(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 107637039 B
(45)授权公告日 2020.12.15

(21)申请号 201680027087.9
(22)申请日 2016.05.11
(65)同一申请的已公布的文献号
申请公布号 CN 107637039 A
(43)申请公布日 2018.01.26
(30)优先权数据
62/172,900 2015.06.09 US
14/865,198 2015.09.25 US
(85)PCT国际申请进入国家阶段日
2017.11.09
(86)PCT国际申请的申请数据
PCT/US2016/031795 2016.05.11
(87)PCT国际申请的公布数据
WO2016/200535 EN 2016.12.15

(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 N·M·史密斯 N·赫尔德-谢拉 S·阿格瓦尔 M·G·阿戈斯坦姆
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 李炜 黄嵩泉

(51)Int.Cl.
H04L 29/06(2006.01)
审查员 曾建琼

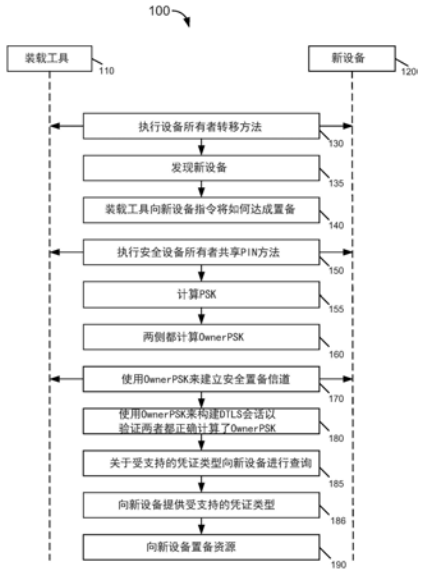
权利要求书3页 说明书17页 附图8页

(54)发明名称

执行所有者转移的系统和转移设备所有权的方法和系统

(57)摘要

在一个实施例中,一种方法包括:在第一网络的装载系统中,接收要将具有受信执行环境的第一设备的所有权转移到新所有者的请求;在该装载系统中,从频谱分析仪接收关于第一网络内的无线信号信息的通知信息;基于该无线信号信息来确定潜在攻击者是否在第一网络的无线电范围内;响应于确定潜在攻击者在无线电范围内,操纵装载系统和第一设备的信号强度以限制装载系统和第一设备的发射范围;以及在装载系统与第一设备之间执行原生通信协议以传达所有者信息,以便于执行到新所有者的所有权转移,并且致使第一设备将所有权信息存储在第一设备的存储器中。



CN 107637039 B

1.一种用于执行所有者转移的系统,包括:

第一设备,具有至少一个处理器和安全存储器并且具有第一受信执行环境TEE;以及

在第一网络内耦合至所述第一设备的装载系统,所述装载系统包括第二TEE,所述装载系统用于:接收要将所述第一设备的所有权转移到新所有者的请求,从频谱分析仪接收关于所述第一网络内的未知无线信号信息的通知信息,所述未知无线信号信息与未知无线信号活动和基于攻击者的无线信号活动中的至少一个有关;以及在所述装载系统与所述第一设备之间执行原生通信协议以传达所有者信息,以便于执行到所述新所有者的所有权转移,以致使所述第一设备将所述所有权信息存储在所述第一设备的存储器中,所述第一设备用于在不依赖于所述装载系统的情况下自治地自断言所述第一设备处于被拥有状态。

2.如权利要求1所述的系统,其特征在于,所述装载系统用于从所述第一设备的制造商接收第一令牌并且将所述第一令牌提供给所述第一设备。

3.如权利要求2所述的系统,其特征在于,所述第一设备包括物联网IoT设备并且用于将所述第一令牌与所存储的令牌作比较,并且至少部分地基于所述比较来更新所述第一设备的所有权指示符以指示所述第一设备被拥有。

4.如权利要求1所述的系统,其特征在于,所述第一设备要以未被拥有的状态被引入所述第一网络中。

5.如权利要求1所述的系统,其特征在于,所述原生通信协议包括用于实现非所有者转移通信的预定通信协议。

6.如权利要求1所述的系统,其特征在于,所述原生通信协议包括所述装载系统与所述第一设备之间的带内通信。

7.如权利要求1所述的系统,其特征在于,所述原生通信协议包括所述装载系统与所述第一设备之间的Diffie-Hellmann会话的建立以建立所有者预先共享的密钥。

8.如权利要求7所述的系统,其特征在于,所述原生通信协议包括要使用所述所有者预先共享的密钥来建立的安全会话。

9.如权利要求7所述的系统,其特征在于,根据所述原生通信协议,所述装载系统用于:

向所述第一设备指令关于用于所述所有权转移的置备技术;

计算所述所有者预先共享的密钥并且将计算所得的所有者预先共享的密钥与接收到的预先共享的密钥作比较,使用所述所有者预先共享的密钥在所述装载系统与所述第一设备之间建立安全置备信道;以及

经由所述安全置备信道向所述第一设备置备一个或多个资源。

10.如权利要求7所述的系统,其特征在于,所述原生通信协议包括用于执行所述所有权转移的共享PIN过程。

11.如权利要求8所述的系统,其特征在于,所述第一设备用于在所述安全会话期间自断言由所述新所有者拥有的所有权。

12.如权利要求1所述的系统,其特征在于,所述装载系统用于:基于所述无线信号信息来确定潜在攻击者是否在第一网络的无线电范围内,以及响应于所述潜在攻击者在所述无线电范围内的确定来操纵所述装载系统和所述第一设备的信号强度,以限制所述装载系统和所述第一设备的发射范围。

13.一种用于转移设备的所有权的方法,包括:

在第一网络的装载系统中，接收要将具有受信执行环境的第一设备的所有权转移到新所有者的请求；

在所述装载系统中，从频谱分析仪接收关于所述第一网络内的未知无线信号信息的通知信息，所述未知无线信号信息与未知无线信号活动和基于攻击者的无线信号活动中的至少一个有关；

基于所述无线信号信息来确定潜在攻击者是否在所述第一网络的无线电范围内；

响应于确定了所述潜在攻击者在所述无线电范围内，操纵所述装载系统和所述第一设备的信号强度以限制所述装载系统和所述第一设备的发射范围；以及

在所述装载系统与所述第一设备之间执行原生通信协议以传达所有权信息，以便于执行到所述新所有者的所有权转移，以使得所述第一设备能够将所述所有权信息存储在所述第一设备的存储器中，所述第一设备用于在不依赖于所述装载系统的情况下自治地自断言所述第一设备处于被拥有状态。

14.如权利要求13所述的方法，进一步包括：

在所述装载系统中，经由带外信道从所述第一设备的制造商接收第一令牌；以及

经由安全信道将所述第一令牌发送到所述第一设备。

15.如权利要求14所述的方法，其特征在于，响应于接收到第一令牌，所述第一设备用于将所述第一令牌与存在于所述第一设备的安全存储器中的所存储的令牌作比较，所述所存储的令牌由所述第一设备的制造商存储，并且至少部分地基于所述比较来更新所有者状态。

16.如权利要求13所述的方法，其特征在于，进一步包括响应于无线电范围确定来阻止所有权信息传递。

17.一种用于转移设备的所有权的方法，包括：

在物联网IoT网络的装载系统与要被引入所述IoT网络的设备之间建立第一安全会话，所述设备在引入时处于未被拥有状态；

在所述第一安全会话中计算所述设备中的所有者预先共享的密钥PSK，将所述所有者PSK存储在所述设备的存储器中，以及之后终止所述第一安全会话；

使用所述所有者PSK在所述装载系统与所述设备之间建立第二安全会话；以及

响应于成功建立所述第二安全会话，在不依赖于所述装载系统的情况下，在所述IoT网络内自治地将所述设备的所有权状态自断言并更新为被拥有状态。

18.如权利要求17所述的方法，进一步包括：

从所述装载系统接收要操纵所述设备的信号强度的命令；以及

响应于接收到所述命令，降低所述第一安全会话的无线信道的信号电平以限制所述设备的发射范围。

19.如权利要求17所述的方法，进一步包括：

从所述装载系统接收第一令牌，所述第一令牌在所述装载系统中经由带外信道从所述设备的制造商接收；

将所述第一令牌与存储在所述设备的安全存储器中的所存储的令牌作比较，所述所存储的令牌由所述设备的制造商存储；以及

至少部分地基于所述比较来更新所述设备的所有权状态。

20.一种计算机可读存储介质,包括计算机可读指令,所述计算机可读指令在被执行时用于实现如权利要求17到19中的任一项所述的方法。

21.一种用于转移设备的所有权的系统,包括:

用于在第一网络的装载系统中接收要将具有受信执行环境的第一设备的所有权转移到新所有者的请求的装置;

用于在所述装载系统中从频谱分析仪接收关于所述第一网络内的未知无线信号信息的通知信息的装置,所述未知无线信号信息与未知无线信号活动和基于攻击者的无线信号活动中的至少一个有关;

用于基于所述无线信号信息来确定潜在攻击者是否在所述第一网络的无线电范围内的装置;

用于响应于确定了所述潜在攻击者在所述无线电范围内来操纵所述系统和所述第一设备的信号强度以限制所述系统和所述第一设备的发射范围的装置;以及

用于在所述系统与所述第一设备之间执行原生通信协议以传达所有权信息,以便于执行到所述新所有者的所有权转移,以使得所述第一设备能够将所述所有权信息存储在所述第一设备的存储器中的装置,所述第一设备用于在不依赖于所述装载系统的情况下自主地自断言所述第一设备处于被拥有状态。

22.如权利要求21所述的系统,其特征在于,进一步包括:

用于经由带外信道从所述第一设备的制造商接收第一令牌的装置;以及

用于经由安全信道将所述第一令牌发送到所述第一设备的装置。

23.如权利要求21所述的系统,其特征在于,进一步包括用于响应于无线电范围确定来阻止所有权信息传递的装置。

执行所有者转移的系统和转移设备所有权的方法和系统

背景技术

[0001] 建立对物联网(IoT)设备的信任是新兴物联网网络所面临的一个挑战,因为IoT网络所提出的增加的攻击表面提高了攻击者可试图通过各种方式渗透以及弱化或破坏IoT以及传统电脑网络两者的可能性。用于建立信任的机制的范围包括从设备内或者通过网络连接试图观察设备的附加安全监视应用。此类观察基于观察组件不受网络内恶意软件攻击的理念。还有一些其他办法纳入了受信计算模块,该受信计算模块可能不期望地增加成本从而使得此类办法不可行。

附图说明

[0002] 图1是解说根据一实施例的装载和所有者转移方法的图示。

[0003] 图2A是解说根据另一实施例的装载和所有者转移方法的图示。

[0004] 图2B是解说根据本发明的又一实施例的装载和所有者转移方法的图示。

[0005] 图3是根据一实施例的另一所有权转移方法的框图。

[0006] 图4是根据一实施例的使用频谱分析仪来递送早期警告通知的方法。

[0007] 图5是可与多个实施例一起使用的示例系统的框图。

[0008] 图6是根据本发明的另一实施例的系统的框图。

[0009] 图7是根据另一实施例的可穿戴模块的框图。

具体实施方式

[0010] 在各实施例中,IoT设备可以被配置为受信设备。为此,各实施例可以对要被直接应用于IoT设备的受信计算技术进行重构,其中信任基础是由设备本身以及将设备装载到IoT网络中的协议来确立的。各实施例可以提供用于装载IoT设备的协议,其中此类设备可以利用传统上针对安全协处理器保留的受信计算方法以及其他安全扩充技术。具体来说,各实施例可以将制造商确立的设备所有者状态安全地转移到设备所有者。注意到,术语“装载”指的是设备通过它被引入所有者环境的一个过程。作为整体装载的一部分,设备的所有权已经从前一所有者或制造商被安全地转移到预期所有者。所有权转移可以是攻击点,因为可能难以在之后检测到这一攻击。在一实施例中,这一装载办法可以重用IoT设备资源模型,以使得用于处理正常IoT功能的基础设施也可以被用于执行安全装载,这可以比定义单独的安全消息收发、接口和数据接口更高效。以此方式,IoT设备能够达成与其他可能的方式相比更高的信任水平。

