(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116848822 A
(43)申请公布日 2023.10.03

(21)申请号 202280015077.9
(22)申请日 2022.02.09
(30)优先权数据
21157226.8 2021.02.15 EP
(85)PCT国际申请进入国家阶段日
2023.08.15
(86)PCT国际申请的申请数据
PCT/EP2022/053096 2022.02.09
(87)PCT国际申请的公布数据
WO2022/171657 EN 2022.08.18
(71)申请人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬
(72)发明人 J·A·C·伯恩森
(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 孟杰雄
(51)Int.Cl.
H04L 9/40(2006.01)

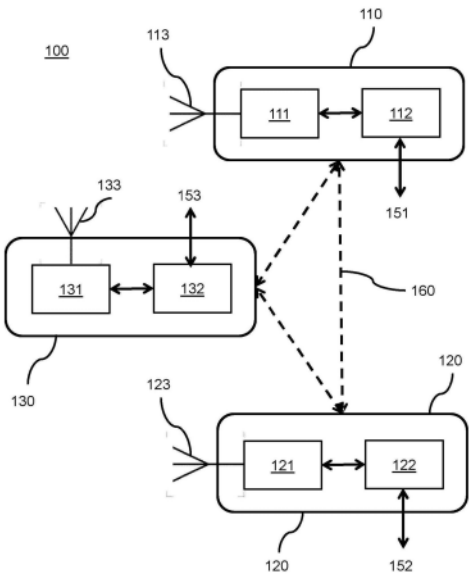
权利要求书3页 说明书17页 附图2页

(54)发明名称

用于提供针对通信的安全水平的方法和设备

(57)摘要

描述了根据安全协议在物理信道上在第一设备与第二设备之间建立安全通信的设备(110、120)和方法。所述协议在所述第一设备中建立第一完整性数据,并且在所述第二设备中建立第二完整性数据。所述协议具有至少两个安全水平。所应用的安全水平是可基于经由物理信道传输的分级信息选择的。有利地,指示如在第一设备(110)和第二设备(120)中的至少一个设备中最低要求的最小安全水平的分级指示器经由物理信道传输,同时基于所述完整性数据提供所述分级指示器的完整性保护。从而,可以防止降级所述安全水平的由另一设备(130)进行的中间人攻击。



CN 116848822 A

1.一种根据安全协议在物理信道上为第一设备与第二设备之间的通信建立安全水平的方法,所述安全协议提供:

-在所述第一设备中建立第一完整性数据,并且在所述第二设备中建立第二完整性数据;以及

-至少两个安全水平,所述安全水平是能基于经由所述物理信道传输的分级信息选择的,其中,根据所述第一安全水平的所述安全协议不阻止基于所述第一设备的消息中的重复数据跨网络中的多个通信会话跟踪所述第一设备,并且

根据所述第二安全水平的所述安全协议要求避免或修改所述重复数据以防止跟踪,

所述方法包括:

-经由所述物理信道传输分级指示器,所述分级指示器指示在所述第一设备和所述第二设备中的至少一个设备中最低要求的最小安全水平;并且

-基于所述完整性数据来提供对所述分级指示器的完整性保护,

-当由所述分级指示器如此指示时,应用所述跟踪防止。

2.一种设备,所述设备是第一设备(110),所述第一设备适于根据安全协议在物理信道上为所述第一设备与第二设备之间的通信建立安全水平,所述安全协议提供:

-在所述第一设备中建立第一完整性数据,并且在所述第二设备中建立第二完整性数据,以及

-至少两个安全水平,所述安全水平是能基于经由所述物理信道传输的分级信息选择的,其中,根据所述第一安全水平的所述安全协议不阻止基于所述第一设备的消息中的重复数据跨网络中的多个通信会话跟踪所述第一设备,并且

根据所述第二安全水平的所述安全协议要求避免或修改所述重复数据以防止跟踪,

所述设备包括处理器(112),所述处理器被布置用于:

-经由所述物理信道发送或接收分级指示器,所述分级指示器指示在所述第一设备和所述第二设备中的至少一个设备中最低要求的最小安全水平;

-当发送时,包括针对基于所述完整性数据的所述分级指示器的保护数据;

-当接收时,基于所述完整性数据来验证所述保护数据;并且

-至少对所述第一设备与所述第二设备之间的通信应用所述最小安全水平,并且

-当由所述分级指示器如此指示时,应用所述跟踪防止。

3.根据权利要求2所述的设备,其中,所述安全协议基于设备供应协议,所述设备供应协议还要求配置器,所述配置器适于在无线网络中建立所述第一设备与所述第二设备之间的通信,

所述配置器被布置用于:

-将所述分级指示器插入在连接器消息中;并且

-向所述第一设备发送所述连接器消息,并且

所述第一设备中的所述处理器(112)被布置用于:

-接收所述连接器消息;并且

-从所述连接器消息中检索所述分级指示器。

4.根据权利要求3所述的设备,其中,

根据所述第一安全水平的所述安全协议基于私钥材料和公钥材料来确定所述第一设

备和所述第二设备两者中的成对主密钥,所述成对主密钥被用于确定所述第一设备与所述第二设备之间的加密通信的会话密钥,并且

根据所述第二安全水平的所述安全协议要求确定涉及短暂Diffie-Hellman密钥对的所述成对主密钥,并且

所述处理器(112)被布置为当由所述分级指示器如此指示时,应用所述第二安全水平。

5.根据权利要求2-4中的任一项所述的设备,其中,在所述安全协议中,所述分级信息的至少一部分缺乏完整性保护。

6.根据权利要求2所述的设备,其中,所述安全协议包括设置协议,所述设置协议包括:

-从证书颁发机构获得证书;

-使用所述证书来提供安全参数,

-经由设置参数将所述安全参数传输到所述设备,

其中,所述证书包括所述分级指示器,所述分级指示器指示对所述安全参数的约束,

并且所述处理器(112)被布置用于:

-从所述证书中检索所述分级指示器;

-接收所述设置消息;并且

-基于所述设置消息和对所述安全参数的所述约束来确定所述安全水平。

7.根据权利要求6所述的设备,其中,所述安全协议提供对密码安全参数的设置,所述密码安全参数包括以下各项中的一项或多项:

-要使用的密码算法;

-要使用的密钥大小;

-要使用的密码散列算法;

-要使用的所述协议的最低版本;

-要使用的所述协议的选项。

8.根据权利要求6或7所述的设备,其中,所述第一设备是客户端设备,并且所述第二设备是服务器设备,并且所述分级指示器指示对要求使用证书进行客户端侧认证的客户端约束,

并且所述处理器(112)被布置用于:

-从所述证书中检索所述客户端约束;

-接收所述设置消息;并且

-基于所述客户端约束来应用客户端侧认证。

9.根据权利要求3所述的设备,其中,所述安全协议基于在[DPP]中定义的用于配置Wi-Fi设备的所述设备供应协议,并且其中,所述连接器消息基于在通过插入所述分级指示器修改的所述设备供应协议中定义的所述连接器;

其中,所述处理器(112)适于接收经修改的连接器。

10.根据权利要求2至4中的任一项所述的设备,其中,所述安全协议基于在[DPP]中定义的用于配置Wi-Fi设备的所述设备供应协议,并且其中,所述连接器消息是基于所述连接器的重新配置连接器,所述重新配置连接器被生成用于在所述设备供应协议中定义的重新配置认证请求消息中使用;

所述配置器将所述分级指示器插入在所述重新配置连接器中,所述分级指示器指示防

止约束,所述防止约束指示想要被重新配置的设备能够或应该使用设备跟踪防止,

并且所述处理器(112)被布置用于:

-从经修改的连接器中检索所述防止约束;

-在基于所述防止约束的重新配置期间应用跟踪防止。

11.根据权利要求2-10中的任一项所述的设备,其中,所述物理信道是无线通信信道。

12.根据权利要求2-11中的任一项所述的设备,其中,所述完整性数据被应用于提供对经由所述物理信道传输的消息的完整性保护。

13.一种用于在设备(110)中使用的方法,所述方法根据安全协议在物理信道上为所述设备与另一设备(120)之间的通信建立安全水平,所述安全协议提供:

-在所述设备中建立第一完整性数据,并且在所述另一设备中建立第二完整性数据,以及

-至少两个安全水平,所述安全水平是能基于经由所述物理信道传输的分级信息选择的,其中,根据所述第一安全水平的所述安全协议不阻止基于所述第一设备的消息中的重复数据跨网络中的多个通信会话跟踪所述第一设备,并且

根据所述第二安全水平的所述安全协议要求避免或修改所述重复数据以防止跟踪,

所述方法被布置用于:

-经由所述物理信道发送或接收分级指示器,所述分级指示器指示在所述设备和所述另一设备中的至少一个设备中最低要求的最小安全水平;

-当发送时,包括针对基于所述完整性数据的所述分级指示器的保护数据;

-当接收时,基于所述完整性数据来验证所述保护数据;并且

-至少对所述设备与所述另一设备之间的通信应用所述最小安全水平,

-当由所述分级指示器如此指示时,应用所述跟踪防止。

14.一种能从网络下载和/或被存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品,所述产品包括用于当在计算机上运行时实施根据权利要求1或13中的任一项所述的方法的程序代码指令。

