(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 102473219 B
(45)授权公告日 2015.01.28

(21)申请号 201080032992.6
(22)申请日 2010.07.01
(30)优先权数据
12/506568 2009.07.21 US
(85)PCT国际申请进入国家阶段日
2012.01.20
(86)PCT国际申请的申请数据
PCT/US2010/040732 2010.07.01
(87)PCT国际申请的公布数据
WO2011/011179 EN 2011.01.27
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 O.T. 乌雷彻 A.M. 塞门科
S. 维纳亚克 C.M. 埃利森
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 董宁 刘鹏
(51)Int.Cl.
G06F 21/60(2013.01)
H04L 9/32(2006.01)
(56)对比文件
CN 1695339 A,2005.11.09,
US 7028185 B2,2006.04.11, 说明书第73段,图73.
审查员 陈安安

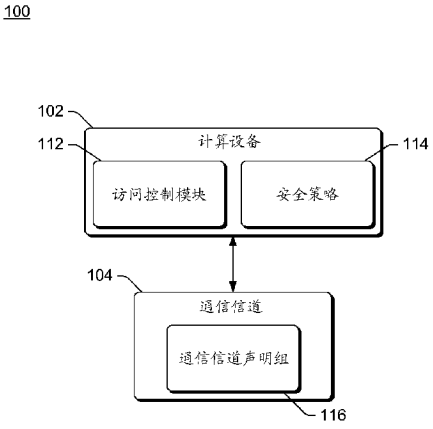
权利要求书2页 说明书9页 附图5页

(54)发明名称

通信信道声明相关的安全防范

(57)摘要

获得用于通信信道的安全声明组,所述安全声明组包括一个或多个安全声明,每一个安全声明标识通信信道的安全特性。这些安全声明被存储,由实体在所述安全声明组上生成的数字签名同样被存储。所述安全声明和数字签名随后在计算设备要向和/或从通信信道传输数据时被访问。将所述安全声明组与计算设备的安全策略进行比较,并且识别数字签名所述安全声明组的实体。计算设备在向和/或从通信信道传输数据时要使用的一个或多个安全防范至少部分地基于所述比较和已经数字签名所述安全声明组的实体来确定。



CN 102473219 B

1. 一种在计算设备中实现的方法，该方法包括：

响应于计算设备期望对通信信道设备的访问以及在确定计算设备和通信信道设备在数据传输期间要使用的安全防范之前：

获取（402）用于通信信道设备的安全声明组，所述安全声明组包括一个或多个安全声明，每个安全声明标识通信信道设备的安全特性，所述通信信道设备是便携式设备；

获得所述通信信道设备的信道标识符和信道类标识符；

将通信信道设备的所述安全声明组、信道标识符和信道类标识符与计算设备的安全策略进行比较（404）；

标识（406）已经数字签名所述通信信道设备的所述安全声明组、信道标识符和信道类标识符的实体；

确定（408）计算设备在向和/或从通信信道设备传输数据时要使用的一个或多个安全防范，所述确定至少部分地基于所述比较和已经数字签名所述通信信道设备的所述安全声明组、信道标识符和信道类标识符的实体。

2. 如权利要求 1 所述的方法，其中所述安全策略指示要使用特定加密类型来加密通信信道设备上的数据，其中所述安全声明组指示通信信道设备是否使用所述特定加密类型加密数据，并且所述确定包括：

如果通信信道设备不使用所述特定加密类型加密数据，确定要使用所述特定加密类型加密向通信信道设备传输的数据；以及

如果通信信道设备使用所述特定加密类型加密数据，确定不需要加密向通信信道设备传输的数据。

3. 如权利要求 1 所述的方法，其中所述安全策略指示要使用特定加密类型加密通信信道设备上的数据，除非特定实体负责控制通信信道设备，其中所述安全声明组指示所述特定实体是否负责控制通信信道设备，并且所述确定包括：

如果负责控制通信信道设备的实体不是所述特定实体，确定使用所述特定加密类型加密向通信信道设备传输的数据；以及

如果负责控制通信信道设备的实体是所述特定实体，确定不需要加密向通信信道设备传输的数据。

4. 如权利要求 1 所述的方法，其中所述安全策略指示通信信道设备要实施关于允许数据向通信信道设备传输的特定协定，其中所述安全声明组指示通信信道设备是否实施所述特定协定，并且所述确定包括：