[0011] 各实施例提供了一种由设备制造商和用户执行的协议以及操作职责以建立其中设备所有者转移可以发生的安全上下文。IoT设备可确定恰适的条件何时被满足以宣告所有权何时被确立。作为对比,传统办法认为设备从属于宣告设备被拥有和信任的权威服务。各实施例使得设备开发者能够将设备所有者转移逻辑包括在IoT设备中,以使得设备所有权的大部分权威断言是自断言。

[0012] 在各实施例中,使用IoT框架(例如,开放互连协会(OIC)、OMA)所使用的资源抽象

模型来表示与安全有关的设备装载状态以捕捉设备所有权转移状态改变。这一办法允许该框架准确地维护其所有权状态以及向其他设备表示其所有权状态而不会有边带表示或因安全而异的表示。各实施例得到在不引入单独的受信协议消息收发栈和接口的情况下用原生设备交互脚本表达的实现预期设备所有者转移协议的一组设备装载流程。通过组织引导序列以使得设备在装载期间不进入非安全状态来建立信任。各实施例可定义显式装载序列，从而导致从受信制造商到预期消费者/所有者的设备所有者转移。要理解，尽管本文的各示例实施例涉及用与开放互连协会布置相兼容的协议来进行通信的设备，但是本文所述的通用所有权转移协议适用于许多其他IoT示例。

[0013] 在各实施例中，在将新设备引入所有者网络时，可以建立预先共享密钥(被称为“OwnerPSK(所有者PSK)”)。OwnerPSK(每个设备一个)是前一所有者/制造商与新所有者(设备所有者转移方法(DOXM))之间的带外所有权转移方法的结果。本文的不同实施例可以产生被用于断言设备所有权的预先共享的密钥值。OwnerPSK被用于生成出于其他目的被使用的(例如)对称密钥。例如，配对的PSK可以被用于保护设备置备数据免遭系统管理工具损害。在一个实施例中，作为一个示例，OwnerPSK生成方法可以如下。OwnerPSK＝PRF(Random，DeviceLabel，NewOwnerLabel，PreviousOwnerLabel)，其中：PRF是用于密钥生成的伪随机函数，其以加密方式组合各函数参数以使得其展现出预图像抵抗性、冲突抵抗性、以及第二预图像抵抗性；Random(随机)是具有足够熵的随机值；DeviceLabel(设备标记)标识其所有权正被转移的设备；NewOwnerLabel(新所有者标记)是由新所有者确认成为新所有者的意图而供应的值；以及PreviousOwnerLabel(前一所有者标记)是前一所有者确认将所有权转移至新所有者的意图而供应的值。如果平台包含平台所有权能力以使得主存于同一平台上的多个OIC设备实例将不会要求在第一OIC设备实例之后取得所有权，NewOwnerLabel标识平台所有权方法并且可以引用平台所有者授权数据。NewOwnerLabel值可以在OIC设备与所有者转移服务之间共享以促进使用伪随机函数进行OwnerPSK计算。

[0014] 在不同实施例中，OwnerPSK值可具有表1和2中示出的不同示例中的以下格式。

[0015] 表1

[0016] 128位密钥：

[0017]

名称	值	类型	描述
长度	16	八位位组	指定长度之后的 8 位的八位位组的数目。
密钥	不透明	八位位组阵列	八位位组的 16 字节阵列。当被用作 PSK 函数的输入时，长度被略去。

[0018] 表2

[0019] 256位密钥：

[0020]

名称	值	类型	描述
长度	32	八位位组	指定长度之后的 8 位的八位位组的数目。
密钥	不透明	八位位组阵列	八位位组的 32 字节阵列。当被用作 PSK 函数的输入时，长度被略去。

[0021] 在不同实施例中,可以实现设备所有者自断言的各种模式。在第一实施例中,可以使用设备装载工具与制造商所拥有的设备之间的协议。现在参考图1,示出了解说根据一实施例的装载和所有者转移方法的图示,其依赖于作为转移所有权意图的指示的制造商供应的令牌。

[0022] 在这一实施例中,制造商经由带外信道来供应所有权转移令牌,并且通过将该令牌与设备内受保护存储器中存储的嵌入式副本作比较来达成对该令牌的验证。该协议取决于Diffie-Hellman密钥协商协议来动态地建立安全连接,而不取决于发放证书的公共公钥基础设施(PKI)或者被假定受到双方信任的某一其他第三方。通常,此类第三方在实践中不存在,因为这只会使设备所有者转移逻辑的实际安全语义混淆。这并非意味着对PKI、证书或非对称加密的使用无法在基于密钥协商协议(诸如Diffie-Hellman,如下图2B中所描述的)的安全会话构建中被使用。

[0023] 图1示出了环境100中装载工具110(其可以是IoT网络所有者的服务器或其他计算系统)与要被纳入给定IoT网络(例如,任何给定类型的IoT计算设备)的新设备120之间的一组交互。为了实现新设备的装载以及例如向拥有装载工具110的公共实体以及IoT网络更新所有权,示出了设备所有者转移方法130。在图1的实施例中,设备所有者转移方法130提供了一通信序列以实现先前处于未被拥有的状态(例如,如由设备制造商原始配置的)的设备的所有权建立。图1的实施例提供方法130以执行共享PIN设备所有者转移方法。

[0024] 一般来说,图1中示出的方法130包括用于例如经由Diffie-Hellmann交换过程来建立所有者预先共享密钥(PSK)的过程。各设备可以执行对要被装载的设备的协商或发现,并且执行一过程以使得该设备能够验证装载工具是真实的且受信的,以使得在建立第一会话以生成所有者PSK并且接着终止该第一会话之后,能够使用这一所有者PSK来建立安全置备通道。这一对安全通道的建立因而向该设备指示,装载工具能够被信任,并且能够在各设备之间进行对要被共享的一组凭证的有效交换。另外,假定该过程被正确地执行,该设备能够自断言它现在被拥有了。

[0025] 为了开始方法130,发现新设备(框135)。注意到,以下编号的通信中的每一者是装载工具110与新设备120之间的所有者转移过程的一部分的给定通信。此外,对于该处理器的每一部分,第一通信可以从装载工具110被发送到新设备120,而最后通信从新设备120被发送到装载工具110,除非另外指明。

[0026] 1.GET/oic/sec/doxm?Owned＝“FALSE”

[0027] 2.RSP({*OxmType“:”oic.sec.doxm.pin*,“Oxm”:“0”,“Owned”:“FALSE”,

[0028] “DidFormat”:“0”,“DeviceID”:“uuidA2IC-E000-0000-0000*....})

[0029] 3.POST/oic/sec/doxm({...”OxmSel”:“oic.sec.doxm.pin”,...})

[0030] 4.RSP 2.04

[0031] 5.GET/oic/sec/pstat

[0032] 6.RSP({“IsOp”:“FALSE”,“Cm”:“bx0011.1110”,“Tm”:“bx0011.1110,“DeviceID”:,“Om”:“bx0000,0000”,“Sm”:“bx0000,0011”,“CommitHash”:})

[0033] 接着,在框140,装载工具指令新设备将如何达成置备。在一实施例中,可以发送以下消息。

[0034] 7.PUT/oic/sec/pstat({....,”Om”:“bx0000,0011”,...})

[0035] 8.RSP2.04

[0036] 接着在框150,可以执行安全设备所有者共享PIN方法。在一实施例中,这一方法可以基于PSK来执行。要理解,在其他情景中,可以使用非对称凭证。在一实施例中,执行该过程的这一部分的通信包括:

[0037] 9.ClientHello(TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA)

[0038] 10.HelloVerifyRequest(cookie)

[0039] 11.ClientHello(cookie)

[0040] 12.ServerHello();ServerKeyExchange(ECDH PublicKey+ECC Curve Param);

[0041] ServerHelloDone()

[0042] 接着在框155,可以例如根据基于口令的密钥推导函数来计算预先共享的密钥,基于口令的密钥推导函数诸如:PBKDF2(PRF,PIN,new device ID,dklen),如下进一步描述的。在一实施例中,Diffie-Hellmann过程可以被执行以建立这一预先共享的密钥。这一运算定义了PIN,PIN可以用于Ga和Gb’值的DH构建,其中a’=a+PIN并且b’b+PIN。只有PIN值被两个端点知晓,才能够找到a’和b’值。如果PIN通过建立物理临近度的带外信道来传递,则这种情况可能发生。例如,一种临近度实现是传达PIN的超声扬声器/话筒,其中物理障碍物可能阻止未经授权的监听者听到/记录PIN广播。因此,它对于其中攻击者无法在物理上靠近端点的一些攻击是有抵抗性的。在一实施例中,用于这一计算的通信可包括:

[0043] 13.ClientKeyExchange(ECDH PublicKey);ChangeCipherSpec+Finish

[0044] 14.ChangeCipherSpec+Finish

[0045] 15.PUT/oic/sec/doxm({...,”DevOwner”:“uuid:B0B0-0000-0000-0000”,....})

[0046] 16.RSP 2.04

[0047] 之后,在框160,两侧都计算所有者PSK。在一实施例中,装载工具110可如下计算所有者PSK:

[0048] 17.OwnerPSK=PRF(MasterSecret,“oic.sec.doxm.jw”,“uuid:B0B0-0000-0000-0000”,“uuid:A21C-E000-0000-0000”,“63”).这一方法因而避免使用PIN来计算Ga和Gb。

[0049] 然而,PIN的PRF构造可以是类似的,以用“...doxm.jw”替代“...doxm.rdp”,从而暗示PIN方法被使用/预期。

[0050] 并且进而,新设备120可如下计算所有者PSK:

[0051] 18.OwnerPsk=PRF(...)

[0052] 19./oic/sec/pstat.Cm=bx0011,1100.注意,在此时,会话可以被终止。

[0053] 之后,所有者PSK可以被用于建立具有安全置备通道的新会话,在一实施例中该会话可以是DTLS会话(框170)。该会话可以通过将所有者PSK用作提供到所供应的加密套件的

预先共享的密钥而在两个方向中都是开放的,在一个实施例中,如下:

[0054] 20.Open DTLS session with OwnerPSK as the PSK for TL5_PSK_...cipher suite.

[0055] 在框180,所有者PSK可以被用于构建DTLS会话以验证所有者PSK的正确计算。在这一操作中,注意到,新设备120可以自断言该设备现在处于被拥有状态。由此,这一所有权的状态改变单独地在新设备120内被发起和执行,而不依赖于装载工具110。以此方式,设备本身自治地管理其自己的所有权状态。在一实施例中,新设备可以根据以下来设置所有者状态:

[0056] 21./oic/sec/doxm.Owned=“TRUE.”