用于提供针对通信的安全水平的方法和设备

技术领域

[0001] 本发明涉及一种用于根据安全协议在物理信道上建立针对第一设备与第二设备之间的通信的安全水平的方法和设备。

[0002] 本发明涉及无线或有线数据通信的安全领域,并且更特别地提供应用安全协议的设备和方法。安全协议在第一设备中建立第一完整性数据,并且在第二设备中建立第二完整性数据。完整性数据可以提供经由物理信道传输的消息的完整性保护。安全协议可以提供各种安全水平,安全水平例如定义了至少一个特定的安全措施、密码算法、安全选项或密钥长度。

背景技术

[0003] 设备可以安全地连接到无线网络,例如根据设备供应协议(DPP,参见[DPP]),该协议是用于使用DPP配置器设备配置Wi-Fi设备以便访问Wi-Fi接入点(AP)的协议。试图获得访问权的设备被称为DPP登记者(Enrolle)。当设备已经由DPP配置时,它已从DPP配置器接收到DPP配置对象。DPP配置对象包含所谓的连接器或DPP连接器。连接器由DPP配置器签名。连接器包含属于设备的公钥、网络访问密钥、netAccessKey或NAK。NAK存在于连接器的透明区域中。连接器中的透明区域中可能存在其他信息,例如期满时间戳。DPP配置对象未签名,因此它缺少完整性保护。然而,在其中它被发送给DPP登记者的消息,即DPP配置响应消息,由DPP配置器与DPP登记者之间在前面的DPP认证协议中协商的对称密钥进行完整性保护。应注意,在本申请中,缩写词DPP意指DPP的任何版本,例如DPP R1、DPP R2和任何后继版本。

[0004] 鉴于连接设备数目的增加,存在对安全的兴趣的增长,例如对隐私和针对第三方的跟踪的保护。跟踪意指跨网络中的多个通信会话跟随设备的位置,例如基于设备的消息中的重复数据。文档WO2020043634A1[2018PF00508]描述了一种升级的安全协议,其具有提供针对所述跟踪的保护的附加的安全选项。

[0005] 因此,现有的安全协议可以利用至少一个增强的安全水平进行升级。对于与现有设备的交互,通常还支持这样的协议的早期版本。所应用的安全水平,例如待使用的安全协议的版本或选项,可以使用分级信息来协商,该分级信息在建立通信期间经由设备之间的物理信道传输。分级信息例如可以是设备支持协议的特定版本或安全选项的明确指示。分级信息也可以由其他协议数据隐含,例如,如果支持多个密钥长度,则通过包括特定长度的密钥。通过交换所述分级信息,确定所应用的安全水平。然而,这样的消息可能由也在物理信道上操作的设备拦截和修改,这被称为“中间人”攻击(MitM)。由于分级信息的所述操纵,可以建立低于预期的安全水平,这可以被称为安全水平的“降级”。

发明内容

[0006] 本发明的目的是提供用于防止安全水平的降级的方法和设备,例如经由所述MitM,以用于减轻上文所提到的安全问题中的至少一个。出于该目的,提供了如权利要求书中定义的设备和方法。根据本发明的方面,如权利要求1中所定义的,提供了一种根据安全

协议在物理信道上为第一设备与第二设备之间的通信建立安全水平的方法。根据本发明的其他方面,提供了如独立权利要求中所定义的设备和方法。

[0007] 所述安全协议可以在所述第一设备中第一完整性数据,并且在所述第二设备中建立第二完整性数据。所述完整性数据可以用于提供经由所述物理信道传输的消息的完整性保护。例如,所述第一完整性数据可以是可以存储在所述第一设备中的第二设备的公钥,而所述第二完整性数据可以是由所述第二设备使用对应私钥设置的签名。所述第一完整性数据也可以是由第三方提供给所述第一设备的连接器或证书的签名。

[0008] 所述安全协议可以提供至少两个安全水平,所述安全水平是可基于分级信息选择的,例如基本安全水平和至少一个升级的安全水平。要应用的实际安全水平是基于经由所述物理信道的分级信息来确定的。所述分级信息经由所述物理信道传输,并且可以是一个或多个协议消息的一部分,要么显式要么隐式,或者可以体现在交换的单独消息中。在本文档中,任何包含显式或隐式分级信息的消息可以称为分级消息。分级消息经由所述物理信道传输。因此,分级信息意指适合于建立设备可以提供的一个或多个安全等级,并在设备之间协商用于通信、隐私保护、完整性保护、认证、访问网络等的等级的任何数据。例如,分级信息可以包含由所述设备支持的安全协议的版本指示器。特定的版本号可以指示如由针对该版本的协议规范指定的其他设备可以选择的安全选项的范围。

[0009] 方法和设备被布置为经由所述物理信道传输分级指示器,该分级指示器指示在第一和第二设备中的至少一个中最低要求的最小安全水平。此外,设备和方法基于所述完整性数据提供所述分级指示器的完整性保护。所述分级指示器可以经由所述物理信道或经由不同信道单独地传输,或者作为分级消息的一部分传输。

[0010] 所述分级信息可以完全、部分或完全不受完整性保护。相反,所述分级指示器始终完全受到完整性保护。因此,所述分级指示器防止对所述分级消息的非完整性保护部分的MitM攻击导致协商的安全性低于某个水平,或者在改变服务器或客户端的设置而不请求新证书的情况下有助于维持某个最小安全性。

[0011] 有效地,设备可以发送所述分级指示器,并且所述设备本身或接收者随后可以应用如由所述分级指示器指示的最小安全水平。而且,当两个设备协作时,它们至少应用如由所述分级指示器所指示的安全水平。此外,当两个设备交换分级消息时,所述分级消息示出在两侧都支持高安全等级,哪个等级高于由分级指示器所要求的水平,还可以选择这样的更高的安全水平。然而,降级到低于所述分级指示器中指示的安全水平的操作被阻止。因此,在分级消息将使传统通信能够在通信链路两侧支持的较低安全等级上的情况下,当这样的链路将应用低于所述分级指示器中指示的水平的安全水平时,现在可以防止这样的链路。类似地,当接收到包含所述分级指示器的消息并且在验证其完整性时,所述设备可以阻止或中止具有低于所述分级指示器中指示的安全水平的任何通信。

[0012] 有利地,所述分级信息指示至少一个安全水平,其可以被视为建议,而所述分级指示器指示可以实际使用的(一个或多个)安全水平的限制。因此,用通用语言来说:“无论(一个或多个)分级消息中已经提到什么,人们必须至少使用水平X”,或者“无论(一个或多个)分级信息中已经提到什么-如果人们支持它,人们就必须使用至少水平X,否则必须使用至少水平Y(水平Y的安全性低于水平X)”。

[0013] 提供完整性保护覆盖发送侧的动作和接收侧的动作。例如,基于所述完整性数据

提供所述分级指示器的完整性保护可以涉及由所述设备对所述分级指示器消息进行签名，并且在接收消息时检查所述签名。而且，提供完整性保护可以是由第一设备发送包含分级指示器的对象的动作，所述对象(因此例如连接器)由又第三设备签名。接收机侧然后使用关于所述第三设备的相应密钥材料来验证所述签名。例如，这可能发生在协商PFS的使用和如稍后描述的网络引入协议期间的跟踪防止期间。

[0014] 根据本发明的另一方面，所述安全协议基于设备供应协议，所述设备供应协议还要求配置器，所述配置器适于在无线网络中建立所述第一设备与所述第二设备之间的通信，例如DPP。所述配置器被布置用于将所述分级指示器插入在连接器消息中并将所述连接器消息发送到所述第一设备。所述第一设备中的处理器被布置用于接收所述连接器消息并从所述连接器消息中检索所述分级指示器。

[0015] 根据本发明的设备和方法的另外的优选实施例在随附的从属权利要求中给出，其公开内容通过引用并入本文。

附图说明

[0016] 本发明的这些和其他方面将根据以下描述中以示例的方式描述的实施例并且参考附图而显而易见并进一步阐明，其中：

[0017] 图1示出了可以在其中实践本发明的系统；

[0018] 图2a示出了计算机可读介质；并且

[0019] 图2b示出了处理器系统的示意性表示。

[0020] 附图仅是图解的并且未按比例绘制。在附图中，对应于已经描述的元件的元件可以具有相同的附图标记。

具体实施方式

[0021] 图1示出了包括第一设备110、第二设备120和第三设备130的系统100。这些设备中的每一个具有通信模块111、121、131，其包括用于通过诸如Wi-Fi、蓝牙或有线网络的物理信道160进行通信的适合的发射器/接收器。设备可以具有用于通过有线物理信道进行通信的输入/输出单元，和/或包括充当用于无线物理信道的输入/输出部的至少一个天线113、123、133。设备中的每一个将在处理器112、122、132的控制下操作。通信模块、处理器和设备的其他元件可以集成在芯片上的单个系统中。设备中的每一个可以具有带有至少一个用户控制元件的用户接口151、152、153。例如，用户控制元件可以包括触摸屏、各种按钮、鼠标或触摸板等。按钮可以是传统物理按钮、触摸传感器、或例如触摸屏上的虚拟按钮或要经由鼠标激活的图标。用户接口还可以是远程用户接口。

[0022] 实际上，第一设备可以对应于具有终端用户的便携式设备，诸如移动电话、膝上型电脑或平板电脑。它也可以是IoT(物联网)类型的设备。第二设备可以对应于服务器、接入点、路由器、另一便携式设备或IoT设备等。第一设备的用户可能对连接到第二设备(接入点)以用于访问经由第二设备提供的一个或多个资源感兴趣。第三设备实际上不是本发明的一部分，但它对应于所谓的中间人，即由恶意第三方用来拦截、修改或替换往返于第一设备的消息的设备。

