量。不良编写的应用也可能引起固有的问题,例如崩溃、数据丢失或其它不期望的行为。因为此种软件本身可能是期望的,所以在ISV变得已知时,它们偶尔提供修复弱点的更新或补丁可能

是有益的。然而,从安全的角度来看,这些更新和补丁本质上是新的。

[0042] 应用存储库160可以表示Window或Apple“app商店”或更新服务、类Unix存储库或端口集合或为用户120提供在客户端装置110上交互或自动地下载和安装应用的能力的其它网络服务。如果应用存储库160具有使攻击者190难以公然分发恶意软件的在适当位置的安全措施,攻击者190可以转而隐秘地将弱点插入到明显有益的应用中。

[0043] 在一些情况下,受保护企业100可以提供限制能够从应用存储库160安装的应用的类型的策略指引。因此,应用存储库160可以包含不是疏忽开发并且不是恶意软件然而但违反策略的软件。例如,一些企业限制娱乐软件(像媒体播放器和游戏)的安装。因此,即使安全的媒体播放器或游戏也可能不适合于企业计算机。安全管理员150可以负责分发与此类限制一致的计算策略,并在客户端装置120上实施它。

[0044] 受保护企业100还可以与可以提供安全服务、更新、防病毒定义、补丁、产品以及服务的安全服务提供方190签约或对其进行订阅。McAfee ® , Inc. 是提供全面安全和防病毒解决方案的此种安全服务提供方的非限制性示例。

[0045] 各种计算装置还可以与可以是可信第三方的证书机构184进行互操作(intemperate)。证书机构184可发起用于对于对方进行签名的数字证书。例如,软件封装可以由对应于证明(certified)的公共密钥的私有密钥进行的签名或断言伴随。这可以用于验证ISV的身份,并验证二进制对象尚未被篡改。

[0046] 在另一示例中,受保护企业100可以简单地是家庭,其中父母承担安全管理员150的角色。父母可能希望保护他们的孩子免于不期望的内容,作为非限制性示例例如色情文艺、广告软件、间谍软件、年龄不适当的内容、对某些政治、宗教或社会运动的主张或讨论非法活动或危险活动的论坛。在这种情况下,父母可以执行安全管理员150的一些或全部职责。

[0047] 集体地,是或能够被指定为属于前述不期望的对象的类的任何的任何对象可以被分类为恶意对象。当在受保护企业100内遇到未知对象时,可以将其初始分类为“候选恶意对象”。此指定可以是要确保其不被授予完全的网络特权直到对象被进一步分析。因此,用户120和安全管理员150的目标是要配置和操作客户端装置110和企业网络170,以便排除所有恶意对象,并且对候选恶意对象进行迅速且准确地分类。

[0048] 使用TEE的一个目的是:候选恶意对象很难通过安全确认并被签名为可信二进制。因此,在TEE内运行的对象不需要被视为候选恶意对象,而在TEE之外遇到的对象可以通过默认被视为候选恶意对象,直到它们被确认或清除。

[0049] 图2是根据本说明书的一个或多个示例的客户端装置110的框图。客户端装置110可以是任何适合的计算装置。在各种实施例中,“计算装置”可以是或者作为非限制性示例包括:计算机、工作站、服务器、大型机、嵌入式计算机、嵌入式控制器、嵌入式传感器、个人数字助理、膝上型计算机、蜂窝电话、IP电话、智能电话、平板计算机、可转变平板计算机、计算器具、网络器具、接收器、可穿戴计算机、手持计算器或用于处理和传递数据的任何其它电子、微电子或微机电装置。

[0050] 客户端装置110包含连接到存储器220的处理器210,存储器具有存储在其中的用于提供操作系统222以及IVE 460和BTE 224的至少软件部分的可运行指令。客户端装置110的其它组件包含存储装置250、网络接口260以及外设接口240。此架构仅作为示例提供,并

且意图是非排它性和非限制性的。此外,所公开的各种部分仅意图是逻辑划分,并且不需要一定表示物理上分离的硬件和/或软件组件。某些计算装置例如在单个物理存储器装置中提供主存储器220和存储装置250,并且在其它情况下,存储器220和/或存储装置250跨许多物理装置功能地分布。在虚拟机或管理程序的情况下,可以可以在虚拟化层上运行的软件或固件的形式提供功能的全部或部分以提供公开的逻辑功能。在其它示例中,诸如网络接口260的装置可以仅提供执行其逻辑操作所必需的最少硬件接口,并且可以依靠软件驱动器来提供附加的必需逻辑。因此,本文公开的每个逻辑块宽泛地意图包含被配置且可操作用于提供那个块的公开的逻辑操作的一个或多个逻辑元件。如本说明书通篇所使用的,“逻辑元件”可以包含硬件、外部硬件(数字、模拟或混合信号)、软件、往复式软件、服务、驱动器、接口、组件、模块、算法、传感器、组件、固件、微代码、可编程逻辑或能够协调以实现逻辑操作的对象。

[0051] 在示例中,处理器210经由存储器总线270-3通信地耦合到存储器220,存储器总线270-3作为示例可以是例如直接存储器访问(DMA)总线,尽管其它存储器架构是可能的,包含其中存储器220经由系统总线270-1或某一其它总线与处理器210进行通信的架构。处理器210可以经由系统总线270-1通信地耦合到其它装置。如本说明书通篇所使用的,“总线”包含任何有线或无线互连线、网络、连接、捆(bundle)、单总线、多总线、交叉开关网络、单级网络、多级网络或可操作以携带计算装置的部分之间或计算装置之间的功率或数据、信号的其它传导媒介。应当注意,这些使用仅作为非限制性示例来公开,并且一些实施例可以省略前述总线中的一个或多个,而其它实施例可以采用附加或不同的总线。

[0052] 在一个示例中,在存储器220内定义飞地230以提供如本文所描述的TEE。在一个示例中,飞地230包含BTE 224和IVE 460。

[0053] 在各种示例中,“处理器”可以包含逻辑元件的任何组合,作为非限制性示例包含微处理器、数字信号处理器、现场可编程门阵列、图形处理单元、可编程逻辑阵列、专用集成电路或虚拟机处理器。在某些架构中,可以提供多核处理器,其中处理器210可以在适当的情况下被视为多核处理器的仅一个核,或者可以被视为整个多核处理器。在一些实施例中,还可以为专用或支持功能提供一个或多个协处理器。

[0054] 处理器210可以经由DMA总线270-3连接到DMA配置中的存储器220。为了简化本公开,存储器220被公开为单个逻辑块,但是在物理实施例中可以包含任何适合的一个或多个易失性或非易失性存储器技术的一个或多个块,包含例如DDR RAM、SRAM、DRAM、高速缓存、L1或L2存储器、片上存储器、寄存器、闪存、ROM、光媒体、虚拟存储器区域、磁性或磁带存储器或类似。在某些实施例中,存储器220可以包括相对低等待时间的易失性主存储器,而存储器250可以包括相对较高等待时间的非易失性存储器。然而,存储器220和存储装置250不需要是物理上分离的装置,并且在一些示例中可以简单地表示功能的逻辑分离。还应该注意的是,尽管作为非限制性示例公开了DMA,但是DMA不是与本说明书一致的唯一协议,并且其它存储器架构是可用的。

[0055] 存储装置250可以是任何种类存储器220,或者可以是单独装置。存储装置250可以包含一个或多个非暂时计算机可读媒介,作为非限制性示例包含,硬盘驱动、固态驱动、外部存储装置、独立磁盘冗余阵列(RAID)、网络附连存储装置、光存储装置、磁带驱动、备份系统、云存储装置或前述的任何组合。存储装置250可以是或可以包含以其它配置存储的数据

或一个或多个数据库在其中，并且可以包含操作软件的存储副本，例如操作系统222和安全引擎224的软件部分。许多其它配置也是可能的，并且意图涵盖在本说明书的宽泛范围内。

[0056] 可以提供网络接口260以将客户端装置110通信地耦合到有线或无线网络。如本说明书通篇使用的“网络”可以包含可操作以在计算装置内或之间交换数据或信息的任何通信平台，作为非限制性示例包含自组织本地网络、为计算装置提供电子交互能力的因特网架构、普通老式电话系统(POTS) (计算装置能够使用其执行事务(其中它们可能由人类操作员辅助，或者其中它们可以手动地将数据键入到电话或其它适合的电子装配中))、提供在系统中的任何两个节点之间的通信接口或交换的任何分组数据网络(PDN)或任何局域网(LAN)、城域网(MAN)、广域网(WAN)、无线局域网(WLAN)、虚拟专用网络(VPN)、内联网或促进网络或电话环境中的通信的任何其它适当的架构或系统。

[0057] 在一个示例中，BTE 224和IVE 460可操作以执行根据本说明书的计算机实现的方法。BTE 224和IVE 460可以包含一个或多个非暂时计算机可读媒介(具有存储在其上的可操作以指令处理器提供适合的功能的可运行指令)。如本说明书通篇所使用的，“引擎”包含可操作用于并且配置成执行由引擎提供的一个或多个方法的类似或不类似种类的一个或多个逻辑元件的任何组合。因此，安全引擎224可以包括配置成提供如本说明书中公开的安全引擎方法的一个或多个逻辑元件。在一些情况下，引擎可以包含被设计成执行方法或其一部分的特殊集成电路，并且还可以包含可操作以指令处理器执行该方法的软件指令。在一些情况下，引擎可以作为“守护程序”进程运行。“守护程序”可以包含任何程序或可运行指令系列(无论是以硬件、软件、固件或其任何组合实现的)，其运行作为后台进程、终止及常驻程序、服务、系统扩展、控制面板、启动规程、BIOS子例程或操作而无需直接的用户交互的任何类似的程序。在某些实施例中，守护程序进程可以在“驱动器空间”或在保护环架构中的环0、1或2中以提升的特权运行。还应当注意，引擎还可以作为非限制性示例包含其它硬件和软件，包含配置文件、注册项以及交互式或用户模式软件。