[0057] 之后,可以在安全会话中执行置备过程以向新设备置备受支持的凭证。首先在框185,装载工具可以查询新设备120以获取受支持的凭证类型(框185)。接着在框186,向新设备置备受支持的凭证类型。在一实施例中并且基于受支持的凭证类型,这些凭证可包括对以下各项的置备:对称配对式、对称分组式、非对称配对式、和/或非对称分组式凭证。进一步注意到,受支持的凭证可进一步包括针对置备服务的凭证,它们可以被用于继续/完成IoT设备的置备。之后在框190,可以向新设备置备各种资源。例如,网络安全服务可以置备用于访问其他服务和设备的附加安全凭证。其可进一步置备访问控制列表(ACL)和其他策略。在一些实施例中,还可以置备设备管理设置、关键/固件更新等。之后,可以关闭DTLS会话。

[0058] 在一个实施例中,图1的基于PIN的设备所有者转移方法使用由征求意见稿(RFC)2898所定义的伪随机函数(例如,PBKDF2)以及经由带外方法交换的PIN来生成预先共享的密钥。如下将经PIN认证的预先共享的密钥(PPSK)供应到接受PSK的给定TLS加密套件:

[0059] PPSK=PBKDF2(PRF,PIN,DeviceID,c,dkLen),其中PBKDF2函数具有以下参数:

[0060] -PRF-使用DTLS PRF;

[0061] -PIN-经由带外信道获得;

[0062] -DeviceID-新设备的UUID;

[0063] -c-被初始化为1000的迭代计数,每一次使用时被递增;以及

[0064] -dkLen-推导出的PSK以八位位组计的期望长度。

[0065] 现在参考图2A,示出了解说根据另一实施例的装载和所有者转移方法的图示。在这一配置中,一实施例可依赖于频谱分析仪来向基于Diffie-Hellman的所有者转移方法通知可能的MITM威胁的信号智能警告。

[0066] 在图2A的实施例中,匿名Diffie-Hellman密钥协商协议可以被用于达成被输入到OwnerPSK计算的对称密钥。在这一实施例中,OwnerPSK计算可以遵循以下格式来确保跨不同厂商产品的互操作性:

[0067] OwnerPSK=PRF(MasterSecret,Message,Length),其中:

[0068] -PRF使用由RFC5246定义的TLS PRF;

[0069] -MasterSecret(主秘密)是从DTLS握手获得的主秘密密钥;

[0070] -Message(消息)是以下各项的串接:

[0071] -用于Just Works方法的DoxmType串(例如,“oic.sec.doxm.jw”);

[0072] -OwnerID(所有者ID)是标识设备所有者标识符以及维护OwnerPSK的设备的URI;

[0073] -DeviceID(设备ID)是新设备的DeviceID(例如，

[0074] “urn:uuid:XXXX-XXXX-XXXX-XXXX”);以及

[0075] -Length(长度)是Message以八位位组计的长度。

[0076] 如同图1那样，图2A示出了在环境200中发生的装载工具210与新设备220之间的一组交互。在图2A的实施例中，设备所有者转移方法230提供了一通信序列以实现被装载到网络中的处于未被拥有状态的这一新设备的所有权建立。更具体地，图2A的实施例提供用于执行“JustWorks”设备所有者转移方法的方法230。

[0077] 为了开始方法230，发现新设备(框235)。在一个实施例中，包括以下操作：

[0078] 1.GET/oic/sec/doxm?Owned＝“FALSE”

[0079] 2.RSP({*OxmType”:”oic.sec.doxm.jw”,“Oxm”:“0”,“Owned”:“FALSE”,

[0080] “DidFormat”:“0”,“DeviceID”:“uuidA2IC-E000-0000-0000*....})

[0081] 3.POST/oic/sec/doxm({...“OxmSel”:“oic.sec.doxm.jw”,...})

[0082] 4.RSP2.04

[0083] 5.GET/oic/sec/pstat

[0084] 6.RSP({“IsOp”:“FALSE”,“Cm”:“bx0011.1110”,“Tm”:“bx0011.1110，“DeviceID”:,“Om”:“bx0000,0000”,“Sm”:“bx0000,0011”,“CommitHash”:})

[0085] 接着，在框240，装载工具指令新设备将如何达成置备。在一实施例中，可以发送以下消息。

[0086] 7.PUT/oic/sec/pstat({....,”Om”:“bx0000,0011”,...})

[0087] 8.RSP 2.04

[0088] 接着，在框250，可以执行安全设备所有者JustWorks方法。在一实施例中，执行该过程的这一部分的通信包括：

[0089] 9.ClientHello(TLS_ECDH_anon_WITHvAES_128_CBC_SHA)

[0090] 10.HelloVerifyRequest()

[0091] 11.ClientHello(cookie)

[0092] 12.ServerHello();ServerKeyExchange(ECDH PublicKey+ECC Curve Param)；

[0093] ServerHelloDone()

[0094] 13.ClientKeyExchange(ECDH PublicKey);ChangeCipherSpec+Finish

[0095] 14.ChangeCipherSpec+Finish

[0096] 15.PUT/oic/sec/doxm({...,”DevOwner”:“uuid:B0B0-0000-0000-0000”,....})

[0097] 16.RSP 2.04

[0098] 要理解，在其他实施例中，可以使用选择采用匿名Diffie-Hellman协议的不同算法的另一配置套件，其中可以使用短暂椭圆曲线方法、基于计数的加密块模式(例如，CCM、GCM)或其他加密模式、或者SHA256或其他加密散列。

[0099] 接着，在框260，可以由两侧来计算所有者PSK。在一实施例中，装载工具210可如下计算所有者PSK：

[0100] 17.OwnerPSK＝PRF(MasterSecret,“oic.sec.doxm.jw”,“uuid:B0B0-0000-0000-0000”,“uuid:A21C-E000-0000-0000”,“63”)

[0101] 并且进而，新设备220可如下计算所有者PSK：

[0102] 18.OwnerPsk＝PRF(...)

[0103] 19./oic/sec/pstat.Cm＝bx0011,1100

[0104] 接着,在这一第一会话的终止之后,如上的所有者PSK可以被用于建立其中构建DTLS会话的具有安全置备通道的新安全会话(框270),并且之后可以向新设备置备受支持的凭证和资源(框280、285、286和290)。如上,在一实施例中,可以在该过程的这一部分中执行以下通信:

[0105] 20.Open DTLS session with OwnerPSK as the PSK for TL5_PSK_...cipher suite

[0106] 21./oic/sec/doxm.Owned＝“TRUE”

[0107] 22.Close DTLS Session

[0108] 在又一实施例中,可以使用另一所有者转移方法,其中签署密钥和证书凭证可以被用于建立安全会话。现在参考图2B,示出了解说根据本发明的又一实施例的装载和所有者转移方法的图示。如图2B所示,环境200′包括类似的装载工具210和新设备220。注意到,执行设备所有者转移操作的方法230可如上在图2A中框235和240处所讨论地类似地继续。之后,在框255,可以使用签署密钥和证书凭证来建立安全DTLS会话。更具体地,可以使用椭圆曲线数字签名算法(ECDSA)或Intel®增强型隐私标识符(EPID)签署密钥和证书凭证来建立DTLS会话。在一实施例中,可以使用Intel®基于Sigma的协议。

[0109] 仍然参考图2B,在框265,装载工具可以关于受支持的凭证类型向新设备进行查询。接着在框275,可以向新设备置备受支持的凭证类型。基于此类受支持的凭证类型,可以置备对称配对式凭证(例如,包括OwnerPSK)、对称分组式、非对称配对式、和/或非对称分组式凭证。注意到,此类凭证可包括用于置备要被用于继续/完成IoT设备置备的服务的凭证。之后,在框284,向新设备置备用于连接到生产IoT网络的设置。注意到,一些设置可涉及连接到不同的无线接入点或网络接口,在一实施例中,其可使用在框275中置备的凭证。之后,在框294,新设备220可以连接到生产网络。接着,在框296,新设备可以联系这一生产网络中的一个或多个置备服务器以继续/完成新设备置备。

[0110] 各实施例可以为不具有安全存储资源或制造能力的制造商提供在制造时嵌入令牌值的灵活性。对于这种模式,可以依赖于装载的上下文。合法设备所有者通过评估在设备寿命期间中间人(MITM)攻击者可能合理地能够持续进行MITM攻击的可能性来确立设备所有者转移的上下文。例如,如果设备依赖于无线通信技术(诸如蓝牙、NFC或WiFi),则MITM攻击者将被要求维持无线连接,这阻止了装载系统直接访问新设备并且确保了新设备仅取决于MITM设备来访问其他合法设备。在实践中,这种攻击是相当具有挑战性的。

[0111] 设备所有者可以采取附加步骤来使装载和所有权转移期间MITM攻击者的概率最小化。这些操作可包括操纵无线广播信号来限制新设备和装载系统两者的无线电范围。附加地,装载环境可包括频谱分析设备,其监视所有无线信号,从而根据广播强度、来源和类型对它们进行排名。可以在可充当早期警告机制和威胁通知系统的信号智能的上下文中执行装载活动。作为一个示例,无线传送和接收设备的信号强度调制可以被用于最小化/缓解MITM攻击的有效性。

[0112] 图3是根据一实施例的另一所有权转移方法的框图。在图3中,带外(OOB)信道可以被制造商用来将所有者转移令牌与所有者的IoT设备装载工具共享。

[0113] 如所解说的，图3示出了包括设备制造商系统310的网络架构300，设备制造商系统310可以是制造IoT设备350的设备制造商的给定系统。另一系统330是其中要置备设备350的IoT网络的装载设备。假定设备350是要被置备到IoT网络中并且以未被拥有状态抵达的新设备。在这一未被拥有状态中，设备350可以存储由设备制造商在制造过程期间置备的令牌360(T2)，其可包括与要被提供到系统330的令牌相同的值，如下所讨论的。

[0114] 如布置300中可以看到的，设备制造商310将令牌315(T1)提供给装载设备330。在一实施例中，令牌的这一传递可以经由带外(OOB)信道320，其可以采用不同的形式。注意到，这一令牌T1可以是用于签署Diffie-Hellmann交换的EPID或非对称密钥。在其他情形中，可以提供具有针对未被拥有的设备群的EPID的证书。这一令牌可以被存储在装载容器335中，其可以是设备的给定TEE。

[0115] 如看到的，在装载设备330与设备350之间建立通信信道340。在一实施例中，这一通信信道可以是无线通信信道。在会话建立之后，该信道可以被用于例如经由Diffie-Hellmann交换将令牌T1提供给设备350。而且，可以执行如本文所描述的设备所有权转移方法。更具体地，假定设备350确认接收到的令牌T1包括与其所存储的令牌360(T2)相同的值(例如，PIN、随机数等等)，确定系统330可以被信任并且所有权转移可有效地发生，以使得新设备350自断言它现在处于未被拥有状态。

[0116] 图4是根据一实施例的在IoT设备装载操作期间使用频谱分析仪来递送可能的无线MITM攻击者的早期警告通知的方法。在装载之后，新设备确立成功完成装载的实体是其预期的设备所有者。该设备接着禁用所有者建立的可能性。

[0117] 现在参考图4，解说了网络400。如看到的，网络400包括第一无线电范围420和第二无线电范围380。注意到，无线电范围420具有较大范围，即，其中信号能够被频谱分析仪410检测到的范围。进而，无线电范围380具有较小范围，并且可以是装载无线电范围，即例如，无线局域网340(诸如蓝牙T^M低能量网络)或者装载设备330和新设备350位于其中的其他短程无线网络中的无线通信范围。这些设备可以参与装载和置备过程，诸如本文描述的其中在设备350内建立设备所有权的过程。为此，为了阻止不期望的入侵，如果在无线电范围420内检测到未知无线信号活动，则频谱分析仪410可以向装载设备330发送通知。以此方式，如果在无线电范围420内检测到未知或预期的基于攻击者的无线信令，则频谱分析仪410可以向装载工具330发出关于虚假无线电干扰的一个或多个通知。响应于这一信息，装载设备330可以采取各种恰适的动作，包括对设备330和350中的一者或多者进行信号强度调制。此类调制可以降低无线通信的功率或强度，以使得它们不在无线电范围420中较宽的区域中进行通信。要理解，在一些情形中，信号强度调制可包括阻止所有者转移通信，至少直到频谱分析仪410指示潜在威胁已经被消除。

[0118] 在针对符合OIC设备的一实施例中，/oic/sec/doxm资源可包含一组受支持的设备所有者转移方法。通过/oic/res资源可以发现安全资源。资源发现处理尊重作为给定安全资源定义的一部分供应的约束(例如，CRUDN)。表3是根据本发明的一实施例的所有者转移方法资源定义。

[0119] 表3

[0120]

固定 URI	资源类型标题	资源类型 ID（“rt”值）	接口	描述	相关功能交互
/oic/sec/doxm	设备所有者转移方法	urn:oic.sec.doxm		用于支持设备所有者转移的资源	配置

[0121] 表4是根据本发明的一实施例的示例所有者转移方法属性定义，其中可以使用现有的设备交互协议来查询设备所有者状态和配置。

[0122] 表4

[0123]