[0023] 在本申请中，词语“证书”意指表示至少包括证书的所有者的公钥的一组数据。本

申请中意指的证书的示例是X509 v3[RFC 5280]证书。所有者可以被称为“主体”,并且公钥可以被称为“主体公钥”。所述组由证书颁发机构(CA)进行数字签名,该证书颁发机构可以被称为“颁发者”。除了所谓的根证书之外,证书由证书中的公钥(“主体公钥”)的所有者(“主体”)以外的另一实体(“颁发者”)签名。根证书由所有者自己签名,即元素“颁发者名称”和“主体名称”相同。

[0024] 用于验证证书的签名的公钥可以在另一个证书中作为“主体公钥”找到,其中“主体名称”与要验证的证书的“颁发者名称”相同。在该其他证书是根证书的情况下,可以使用其中的“主体公钥”来验证其签名。如果它不是由又一个颁发者Issuer2颁发的根证书,则可以使用又一个在其“主体名称”元素中列出Issuer2的证书中的“主体公钥”来检查其签名。因此,证书的签名检查可能涉及检查所谓的证书树中的若干证书的签名,直到并包括该证书树的根证书。

[0025] 与证书一样,DPP连接器也是一组数据,其至少包括DPP连接器的所有者的公钥,即已经由DPP配置器利用其配置的设备。该组不由CA进行数字签名,而是由DPP配置器进行数字签名。后两者之间的一个差异在于,CA是公开已知的,并且其中若干特性,诸如其颁发者名称或其根证书,是公共知识并且可以在互联网上找到,而DPP配置器不是公开已知的。例如,Digicert提供CA(www.Digicert.com)。根证书的列表提供在https://www.digicert.com/kb/digicert-root-certificates.htm上并且"DigiCert Assured ID Root CA"在https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt处可用。当使用适当的工具(例如网站https://lapo.it/asn1js/)检查该根证书时,例如,人们可以看到“颁发者名称”和“主体名称”是“countryName US;organizationName DigiCert Inc;organisationalUnitName www.DigiCert.com;commonName DigiCert Assured ID Root CA”。

[0026] 证书与连接器之间的另一差异是如何利用公钥配置设备以验证签名。在证书签名验证的情况下,这样做的公钥连同证书树中的所有证书一起以证书本身的形式提供,直到并包括该树的根证书。证书树通过特殊的安全机制安装在设备中。这可以例如在制造时进行。这也可以例如通过使用安全的互联网连接来完成。例如,Microsoft使用Windows设备与其服务器之间的专用安全连接向Windows设备提供最新的证书树。即使在Windows操作系统下运行时,网络浏览器Firefox也在Firefox安装与来自Mozilla的服务器之间使用其自己的专用安全通道,用于向Firefox安装提供最新的证书树。所涉及的安全性并不意指用于对证书保密,而是用于确保只提供有效的证书树。例如由黑客提供恶意根证书的设备将开始信任提供用该根证书中的公钥签名的证书(由其签名的证书)的网站。相反,DPP配置器公钥不是以证书的形式在登记者中提供的,而是由对称密钥(完整性)保护的消息中提供的。在以下中,讨论了DPP中的分级信息的各种示例。

[0027] 在DPP重新配置认证协议中,第一消息是DPP重新配置通告消息。它没有受到完整性保护。

[0028] 登记者->配置器:SHA256(C-sign-key),组,A-NONCE,E'-id

[0029] 属性“SHA256(C-sign-key)”指示配置器签名密钥。配置器可以具有多个签名密钥。它们可以属于相同的椭圆曲线组(例如NIST P-256),或者可以属于不同的椭圆曲线组(例如NIST P-256和NIST P-384)。因此,该属性指示配置器签名算法和签名算法安全水平,

因此用作分级信息。

[0030] 属性“组”指示登记者的NAK的椭圆曲线组。因此,该属性指示用于计算PMK的算法,并且它指示PMK的安全水平(此处更具体地比特数),因此也有助于分级信息。

[0031] 属性“A-NONCE”和“E'-id”是与配置器签名密钥在同一椭圆曲线上的椭圆点,因此不添加关于安全水平的更多信息。

[0032] 如果登记者仅支持一条曲线,例如强制性的NIST P-256曲线,那么设备仅支持这作为第一水平。然后,第二安全水平是P-256加上跟踪防止,这可以由参数或版本指示来指示。因此,在这一点上,配置器知道功能跟踪防止,但不要求如此。

[0033] DPP重新配置认证协议中的第二消息是DPP重新配置认证请求消息。除了属性“C-Connector”之外,它不受完整性保护。

[0034] 配置器->登记者:TransId、协议版本、C-Connector、C-nonce

[0035] 属性“TransId”是要在接下来的两个协议消息中复制的随机数。属性“协议版本”指代配置器支持的DPP协议版本。如果不同的版本提供或规定了其他水平的安全性,则该属性指示安全水平。该属性没有受到完整性保护。当DPP R3规范将支持使用跟踪防止时,该属性可以被用于选择“升级的安全水平”,即在重新配置期间使用跟踪防止。备选地,在DPP R3中,用于属性“协议版本”的3的值(指代DPP版本3)可以指定配置器支持登记者可以在下一个消息中对登记者连接器中的NAK使用跟踪防止。属性“协议版本”用作分级信息,由此该消息可以被认为是分级消息,其中配置器指示登记者具有两个选项,即是否使用跟踪防止。属性“C-Connector”包含配置器签名密钥的指示,即连接器的JSON Web签名(JWS)保护报头中的标识符“kid”,参见[WFEC_2]的第4.2节。配置器可以具有多个签名密钥。它们可以属于相同的椭圆曲线组(例如NIST P-256),或者可以属于不同的椭圆曲线组(例如NIST P-256和NIST P-384)。配置器签名密钥应为由登记者指示的具有“组”属性的密钥。因此,该属性指示配置器签名算法和签名算法安全水平。该属性还包含NAK。它应该与登记者的NAK在同一曲线上。因此,该属性还指示用于计算PMK的算法,并且它指示PMK的安全水平(例如,具体地,比特数)。

[0036] 属性“C-Connector”可能包含分级指示器,以指示登记者可以或必须对其NAK使用跟踪防止。指示登记者在与配置器通信时必须对其NAK使用跟踪防止的分级指示器也可以由配置器作为DPP配置响应消息的一部分发送,要么在该消息中的连接器的一个内要么该消息的另一部分中。

[0037] 另一示例涉及网络引入协议。以下消息是DPP对等发现请求消息:

[0038] 设备B→设备A:TransID,ConnectorB,[协议版本]

[0039] 设备B是非AP Wi-Fi设备,并且设备A是Wi-Fi AP设备。

[0040] 属性“TransID”是将在接下来的协议消息中复制的随机数。属性“ConnectorB”包含配置器签名密钥和非AP设备的NAK的指示器,该信息可以被认为是分级信息。如果非AP设备仅支持一条曲线,例如P-256,则利用该信息可以选择仅一个安全水平。属性“ConnectorB”可能包含分级指示器,以指示AP可以或必须对其连接器中的NAK使用跟踪防止,或者必须使用PFS。任选属性“协议版本”指示非AP设备支持的DPP协议的版本。PFS已在DPP R2中定义。当在该属性中指示DPP R2时,AP可以决定使用或不使用PFS。因此,该属性也可能有助于分级信息。

[0041] 注意,如果登记者想要在其连接器中对NAK使用跟踪防止,则它必须以另一种方式获得AP支持该功能的信息,例如从指代AP在其信标或探头响应中包括该信息的另一信息元素获得该信息。这样的元素可以被认为是分级信息。

[0042] 在另一示例中,DPP对等发现响应消息是:

[0043] 设备A→设备B:事务ID,DPP状态,ConnectorA,[协议版本]

[0044] 在这种情况下,属性“DPP状态”包含DPP_Status_OK值。当该属性具有另一值时,将省略属性“ConnectorA”和“Protocol Version”。其他属性的功能与如上文针对DPP对等发现请求消息所描述的相同,但是具有交换的设备。

[0045] 在以下中,本发明的特定实施例是关于上述一般系统来描述的。

[0046] 在第一示例性实施例中,设备充当第一设备,其适于根据如先前所描述的安全协议在物理信道上为第一设备与第二设备之间的通信建立安全水平。设备具有处理器,其被布置用于经由物理信道发送或接收分级指示器,分级指示器指示如在第一和第二设备中的至少一个中最低要求的最低安全水平。当发送时,处理器包括用于基于完整性数据的分级指示器的保护数据。当接收时,处理器基于完整性数据来验证保护数据。随后,处理器至少对第一设备与第二设备之间的通信应用最小安全水平。

[0047] 任选地,安全协议基于设备供应协议,该设备供应协议还要求配置器,该配置器适于在无线网络中建立第一设备与第二设备之间的通信。配置器被布置用于将分级指示器插入连接器消息中并将连接器消息发送到第一设备。第一设备中的处理器被布置用于接收连接器消息并从连接器消息中检索分级指示器。