[0058] 在一个示例中，BTE 224和IVE 460包含存储在可操作以执行根据本说明书的方法的非暂时媒介上的可运行指令。在适当的时间，例如在引导客户端装置110时或者在来自操作系统222或用户120的命令时，处理器210可以从存储装置250检索适当引擎(或其软件部分)的副本并将其加载到存储器220中。处理器210然后可以迭代地运行引擎的指令以提供期望的方法。

[0059] 外设接口240可以配置成与连接到客户端装置110但不一定是客户端装置110的核心架构的一部分的任何辅助装置进行对接。外设可以可操作以向客户端装置110提供扩展的功能性，并且可以或可以不完全取决于客户端装置110。在一些情况下，外设就其本身而言可以是计算装置。外设作为非限制性示例可以包含诸如显示器、终端、打印机、键盘、鼠标、调制解调器、网络控制器、传感器、换能器、致动器、控制器、数据采集总线、相机、麦克风、扬声器或外部存储装置的输入和输出装置。

[0060] 图3是根据本说明书的一个或多个示例的服务器140的框图。服务器140可以是如结合图2所描述的任何适合的计算装置。通常，图2的定义和示例可以被考虑为同样可适用于图3，除非另外具体陈述。本文单独描述了服务器140以图示在某些实施例中，根据本说明书的逻辑操作可以沿客户端-服务器模型进行划分，其中客户端装置110提供某些局部任务，而服务器140提供某些其它的集中式任务。

[0061] 服务器140包含连接到存储器320的处理器310,存储器320具有存储在其上的用于提供操作系统322以及服务器引擎324的至少软件部分的可运行指令。服务器140的其它组件包含存储装置350、网络接口360和外设接口340。如图2中所描述的,每个逻辑块可以由一个或多个类似或不类似的逻辑元件提供。

[0062] 处理器310可以是任何适合的处理器。在某些实施例中,处理器310可以是包括多个核的服务器级处理器或处理阵列和/或多个处理器。在示例中,处理器310经由存储器总线370-3通信地耦合到存储器320,存储器总线370-3可以例如是直接存储器访问(DMA)总线。处理器310可以经由系统总线370-1通信地耦合到其它装置。

[0063] 处理器310可以在DMA配置中经由DMA总线370-3或经由任何其它适合的存储器配置连接到存储器320。如图2中所讨论的,存储器320可以包含任何适合类型的一个或多个逻辑元件。

[0064] 存储装置350可以是任何种类的存储器320,或者可以是如结合图2的存储装置250所描述的单独的装置。存储装置350可以是或可以包含在其它配置中存储的数据或一个或多个数据库在其中,并且可以包含操作软件(例如操作系统322和服务器引擎324的软件部分)的存储的副本。

[0065] 可以提供网络接口360以将服务器140通信地耦合到有线或无线网络,并且可以包含如图2所描述的一个或多个逻辑元件。

[0066] 服务器引擎324是如图2中所描述的引擎,并且在一个示例中,包含可操作以执行计算机实现的方法(包含为受保护企业100提供安全功能)的一个或多个逻辑元件。这可以包含二进制的初始审查和确认,其可以被签名并作为可信二进制提供到客户端装置110。服务器引擎324的软件部分可以作为守护程序进程运行。

[0067] 服务器引擎324可以包含一个或多个非暂时计算机可读媒介,其具有在其上存储的可操作以指令处理器提供安全引擎的可运行指令。在适当的时间,例如在引导服务器140时或者在来自操作系统222或用户120或安全管理员150的命令时,处理器310可以从存储装置350检索服务器引擎324(或其软件部分)的副本并将其加载到存储器320中。处理器310然后可以迭代地运行服务器引擎324的指令以提供期望的方法。

[0068] 外设接口340可以配置成与连接到服务器140但不一定是服务器140的核心架构的一部分的任何辅助装置进行对接。外设可以可操作以将扩展的功能性提供到服务器140,并且可以或者可以不完全取决于服务器140。外设作为非限制性示例可以包含图2中公开的任何外设。

[0069] 图4A是本说明书的所选元件的功能框图。

[0070] 总之,可以对供应有ISV的公共密钥的TEE内的客户端装置110执行诸如编译、解释或转换的二进制转换。TEE可以然后使用公共密钥或具有相同出处的密钥来对所产生的推导的代码进行签名。

[0071] 因此,提供了通过TEE中的代码签名和验证以及通过诸如远程认证的确认机制来保证软件完整性的可信通道。

[0072] 这可以通过三阶段(phase)方法来完成,其中第二阶段桥接第一和第三阶段,如下所述:

ISV或开发人员将代码编译并签名成递送到客户端装置110的中间表示(可信二进制对

象420)。

[0073] 在客户端装置110上,供应了飞地230来执行本说明书的方法。在飞地230内,验证ISV的签名。可信二进制对象420然后由BTE 224编译、转换或以其它方式修改,以产生处于第二格式的第二对象。取决于ISV对于传播签名的信任链的偏好,可以获得在可信二进制对象420中指定的密钥,按需安全供应的密钥或新的本地生成的密钥。TEE用此第二密钥来对第二对象进行签名。

[0074] TEE通过在运行签名之前验证签名来验证推导的代码的完整性。

[0075] 用于在上面阶段2中对第二二进制进行签名的选项可以包含以下:

当ISV处于第一密钥编译代码并对代码进行签名时,它可以捆绑或包含要用来对第二对象进行签名的第二密钥。由于可信二进制对象420的密钥是可信且验证的,所以第二密钥也可以是可信的。

[0076] ISV可以供应第二签名密钥到飞地230。在此实现中可能存在变化。飞地230能够周期性地查询例如安全服务提供方190或企业安全控制器140以拉入用于各种ISV的第二密钥并将它们本地存储(使用SGX的安全存储能力或类似技术)。它能够备选地查找ISV的密钥(其代码/二进制将被它处理)。它能够在已将其组装的中央服务器处进行此查找,或者它能够直接在预定位置处查找ISV服务。

[0077] 可以本地生成新的密钥对,特别是为了对推导的代码进行签名的目的。飞地 230可以将新的密钥对上传到服务(诸如证书机构184的中央服务或由ISV操作的中央服务),如果它想要实现远程签名验证的话。否则,它能够更新其本地签名数据库以提供验证。

[0078] 无论何时存在与中央服务或ISV自身拥有服务的任何通信,上面前两个示例使用飞地的远程认证能力。它们还可以使用飞地的本地认证能力以用于本地跨飞地的通信,例如当将本地生成的密钥添加到飞地230的本地密钥存储时。

[0079] 还可以提供有自动刷新签名密钥或通知证书机构184来刷新密钥的撤销路径或密钥旋转进程。例如,BTE 224可以在对二进制进行签名之前咨询撤销或过期列表。

[0080] 在某些实施例中,上面的阶段2能够在继续到阶段3之前采用工具/技术方面的变化重复一次或多次。最简单的情况是单个密钥用于阶段2的所有迭代。备选地,装置特定、工具特定或应用特定密钥可以传播向下,或者可以通过对证书机构184或ISV验证服务的证书签名请求来生成和上传新的密钥对。

[0081] 这也可以延伸回源控制,使得信任链能够从特定的签名版本(versioning)系统标记(例如Git标记)一路向下延伸到平台特定的动态签名的二进制。在每个转换层处,新签名的二进制可以包含进行转换的实体(例如,飞地230的BTE 224)的认证,使得可以验证涉及在生成可信二进制对象420中的代码的起源和工具链实体。

[0082] 在一个示例中,应用存储库160和/或证书机构184可以提供可信二进制对象420。例如,ISV可以经由应用存储库160提供应用,并且应用可以由证书机构184签名和验证。应用存储库160然后将可信二进制对象420提供给客户端装置110。

[0083] 提供可信二进制对象420到飞地230。可以在任何适合的客户端装置110中或在某些实施例中在企业安全控制器140中提供飞地230。还应当注意,飞地230仅是如本文描述的TEE的一部分。

[0084] 在一个示例中,飞地230包含接口定义(ID)和应用编程接口(API)层410。ID和API

层410可以提供用于通信地耦合到外设242的适当接口。

[0085] 飞地230还包含BTE 224和IVE 460。在此示例中，IVE 460通信地耦合到BTE 224，使得BTE 224能够从外设242接收签名和确认的输入。飞地230还可以包含清单(manifest)470、证书450(其可以包含用来对可信二进制对象420进行签名的公共密钥)和私有密钥452。

[0086] 在某些实施例中，代码确认对加载到TEE中的代码执行完整性检查。清单470可以是描述可接受代码的白名单或描述不可接受代码的黑名单。该清单可以由信任域(例如企业IT部门或原始装配制造商)使用由该域供应的密钥进行签名。

[0087] 当TEE在引导时间、TEE软件/固件更新时间初始化时或当将新的代码对象添加到TEE或从TEE中去除时，可以应用清单和代码确认操作。在某一示例中，“可信引导”和“安全引导”是指上面初始化步骤的至少一些的行业术语。

[0088] 在一个示例中，二进制转换引擎是加载到TEE中的映射的一部分，并且因此经受可以检测对BTE和IVE组件的攻击的可信引导策略。

[0089] 应当注意，在一些情况下，特别是在IoT、传感器、致动器或可穿戴装置上下文中，整个装置在安全引导操作之后可被考虑是TEE。

[0090] 将可信二进制对象420从第一格式转换成第二格式可能是必需的。例如，可信二进制对象420可以是Java字节代码，其需要通过提前编译器编译成本机二进制格式。在另一示例中，可信二进制对象420可以是将由即时编译器编译的Java字节代码程序。在还有其它示例中，BTE作为非限制性示例可以是运行时间引擎、解释器、即时编译器、提前编译器、虚拟机(例如Java虚拟机(JVM))、编译器、链接器和工具链实用程序中的任何。BTE 224的一个目的可以是提供用于在飞地230内实时使用的二进制对象，以存储在例如图2的存储器装置250上，或提供到另一计算装置。