属性名称	操作	实例	强制性	类型	范围	描述
Oxm	R	多个	是	Oxm 类型	-	标识定义所有者转移方法和方法名称的组织的URN。
OxmSel	R	单个	是	Oxm 类型	-	被选择用于设备所有权转移的Oxm。
Owned	R	单个	是	Boolean	TIF	指示设备所有权是否已经被建立。FALSE 指示设备未被拥有。
DidFormat	R	单个	是	UINT8	0-255	枚举的设备 ID 格式。[0-URN] （例如 urn:uuid:XXXX-XXXX-XXXX-XXXX-XXXX）
DeviceID	R	单个	是	八位位组[]	-	指派到 OIC 框架的这一实例的 DeviceID（设备 ID）DidFormat 确定如何解读八位位组串
DevOwner	R	单个	是	oic.sec.svc	-	标识作为设备所有者的服务的URI。这可以是由设备所有者选择的任何值。

[0124]

属性名称	操作	实例	强制性	类型	范围	描述
Rowner	R	单个	是	oic.sec.svc	-	这一资源的所有者。通常这是实例化这一资源的引导服务。
Supported Credential Types（受支持的凭证类型）	R	单个	是	位掩码	-	这一设备能够支持的凭证类型的位掩码。

[0125] 如表4中所示，所有者转移方法资源包含所有者转移方法的经排序的列表，其中该列表中的第一条目是最高优先级方法而最后一个条目是最低优先级。设备制造商可以例如通过具有最高优先级的最期望的(最安全的)方法以及具有低优先级的最不期望的方法来配置这一资源。在网络管理工具选择最恰适的方法时，网络管理工具可以在装载时查询这一列表。在所有者转移方法被选择之后，使用OxmSel属性将经协商一致的方法输入/doxm资源。

[0126] 在一实施例中，所有者转移方法包括两个部分，标识厂商或组织的URN以及具体方法。

[0127] <OxmType>::=″urn:″<NID>″:″<NSS>

[0128] <NID>::=1<Vendor-Organization>

[0129] <NSS>::=<Method>|{<NameSpaceQualifier>“.”}<Method>

[0130] <NameSpaceQualifier>::=String

[0131] <Method>::=String

[0132] <Vendor-Organization>::=String

[0133] 当所有者转移方法成功完成时，Owned(被拥有)属性被设置为‘1’(真)。因此，取得该设备的所有权的后续尝试都将失败。安全资源管理器(SRM)响应于成功的所有权转移来生成被存储在/oic/sec/doxm资源中的设备标识符(DeviceID)。所有者转移方法可以将DeviceID传递到取得所有权的服务。该服务可以将该DeviceID与安全数据库中的OwnerPSK进行关联。一旦被拥有，引导服务可以将owned状态改变为‘0’(假)。

[0134] 表5示出了根据一实施例的所有者转移方法。

[0135] 表5

[0136]

值类型名称	值类型 URN	枚举值	描述
OICJustWorks	urn:oic:oic”sec.doxm.jw	0	Just works 方法依赖于匿名 Diffie-Hellman 交换来实现共享秘密。它经受中间人威胁。
OIC 共享 Pin	urn:oic:oic”sec.doxm.pin	1	共享 PIN 方法依赖于带外 PIN 分发方法来生成共享秘密，其缓解了许多中间人威胁。

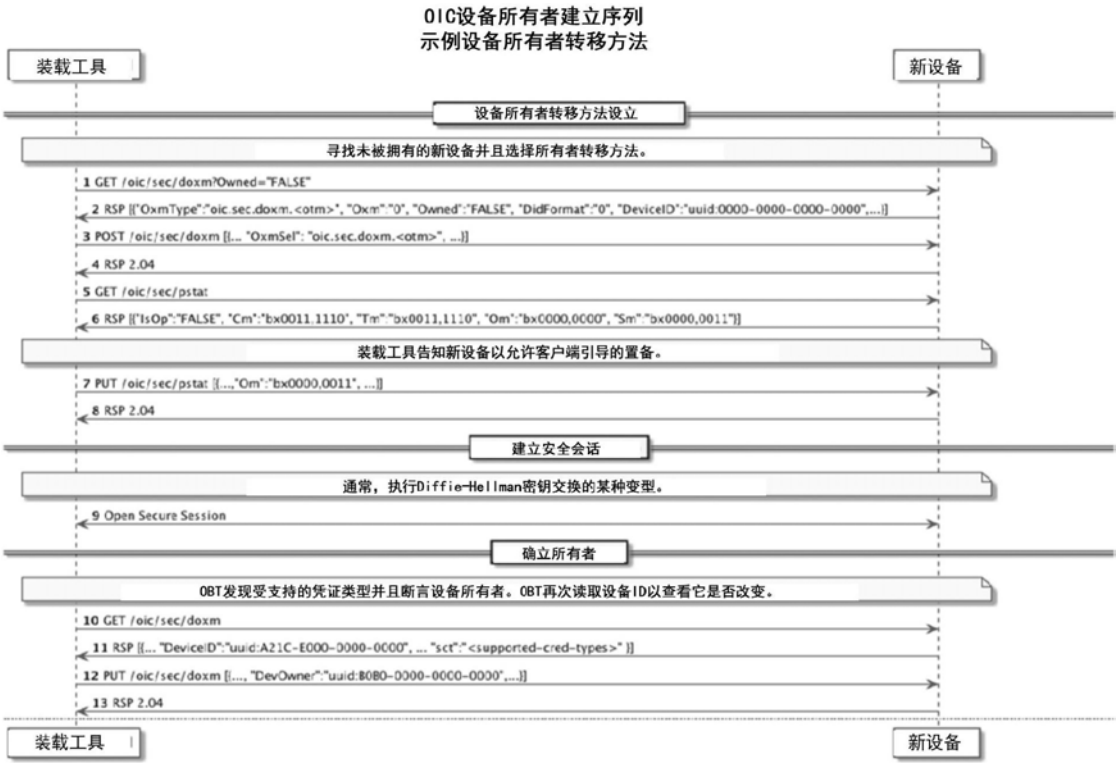
[0137] 如上所讨论的，在一些实施例中，在执行设备所有者转移方法中可以使用签署和MAC协议。以下的表6示出了在针对IoT设备执行设备所有者转移中使用的示例Intel®基于Sigma的Diffie-Hellman交换的高级视图。如表6中所解说的，交换所有者转移授权因子的组合，这些因子包括临近度PIN，加上新设备的受信执行环境配置的证明散列，加上使用EPID签署密钥对DH消息的签名。要理解，其他实施例不限于EPID签署。在表6之后的表7和8描述了如图2B中描述的此类设备所有者转移的装载序列的其他细节。

[0138] 表6

[0139]

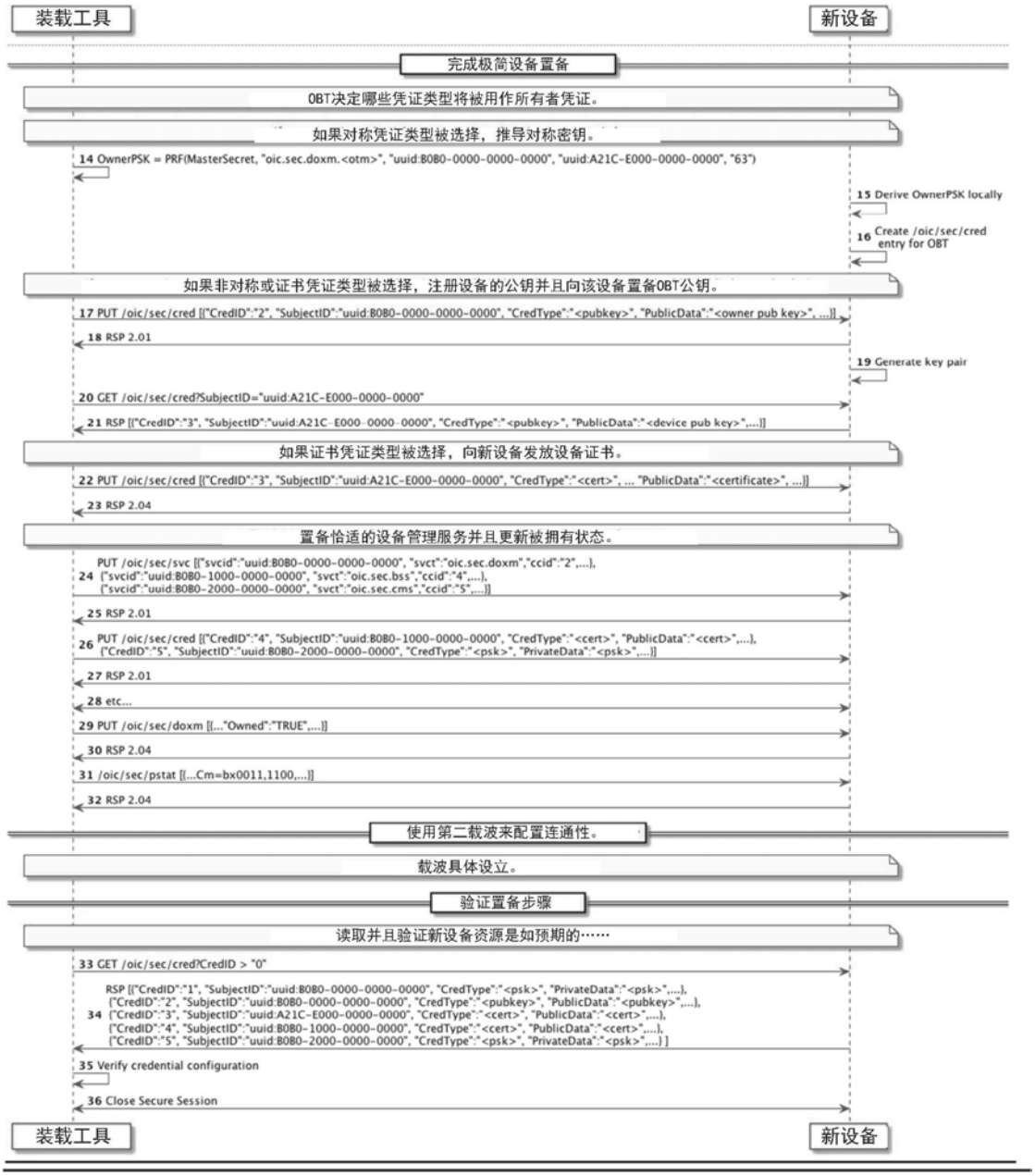
[0140] 表7

[0141]


OIC设备所有者建立序列
示例设备所有者转移方法
装载工具
新设备
设备所有者转移方法设立
寻找未被拥有的新设备并且选择所有者转移方法。
1 GET /oic/sec/doxm?Owned="FALSE"
2 RSP [{"OxmType":"oic.sec.doxm.<otm>", "Oxm":"0", "Owned":"FALSE", "DidFormat":"0", "DeviceID":"uuid:0000-0000-0000-0000",...}]
3 POST /oic/sec/doxm [{... "OxmSel": "oic.sec.doxm.<otm>", ...}]
4 RSP 2.04
5 GET /oic/sec/pstat
6 RSP [{"IsOp":"FALSE", "Cm":"bx0011,1110", "Tm":"bx0011,1110", "Om":"bx0000,0000", "Sm":"bx0000,0011"}]
装载工具告知新设备以允许客户端引导的置备。
7 PUT /oic/sec/pstat [{...,"Om":"bx0000,0011", ...}]
8 RSP 2.04
建立安全会话
通常，执行Diffie-Hellman密钥交换的某种变型。
9 Open Secure Session
确立所有者
OBT发现受支持的凭证类型并且断言设备所有者。OBT再次读取设备ID以查看它是否改变。
10 GET /oic/sec/doxm
11 RSP [{... "DeviceID":"uuid:A21C-E000-0000-0000", ... "sct":"<supported-cred-types>" }]
12 PUT /oic/sec/doxm [{..., "DevOwner":"uuid:B0B0-0000-0000-0000",...}]
13 RSP 2.04
装载工具
新设备

[0142] 表8

[0143]



[0144] 因而，在各实施例中，在IoT设备的设备所有者转移期间，网络分析器可以向所有者转移端点通知关于无线网络的可能的MITM攻击。可以使用可在IoT设备中在安全存储器中供应的制造商发出的令牌以及带外信道(诸如产品包装、QR码、IM、文本、电子邮件、CDROM、明信片或社交媒体)来传递令牌值。