如果通信信道设备实施所述特定协定，确定数据能够从通信信道设备传输；以及

如果通信信道设备没有实施所述特定协定，确定数据不从通信信道设备传输。

5. 如权利要求 1 所述的方法，进一步包括：

针对安全声明的附加组重复所述获取、比较和标识，所述安全声明的附加组和所述安全声明组已被不同的实体数字签名；以及

其中所述确定至少部分地基于比较所述安全声明组与所述安全策略，比较所述安全声明的附加组与所述安全策略，已经数字签名所述安全声明组的实体和已经数字签名所述安全声明的附加组的实体。

6. 如权利要求 5 所述的方法，其中所述安全声明组包括标识通信信道设备用来加密通

信信道设备接收的数据的加密类型的安全特性，并且所述安全声明的附加组包括标识通信信道设备用来加密通信信道设备接收的数据的密钥的源的安全特性。

7. 如权利要求 1 所述的方法，其中所述确定进一步至少部分地基于验证具有所述安全声明组的、已被所述实体数字签名的通信信道标识符与通信信道设备的通信信道标识符相同。

8. 如权利要求 1 所述的方法，其中所述安全声明组满足的安全防范不需要被包括在计算设备在向和 / 或从通信信道设备传输数据时要使用的所述一个或多个安全防范中。

9. 一种计算设备，包括：

处理器（502）；以及

一个或多个计算机可读介质（504），其耦合到该处理器并且存储多个指令，当这些指令由处理器执行时使得处理器：

获取（302）通信信道设备的信道标识符和信道类标识符，所述通信信道设备是便携式设备；

获取（304）通信信道设备的安全声明组，所述安全声明组包括一个或多个安全声明，每个安全声明标识通信信道设备的安全特性；

从信任机构获取（308）在所述安全声明组、所述信道标识符和所述信道类标识符上的数字签名；

生成（310）信道安全描述符，其包括所述信道标识符、所述信道类标识符、所述安全声明组和所述数字签名，当计算设备期望对通信信道设备的访问时所述信道安全描述符可用于计算设备分析；以及

存储（312）所述信道安全描述符。

10. 如权利要求 9 所述的计算设备，所述多个指令进一步使得处理器：

获取通信信道设备的安全声明的一个或多个附加组；

针对所述安全声明的一个或多个附加组中的每一个，获取在所述安全声明的附加组和信道标识符上的数字签名；以及

其中生成所述信道安全描述符是生成包括所述信道标识符、所述安全声明组、所述安全声明的附加组的每一个和所述数字签名的信道安全描述符。

11. 如权利要求 10 所述的计算设备，其中所述安全声明组包括指示通信信道设备用来加密由通信信道设备接收的数据的加密类型的第一安全特性，并且其中所述安全声明的附加组之一包括指示通信信道设备用来加密由通信信道设备接收的数据的密钥的源的第二安全特性。

12. 如权利要求 9 所述的计算设备，其中所述安全声明组包括指示通信信道设备用来加密由通信信道设备接收的数据的加密类型的安全特性。

通信信道声明相关的安全防范

背景技术

[0001] 随着计算机技术进步以及计算机变得日益普及，电子传输地数据量也得到增加。尽管这样的传输可能是非常有益的，但是它们不是没有它们的问题。一个这样的问题是进行传输的计算机能够信任它所传输的数据是以该计算机期望的方式保护的。给出可以电子地传输数据的多种不同方式，获得这种信任可能是困难的。

发明内容

[0002] 提供该发明内容以通过简化形式介绍在下面的具体实施方式中进一步描述的概念的选择。该发明内容不旨在标识要求保护的主题的关键特征或必要特征，也不旨在用于限制要求保护的主题的范围。