[0091] 在一个示例中，BTE 224接收可信二进制对象420以及来自IVE 460的任何必需输入，并且产生签名的本机二进制430。签名的本机二进制430可以由私有密钥452签名，私有密钥452可以具有与用来对可信二进制对象420进行签名的密钥相同的出处。在另一示例中，私有密钥452可以是用来对可信二进制对象420进行签名的相同的密钥。只有可信二进制对象420携带密钥本身与其一起，这才是可能的。

[0092] 因为BTE 224也是在飞地230内运行的签名和可信二进制，并且由于可信二进制对象420也是签名和验证的对象，因此假设签名的本机二进制430也能够被视为二进制是合理的。因此，签名的本机二进制430可以被视为类似于可信二进制对象420的可信二进制对象。因此，签名的本机二进制430可以在飞地230内使用，或者可以被提供到具有TEE能力的某一其它计算装置。

[0093] 也可以产生未签名的本机二进制440，并且可以包含与签名的本机二进制430完全相同的二进制对象。然而，未签名的本机二进制440不由私有密钥452签名。未签名的本机二进制440可以提供到不具有TEE功能的计算装置。例如，在IoT上下文中，未签名的本机二进制440可以被提供到可能不具有TEE能力的具因特网能力的装置或传感器。然而，在一些情况下，IoT装置可能具有安全的引导能力，使得整个装置能够被视为TEE。在其它示例中，不具有TEE能力的IoT装置可以被放置在具有TEE能力的网关之后，其可以验证签名的本机二进制430、剥离(strip out)其TEE属性并将未签名的本机二进制440提供到IoT装置。许多其

它的可能性也可是可用的。

[0094] 图4B是本说明书的所选元件的第二功能框图。在图4B的示例中,再次提供具有与图4A的飞地230相同的元件的飞地230。然而,在此情况下,可信二进制对象420不直接提供到BTE 224。相反,可信二进制对象420被提供到IVE 460,IVE 460将可信二进制对象420视为类似于来自其它源的输入的输入。IVE 460然后可以分析可信二进制对象420并标记适当的部分供在飞地230内的运行,如图6中更详细地描述的。然后,IVE 460可以将确认的输入分组提供到BTE 224。BTE 224然后可以执行其二进制转换功能(包含指定标记部分供在飞地230内的运行),并且提供签名的本机二进制430以及未签名的本机二进制440中的一个或两者。

[0095] 图5是本说明书的所选元件的功能框图。在此情况下,第一计算装置包含飞地230-1,而第二计算装置包含飞地230-2。在此示例中,飞地230-1首先接收可信二进制对象420。飞地230-1可以配置为如图4A所示、在图4A中或者任何其它适合的配置中所示的。如先前的,BTE 224生成签名的本机二进制430。这在一个示例中可以通过提供有证书450的公共密钥签名。

[0096] 飞地230-1可以经由网络170将签名的本机二进制430提供到飞地230-2。在此示例中,在其它装置500上提供飞地230-2。

[0097] 其它装置500可能希望使用签名的本机二进制430,并且因此可以参与与飞地230-1的远程认证520。通过远程认证520,其它装置500可以验证证书450是由飞地230-1生成或提供的有效证书。因此,其它装置500然后可以将签名的本机二进制430视为可信二进制,并且特别地,签名的本机二进制430可以变成其它装置500的可信二进制对象420。

[0098] 图6是本说明书的所选元件的功能框图。图6描述了具有更多特殊性的IVE 460。

[0099] 总之,TEE可以提供API以允许用户空间应用与飞地230交互。例如,英特尔® SGX软件开发工具包(SDK)提供C/C++ API来实例化飞地230并在飞地230内提供本机C/C++软件。

[0100] Android应用可能需要访问敏感数据并执行输入确认,例如验证通过用户使有效字符进入像出生日期、电子邮件地址、电话或社会安全号码的字段。输入确认可能要求与适当配置的服务器(例如企业安全控制器140)进行通信,从而潜在地将敏感数据暴露于恶意眼睛或实例化飞地230,从而要求ISV在输入确认方面熟练。

[0101] 然而,Android应用通常以Java代码编写。因此,为了采用SGX保护Android应用的部分,ISV可以以C/C++重新实现应用的被保护的部分、将其包装在Java本机接口(JNI)包装器中,并从Android应用调用JNI接口。

[0102] 在一个示例中,不同的ISV(例如安全服务提供方190)可以提供多个预构建的本机C/C++输入验证模块作为IVE 460的部分。这些可以构建成利用飞地230并在TEE内操作以提供可信输入验证。

[0103] 因此,Android ISV例如可以能够使用输入验证模块作为构建块来构建app以执行普通任务,例如使用受保护网络栈与web服务器进行通信、使用安全图形引擎将数据输出到屏幕以及使用受保护的触摸屏输入引擎从用户接收输入。

[0104] 当敏感数据离开飞地230的被保护的边界时,它们可以被加密。因此,这些安全数据将不会以简单的形式暴露于其它应用之外。这允许Android app在潜在的恶意环境(包含

许多候选恶意对象)中运行,而不会对敏感数据造成风险。

[0105] 在另一示例中,本说明书的IVE 460可以允许Android ISV例如指定其应用代码的一部分来访问来自被保护输入(例如触摸屏)的敏感数据,并且确认输入而不损害数据。在一个示例中,IVE 460可以在使用JVM运行Java代码的自动生成的飞地230中运行。因此,ISV可以使用他用来创建Android应用本身的相同工具和语言对敏感数据执行输入确认。

[0106] 在另一示例中,IVE 420可以分析诸如可信二进制对象420或另一二进制对象的二进制对象,并且注释接收敏感数据的变量。然后,IVE 420可以跟踪访问那些变量的所有代码,并要求那个代码在飞地230内运行。这可以包含“伪编译”,以确保标示(mark)的Java代码不执行在飞地230内不允许的任何禁止的调用或操作,例如访问文件系统或执行系统调用。任何此种尝试可能采用错误代码标记,其能够被提供到ISV,使得他能够解决问题。

[0107] ISV还可以采用特殊标记来标示应用源代码,包含访问敏感数据的特定类、功能或变量。然后,ISV 460可以自动地标示所有相关代码,并且在飞地230内的JVM 680内部运行那个Java代码。然后可以将相关的输入作为签名的验证输入630无缝地传递到Java应用610。

[0108] 因此,ISV可以能够使用他用来开发Android app本身的相同工具来定义Android应用的哪些部分应该访问敏感数据并且因此在飞地内部运行,并且被保护的代码可能仍然是Java代码。这允许ISV使用Java代码来实现其自己的输入数据确认功能性,而没有它们可能不熟悉并且实质上为它们提供更多的用来吊死它们自己的绳索的C/C++的陷阱。

[0109] 在一个示例中,IVE 460包含自动生成包含JVM 680的飞地230的预编译器。在一个示例中,这可以是被限定或修整的JVM,其仅提供处理和验证输入的基本功能性。注释的Java代码可以生成JNI包装器、参数转变器和其它工具来实现飞地调用和回调。

[0110] 在一个示例中,飞地230可以经由ID/API层410从外设242接收某些用户或网络输入640。然后可以将那些输入提供到IVE 460。在此示例中,IVE 460还接收可信二进制对象420。在一个示例中,IVE 460可以参与认证交换(例如图5的远程认证520)以确认可信二进制对象420。然后,IVE 460可以“伪编译”可信二进制对象420并将适当的标记插入到执行受保护输入操作的类、函数或变量。因此,当BTE 224创建新的二进制时,只有新二进制的一部分可配置成在飞地230内运行。

[0111] 在此示例中,还提供了Java应用610。Java应用610可配置成对敏感数据进行操作,或者可以以其它方式是安全关键的。因此,确认Java应用610的输入是期望的。

[0112] 为Java应用610的ISV提供可能支持若干确认方法的IVE 460可能是有利的。这允许Java应用610通过提供在飞地230的JVM 680中运行的定制Java例程,或者通过使用由IVE 460提供的若干预构建的C/C++输入确认工具中的一个来执行输入确认。

[0113] JNI包装器620是使Java应用610能够与IVE 460中提供的方法对接的标准Java包装器。还应当注意,仅作为非限制示例提供JNI包装器620、Java应用610、JVM 680以及其它Java特定元件。在更一般的意义上,JNI包装器620可以是使处于第一编程语言的代码能够与来自第二编程语言的代码进行互操作的任何适合的包装器或接口。JVM 680可以是任何适合的解释器引擎,例如虚拟机、脚本解释器、脚本引擎、转换器或类似。

[0114] 在一个示例中,IVE 460从外设242接收用户或网络输入640。IVE 460还可以接收可信二进制对象420并且适当地标记可信二进制对象420。

[0115] IVE 460然后可以提供签名和验证的输入630供与Java应用610一起使用。JNI包装器620使Java应用610能够从IVE 460接收签名的验证的输入630。然后,Java应用610可以以输入是有效的而不是恶意的信心对签名并验证的输入630起作用。

[0116] 图7是IVE 260的功能框图。在图7的示例中,作为非限制性示例示出了某些功能块。IVE 260可以具有零个或多个所示的块,并且可以具有零个或多个附加块以提供其它功能。

[0117] 在此示例中,IVE 260提供安全网络栈710、安全图形引擎720、安全人性化输入装置(HID)接口引擎730、安全音频引擎740、安全图像处理引擎750、安全遥测引擎760、安全GPS接收器770以及二进制输入分析器780。

[0118] 在一个示例中,安全网络栈710可以在多个不同通道上提供安全通信。通信可以通过IP网络、电话网络、Wi-Fi网络、蓝牙网络、本地有线或无线网络或任何其它适合的网络。在一个示例中,安全网络栈710可以提供例如通过HTTPS的加密通信。安全网络栈710还可以执行对通过网络发送或从网络接收的分组的确认。

[0119] 安全图形引擎720可以将输出安全地驱动到屏幕或其它显示装置。

[0120] 安全HID接口引擎730可以处置和确认人性化输入。这可以包含例如智能装置、混合平板电脑或其它触摸屏使能装置上的触摸屏输入。这也可能包含输入形式的确认和验证。例如,安全HID接口引擎730可以确保输入字符串不会过长、它们处于正确的格式以及它们由应用610可使用。