[0145] 更具体地，令牌被输入到Diffie-Hellman密钥协商协议，其中安全DH端点也是安全存储端点。通过带外信道获得的令牌值的比较被安全地递送到安全存储端点，并且与被嵌入的令牌值作比较以确定设备所有权被确立。在一实施例中，TEE可以被用于安全地处理DH端点，保护令牌值，以及维护/更新设备所有者状态。

[0146] 在一些实施例中，IoT资源框架可以被用于使用另一IoT设备的原生消息收发协议向该另一IoT设备表示设备所有者转移协议和状态。

[0147] 各实施例实现对无线频谱分析仪的使用以在计算Diffie-Hellman密钥协商协议时向所有者转移端点通知可能的无线MITM攻击者。在一些实施例中，当制造商令牌通过带

外信道被传递到预期所有者时，该令牌可以可任选地被用来断言设备的所有权转移。

[0148] 现在参考图5，所示为可与多个实施例一起使用的示例系统的框图。如所见，系统900可以是智能电话或其他无线通信器或任何其他IoT设备。基带处理器905被配置成执行关于会从该系统传输或由该系统接收的通信信号的各种信号处理。进而，基带处理器905被耦合到应用处理器910，该应用处理器910可以是系统的主CPU，以执行除了诸如许多公知的社交媒体与多媒体应用的用户应用之外的OS以及其他系统软件。应用处理器910可以进一步被配置成为该设备执行各种其他计算操作。

[0149] 进而，应用处理器910可以耦合到用户接口/显示器920，例如，触摸屏显示器。此外，应用处理器910可以耦合到包括非易失性存储器(即闪存930)与系统存储器(即DRAM 935)的存储器系统。在一些实施例中，闪存930可包括安全部分932，其中可以存储秘密以及其他敏感信息。如进一步所见，应用处理器910也耦合到捕捉设备945，诸如可记录视频和/或静止图像的一个或多个图像捕捉设备。

[0150] 仍然参考图5，通用集成电路卡(UICC)940包括订户身份模块，其在一些实施例中包括存储安全用户信息的安全存储器942。系统900还可包括安全处理器950，该安全处理器950可实现如早先描述的TEE并且可以耦合到应用处理器910。此外，应用处理器910可实现诸如Intel®SGX等用于主存TEE的安全操作模式，如早先描述的。多个传感器925(包括一个或多个多轴加速计)可以耦合到应用处理器910以实现各种感测到的信息(诸如运动和其他环境信息)的输入。此外，可以使用一个或多个认证设备995来接收，例如用户生物计量输入以用于认证操作。

[0151] 如进一步所示出的，提供近场通信(NFC)非接触式接口960，其经由NFC天线965在NFC近场中通信。尽管图5中示出分离的天线，请理解在一些实现中，可以提供一根天线或不同组的天线以实现各种无线功能。

[0152] 功率管理集成电路(PMIC)915耦合到应用处理器910以执行平台级别功率管理。为此，PMIC915可以根据需要发出功率管理请求至应用处理器910以进入某些低功率状态。此外，基于平台约束，PMIC 915也可以控制系统900的其他组件的功率级别。

[0153] 为了实现诸如在一个或多个IoT网络中传送与接收通信，可以在基带处理器905与天线990之间耦合各种电路系统。具体而言，可以存在射频(RF)收发机970与无线局域网(WLAN)收发机975。一般而言，可以根据诸如3G或4G无线通信协议(诸如根据码分多址(CDMA)、全球移动通信系统(GSM)、长期演进(LTE)或其他协议)的给定的无线通信协议，使用RF收发机970接收并传送无线数据和呼叫。此外，当在配对过程中要使用上下文信息时，可以存在GPS传感器980，并且位置信息被提供给安全处理器950以如本文所述使用。也可以提供诸如无线电信号(例如，AM/FM与其他信号)的接收与传送的其他无线通信。此外，经由WLAN收发机975，也可以实现诸如根据Bluetooth™或IEEE 802.11标准的局部无线通信。

[0154] 现在参照图6，所示为根据本发明的另一实施例的系统的框图。如图6所示，多处理器系统1000是点对点互连系统(诸如服务器系统)，且包括经由点对点互连1050耦合的第一处理器1070和第二处理器1080。如图6所示，处理器1070与1080中的每一个处理器可以是包括第一与第二处理器核(即，处理器核1074a与1074b以及处理器核1084a和1084b)的诸如SoC的多核处理器，尽管这些处理器中可能存在多得多的核。另外，处理器1070和1080各自可包括用于执行诸如证明、IoT网络装载等安全操作的安全引擎1075和1085。

[0155] 仍参考图6,第一处理器1070还包括存储器控制器中枢(MCH)1072和点对点(P-P)接口1076和1078。类似地,第二处理器1080包括MCH 1082和P-P接口1086与1088。如图6所示,MCH' 1072与1082将处理器耦合到相应的存储器,即存储器1032与存储器1034,它们可以是本地附连到相应的处理器的主存储器(例如,DRAM)的部分。第一处理器1070与第二处理器1080可以分别经由P-P互连1052与1054耦合到芯片组1090。如图6中所示,芯片组1090包括P-P接口1094和1098。

[0156] 此外,芯片组1090包括通过P-P互连1039将芯片组1090与高性能图形引擎1038耦合的接口1092。进而,芯片组1090可以经由接口1096被耦合到第一总线1016。如图6所示,各种输入/输出(I/O)设备1014以及总线桥接器1018可耦合到第一总线1016,总线桥接器1018将第一总线1016耦合到第二总线1020。各个设备可以耦合到第二总线1020,包括,例如,键盘/鼠标1022、通信设备1026和数据存储单元1028(诸如非易失性存储器或其他大容量存储设备)。如所见,在一个实施例中数据存储单元1028可包括代码1030。如进一步看到的,数据存储单元1028还包括用于存储要保护的敏感信息的可信存储1029。此外,音频I/O1024可以被耦合到第二总线1020。

[0157] 各实施例可以在其中IoT设备可包括可穿戴设备或其他小形状因子的IoT设备的环境中使用。现在参考图7,示出了根据另一实施例的可穿戴模块1300的框图。在一个特定实现中,模块1300可以是Intel®Curie™模块,其包括被适配到能够被实现为可穿戴设备的全部或一部分的单个小型模块中的多个组件。如所见,模块1300包括核1310(当然,在其他实施例中,可存在一个以上的核)。此类核可以是相对低复杂度的有序核,诸如基于Intel Architecture®Quark™设计。在一些实施例中,核1310可以实现TEE,如本文所述。核1310耦合到包括传感器中枢1320的各个组件,其可以被配置成与多个传感器1380交互,诸如一个或多个生物测定、运动环境或其他传感器。存在功率递送电路1330以及非易失性存储器1340。在一实施例中,这一电路可包括可充电电池以及充电电路,它们在一个实施例中可以无线接收充电功率。可存在诸如与USB/SPI/I^2C/GPIO协议中的一者或多者兼容的一个或多个接口的一个或多个输入/输出(IO)接口1350。另外,存在无线收发机1390(其可以是蓝牙™低能量或其他短程无线收发机)以实现如本文所述的无线通信。要理解,在不同实现中,可穿戴模块可采取许多其他形式。

[0158] 以下示例关于进一步的实施例。

[0159] 在示例1中,一种系统包括:第一设备,其具有至少一个处理器和安全存储器并且具有第一TEE;以及在第一网络内耦合至第一设备的装载系统。该装载系统可包括第二TEE,并且可接收将第一设备的所有权转移到新所有者的请求,从频谱分析仪接收关于第一网络内的无线信号信息的通知信息,以及执行装载系统与第一设备之间的原生通信协议以传达所有权信息,从而执行到新所有者的所有权转移,以致使第一设备将所有权信息存储在第一设备的存储器中。

[0160] 在示例2中,该装载系统用于从第一设备的制造商接收第一令牌并且将第一令牌提供给第一设备。

[0161] 在示例3中,第一设备包括IoT设备并且用于将第一令牌与所存储的令牌作比较,并且至少部分地基于该比较来更新第一设备的所有权指示符以指示第一设备被拥有。

[0162] 在示例4中,第一设备要以未被拥有的状态被引入第一网络中。

[0163] 在示例5中，该原生通信协议包括用于实现非所有者转移通信的预定通信协议。

[0164] 在示例6中，该原生通信协议包括装载系统与第一设备之间的带内通信。

[0165] 在示例7中，第一设备用于自断言它要被新所有者拥有，而不依赖于装载系统。

[0166] 在示例8中，该原生通信协议包括装载系统与第一设备之间的Diffie-Hellmann会话的建立以建立所有者预先共享的密钥。

[0167] 在示例9中，该原生通信协议包括要使用所有者预先共享的密钥来建立的安全会话。

[0168] 在示例10中，根据该原生通信协议，装载系统用于：向第一设备指令关于所有权转移的置备技术；计算所有者预先共享的密钥并且将计算所得的所有者预先共享的密钥与接收到的预先共享的密钥作比较，使用所有者预先共享的密钥在装载系统与第一设备之间建立安全置备信道，以及经由该安全置备信道向第一设备置备一个或多个资源。

[0169] 在示例11中，该原生通信协议包括用于执行所有权转移的共享PIN过程。

[0170] 在示例12中，第一设备用于在该安全会话期间自断言由新所有者拥有的所有权。

[0171] 在示例13中，装载系统用于基于无线信号信息来确定潜在攻击者是否在第一网络的无线电范围内，以及响应于潜在攻击者在无线电范围内的确定来操纵装载系统和第一设备的信号强度，以限制装载系统和第一设备的发射范围。

[0172] 在示例14中，一种方法包括：在第一网络的装载系统中，接收要将具有受信执行环境的第一设备的所有权转移到新所有者的请求；在该装载系统中，从频谱分析仪接收关于第一网络内的无线信号信息的通知信息；基于该无线信号信息来确定潜在攻击者是否在第一网络的无线电范围内；响应于确定潜在攻击者在无线电范围内，操纵装载系统和第一设备的信号强度以限制装载系统和第一设备的发射范围；以及在装载系统与第一设备之间执行原生通信协议以传达所有权信息，以便于执行到新所有者的所有权转移，以使得第一设备能够将所有权信息存储在第一设备的存储器中。

[0173] 在示例15中，该方法进一步包括：在装载系统中，经由带外信道从第一设备的制造商接收第一令牌；以及经由安全信道将第一令牌发送到第一设备。

[0174] 在示例16中，响应于接收到第一令牌，第一设备用于将第一令牌与存在于第一设备的安全存储器的所存储的令牌作比较，所存储的令牌被第一设备的制造商存储，并且至少部分地基于该比较来更新所有者状态。

[0175] 在示例17中，该方法进一步包括响应于无线电范围确定来阻止所有权信息传递。

[0176] 在示例18中，一种方法包括：在IoT网络的装载系统与要被引入IoT网络的设备之间建立第一安全会话，该设备在引入时处于未被拥有状态；在第一安全会话中计算该设备中的所有者PSK，将该所有者PSK存储在该设备的存储器中，以及之后终止该第一安全会话；使用该所有者PSK在装载系统与该设备之间建立第二安全会话；以及响应于成功建立第二安全会话，自治地将该设备的所有权状态更新为被拥有状态。

[0177] 在示例19中，该方法还包括：从装载系统接收要操纵该设备的信号强度的命令；以及响应于接收到该命令，降低第一安全会话的无线信道的信号电平以限制该设备的发射范围。

[0178] 在示例20中，该方法还包括：从装载系统接收第一令牌，第一令牌在装载系统中经由带外信道从该设备的制造商接收；将第一令牌与存储在该设备的安全存储器中的所存储