[0003] 根据一个或多个方面，获得用于通信信道的安全声明(claim)组，所述安全声明组包括一个或多个安全声明，每一个安全声明标识通信信道的安全特性。将所述安全声明组与计算设备的安全策略进行比较。此外，识别已经数字签名所述安全声明组的实体。一个或多个在向和/或从通信信道传输数据时计算设备要使用的安全防范至少部分地基于所述比较和已经数字签名所述安全声明组的实体来确定。

[0004] 根据一个或多个方面，获得通信信道的信道标识符。还获得通信信道的安全声明组，所述安全声明组包括一个或多个安全声明，每一个标识通信信道的安全特性。从信任机构获得所述安全声明组和信道标识符上的数字签名。生成并且存储包括信道标识符、安全声明组和数字签名的信道安全描述符。

附图说明

[0005] 在整个附图中，相同的数字用于引用相似的特征。

[0006] 图 1 图示了根据一个或多个实施例的实现通信信道声明相关的安全防范的示例系统。

[0007] 图 2 图示了根据一个或多个实施例的示例通信信道安全描述符。

[0008] 图 3 是图示根据一个或多个实施例的用于创建信道安全描述符的示例过程的流程图。

[0009] 图 4 是图示根据一个或多个实施例的用于确定要在向和/或从通信信道传输数据时使用的安全防范组的示例过程的流程图。

[0010] 图 5 图示了根据一个或多个实施例的、可以被配置成实现通信信道声明相关安全防范的示例计算设备。

具体实施方式

[0011] 本文讨论通信信道声明相关的安全防范。通信信道具有一个或多个标识由通信信道提供的安全或保护的安全声明的关联组。信道标识符和/或信道类标识符也与通信信道相关联。所述安全声明组以及信道标识符和信道类标识符中之一或两者被实体数字签名。

当确定是否向和 / 或从通信信道传输数据时，计算设备分析所述安全声明组、信道标识符和信道类标识符之一或两者、以及生成数字签名的特定实体。取决于该分析，计算设备确定在向和 / 或从通信信道传输数据时要采取的安全防范。

[0012] 本文参考对称密钥加密、公钥加密和公 / 私钥对。尽管这样的密钥加密对本领域技术人员而言是众所周知的，但是这里包括对这样的加密的简要概述以辅助读者。在公钥加密中，实体（比如用户、硬件或软件组件、设备、域等等）将它与公 / 私钥对相关联。可以使得公钥是可公开获得的，但是实体将私钥作为秘密保留。在没有私钥的情况下，对使用公钥加密的数据进行解密在计算上是非常困难的。所以，数据可以由具有公钥的任何实体加密并且仅由具有对应的私钥的实体解密。此外，用于数据的数字签名可以通过使用该数据和私钥来生成。在没有私钥的情况下，创建可以使用公钥验证的签名在计算是非常困难的。具有公钥的任何实体可以使用公钥通过对公钥、签名和被签名的数据执行适当的数字签名验证算法来验证数字签名。

[0013] 另一方面，在对称密钥加密中，共享密钥（也被称为对称密钥）被两个实体知道和保密。具有共享密钥的任何实体典型地能够解密利用该共享密钥加密的数据。在没有共享密钥的情况下，对利用共享密钥加密的数据进行解密在计算上是非常困难的。所以，如果两个实体都知道共享密钥，每个实体均可以加密数据，加密的数据可以由另一实体解密，但是其他实体在不知道共享密钥的情况下不能解密该数据。

[0014] 图 1 图示了根据一个或多个实施例的实现通信信道声明相关的安全防范的示例系统 100。系统 100 包括计算设备 102 和通信信道 104。计算设备 102 可以向和 / 或从通信信道 104 传输数据，从而允许设备 102 存储和并获取稍后使用的数据、向其他设备传输数据等等。该数据可以采取多种不同形式，比如程序指令或代码、用于程序的数据、表示图片（或视频、音乐等）的数据、其他类型的信息等等。

[0015] 计算设备 102 可以是多种不同类型的计算设备。例如，计算设备 102 可以是台式计算机、移动站、膝上型计算机或上网本、娱乐工具（appliance）、通信地耦合到显示设备的机顶盒、蜂窝或其他无线电话、个人数字助理（PDA）、游戏控制台、车用计算机等等。因此，计算设备 102 的范围可以是从具有大量存储器和处理器资源的全资源设备（例如个人计算机、游戏控制台）到具有有限的存储器和 / 或处理资源的低资源设备（例如，传统的机顶盒、手持式游戏控制台）。