[0121] 安全音频引擎740可以安全地处置与扬声器和/或麦克风的通信。这可以使应用610既能够从用户接收音频输入,并且能够在扬声器上提供音频输出。

[0122] 安全图像处理引擎750可以处置例如从客户端装置110上的内建相机接收的输入。

[0123] 可以提供安全遥测引擎760以与装置上的各种传感器和致动器对接。例如,遥测装置可以包含加速度计、温度计、罗盘或其它环境传感器。在其中计算装置110是IoT装置的情况下,提供遥测到安全遥测引擎760的传感器实际上可以是装置的主要目的。在此上下文下,遥测装置能够是提供环境测量的任何类型的装置。

[0124] 安全GPS接收器770可以提供与GPS卫星的安全通信,并且可以接收装置的全球定位坐标。

[0125] 最后,二进制输入分析器780可以接收和确认二进制对象,例如可信二进制对象420或其它二进制对象。对象的确认可以包含验证其具有良好的签名和/或验证发布者的身份。二进制输入分析器780还可以通过对对其进行伪编译并识别处置安全输入的函数、类或变量并标记它们用于在飞地230内运行来对二进制对象进行分析(analyzer)。

[0126] 这些功能块中的任何可以以加密形式将签名和验证的输入630提供到Java应用610。

[0127] 图8是根据本说明书的一个或多个示例的由BTE 224执行的方法800的流程图。

[0128] 在框810中,飞地230接收处于第一形式的要被转换成处于第二形式的第二二进制对象的可信二进制对象。

[0129] 在框820中,可信二进制对象被传递到BTE 224。

[0130] 在框830中,BTE 224将可信二进制对象转换成处于第二形式的第二二进制对象。

[0131] 在框850中,BTE 224例如采用用其与对原始可信二进制进行签名的相同的密钥或

采用具有与那个密钥相同出处的密钥来对新的第二二进制对象进行签名。

[0132] 在框870中,在适当或必需的情况下,BTE 224可以将新的签名的本机二进制430导出离开飞地230。

[0133] 在框890中,完成该方法。

[0134] 图9是根据本说明书的一个或多个示例的由IVE 460执行的方法900的流程图。

[0135] 在框910中,IVE 460接收未确认的输入。

[0136] 在框920中,IVE 460的适当的功能块可以验证和确认新的输入。

[0137] 在框930中,适当的功能块可以生成确认的输入分组。

[0138] 在框950中,IVE 460加密确认的输入分组。

[0139] 在框970中,IVE 460对确认的输入分组进行签名。

[0140] 在框980中,IVE 460可以将签名且确认的输入分组例如导出到JNI包装器620。

[0141] 在框990中,完成该方法。

[0142] 图10是根据本说明书的一个或多个示例的IVE 460和BTE 224之间的交互方法的框图。

[0143] 在框1010中,IVE 460接收诸如可信二进制对象420的二进制对象。

[0144] 在框1020中,IVE 460可以伪编译二进制对象以识别访问被保护的输入和输出的函数、类和/或变量。

[0145] 在框1030中,IVE 460标记用于在飞地230内运行的那些函数、类和/或变量。

[0146] 在判定块1040中,IVE 460确定在二进制的标记部分内是否存在受限的操作。例如,这可以包含尝试向文件系统写或从文件系统读,或者执行从飞地230内受限的另一操作。

[0147] 在框1050中,如果发现受限的操作,则可以通知ISV关于错误。返回到框1040,如果不存在受限的操作,则在框1070中,IVE 460可以将新标记的二进制传递给BTE 224用于二进制转换。

[0148] 在框1080中,BTE 224根据本说明书中描述的方法转换二进制。

[0149] 前述概述了若干实施例的特征,使得本领域技术人员可以更好地理解本公开的方面。本领域技术人员应当意识到,他们可以容易地将本公开用作用于设计或修改用于执行本文介绍的实施例的相同目的和/或实现本文介绍的实施例的相同优点的其它过程和结构的基础。本领域技术人员还应该认识到,此类等效的结构不脱离本公开的精神和范围,并且在不脱离本公开的精神和范围的情况下,它们可以进行各种改变、替换和变更。

[0150] 本公开的具体实施例可以容易地包含片上系统(SOC)中央处理单元(CPU)封装。SOC表示将计算机或其它电子系统的组件集成到单个芯片中的集成电路(IC)。它可以包含数字、模拟、混合信号和射频功能:所有这些功能可以在单个芯片衬底上提供。其它实施例可以包含多芯片模块(MCM),其中多个芯片位于单个电子封装内并且配置成通过电子封装彼此紧密地交互。在各种其它实施例中,数字信号处理功能性可以在专用集成电路(ASIC)、现场可编程门阵列(FPGA)和其它半导体芯片中的一个或多个硅核中实现。

[0151] 另外,与所描述的微处理器关联的一些组件可以被去除或以其它方式巩固。在一般意义上,附图中所描绘的布置在其表示中可能是更逻辑的,而物理架构可以包含这些元件的各种排列、组合和/或混合。注意无数可能的设计配置能够用来实现本文概述的操作目

标是必要的。因此,关联的基础设施具有无数的替代布置、设计选择、装置可能性、硬件配置、软件实现、装配选项等。

[0152] 任何适合配置的处理器组件能够运行与数据关联的任何类型的指令以实现本文详述的操作。本文公开的任何处理器能够将元件或物品(例如,数据)从一个状态或事物变换到另一状态或事物。在另一示例中,本文中概述的一些活动可以采用固定逻辑或可编程逻辑(例如,由处理器运行的软件和/或计算机指令)来实现,并且本文标识的元件能够是某一类型的可编程处理器、可编程数字逻辑(例如,现场可编程门阵列(FPGA)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)、包含数字逻辑的ASIC、软件、代码、电子指令、闪速存储器、光盘、CD-ROM、DVD ROM、磁或光卡、适合于存储电子指令的其它类型的机器可读媒介,或其任何适合的组合。在操作中,处理器可以在适当的情况下且基于具体需要将信息存储在任何适合类型的非暂时存储媒介(例如,随机存取存储器(RAM)、只读存储器(ROM)、现场可编程门阵列(FPGA)、可擦除可编程只读存储器(EPROM)、电可擦除可编程ROM(EEPROM)等)、软件、硬件中或在任何其它适合的组件、装置、元件或对象中。此外,能够基于具体的需要和实现,在任何数据库、寄存器、表、高速缓存、队列、控制列表或存储结构中提供在处理器中被跟踪、发送、接收或存储信息,所有这些能够在任何适合的时帧中引用。本文讨论的任何存储器项都应被解释为涵盖在宽泛术语“存储器”内。

[0153] 实现本文描述的全部或部分功能性的计算机程序逻辑以各种形式体现,包含但不限于源代码形式、计算机可运行形式和各种中间形式(例如,通过汇编器、编译器、链接器或定位器生成的形式)。在示例中,源代码包含以各种编程语言(例如目标代码、汇编语言或诸如OpenCL、Fortran、C、C++、JAVA或HTML的高级语言)实现的一系列计算机程序指令,供与各种操作系统或操作环境一起使用。源代码可以定义和使用各种数据结构和通信消息。源代码可以处于计算机可运行形式(例如,经由解释器),或者可以将源代码转变(例如,经由转换器、汇编器或编译器)成计算机可运行形式。

[0154] 在一个示例实施例中,图的任何数量的电气电路可以在关联的电子装置的板上实现。该板能够是能够保持电子装置的内部电子系统的各种组件并且另外为其它外设提供连接器的通用电路板。更具体地,板能够提供电连接,通过该电连接系统的其它组件能够电气地通信。基于具体配置需要、处理需求、计算机设计等,任何适合的处理器(包含数字信号处理器、微处理器、支持芯片组等)、存储器元件等都能够适合地耦合到板上。诸如外部存储装置、附加传感器、用于音频/视频显示的控制器以及外设装置的其它组件可以作为插件卡经由线缆附连到板上,或者被集成到板本身中。在另一示例实施例中,附图的电气电路可以被实现为独立模块(例如,具有配置成执行特定应用或功能的关联的组件和电路的装置)或被实现为到电子装置的应用特定硬件的插件模块。

[0155] 注意,通过本文提供的许多示例,交互可以在两个、三个、四个或更多个电气组件方面来描述。然而,这仅仅是为了清楚和示例的目的而进行的。应当意识到,能够以任何适合的方式来巩固该系统。沿着类似的设计备选方案,附图的所图示的组件、模块和元件中的任何可以以各种可能的配置组合,所有这些配置都明确地在本说明书的宽泛范围内。在某些情况下,仅通过引用有限数量的电气元件来描述给定组流程的一个或多个功能可能性可能更容易。应当意识到,附图的电气电路及其教导是容易地可扩展的并且能够容纳大量组件以及更复杂/繁杂的布置和配置。因此,所提供的示例不应该限定电气电路的范围或禁止

电气电路的宽泛教导,如潜在地应用于无数其它架构的。

[0156] 许多其它改变、替代、变化、变更和修改对本领域技术人员可以是确定的,并且意图是本公开涵盖如落在所附权利要求的范围内的所有此类改变、替代、变化、变更和修改。为协助美国专利和商标局(USPTO)并且,另外在本申请上发表的任何专利的任何读者解释所附于此的权利要求时,申请人希望注意到的是:申请人:(a)不使所附权利要求中的任何意图调取35 U.S.C.章节112的段落6(6),因为它在其提交的日期存在,除非在特定权利要求中具体使用“用于…的部件”或“用于…的步骤”的词语);以及(b)并不意图通过说明书中的任何声明以在所附权利要求中没有以其它方式反映的任何方法来限定本公开。