的令牌作比较，所存储的令牌由该设备的制造商存储；以及至少部分地基于该比较来更新该设备的所有权状态。

[0179] 在另一示例中，一种包括指令的计算机可读介质要执行上述示例中的任一项的方法。

[0180] 在另一示例中，一种包括数据的计算机可读介质要由至少一个机器使用以制造至少一个集成电路来执行上述示例中的任一项的方法。

[0181] 在另一示例中，设备包括用于执行上述示例中的任一项的方法的装置。

[0182] 在示例21中，一种系统包括：用于接收要将具有受信执行环境的第一设备的所有权转移到新所有者的请求的装置；用于从频谱分析仪接收关于网络内的无线信号信息的通知信息的装置；用于基于该无线信号信息来确定潜在攻击者是否在第一网络的无线电范围内的装置；用于响应于确定潜在攻击者在无线电范围内来操纵该系统和第一设备的信号强度以限制该系统和第一设备的发射范围的装置；以及用于在该系统与第一设备之间执行原生通信协议以传达所有权信息，以便于执行到新所有者的所有权转移，以使得第一设备能够将所有权信息存储在第一设备的存储器中的装置。

[0183] 在示例22中，该系统进一步包括：用于经由带外信道从第一设备的制造商接收第一令牌的装置；以及用于经由安全信道将第一令牌发送到第一设备的装置。

[0184] 在示例23中，该系统进一步包括用于响应于无线电范围确定来阻止所有权信息传达的装置。

[0185] 应理解，上述示例的各种组合是可能的。

[0186] 实施例可以被用于许多不同类型的系统中。例如，在一个实施例中，可以将通信设备布置为用于执行本文所述的各种方法与技术。当然，本发明的范围不限于通信设备，相反，其他实施例可以涉及用于处理指令的其他类型的装置，或一个或多个机器可读介质，该机器可读介质包括指令，响应于在计算设备上执行这些指令，这些指令使该设备执行本文所述的方法与技术中的一个或多个。

[0187] 实施例可以实现在代码中，并且可以存储在非暂态存储介质中，该非暂态存储介质具有存储于其上的指令，该指令可以被用来对系统编程以执行指令。实施例还可以实现在数据中，并且可以存储在非暂态存储介质中，该非暂态存储介质如果被至少一个机器使用，将使得至少一个机器制造至少一个集成电路以执行一个或多个操作。存储介质可以包括但不限于，任何类型的盘，包括软盘、光盘、固态驱动器(SSD)、紧致盘只读存储器(CD-ROM)、紧致盘可重写(CD-RW)以及磁光盘；半导体器件，诸如，只读存储器(ROM)、诸如动态随机存取存储器(DRAM)与静态随机存取存储器(SRAM)的随机存取存储器(RAM)、可擦除可编程只读存储器(EPROM)、闪存、电可擦除可编程只读存储器(EEPROM)；磁卡或光卡；或适用于存储电子指令的任何其他类型的介质。

[0188] 虽然已参照有限数量的实施例描述了本发明，但是本领域技术人员将从中领会很多修改和变型。所附权利要求旨在涵盖落入本发明的真实精神与范围的所有此类修改与变型。

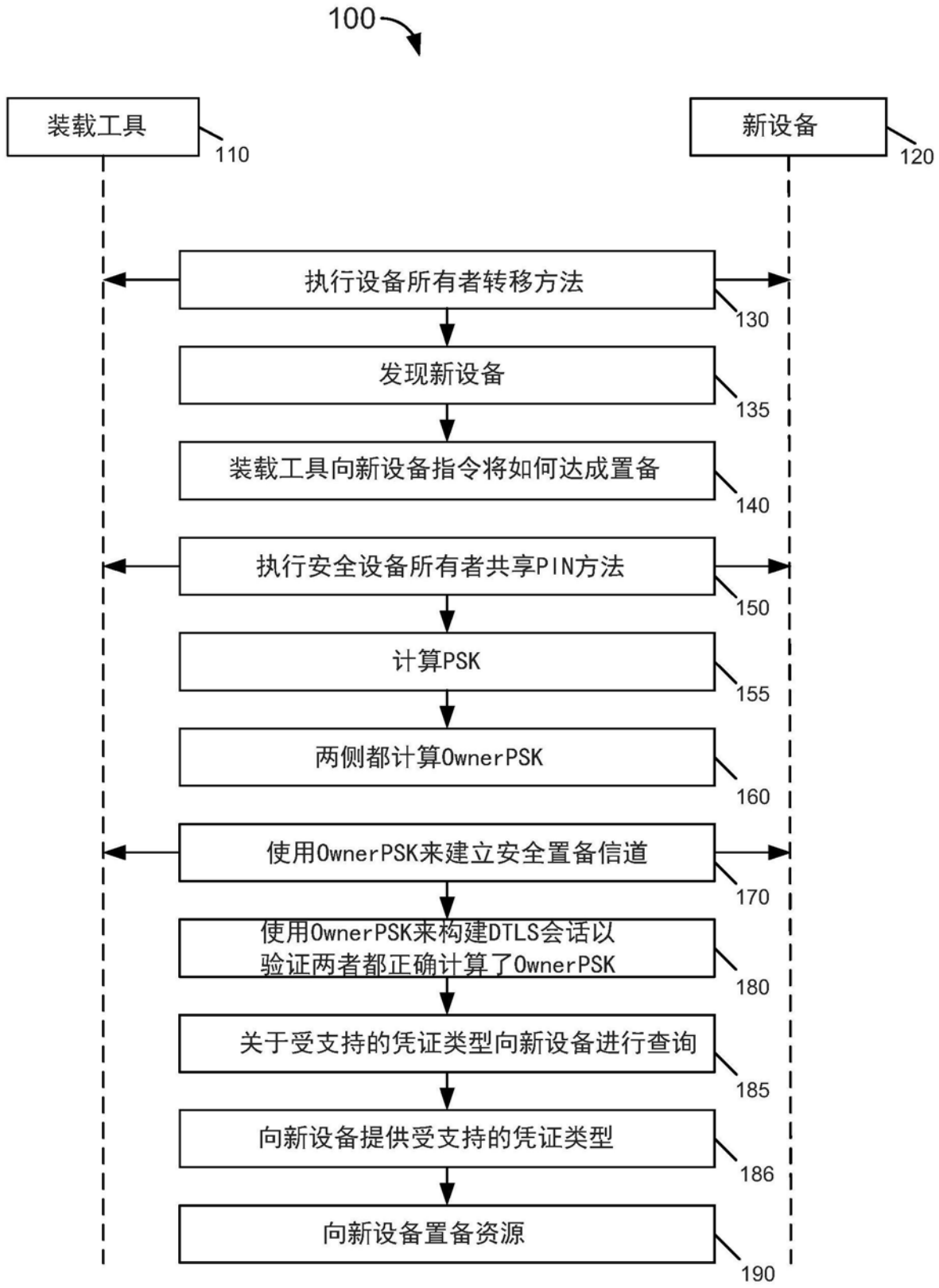

100
装载工具
110
新设备
120
执行设备所有者转移方法
130
发现新设备
135
装载工具向新设备指令将如何达成置备
140
执行安全设备所有者共享PIN方法
150
计算PSK
155
两侧都计算OwnerPSK
160
使用OwnerPSK来建立安全置备信道
170
使用OwnerPSK来构建DTLS会话以
验证两者都正确计算了OwnerPSK
180
关于受支持的凭证类型向新设备进行查询
185
向新设备提供受支持的凭证类型
186
向新设备置备资源
190

图1

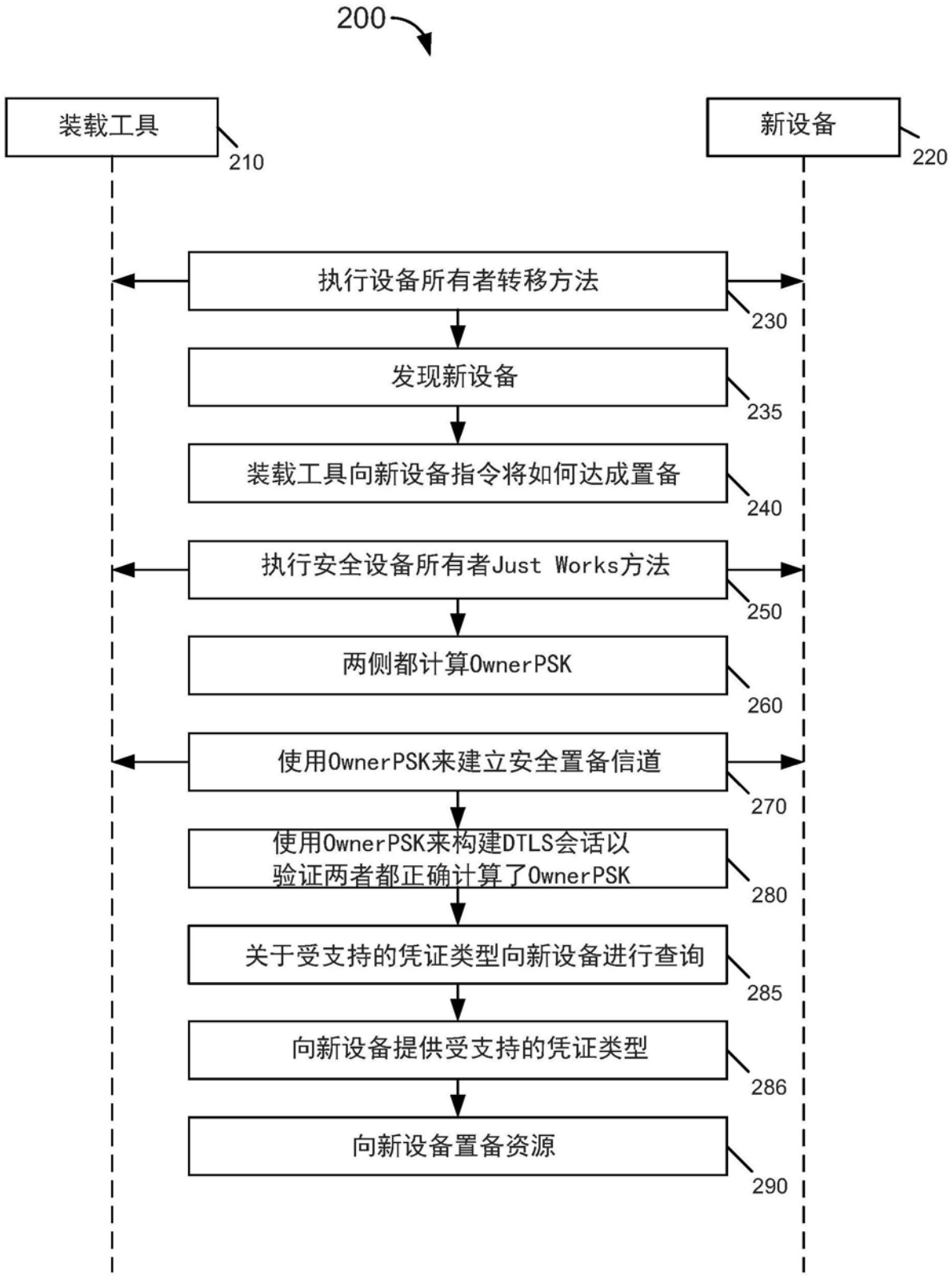

200
装载工具
210
新设备
220
执行设备所有者转移方法
230
发现新设备
235
装载工具向新设备指令将如何达成置备
240
执行安全设备所有者Just Works方法
250
两侧都计算OwnerPSK
260
使用OwnerPSK来建立安全置备信道
270
使用OwnerPSK来构建DTLS会话以
验证两者都正确计算了OwnerPSK
280
关于受支持的凭证类型向新设备进行查询
285
向新设备提供受支持的凭证类型
286
向新设备置备资源
290