[0048] 任选地,根据第一安全水平的安全协议基于私钥和公钥材料来确定第一设备和第二设备两者中的成对主密钥,成对主密钥用于确定第一设备与第二设备之间的加密通信的会话密钥。此外,根据第二安全水平的安全协议要求确定涉及短暂Diffie-Hellman密钥对的成对主密钥,并且设备中的处理器被布置为当由分级指示器如此指示时,应用第二安全水平。作为“涉及短暂的Diffie-Hellman密钥对”的示例,PFS如下文所描述的,PFS提供了升级的安全水平的示例。

[0049] 通常,在上述实施例中,在安全协议中,至少一个分级消息缺乏完整性保护。因此,这样的消息容易受到MitM攻击。任选地,可以通过在增强的安全协议中的某个点处传输所述分级指示器来保护这样的消息中的各种参数。分级指示器可以提供对各种元素的限制、边界或要求,这些元素可能受到操纵缺乏完整性保护的所述分级消息的影响。

[0050] 在各种实施例中,通信信道可以是Wi-Fi。第二设备可以对应于接入点(AP),第一设备试图连接到AP,例如经由SAE协议,参见[WPA3]或[802.11]的条款12.4。在每个设备中,根据本发明的协议在模块控制器(113、123)、处理器(114、124)中执行,或者通过两者协作执行协议来执行。实施例涉及协商完美前向安全(PFS)功能,该功能已添加在DPP的版本2中,参见[WFEC_2]的第6.6.3节“网络访问协议”。因此,分级消息可以包含由设备支持的安全协议的版本指示器。例如,版本指示可以体现未受保护的“分级信息”,指示设备支持特定的安全水平,例如,如果它是V3设备,则为“V3”,而V3隐含可以使用类似PFS的安全选项。

[0051] 当设备想要使用DPP连接到AP时,它在所谓的DPP对等发现请求帧中将其连接器发送到AP。该帧未加密。该帧也没有受到完整性保护,这意味着它可以由中间人(MitM)攻击者改变。注意,在接收者未注意到该改变的情况下,连接器不能由MitM改变,因为它受到来自

DPP配置器设备的签名的完整性保护,但DPP对等发现请求帧中的所有其他属性没有完整性保护。

[0052] 接收DPP对等发现请求帧的AP将检查其中的连接器。当它发现连接器合法时,即签名正确,连接器未期满,并且连接器关于AP提供的网络时,AP可以用DPP对等发现响应帧进行应答。该帧包含AP的连接器,该连接器必须由签名设备连接器的同一配置器签名。接收DPP对等发现响应帧的设备将以与AP相同的方式检查AP连接器。当设备发现AP连接器正确并与其自己的连接器匹配时,参见[DPP]的第6.4.2节“连接器组比较”,它可以使用其自己的私有NAK和来自AP连接器的公共NAK来计算成对主密钥(PMK),参见[DPP]的第6.4节“网络引入协议”,以Diffie-Hellman方式,参见[DH]。AP可以使用其自己的私有NAK和设备连接器中的公共NAK来计算用于PMK的相同值。PMK是使用所谓的4次握手计算设备与AP之间的会话密钥的基础,参见[8.11]。在成功的4次握手之后,设备与AP相关联,并且设备与AP之间的传输被加密,并且利用从PMK和在4次握手期间发送的透明区域信息中导出的会话密钥来保护完整性。

[0053] 在DPP的版本2(其现在称为Wi-Fi Easy Connect™[WFEC_2])中,已经改进了DPP引入协议。关于版本1的问题在于Wi-Fi设备与AP之间的PMK总是相同的。假设攻击者已经捕获了设备与AP之间的所有Wi-Fi流量,因此DPP网络引入协议交换、用于计算会话密钥的4次握手以及关联后的加密交换。当攻击者对设备或AP进行黑客攻击并获得私有NAK中的一个时,攻击者可以计算它们之间的PMK,因为黑客已经从另一设备的连接器获得了来自另一设备的公共NAK,该连接器是以明文形式发送的。使用捕获的4次握手中的PMK和随机数,攻击者可以计算会话密钥,并且然后解密两个设备之间的所有加密传输。

[0054] 为了防止该攻击,已经在DPP的版本2中添加了PFS功能。PMK的计算现在还涉及短暂Diffie-Hellman密钥对(公共/私有ECC密钥)。由于短暂Diffie-Hellman密钥对的私钥在使用之后必须由设备删除,因此黑客攻击这两个设备中的任何一个的攻击者将不能够获得这些短暂私钥,并且因此不能够计算所使用的PMK,并且不能够解密过去在设备与AP之间发生的加密传输。

[0055] 如[WFEC_2]中指定的PFS的问题在于其使用是以非安全的方式协商的。当设备想要使用PFS时,它向DPP对等发现请求帧添加具有值2或更高的协议版本属性。当AP接收到具有带有2或更高的值的协议版本属性的DPP对等发现请求帧时,并且如果它支持PFS,则它将用具有2或更高的值的协议版本的DPP对等发现响应帧来响应。在该情况下,两个设备将使用如[WFEC_2]的第6.6.3节“网络访问协议”中指定的PFS计算PMK。由于DPP对等发现请求或响应帧中除连接器之外的任何属性都不受完整性保护,因此MitM攻击者可以改变这两个对等发现帧中的任一个,使得协议版本属性获得小于2的值,或者协议版本属性完全被移除。如果在对等发现帧中的一个或两个帧中都是这种情况,则设备和AP将不使用PFS。这样的攻击是降级攻击的示例,其应该加以防止。

[0056] 一个可能的、明显简单的选项是,设置设备或AP,使得其在不使用PFS的情况下将不计算PMK,但这是不灵活的。例如,如果通过该AP可获得的信息不要求高度的安全性,例如公共网络,则设备在不使用PFS的情况下连接到AP可能是完全可以的。然而,可能设备必须始终将PFS用于提供对私有或公司网络的访问的AP。

[0057] 关于该明显简单的选项的另一问题是,用户现在必须做两件单独的事情来设置设

备或AP。第一件事是，用户必须使用DPP配置器来配置设备或AP，第二件事是，用户必须通过设备或AP设置流程来配置其始终使用PFS。

[0058] 现在描述了一种解决方案，该解决方案使PFS的设置对于用户来说比上文所描述的明显简单的解决方案的设置更简单，并且使PFS的使用比上述简单选项更灵活。

[0059] 配置器是DPP中配置网络的中央设备。配置器现在还被用于以安全的方式控制PFS是否必须用于网络，因此防止了对PFS的使用的降级攻击，并且使用户设置PFS的使用更简单，这是两种设备都必须使用的技术。如果PFS必须用于某个网络，则配置器在其为该网络生成的每个连接器中插入分级指示器，即指示必须使用PFS的信息，因此两者用于设备以及AP。该信息可以例如采取最低限度使用的最小版本号的形式，例如{…,"minVersion:3",…}，或采取更具体的指示的形式，例如{…,"usePFS":true,…}。在对等发现帧中使用连接器(该连接器包含使用PFS的信息)的设备将拒绝连接到从其中它们接收到未指定必须使用PFS的连接器的设备。

[0060] 因此，即使MitM已经改变了对等发现帧中的版本信息，它也不能改变连接器中指示设备使用PFS的信息，因为连接器受到签名的完整性保护，并且在已经改变连接器时检查将失败。

[0061] 对于不要求使用PFS的网络，配置器可以通过在为该网络生成的所有连接器中插入例如{…,"usePFS":false,…}来插入PFS不必使用的信息，或者配置器可以不在所有连接器中插入关于PFS的使用的信息，从而将其留给设备和AP自己来使用或不使用PFS，例如通过使用DPP版本1或DPP版本2以及对等发现帧中的协议版本属性值的适当设置。

[0062] 任选地，出于向后兼容性原因，配置器可以配置支持某个最低版本规范的设备，例如版本3，其具有连接器，其指示如果使用PFS，则该设备将仅连接到支持该最低版本或更高版本的其他设备，但是允许在不使用PFS的情况下连接到支持低于最低版本的版本的设备。作为示例，配置器可以在连接器中使用{…,"mustUsePFSIfVersionAtLeast":3,…}来指示这一点，并且配置有这样的DPP连接器的设备将在不坚持使用PFS的情况下连接到具有连接器的设备，而没有是否必须使用PFS的任何指示，因此例如连接到符合DPP版本1[DPP]或版本2[WFEC_2]的设备。这是因为DPP版本1[DPP]或版本2[WFEC_2]连接器不包含PFS信息的版本或使用。注意，关于{…,XYZ,…}，我们意指“,XYZ”插入到DPP连接器的JSON代码中。

[0063] 应注意，DPP登记者和DPP配置器可以在DPP认证请求和DPP认证响应消息中安全地通知另一个设备它们支持的最高版本的DPP，因为用于版本信息的属性在这两个消息中的每一个消息中受到完整性保护。如分级指示器中所指示的，最高支持版本不得与最低要求版本混淆。此外，注意，对于设备或AP支持DPP版本2[WFEC_2]中的PFS是强制的。因此，配置器确定DPP登记者支持的DPP版本，因此确定登记者是否支持PFS，并且因此确定其是否可以或不能包括必须在登记者连接器中使用PFS的信息。

[0064] 另一实施例涉及设备跟踪防止的协商，其中，根据第一安全水平的安全协议不防止基于第一设备的消息中的重复数据跨网络中的多个通信会话跟踪第一设备，并且根据第二安全水平的安全协议要求避免或修改所述重复数据以防止跟踪。在设备中，处理器被布置为当由分级指示器如此指示时，应用所述跟踪防止。