[0157] **示例实现**

在示例1中公开有一种计算设备,其包括:可信运行环境(TEE);一个或多个逻辑元件,所述一个或多个逻辑元件包括TEE内的输入验证引擎(IVE),该IVE可操作用于:接收可信二进制对象;分析可信二进制对象以识别执行输入/输出操作的部分;标记所述部分以创建具有标记部分的标记的可信二进制;并将所述部分提供到二进制转换引擎;以及一个或多个逻辑元件,所述一个或多个逻辑元件包括所述TEE内的二进制转换引擎(BTE),所述BTE可操作用于:接收处于第一格式的所述标记的可信二进制;将所述标记的可信二进制转换成处于第二格式的第二二进制对象,其中转换包括保留所述标记的部分以供在飞地内的运行。

[0158] 在示例2中公开有示例1的计算设备,其中所述IVE还可操作用于:在TEE内供应飞地;以及在飞地内执行其功能的至少一些。

[0159] 在示例3中公开有示例2的计算设备,其中所述IVE还可操作用于在飞地内供应所述BTE。

[0160] 在示例4中公开有示例3的计算设备,其中所述BTE包括二进制转换器,其从由运行时间引擎、解释器、即时编译器、提前编译器、虚拟机、编译器、链接器和工具链实用程序组成的组中选择。

[0161] 在示例5中公开有示例3的计算设备,其中所述BTE包括Java虚拟机,并且其中所述IVE至少部分地以Java实现并且配置成在所述BTE内操作。

[0162] 在示例6中公开有示例1的计算设备,其中所述IVE还可操作用于执行输入验证。

[0163] 在示例7中公开有示例6的计算设备,其中所述IVE包括从由安全网络栈、安全图形引擎、安全人性化输入装置接口引擎、安全音频引擎、安全图像处理引擎、安全遥测引擎、安全全球定位系统接收器和二进制输入分析器组成的组中选择的模块。

[0164] 在示例8中公开有示例1-7中任一项的计算设备,其中所述BTE还可操作用于对所述第二二进制对象进行签名。

[0165] 在示例9中公开有示例8的计算设备,其中第一签名的对象要由密钥签名,并且其中对第二对象进行签名包括采用密钥对第二对象进行签名。

[0166] 在示例10中公开有示例8的计算设备,其中第一签名的对象要采用第一密钥签名,并且其中对第二对象进行签名包括采用由第一密钥的共同发起者签名的第二密钥对第二对象进行签名。

[0167] 在示例11中公开有示例8的计算设备,其中第一签名的对象要采用第一密钥签名,并且其中对第二对象进行签名包括采用由第一对象的供应商提供的第二密钥对第二对象进行签名。

[0168] 在示例12中公开有示例8的计算设备,其中第一签名的对象要采用第一密钥签名,并且其中对第二对象进行签名包括采用由第一密钥签名的第二密钥来对第二对象进行签名。

[0169] 在示例13中公开有示例8的计算设备,其中所述二进制转换引擎还可操作用于在对第二对象进行签名之前咨询证书过期或撤销列表。

[0170] 在实施例14中公开有一个或多个计算机可读媒介,在其上存储有指令,所述指令在被运行时指令处理器用于:在TEE内提供输入验证引擎(IVE),所述IVE可操作用于:接收可信二进制对象;分析所述可信二进制对象以识别执行输入/输出操作的部分;标记所述部分以创建具有标记部分的标记的可信二进制;以及将所述部分提供到二进制转换引擎;以及在所述TEE内提供所述二进制转换引擎(BTE),所述BTE可操作用于:接收处于第一格式的所述标记的可信二进制;将所述标记的可信二进制文件转换成处于第二格式的第二二进制对象,其中转换包括保留所述标记的部分以供在飞地内的执行。

[0171] 在示例15中公开有示例14的一个或多个计算机可读媒介,其中所述IVE还可操作用于:在所述TEE内供应飞地;以及在所述飞地内执行其功能的至少一些。

[0172] 在示例16中公开有示例15的一个或多个计算机可读媒介,其中所述IVE还可操作用于在所述飞地内供应所述BTE。

[0173] 在示例17中公开有示例16的一个或多个计算机可读媒介,其中所述BTE包括Java虚拟机,并且其中所述IVE至少部分地以Java实现并且配置成在所述BTE内操作。

[0174] 在示例18中公开有示例14的一个或多个计算机可读媒介,其中所述IVE还可操作用于执行输入验证。

[0175] 在示例19中公开有示例14-18中任一项的一个或多个计算机可读媒介,其中所述BTE还可操作用于对第二二进制对象进行签名。

[0176] 在示例20中公开有示例19的一个或多个计算机可读媒介,其中所述第一签名的对象要由密钥签名,并且其中对所述第二对象进行签名包括采用所述密钥对所述第二对象进行签名。

[0177] 在示例21中公开有示例19的一个或多个计算机可读媒介,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由第一密钥的共同发起者签名的第二密钥对所述第二对象进行签名。

[0178] 在示例22中公开有示例19中任一个的一个或多个计算机可读媒介,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一对象的供应商提供的第二密钥对所述第二对象进行签名。

[0179] 在示例23中公开有示例19的一个或多个计算机可读媒介,其中第一签名的对象要采用第一密钥签名,并且其中对所述第二对象进行签名包括采用由所述第一密钥签名的第二密钥对所述第二对象进行签名。

[0180] 在示例24中公开有一种用于在可信运行环境(TEE)内的运行的计算机实现的方法,包括:接收可信二进制对象;分析所述可信二进制对象以识别执行输入/输出操作的部分;标记所述部分以创建具有标记部分的标记的可信二进制;以及将所述标记的可信二进制转换成处于第二格式的第二二进制对象,其中转换包括保留所述标记的部分以供在飞地内的执行。

- [0181] 在示例25中公开有示例24的方法,还包括对所述第二二进制对象进行签名。
- [0182] 在示例26中公开有一种方法,其包括执行示例14-23中任一项中公开的指令。
- [0183] 在示例27中公开有一种设备,其包括用于执行示例26的方法的部件。
- [0184] 在示例28中公开有权利要求27的设备,其中所述设备包括处理器和存储器。
- [0185] 在示例29中公开有权利要求28的设备,其中所述设备还包括计算机可读媒介,在其上存储有用于执行示例26的方法的软件指令。