图2A

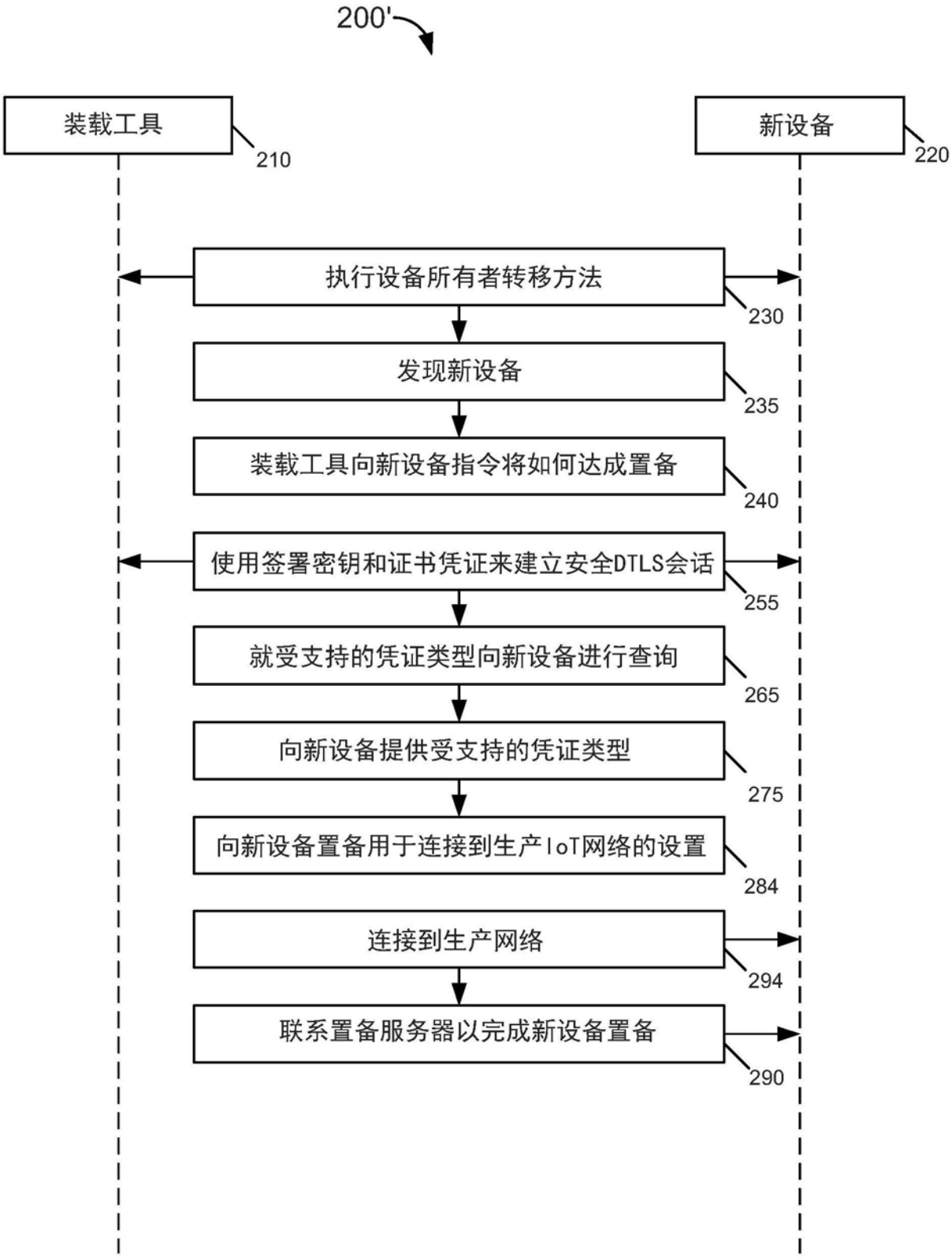

200'
装载工具
210
新设备
220
执行设备所有者转移方法
230
发现新设备
235
装载工具向新设备指令将如何达成置备
240
使用签署密钥和证书凭证来建立安全DTLS会话
255
就受支持的凭证类型向新设备进行查询
265
向新设备提供受支持的凭证类型
275
向新设备置备用于连接到生产IoT网络的设置
284
连接到生产网络
294
联系置备服务器以完成新设备置备
290

图2B

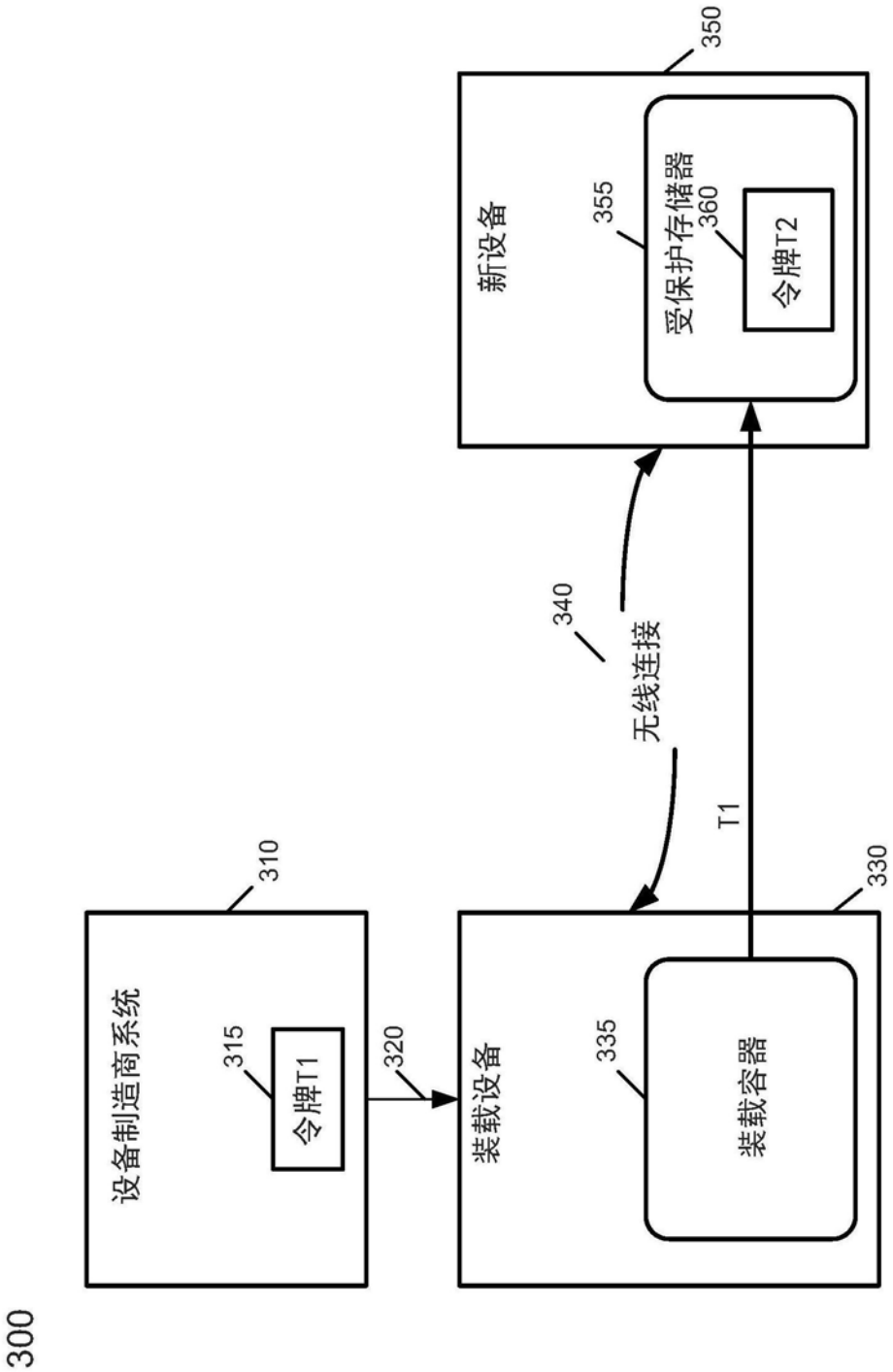

300
设备制造商系统
310
315
令牌T1
320
装载设备
330
335
装载容器
T1
340
无线连接
新设备
350
355
受保护存储器
360
令牌T2