[0016] 通信信道 104 可以是数据可以向和 / 或从其传输的多种不同类别或类型的信道。在一个或多个实施例中，通信信道 104 是可移动存储设备，比如闪存设备、磁盘、光盘等等。这样的可移动存储设备可以以多种不同的有线和 / 或无线方式耦合到计算设备。例如，可移动设备可以经由通用串行总线（USB）连接、无线 USB 连接、IEEE 1394 连接、蓝牙连接等等耦合到设备 102。

[0017] 在通信信道 104 是可移动存储设备的实施例中，这样的可移动存储设备典型地是可以容易运送到不同位置的便携式设备。该便携性允许用户容易移动设备并且将存储设备连接到不同的计算设备。例如，这种可移动存储设备可被称为拇指（thumb）驱动器。

[0018] 在其他实施例中，通信信道 104 可以采取其他的形式，比如允许信号或消息在计算设备 102 与另一个计算设备（其可以是类似于上面关于设备 102 所讨论的多种不同类型的设备的任意一种）之间传送的通信管道。多种不同的通信协议可以用于建立这种通信管

道，比如 TLS（传输层安全）协议、SSL（安全套接字层）协议、其他加密或非加密协议等等。通信管道可以经由各种通信链路来建立。例如，通信信道 104 可以是经由诸如因特网、局域网（LAN）、个域网、公用电话网、蜂窝或其他无线电话网等等之类的网络建立的通信管道。作为另一个示例，通信信道 104 可以是使用其他类型的耦合计算设备 102 和另一个计算设备的有线和 / 或无线链路建立的通信管道，该链路比如 USB 连接、无线 USB 连接、IEEE 1394 连接、蓝牙连接等等。

[0019] 计算设备 102 包括访问控制模块 112 和安全策略 114。访问控制模块 112 控制对通信信道 104 的访问，并且可以在软件、固件、硬件或其组合中实现。安全策略 114 标识要由访问控制模块 112 在控制对通信信道 104 的访问时实施的一个或多个安全防范。这些安全防范可以包括多种不同的安全防范，比如关于通信信道 104 是否加密数据、通信信道 104 加密数据的方式、负责管理或控制通信信道 104 的实体等等的限制。这些安全防范在下文中更详细地讨论。

[0020] 与通信信道 104 相关联的是通信信道声明组 116。声明组 116 标识关于通信信道 104 的一个或多个安全声明，每个安全声明标识通信信道 104 的安全特性。安全特性描述信道 104 的安全的一个或多个方面。可以描述信道 104 的安全的多种不同方面，比如通信信道 104 是否加密由信道 104 接收的数据、通信信道 104 加密由信道 104 接收的数据所使用的加密类型（例如，高级加密标准（AES）、数据加密标准（DES）、Rivest Shamir Adleman（RSA）等）、通信信道 104 的加密算法所使用的密钥的源、通信信道 104 的加密算法所使用密钥的生成方式、负责控制信道 104 的实体（例如，建立信道 104 的设备或模块、物理地携带并跟踪信道 104 的个体或群组等）、在允许数据被传输到信道 104 时由通信信道 104 实施的协定（比如保密协定）、通信信道 104 使用的协议（因特网协议安全（IPsec）、安全套接字层（SSL）、传输层安全（TLS）等），等等。

[0021] 通信信道声明组 116 可以存储在通信信道 104 上或者可替代地可以从其他源获取。例如，声明组 116 可以从另一个计算设备获取，可以被存储在计算设备 102（例如，保持在在计算设备 102 的高速缓存中），等等。

[0022] 在操作期间，访问控制模块 112 获取通信信道声明组 116 和安全策略 114。模块 112 将声明组 116 与安全策略 114 比较并且确定模块 112 在向和 / 或从通信信道 104 传输数据（例如，向其写入数据和 / 或从中读取数据）时要采取安全防范（如果有的话）。模块 112 在确定在向和 / 或从通信信道 104 传输数据时要采取安全防范（如果有的话）时，可以分析描述制造声明组 116 的声明的通信信道 104 和 / 或实体的附加信息。