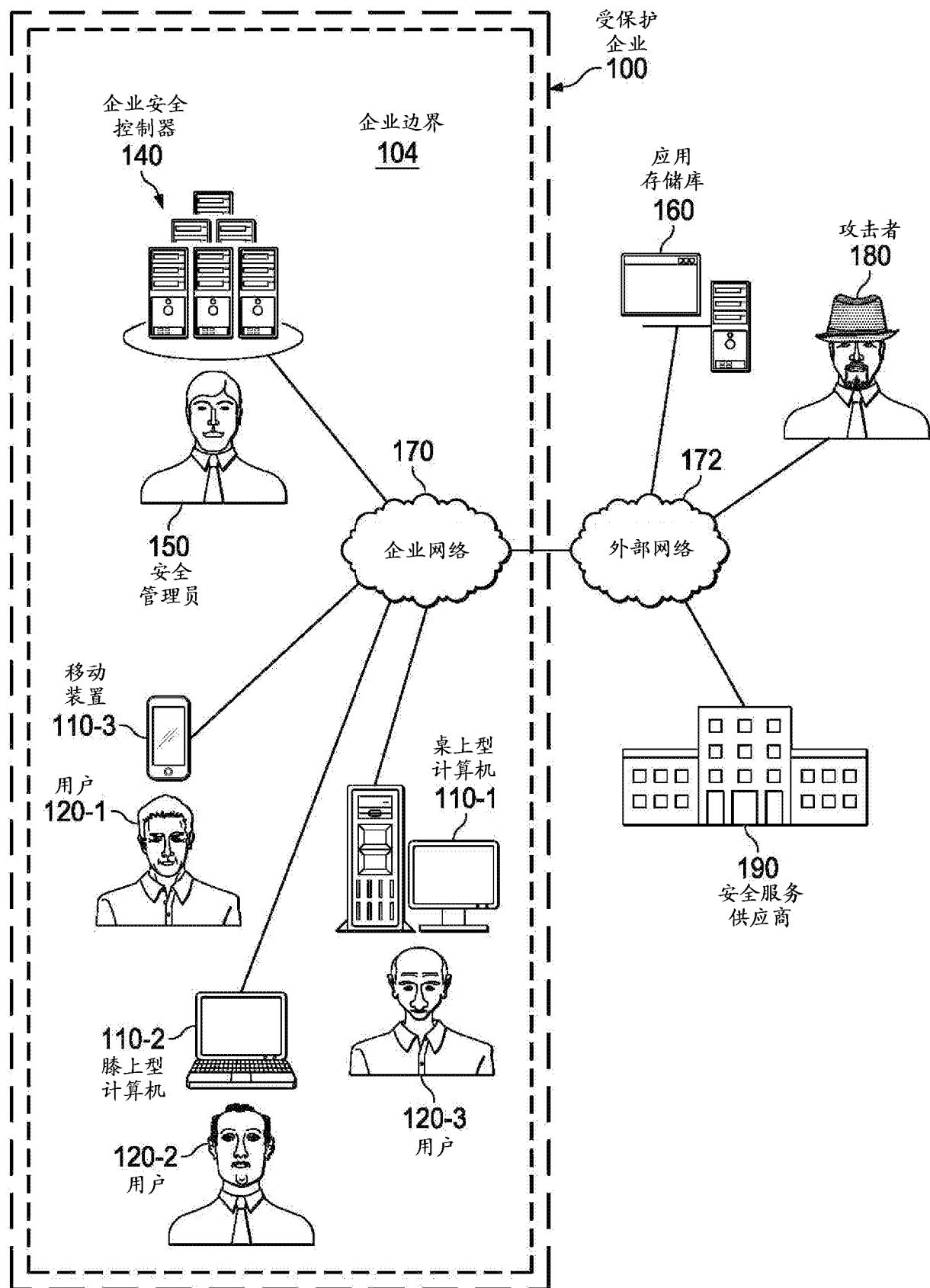


图 1

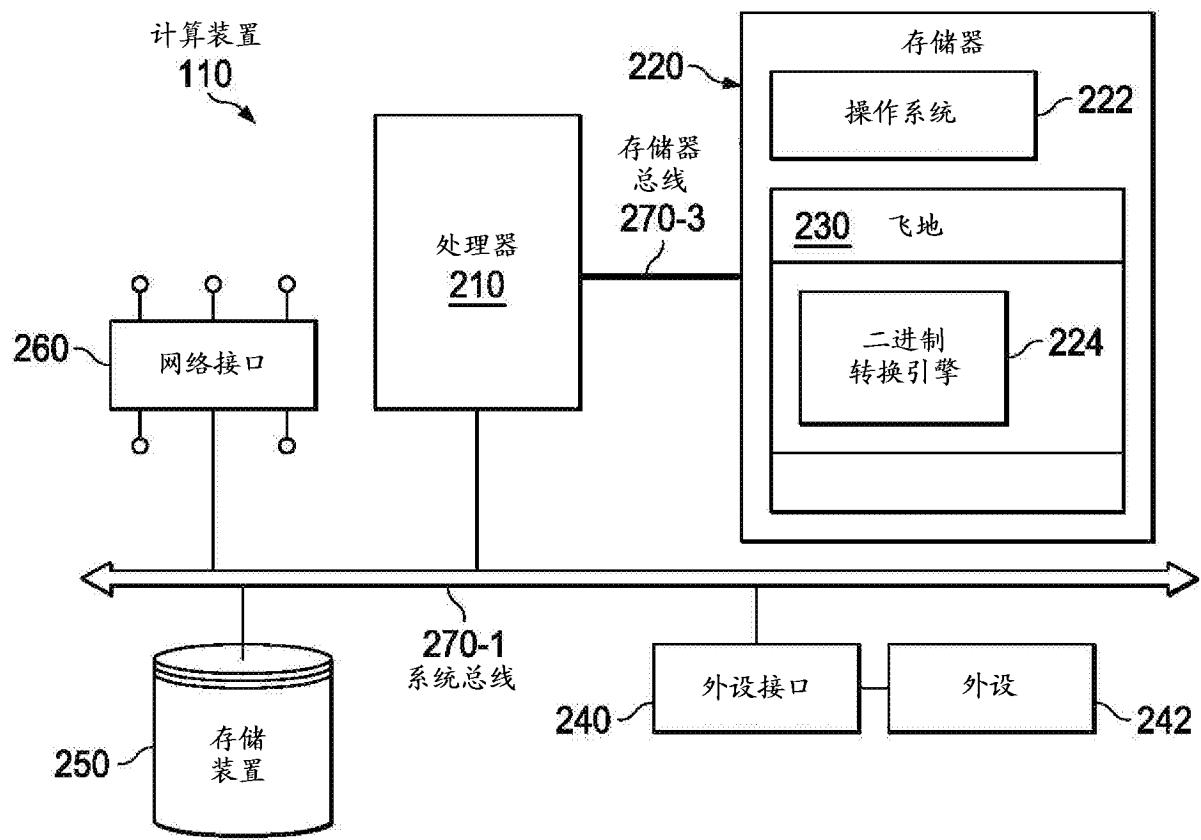


图 2

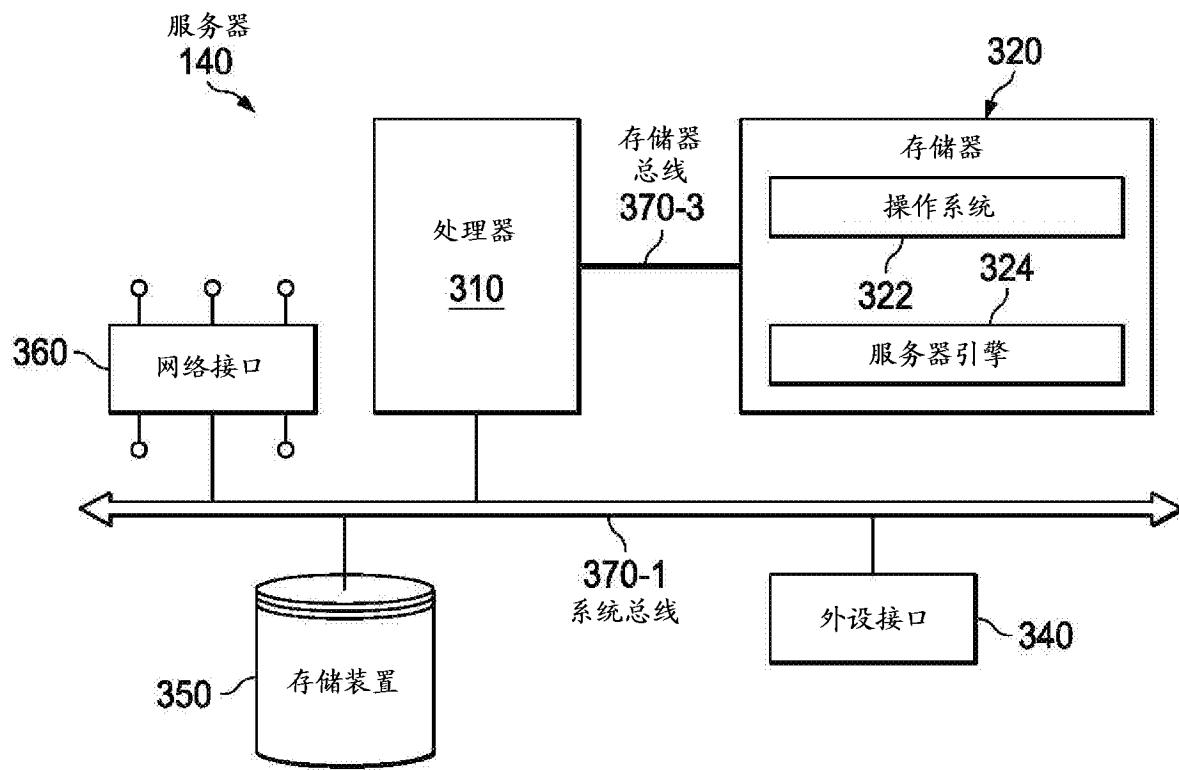


图 3

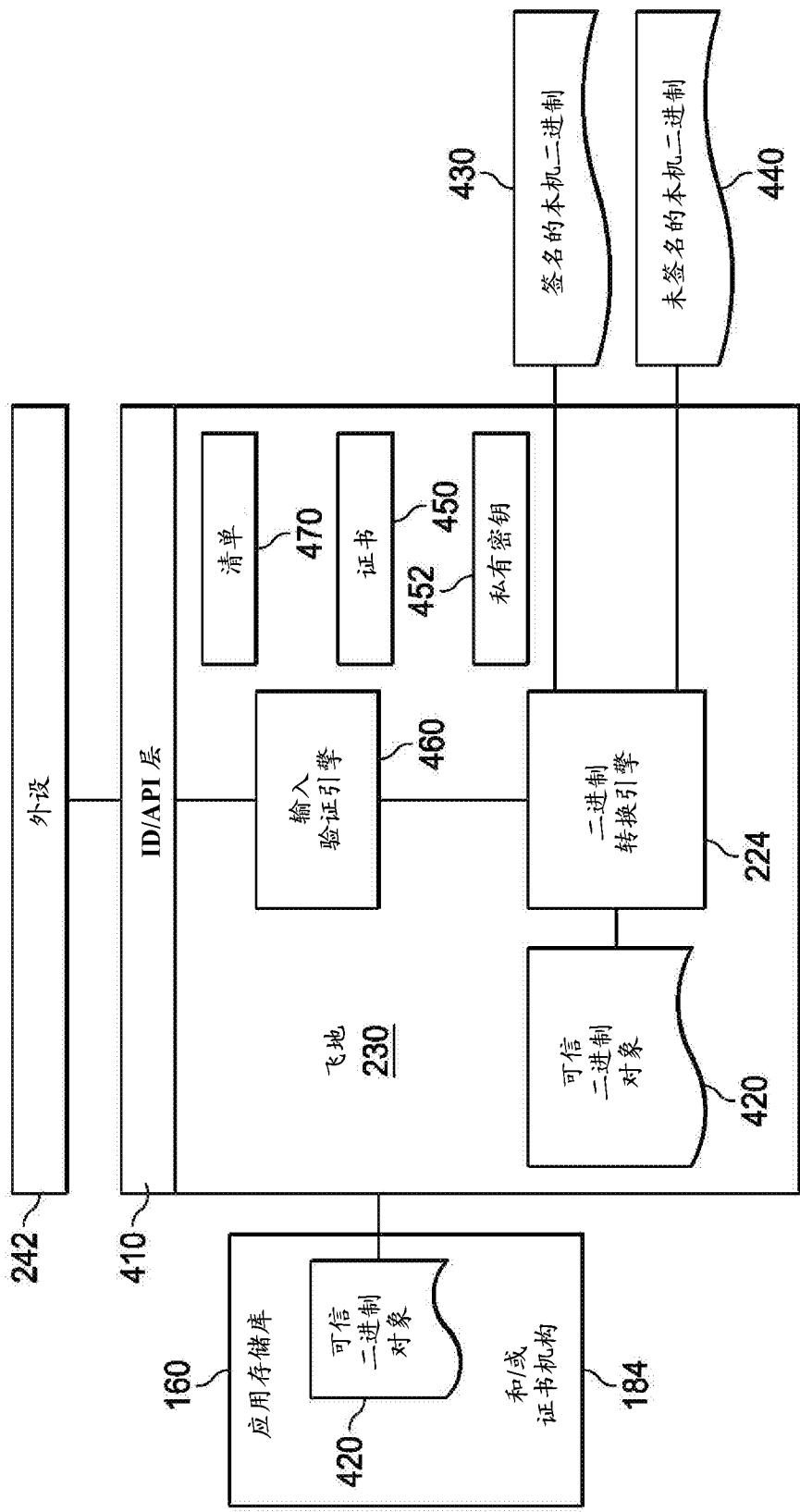