图3

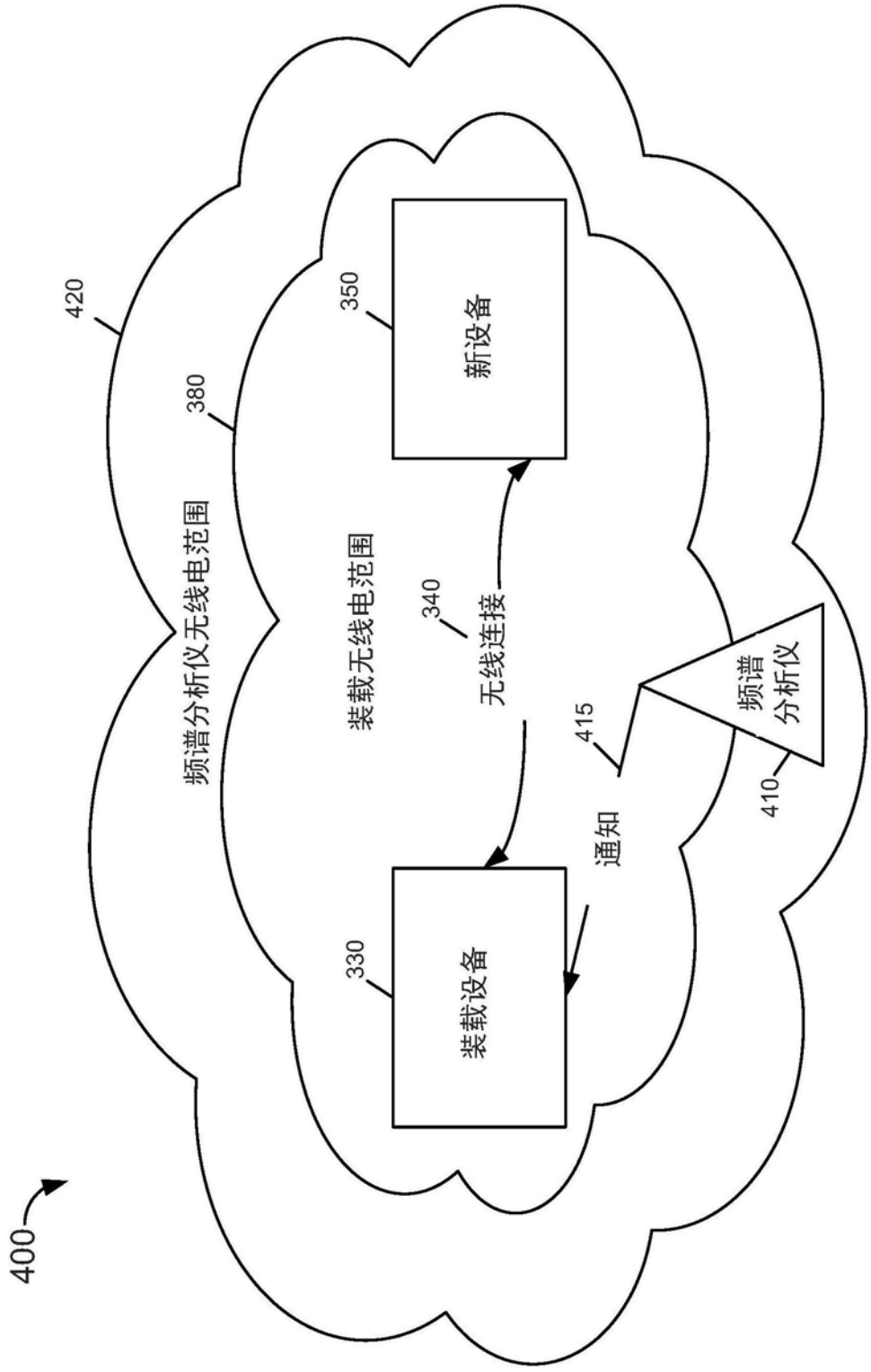

400
420
频谱分析仪无线电范围
380
装载无线电范围
350
新设备
340
无线连接
330
装载设备
通知
415
频谱
分析仪
410

图4

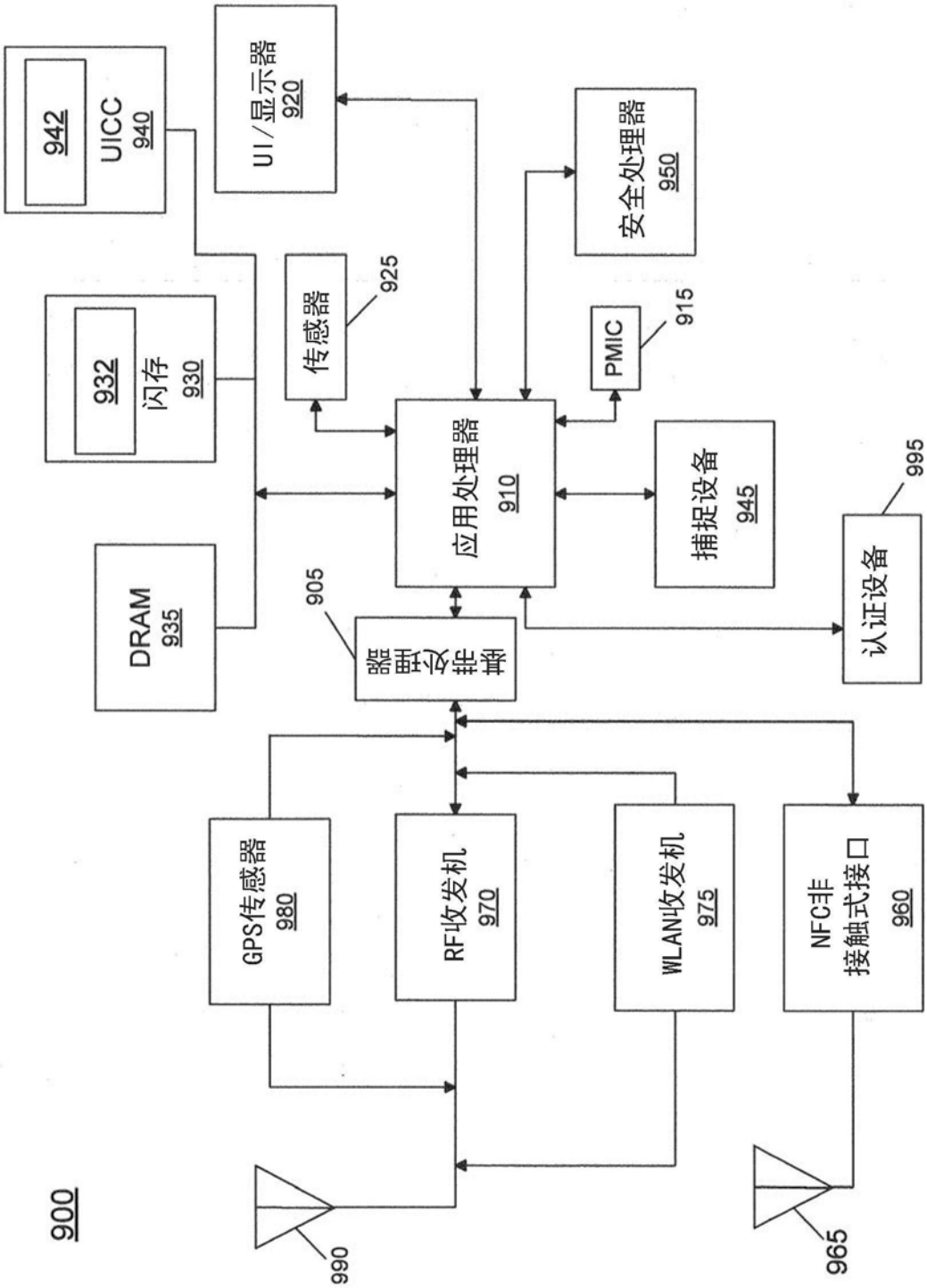

900
UICC 940
942
UI/显示器 920
安全处理器 950
传感器 925
PMIC 915
闪存 930
932
应用处理器 910
捕捉设备 945
995
认证设备
DRAM 935
905
GPS传感器 980
RF收发机 970
WLAN收发机 975
NFC非接触式接口 960
990
965

图5

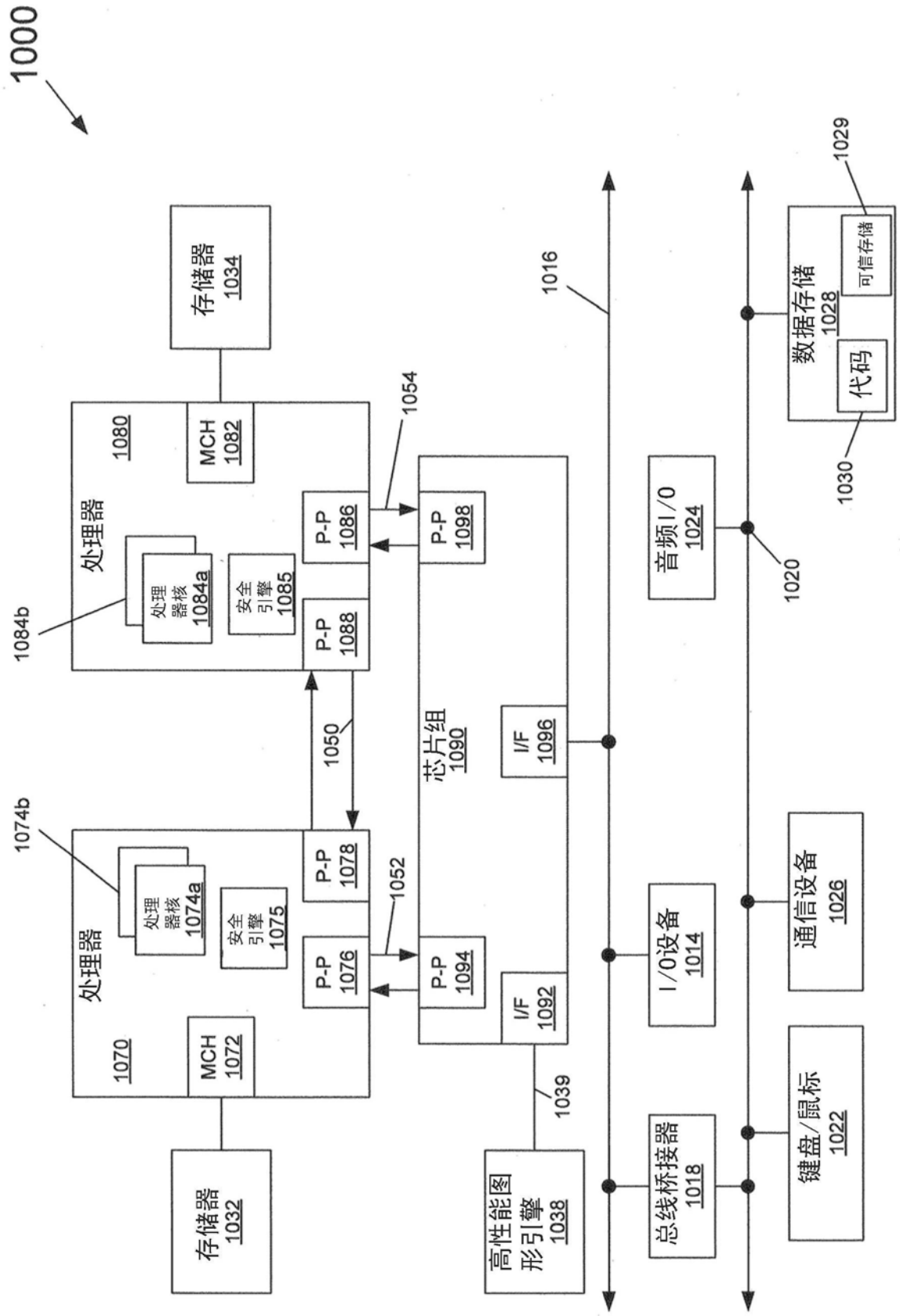

1000
存储器
1034
MCH
1082
处理器
1080
处理器核
1084a
安全引擎
1085
P-P
1086
P-P
1088
1084b
1054
P-P
1098
芯片组
1090
1050
I/F
1096
1016
1074b
处理器
1070
处理器核
1074a
安全引擎
1075
P-P
1078
P-P
1076
1052
P-P
1094
I/F
1092
MCH
1072
存储器
1032
1039
高性能图形引擎
1038
音频I/O
1024
1020
数据存储
1028
可信存储
1029
代码
1030
I/O设备
1014
通信设备
1026
总线桥接器
1018
键盘/鼠标
1022

图6

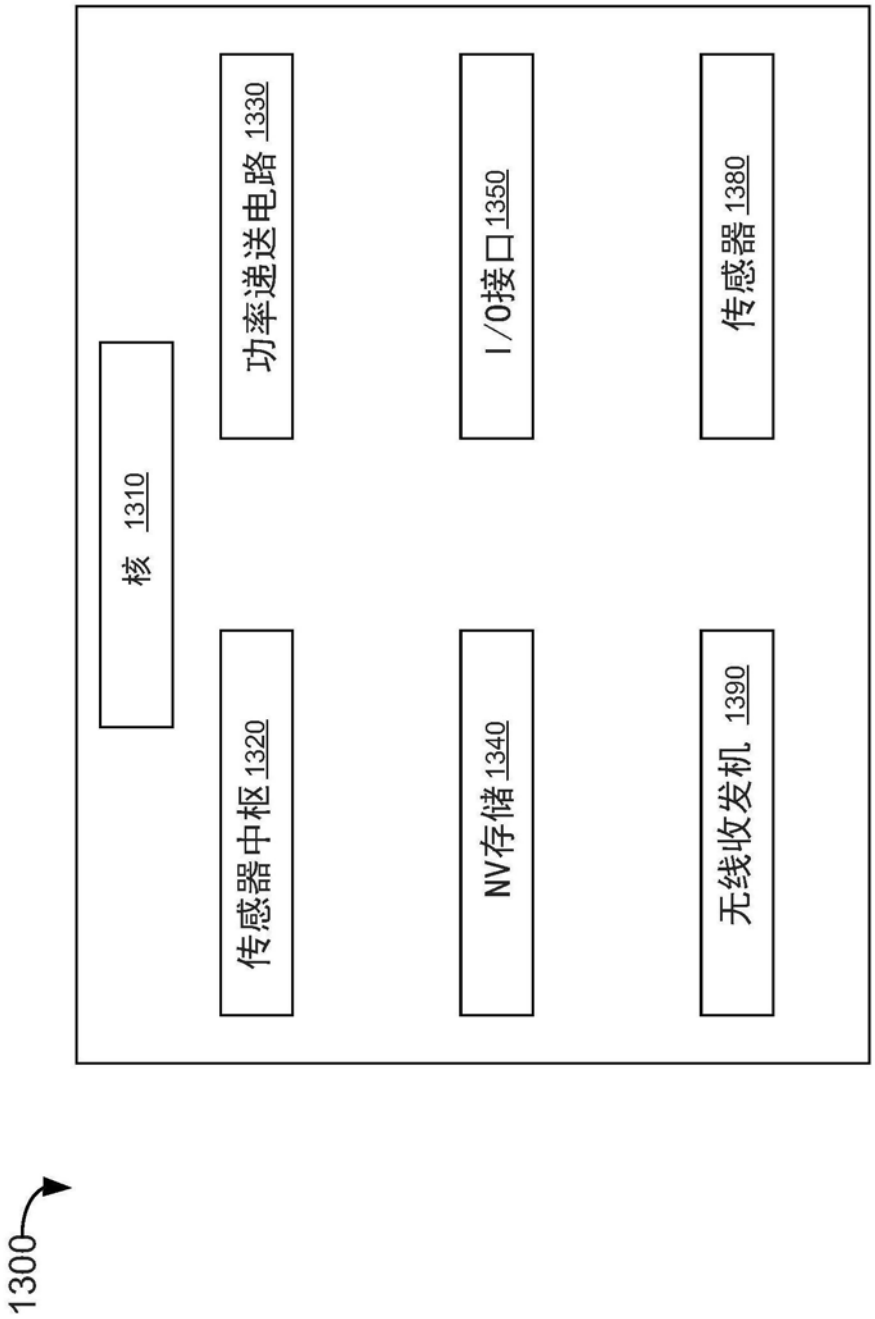

核 1310
功率递送电路 1330
I/O接口 1350
传感器 1380
传感器中枢 1320
NV存储 1340
无线收发机 1390
1300

图7