[0065] 任选地，安全协议基于如[DPP]中定义的用于配置Wi-Fi设备的设备供应协议。连接器消息是基于连接器的重新配置连接器，该重新配置连接器被生成用于如在设备供应协

议中定义的重新配置认证请求消息中使用。配置器被布置用于将分级指示器插入到重新配置连接器中，分级指示器指示防止约束，该防止约束指示设备跟踪防止应当由想要被重新配置的设备使用。

[0066] 在设备中，处理器被布置用于从重新配置连接器检索防止约束，并且用于在基于防止约束的重新配置期间应用跟踪防止。在实际示例中，基于配置器对登记者的分级指示器，其中，配置器向登记者指示配置器本身支持跟踪防止，登记者可以在其连接器中对其在DPP重新配置响应消息中发送给配置器的NAK使用跟踪防止。防止约束可以发送如下：

[0067] 作为其在DPP重新配置请求消息中的C连接器的一部分；

[0068] 在配置期间由配置器发送给登记者的连接器中，因此在DPP配置响应消息中；或

[0069] 作为DPP配置响应消息的一部分，但不在该消息中的任何连接器中。

[0070] 注意，在这三种情况中的每一种情况下，分级指示器未受到完整性保护。

[0071] 应注意，除了已经解释的内容之外，所述“指示作为最低要求的最低安全水平的分级指示器”可能意味着，例如出于向后兼容性原因或为了使能支持低成本设备，不支持最低安全水平的设备可以使用较低水平，然而仅以进一步的限制为条件。例如，在接收到分级指示器并发现最低安全水平不受支持时，可以首先安全地交换额外请求，其中，传统或低成本设备请求使用较低水平。或者，例如，指示向后兼容设备的较低允许水平的额外参数也可以是分级指示器的一部分。然而，如果设备确实支持最低安全水平，则它必须至少使用该最低水平。

[0072] 在实际示例中，根据DPP版本1[DPP]和版本2[WFEC_2]的设备在DPP对等发现请求帧中向AP发送其透明区域连接器，并且AP在DPP对等发现响应帧中向Wi-Fi设备发送其透明区域连接器。由于设备或AP的连接器包含该设备的(恒定)公钥，因此NAK、设备或AP可以由RF范围内的任何Wi-Fi设备跟踪。公共NAK可以用作设备的身份。这可能侵犯该设备的隐私，并且因此是一个问题。

[0073] DPP版本2[WFEC_2]中的扩展之一是DPP重新配置认证协议。由DPP配置器配置的设备可能已成功连接到其被配置用于的网络，但在以后使用其连接器连接到AP时它可能遇到问题。例如，它可能是其连接器期满，或者第一设备和/或AP已经移动，使得它们意外地变得脱离了彼此的RF范围。在设备经历与AP的连接问题的情况下，它可以使用DPP重新配置认证协议，参见[WFEC_2]，向配置器指示该问题并重新配置。在DPP版本2规范[WFEC_2]中，使用该协议进行重新配置的设备被称为登记者。

[0074] 根据DPP版本2[WFEC_2]的设备在DPP重新配置认证响应消息中将其连接器透明区域发送给配置器。该消息中的连接器是与设备在DPP对等发现请求帧中用于访问AP相同的连接器。因此，设备也可以由捕获其DPP重新配置认证响应消息或DPP对等发现请求帧的其他设备跟踪。

[0075] 根据DPP版本2[WFEC_2]的配置器在DPP重新配置认证请求消息中将其连接器透明区域发送给登记者。然而，配置器连接器中的NAK是短暂的，即它是随机生成的，仅用于发送一次，因此配置器无法通过这些消息跟踪。

[0076] 如上文所解释的，防止设备和AP被跟踪不由DPP版本2[WFEC_2]支持。然而，基于DPP重新配置认证协议中的信息的设备跟踪可能由隐私保护措施阻止，诸如加密连接器中的NAK，如[2018PF00508]中所描述的。另外，隐私保护措施的使用必须在他们之间进行协

商。

[0077] 在DPP版本2[WFEC_2]中,不支持基于DPP对等发现请求和结果消息的信息协商防止设备跟踪。类似于如上文所解释的协商PFS的使用的简单选项将是在DPP对等发现请求和/或响应帧中使用协议版本属性。然而,这些不受完整性保护,并且MitM可以通过改变或移除协议版本属性来执行降级攻击。

[0078] 在DPP版本2[WFEC_2]中,不支持基于DPP重新配置认证消息的信息协商防止设备跟踪。在另一简单的选项中,配置器可以向DPP重新配置认证请求消息添加属性,向想要重新配置的设备登记者发出信号,其配置器支持设备跟踪防止。这将使得设备能够在其对配置器的应答DPP重新配置认证响应消息中隐藏其设备连接器中的NAK。然而,DPP重新配置认证请求消息不提供任何完整性保护-协议中没有在该点处建立共享密钥来启用完整性保护-并且原则上,MitM可以移除该属性,并且因此执行降级攻击。

[0079] 以下解决方案防止了对DPP重新配置认证响应消息和DPP对等发现响应帧中的设备跟踪防止的使用的协商的降级攻击。

[0080] 配置器可以安全地控制DPP中设备跟踪防止的使用,类似于控制上文所描述的PFS的使用。与PFS相反,设备跟踪防止是任一种设备或两者可以使用的技术。例如,AP可以或可以不是固定的。固定AP的位置可以是已知的并且将不改变。因此,固定AP在DPP对等发现响应帧中不对其自身连接器使用设备跟踪防止是可以接受的,而它支持在其发送给AP的DPP对等发现请求帧中对其连接器应用设备跟踪防止的设备。然而,许多智能电话能够用作热点,即它们可以用作移动Wi-Fi AP,通过该移动Wi-Fi AP与该移动AP相关联的Wi-Fi设备可以通过智能电话的移动互联网订阅来获得互联网接入。与固定AP相反,对移动电话中的热点或智能电话以外的移动Wi-Fi热点使用设备跟踪防止是有意义的。

[0081] AP可以在分级消息中(例如在DPP对等发现请求帧中)用信号通知想要与AP相关联的设备,该设备可以或必须对其连接器使用设备跟踪防止。然而,在协议的这一点上缺乏完整性保护,因为设备尚未接收到AP的连接器。在[2018PF00508]中描述了检测连接器中是否使用设备跟踪防止的无保护方法。

[0082] 现在描述了一种用于想要与AP相关联的设备的解决方案,以使AP以安全的方式知道AP可以在其连接器中使用设备跟踪防止。在AP已经在先前的DPP对等发现请求帧中接收到设备连接器之后,AP可以向设备发送DPP对等发现响应帧。配置器现在在其为该设备生成的每个连接器中插入分级指示器。分级指示器指示设备跟踪防止可以或必须由AP在DPP对等发现响应帧中使用。该信息可以例如以一般指示的形式,例如版本号,例如{…,"version":3,…},或以更具体的指示的形式,例如{…,"mayUseTrackingPrevention":true,…},或{…,"hasToUseTrackingProvention":true,…}。注意,对于{…,XYZ,…},我们意指",XYZ"插入到DPP连接器的JSON代码中。在设备在DPP对等发现请求帧中向AP发送这样的连接器并且设备本身也使用设备跟踪防止的情况下,例如通过在[2018PF00508]中描述的方法加密其连接器中的NAK,在其可以检查所接收的连接器的签名之前,以及在成功的签名检查可以安全地确定其是否可以或必须使用设备跟踪防止之后,AP首先必须恢复接收到的连接器,如[2018PF00508]中所描述的。

[0083] 根据DPP版本2[WFEC_2]的设备(DPP登记者)在DPP重新配置认证响应消息中将其连接器透明区域发送给配置器。该消息中的连接器是与设备在DPP对等发现请求帧中用于

访问AP相同的连接器。因此，设备也可以由捕获其DPP对等发现请求帧的其他设备跟踪。

[0084] 在实施例中，当DPP配置器向想要被重新配置的设备(DPP登记者)发送DPP重新配置认证请求消息时，DPP配置器使用连接器中的分级指示器来让登记者安全地知道，当该登记者用DPP重新配置认证响应消息应答时，它可以或必须使用设备跟踪防止。因此，配置器在其生成的连接器中插入分级指示器，用于其DPP重新配置认证请求消息。分级指示器指示设备跟踪防止可以由想要重新配置的登记者使用。该信息可以例如采取一般指示的形式，例如版本号，例如{…,″version″:3,…}，或采取更具体的指示的形式，例如{…,“mayUseTrackingPrevention”:true,…}，或{…,“useTrackingPrevention”:true,…}。如果登记者支持设备跟踪防止，并且如果在DPP配置器连接器中看到它可以使用设备跟踪防止的信息，则它可以例如通过加密其连接器中的NAK来使用设备跟踪防止，如[2018PF00508]中所描述的。

[0085] 在另一实施例中，安全协议包括提供以下动作的设置协议。初始地，证书是从证书颁发机构获得的。随后，使用证书来提供安全参数，例如基于证书生成并加密或完整性保护的证书，例如使用证书中指示的生成密钥或安全算法。随后，安全参数经由设置消息传输到设备。证书包括分级指示器，该分级指示器指示安全参数的约束。例如，证书可以由认证服务器基于来自要配置的设备或来自配置器的证书请求消息来提供。请求可以包含包括分级指示器的请求，或者经由分级指示器来保护的参数或设置的指示。