图 4A

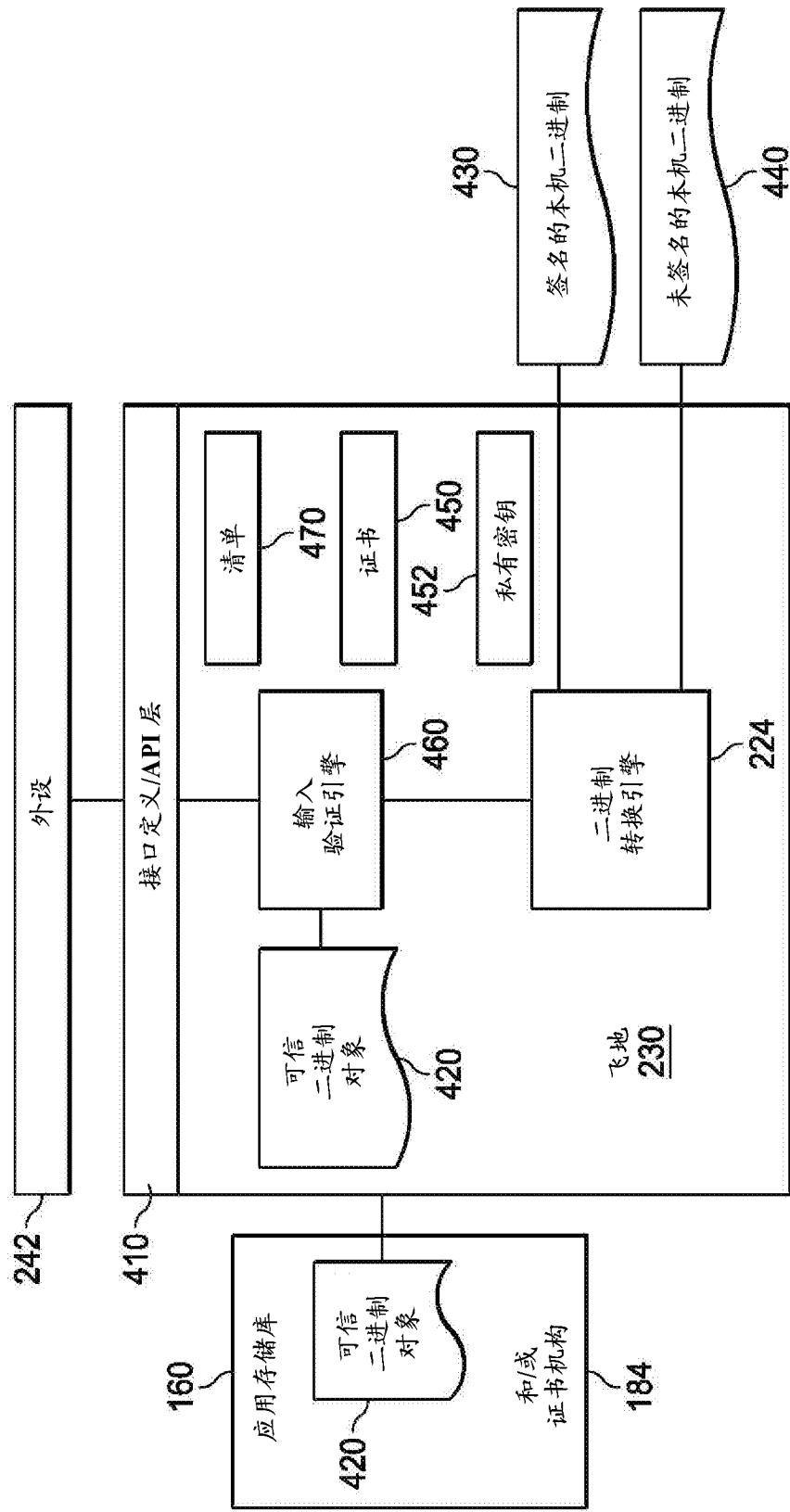


图 4B

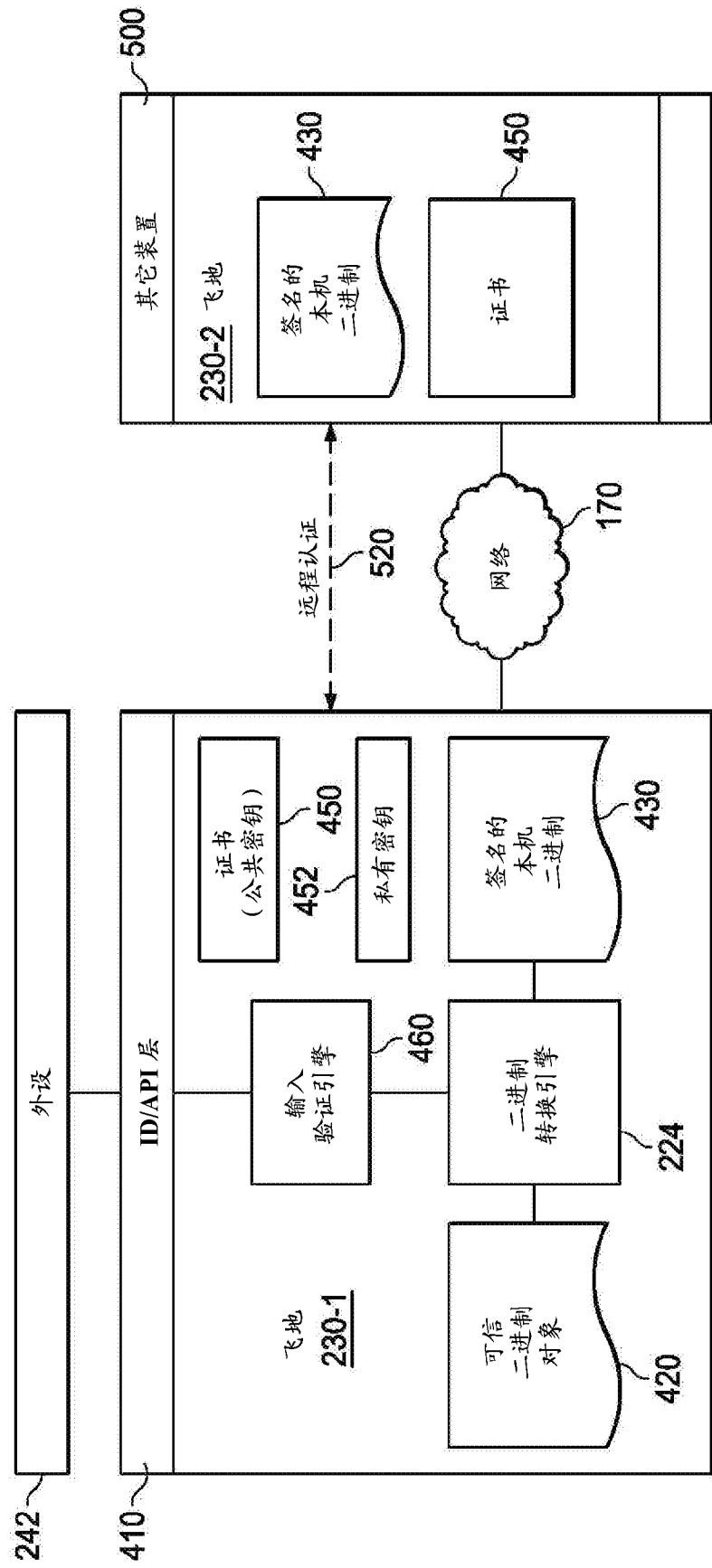


图 5

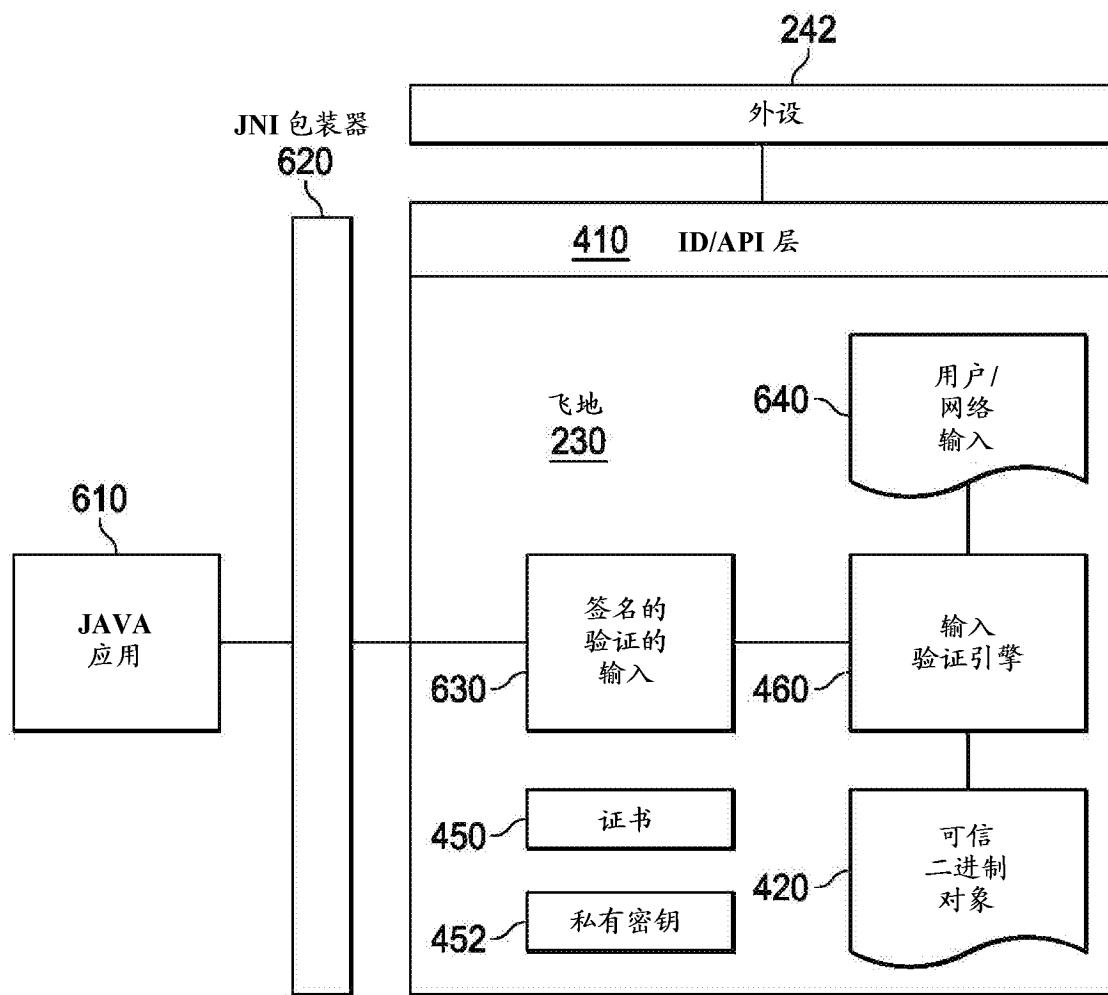


图 6