[0086] 在布置为应用上述安全协议的设备中，设备处理器被布置用于从证书中检索分级指示器。随后，处理器被布置为接收和/或传送设置消息。而且，处理器被布置为基于设置消息和安全参数的约束来确定安全水平。任选地，安全协议提供密码安全参数的设置。密码安全参数可以包括要使用的密码算法、要使用的密钥大小、要使用的密码散列算法、或者要使用的安全协议或密码过程的另外的选项或参数中的一个或多个。

[0087] 密码参数的上述协商或设置的示例是传输层安全性(TLS)。许多密码协议(TLS1.3[RFC 8446]是其中之一)对于使用密码基元具有内置灵活性，诸如要使用的密码算法、要使用的密钥大小、要使用的密码散列算法或要使用的协议的变型，例如是否使用完美前向保密(PFS)。下面将进一步阐述TLS1.3[RFC 8446]，以示出如何使用上述增强。在其他密码协议中的使用可以容易地从该解释中导出。

[0088] 在TLS协商阶段中，客户端发送的第一消息是ClientHello消息，其指定其支持的最高TLS协议版本、随机数、建议的密码套件和压缩方法的列表。服务器对ClientHello消息的应答可以是ServerHello消息，其中包含所选择的密码套件。ClientHello和ServerHello消息最初没有受到完整性保护。然而，使用三种可能模式(EC)DHE(有限域或椭圆曲线上的Diffie-Hellman)、仅预共享密钥(PSK)或具有(EC)DHE的PSK中的任何一种，当在客户端与服务器之间成功建立共享密钥时，TLS设置通过服务器在整个设置交换上向客户端发送包含密钥散列的“完成”消息来完成，因此包括ClientHello和ServerHello消息，基于从他们刚刚建立的共享密钥导出的密钥。在那之后，客户端向服务器发送其自己的“Finished”消息，该消息还包含整个设置交换的密钥散列，因此包括ClientHello和ServerHello消息。密钥散列函数是散列函数，其在基于其输入的基础上创建散列，该散列值也基于(秘密)密钥的值。因此，ClientHello和/或ServerHello消息稍后在TLS协议中受到完整性保护。

[0089] TLS具有许多变化，并且存在针对TLS的密码参数的若干可能性。黑客改变TLS服务

器或客户端中的TLS的设置可能是可能的。TLS服务器或客户端的设置也可能由TLS服务器或客户端的任何管理员意外地或故意地从最初打算的设置改变。例如，浏览器Internet Explorer的“Internet选项”菜单为用户给出了允许或不允许使用特定TLS版本的可能性。

[0090] 因此，通信协商协议的设置可能需要针对降级攻击进行保护。上述配置参数也可能由服务器的管理员改变，例如意外改变。它们也可能由黑客或恶意内部人员故意改变。上述增强可以使TLS的设置对于TLS服务器或客户端的管理员更安全。这也可以应用于其他协议中，其中，用于协商参数值的消息不受完整性保护。

[0091] 当为TLS设置服务器时，初始管理员必须从证书颁发机构(CA)获得证书。一旦创建，则证书不能意外或故意改变，因为TLS客户端将不再接受该证书。除了获取证书之外，(可能不同的)管理员还必须设置TLS的使用。这样的管理员必须设置例如：

[0092] • 允许服务器使用的具有基于关联数据的认证加密(AEAD)算法/HMAC的提取和扩展密钥推导函数(HKDF)散列对，

[0093] • 允许服务器使用的(EC)DHE组，

[0094] • 允许服务器使用的签名算法，以及

[0095] • 允许证书的所有者设备使用的TLS的最低版本。

[0096] 应注意，允许使用的TLS协议的最低版本在功能上与证书本身的TLS版本不同。例如，TLS证书可以具有其根据TLS V1.4格式化的指示器，但是该TLS V1.4证书中的分级指示器可以例如指示仅允许来自TLS V1.4的TLS版本，或者必须使用TLS V1.2或更高版本。

[0097] 当从证书颁发机构请求用于服务器的证书时，初始管理员可以在请求中包括专用分级数据，以请求证书包括分级指示器，例如指示约束、安全选项、用于上文所提及的允许或不允许的值或其他TLS配置参数等。

[0098] 证书的当前语法是在X509 v3[RFC 5280]中使用抽象语法符号一(ASN.1)[X.680]作为规范语言指定的。证书使用对象标识符(OID)作为用于许多事情的指示器。例如，用于organizationName的指示的OID是2.5.4.10，而指示RSA加密(一种特定的非对称加密算法)的OID是1.2.840.113549.1.1.1。指示证书的“扩展”部件中的特定扩展的OID从2.5.29开始，并且指示X509v3[RFC 5280]的第4.2.1.9节的基本约束扩展的OID是2.5.29.19。

[0099] TLS的TLS参数的可能值在TLS消息中由TLS1.3[RFC 8446]中指定的数字指示，例如，十六进制值(0x0403)指示签名算法“椭圆曲线数字签名算法”，参见[FIPS186-4]，使用椭圆曲线P-256，参见[FIPS186-4]和SHA256作为哈希算法，参见[FIPS180-4]。

[0100] 因此，为了增强如所提出的证书，X509可以用扩展进行扩展，例如称为“allowedTLSParameters”，其由新的OID 2.5.29.19.x指示，其中，x是从维护OID树的该分支的组织获得的适当值，其中，该新扩展包含允许的TLS参数的数组，该数组利用如TLS1.3[RFC 8446]中指定的值指示。作为示例，用于该新扩展的类型可以在ASN.1中表达为AllowedTLSParameters::=SEQUENCE{allowedTLSParameter INTEGER}

[0101] 类型“AllowedTLSParameters”的实例化的ASN.1der编码可以存储在类型“TBSCertificate”的“扩展”部件中的称为“extnValue”的部件中，参见X509 v3[RFC 5280]的A.1条款。

[0102] 代替于TLS1.3[RFC 8446]中指定的十六进制值，新扩展还可以使用对象标识符(OID)来指示允许的参数值。使用OID的优点在于，OID可以由任何协议用来指示密码参数，

并且在TLS1.3[RFC 8446]中指定的十六进制值仅可以被用于指示TLS协议的这一点。作为示例,用于使用OID的该新扩展的类型可以在ASN.1中表达为:

[0103]
```
AllowedTLSParameters ::= SET OF AllowedTLSParameter
AllowedTLSParameter ::= SEQUENCE {
        allowedTLSParameterTypeOBJECT IDENTIFIER,
        allowedTLSParameterValuesAllowedTLSParameterValues OPTIONAL
        -- allowedTLSParameterValuesmay be needed if the object identifier alone is not sufficient
}
AllowedTLSParameterValues::= SET OF AllowedTLSParameterValue
AllowedTLSParameterValue ::= INTEGER
```

[0104] 上述类型AllowedTLSParameterValues仅是示例。除了整数之外,其中能够存在其他信息,例如指定密码算法的对象标识符,或类似于AllowedTLSParameter类型的类型/值对。

[0105] 用于部件allowedTLSParameterType的可能OID之一可以是指示TLS协议的最低允许版本号的OID,在将该证书与TLS一起使用时必须使用该OID。在这种情况下,部件allowedTLSParameterValues可以例如是包含具有值11的一个INTEGER部件的SET,其指代TLS版本1.1。

[0106] 当增强型TLS服务器发送证书或TLS客户端接收到具有使用的允许TLS参数的信息的证书,并且证书中的允许TLS参数列表中未提及协商的TLS参数时,服务器或客户端必须中止设置TLS协议。因此,分级指示器可以指示这样的列表,但也可以包含类似算法X的构造,如果其版本号高于或等于Y或其质量优于或等于Y,则允许使用算法X,例如,可以使用具有256比特或更大素数的长度的ECC曲线。分级指示器还可以指示黑名单。即不允许使用的TLS参数的列表。黑名单还可以包含类似算法X的构造,如果其版本号低于或等于Y或其质量差于或等于Y,则不允许使用算法X,例如,可以不使用具有255比特或更小素数的长度的ECC曲线。

[0107] TLS客户端还可以具有TLS服务器可以用来对TLS客户端进行认证的证书,并且其用于TLS设置和会话密钥的派生。类似于上述TLS服务器证书,TLS客户端证书也可以包含用于TLS参数的允许的值或不允许的值,或允许的最小值。

[0108] 因此,当使用用于TLS的分级指示器时,TLS服务器或客户端的管理员可以请求用于TLS客户端或服务器的证书,该证书具有用于TLS参数的允许或不允许的值或允许的最小值的指示。这样的TLS客户端或服务器将仅使用由证书允许的TLS参数的值。改变TLS客户端或服务器的配置将不导致TLS客户端或服务使用不允许的值,因此TLS服务器或客户端的设置对其(一个或多个)管理员更安全。

[0109] 在另一实施例中,使用WPA-Enterprise作为详细示例,描述了使用证书无线访问网络的密码参数的协商。WPA(Wi-Fi保护访问)是用于Wi-Fi无线网络安全的规范。Wi-Fi联盟(WFA)维护WPA规范和用于WFA的证书程序。WPA以两种风格出现,一方面是WPA-PSK(预共享密钥)或WPA-Personal,并且另一方面是WPA-Enterprise。存在WPA的三个主要版本,即WPA、WPA2和WPA3[WPA3],其中,三个版本中的每一个支持这两种风格。

[0110] WPA-PSK要求每个Wi-Fi设备(也是AP)拥有要连接的网络的PSK(预共享密钥)。对于特定网络的所有用户,PSK通常是相同的。相反,WPA-Enterprise要求RADIUS服务器,其处

理认证网络用户访问的任务。实际的认证过程在[802.1x]中指定，基于802.1x策略，并且在若干不同的系统中标记为EAP(可扩展认证协议)。由于每个设备在其连接之前进行了认证，因此在设备与网络之间有效地创建了个人加密隧道。

[0111] WPA-Enterprise AP将仅允许未授权的Wi-Fi设备与RADIUS服务器通信。一旦RADIUS服务器已经认证了设备，则刚刚认证的设备和AP为它们之间的Wi-Fi安全性建立PMK(成对主密钥)，该PMK也基于在与RADIUS服务器的认证过程中交换的信息。

[0112] 若干EAP协议可以由RADIUS服务器使用，其中，EAP-TLS[RFC 5216]和EAP-TTLS/PAP[RFC 5281]是使用证书的EAP版本。

[0113] EAP-TLS要求所有Wi-Fi设备具有用于网络访问的证书，而用于(RADIUS)服务器认证的服务器证书是任选的。这对于EAP-TTLS/PAP相反，其中，服务器证书是强制性的，并且客户端证书是任选的。

[0114] WPA3-Enterprise与WPA2-Enterprise之间的差异在于，WPA3-Enterprise提供了服务器证书验证要被配置为确认设备连接到的服务器的身份的要求。

[0115] 在本描述中，WPA-Enterprise可以意指WPA-Enterprise、WPA2-Enterprise、WPA3-Enterprise或它们未来的任何后继者。`类似于上述实施例，请求用于在WPA-Enterprise中使用的证书的实体和配置用于WPA-Enterprise的AP或Wi-Fi设备的实体可以是不同的。所提出的增强使WPA-Enterprise的设置对于TLS服务器或客户端的(一个或多个)管理员更安全。

[0116] Wi-Fi设备与AP之间的Wi-Fi连接的安全性的协商可以在设备可以与AP相关联之前，因此例如在由设备发送的探头请求以及由AP发送的探头响应和信标中，在它们之间交换的消息中使用鲁棒安全网络元件(RSNE，[802.11]的第9.4.2.25条)来完成。RSNE可以包含成对密码套件列表和AKM(认证和密钥管理)套件列表。成对密码套件列表列出了设备支持的密码，其由密码套件选择器指示，例如密码套件选择器00-0F-AC:4指示CCMP-128算法。AKM套件列表列出了设备支持的AKM，由AKM套件选择器指示。AKM是一种对设备和/或AP进行认证的协议。例如，AKM套件选择器00-0F-AC:1指示通过IEEE Std 802.1X协商的认证，这意味着使用Radius服务器进行认证。

[0117] 探头请求、探头响应和信标不受完整性保护，并且可能由MitM攻击者更改。然而，设备永远无法使用它不支持的协议或算法。它也不能成功地完成它不具有所要求的信息的协议。例如，不知道密码短语的设备不能使用WPA-Personal用于与AP相关联。类似地，其他安全过程，例如EAP-TLS和EAP-TTLS/PAP，也可以进行一些协商。

[0118] 在已经向设备、服务器或AP提供了初始证书之后，仍然可以为安全的设置做出若干选择，并且攻击者或粗心的管理员可能改变这些选择。例如，为EAP-TLS设置的设备必须具有证书。然而，在这种情况下，对于RADIUS服务器具有用于服务器认证的证书也是任选的。可能是设备最初被设置为在RADIUS服务器可以参与服务器侧认证时仅接受RADIUS服务器。粗心的其他管理员或黑客可能在以后改变，从而降低安全水平。通过使用以上关于分级指示器的增强，原始管理员可以申请设备证书，其包括使用服务器证书的服务器侧认证必须始终被使用的约束。设备然后将拒绝向不执行服务器侧认证的RADIUS服务器进行认证，即使后来，粗心的管理员或黑客将设备的设置改变为不要求这样做。添加到证书的另一约束可以是在认证之后要使用的PMK的大小。例如，约束可以是要使用的PMK必须大于128比

特。可以经由分级指示器将约束包括在证书中，例如，如与先前实施例所讨论的。

[0119] 在另一实施例中，第一设备是客户端设备，并且第二设备是服务器设备，并且分级指示器指示要求使用证书进行客户端侧认证的客户端约束。客户端设备中的处理器被布置用于从证书中检索客户端约束。随后，处理器被布置为接收设置消息并基于客户端约束应用客户端侧认证。在实际示例中，类似于为EAP-TLS设置的设备，为EAP-TTLS/PAP设置的AP必须具有证书。但是，客户端侧认证是任选的。请求用于AP的证书的管理员可以使用本发明来请求具有约束的证书，即始终要求使用证书的客户端侧认证。然后，AP将始终拒绝使用在该协议期间无法呈现证书的设备成功完成EAP-TTLS/PAP，即使后来，粗心的管理员或黑客将AP的设置改变为不要求客户端证书。

[0120] 因此，上述增强使WPA-Enterprise在使用EAP-TLS或EAP-TTLS/PAP的设备和AP上的设置更安全，并且为改变安全协商消息的MitM攻击者提供了保护。

[0121] 已经使用设备描述了上述实施例。然而，各种协议、消息和处理器动作可以通过对应的方法步骤来执行，其可以容易地从上述描述中导出。方法可以例如通过Wi-Fi控制器中的处理器中的电路和软件执行。上文已经描述了适合的加密和解密功能。实现方法的许多不同的方式是可能的，如对于本领域技术人员而言将是明显的。例如，阶段或步骤的次序可以变化或者一些阶段可以并行执行。而且，在步骤之间可以插入其他方法步骤。插入的步骤可以表示诸如本文所描述的方法的细化，或者可以与方法无关。

[0122] 提供了可从网络下载和/或存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品，所述计算机程序产品包括用于当在计算机设备上执行时实施以上方法、连接序列、安全过程和其他操作的程序代码指令。因此，根据本发明的方法可以使用软件执行，该软件包括用于使得处理器系统执行相应方法的指令。

[0123] 图2a示出了具有包括计算机程序1020的可写部件1010的计算机可读介质1000，计算机程序1020包括用于使得处理器系统执行如参考1所描述的系统中的以上方法中的一个或多个的指令。计算机程序1020可以作为物理标记或借助于计算机可读介质1000的磁化体现在计算机可读介质上。然而，任何其他适合的实施例也是可以想象的。此外，将意识到，尽管计算机可读介质1000此处被示为光盘，但是计算机可读介质1000可以是任何适合的计算机可读介质，诸如硬盘、固态存储器、闪存等，并且可以是不可记录的或可记录的。计算机程序1020包括用于使得处理器系统执行所述方法的指令。

[0124] 通常，执行上述过程的设备各自包括耦合到包含存储在设备处的适当的软件代码的存储器；例如，该软件已经被下载和/或存储在对应的存储器(例如，诸如RAM的易失性存储器或诸如闪存(未示出)的非易失性存储器)中。设备可以例如装备有微处理器和存储器(未示出)。备选地，设备可以全部或部分地在可编程逻辑中实现，例如作为现场可编程门阵列(FPGA)。设备和服务器可以全部或者部分地被实现为所谓的专用集成电路(ASIC)，即，针对其特定使用定制的集成电路(IC)。例如，电路可以例如使用诸如Verilog、VHDL等硬件描述语言在CMOS中实现。

[0125] 图2b示出了根据如参考1所描述的设备或服务器的实施例的处理器系统1100的示意性表示。处理器系统可以由一个或多个电路1110来实现，例如每个电路包括一个或多个集成电路。电路1110包括处理单元1120，例如CPU，用于运行计算机程序部件以执行根据实施例的方法和/或实施其模块或单元。电路1110包括用于存储编程代码、数据等的存储器

1122。存储器1122的部分可以是只读的。电路1110可以包括通信元件1126，例如，具有天线的收发器、连接器或两者等。电路1110可以包括专用集成电路1124，用于执行方法中定义的处理的一部分或全部。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由互连1130(比如说总线)彼此连接。处理器系统1110可以被布置用于分别使用天线和/或连接器的接触和/或无接触通信。

[0126] 软件可以仅包括由系统的特定子实体所采取的那些步骤。软件可以被存储在适合的存储介质(诸如硬盘、软盘、存储器等)中。软件可以沿着有线或者无线或者使用数据网络(例如，因特网)发送。软件可用于下载和/或用于在服务器上远程使用。根据本发明的方法可以使用被布置为将可编程逻辑(例如，现场可编程门阵列(FPGA))配置为执行方法的位流来执行。将意识到，软件可以以源代码、目标代码、代码中间源和目标代码的形式(诸如部分编译形式)或以适于使用在根据本发明的方法的实施方式中的任何其他形式。与计算机程序产品相关的实施例包括对应于本文所阐述的方法中的至少一个的处理步骤中的每一个的计算机可执行指令。这些指令可以细分为子例程和/或存储在可以静态或动态链接的一个或多个文件中。与计算机程序产品相关的另一实施例包括对应于系统和/或产品中的至少一个的每个装置的计算机可执行指令。