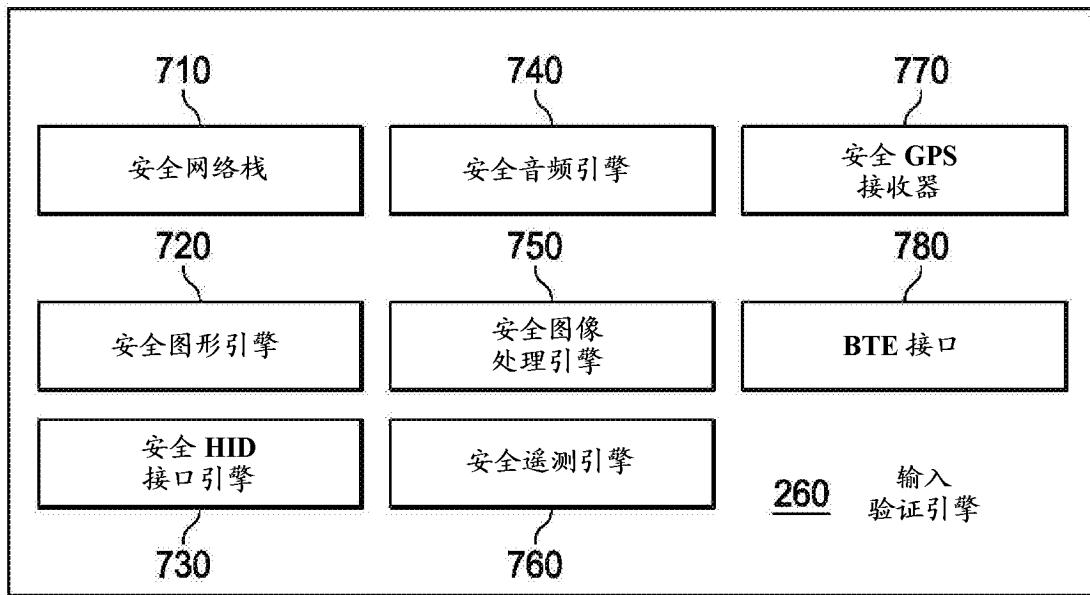


图 7

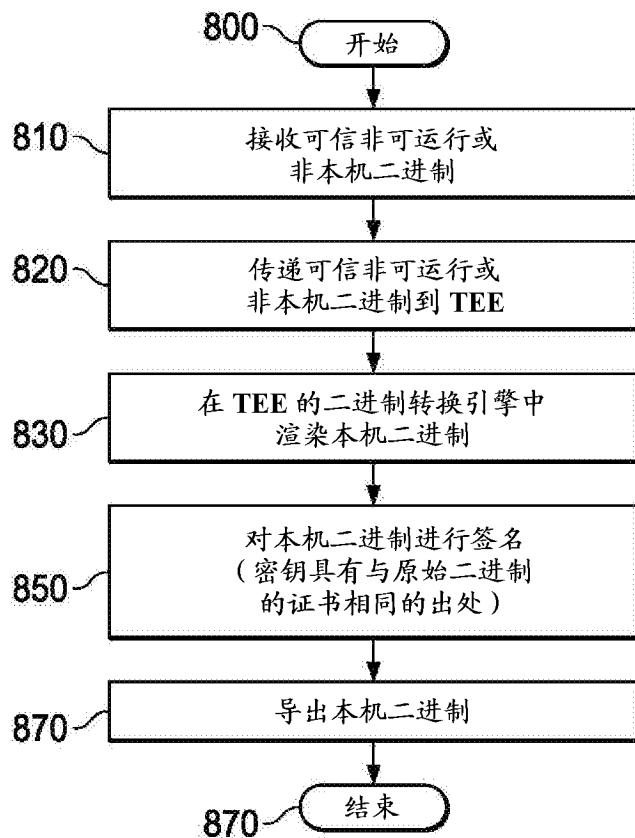


图 8

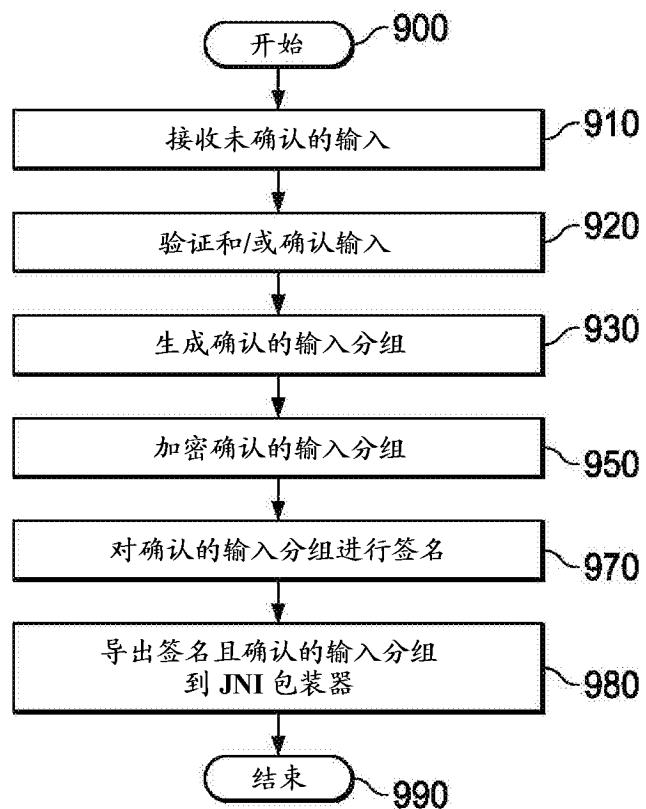


图 9

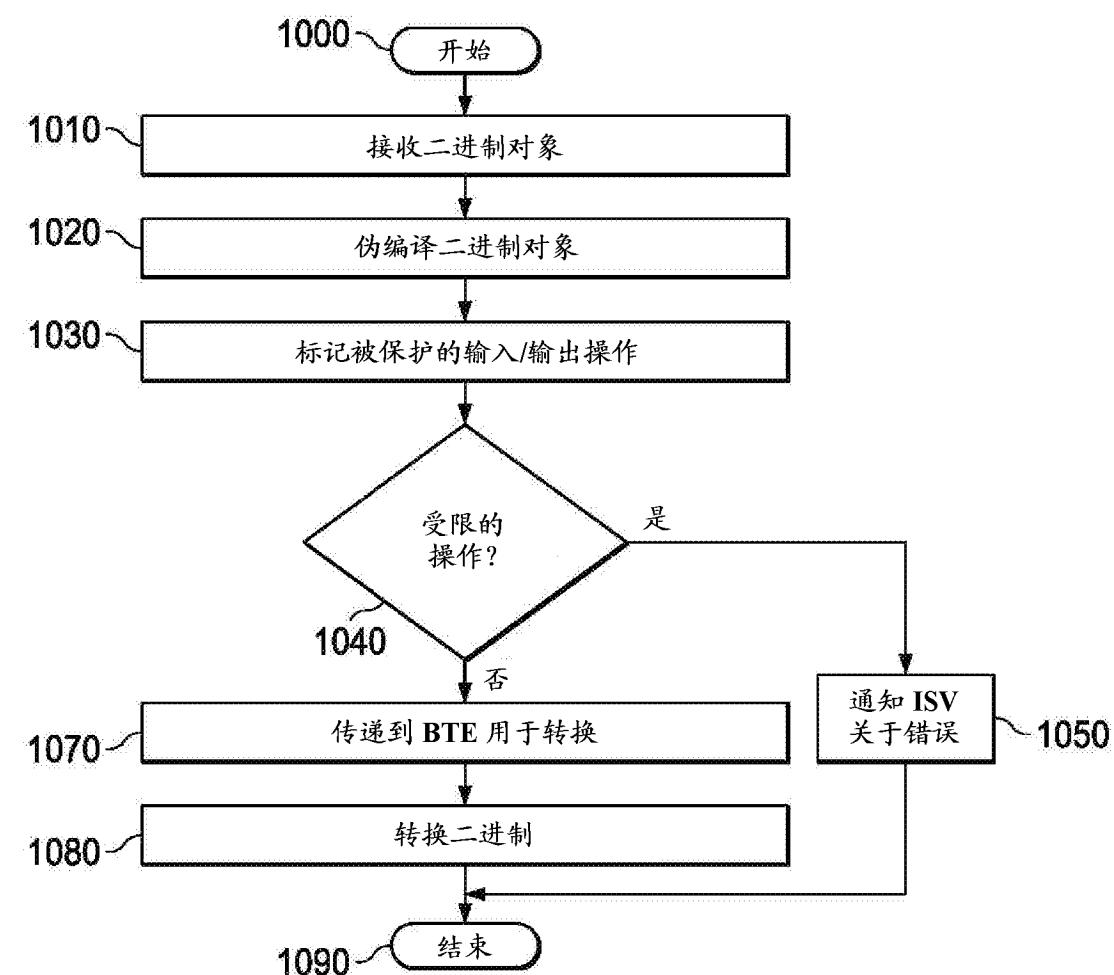


图 10