[0127] 将意识到，为了清晰起见，以上描述参考不同的功能单元和处理器描述本发明的实施例。然而，显而易见的是，可以在不同功能单元或处理器之间使用任何适合的功能分布而不脱离本发明。例如，图示为由单独的单元、处理器或控制器执行的功能可以由相同的处理器或控制器执行。因此，对特定功能单元的引用仅被看作对用于提供所描述的功能的适合模块的引用，而不是指示严格的逻辑或物理结构或组织。本发明可以以任何适合的形式实施，包括硬件、软件、固件或这些的任何组合。

[0128] 应注意，在该文档中，词语“包括”不排除除列出的那些之外的元件或步骤的存在，并且在元件前面的词语“一”或“一个”不排除多个这样的元件的存在，任何附图标记都不限制权利要求的范围，本发明可以通过硬件和软件两者实施，并且若干“模块”或“单元”可以由相同的硬件或软件表示，并且处理器可以可能与硬件元件协作来实现一个或多个单元的功能。而且，本发明不限于实施例，并且本发明位于每个新颖特征或者上文所描述或者在相互不同的从属权利要求中记载的特征的组合中。

[0129] 总之，本申请涉及根据安全协议在物理信道上在第一设备与第二设备之间建立安全通信的设备和方法。协议在第一设备中建立第一完整性数据，并且在第二设备中建立第二完整性数据。协议具有至少两个安全水平。所应用的安全水平是基于经由物理信道传输的分级信息可选择的。有利地，指示在第一和第二设备中的至少一个设备中最低要求的最小安全水平的分级指示器经由物理信道传输，同时基于完整性数据提供分级指示器的完整性保护。从而，可以防止降低安全水平的中间人攻击。

[0130] 参考文献：

[0131] [802.11]IEEE Computer Society,“IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific requirements Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications,”((IEEE Std.802.11-2016),2016年12月)

[0132] [802.1X]IEEE Std 802.1X™-2020,IEEE Standard for Local and Metropolitan Area Networks:Port-Based Network Access Control.

[0133] [X.680]ITU-T Recommendation X.680(2002)|ISO/IEC 8824-1:2002, Information technology-Abstract Syntax Notation One(ASN.1):Specification of basic notation.

[0134] [DH]Diffie,W.;Hellman,M.(1976),"New directions in cryptography"(IEEE Transactions on Information Theory,22(6):644-654)

[0135] [DPP]Device Provisioning Protocol-Technical Specification-Version 1.0,Wi-Fi Alliance,2018.

[0136] [FIPS180-4]FIPS180-4,"Secure Hash Standard"(United States of America, National Institute of Standards and Technology,Federal Information Processing Standard(FIPS)180-4)

[0137] [FIPS186-4]U.S.National Institute of Standards and Technology, "DIGITAL SIGNATURE STANDARD"(Federal Information Processing Standard FIPS-186-4,2013年7月)

[0138] [RFC 5216]RFC 5216,The EAP-TLS Authentication Protocol,2008年3月, https://datatracker.ietf.org/doc/rfc5216/

[0139] [RFC 5280]RFC 5280,Internet X.509Public Key Infrastructure Certificate and Certificate Revocation List(CRL)Profile,2008年5月,https://datatracker.ietf.org/doc/rfc5280/

[0140] [RFC 5281]RFC 5281,Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0(EAP-TTLSv0),2008年8月,https://datatracker.ietf.org/doc/rfc5281/

[0141] [RFC 8446]RFC 8446,The Transport Layer Security(TLS)Protocol Version 1.3,2018年8月,https://datatracker.ietf.org/doc/rfc8446/

[0142] [WFEC_2]Wi-Fi Easy Connect™Specification,Version 2.0,2020年12月14日, Wi-Fi Alliance.

[0143] [WPA3]WPA3™Specification,Version 3.0,2020年12月14,Wi-Fi Alliance, (WFA),www.wi-fi.org[2018PF00508]Patent application WO2020043634A1

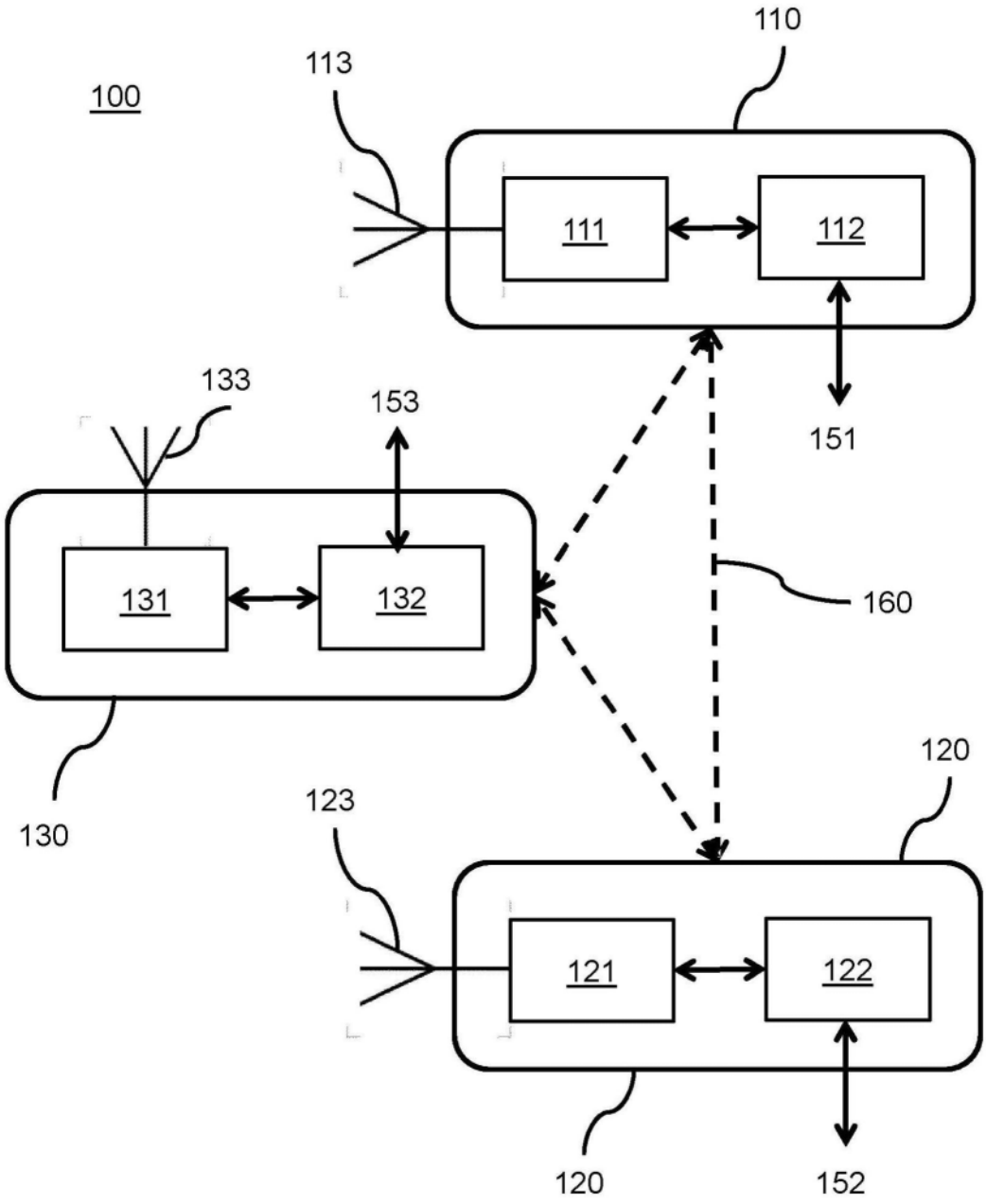

100
110
113
111
112
151
133
153
131
132
160
130
120
123
121
122
120
152

图1

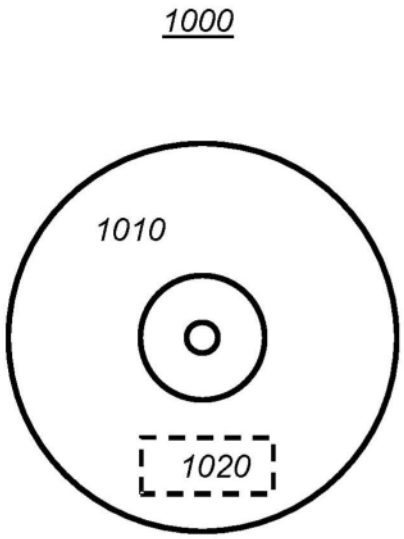


图2a

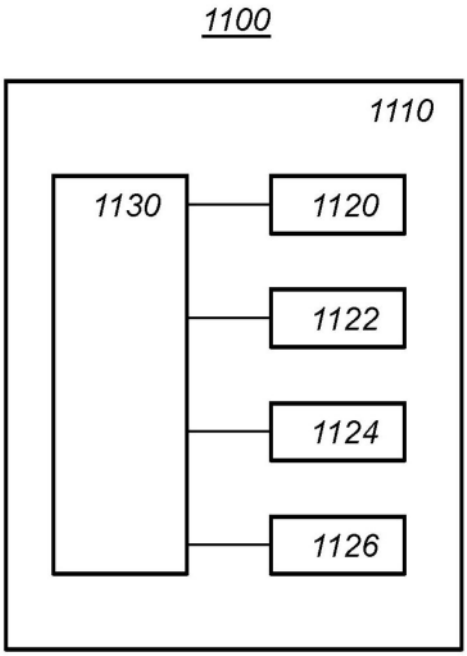


图2b