[0023] 图 2 图示了根据一个或多个实施例的示例通信信道安全描述符 200。在这样的实施例中，每个通信信道具有相关联的通信信道安全描述符 200。安全描述符 200 可以存储在相关联的通信信道上，并且 / 或者单独存储（例如，从不同设备获取，由将数据向和 / 或从通信信道传输的计算设备保持，等等）。

[0024] 通信信道安全描述符 200 包括一个或多个（n 个）声明组 202、信道类标识符 204、信道标识符 206 和一个或多个（x 个）数字签名 208。可替代地，一个或多个声明组 202、标识符 204 和 208 以及数字签名 208 可以独立于描述符 200 存储。在其他可替代方案中，一个或多个声明组 202、标识符 204 和 208 以及数字签名 208 不需要被本文讨论的通信信道声明相关的安全防范使用。例如，信道类标识符 204 可以不包括在描述符 200 中或不被本文

所讨论的通信信道声明相关的安全防范使用。

[0025] 每个声明组 202 包括一个或多个(m 个)安全声明 212。每个声明组 202 可以是例如图 1 的声明组 116。每个安全声明 212 标识如上所讨论的相关联的通信信道的安全特性。每个声明组 202 与关联于通信信道的实体相关联,所述实体比如通信信道的制造商、通信信道的经销商、建立通信信道的模块或设备、控制通信信道的实体,等等。

[0026] 不同的实体可以制造关于相关联的通信信道的安全特性的不同声明,并且这些声明被存储为不同的声明组 202。例如,一个实体可以制造关于通信信道所使用的加密类型的声明,而另一个实体可以制造关于通信信道为加密所使用的密钥的源(或生成密钥的方式)的声明。作为另一个示例,一个实体可以制造关于通信信道的物理特性的声明(例如通信信道是无线的 USB 闪存设备),而另一个实体可以制造关于通信信道所使用的加密类型的声明。

[0027] 信道类标识符 204 是通信信道的特定类或类型的标识符。信道类标识符 204 允许不同类或类型的通信信道彼此区分。如上讨论,通信信道可以是不同类或类型的,其中每一个类或类型可以被分配不同的信道类标识符。相同的类的不同通信信道具有相同的类标识符 204。例如,一个类标识符可以用于闪存 USB 设备,另一个类标识符可以用于闪存无线 USB 设备,又一个类标识符可以用于 SSL 通信管道,等等。

[0028] 信道类标识符 204 可以以多种不同方式获得。如果通信信道是可移动存储设备,则信道类标识符 204 可以是在存储设备被创建时作为存储设备的一部分而包括在内的可移动存储设备的类的标识符、在存储设备首次使用时存储在存储设备上的标识符、在其他时间存储在存储设备上的标识符,等等。如果通信信道是通信管道,则信道类标识符 204 可以是从通信管道的不同参数或特性得出的标识符。例如,信道类标识符 204 可以通过确定用于通信管道的通信协议、确定通信管道是有线还是无线管道等等来获取。

[0029] 信道标识符 206 是特定通信信道的标识符。信道标识符 206 允许不同的通信信道彼此区分。两个不同的通信信道可以具有不同的信道标识符 206,即使它们可以具有相同的信道类标识符 204。

[0030] 信道标识符 206 可以以多种不同方式获取。如果通信信道是可移动存储设备,则信道标识符 206 可以是在存储设备被创建时作为存储设备的一部分而包括在内的可移动存储设备的标识符、在存储设备首次使用时存储在存储设备上的标识符、在其他时间存储在存储设备上的标识符,等等。如果通信信道是通信管道,则信道标识符 206 可以是从通信管道的不同参数或特性得出的标识符。例如,信道标识符 206 可以将特定算法应用到一个或多个用作通信管道的一部分的加密密钥、应用到通信管道的一个或多个配置设置等等来获取。

[0031] 每个声明组 202 由特定信任机构来证明。声明组 202 的该证明是由信任机构给出的、关于该声明组 202 中的一个或多个安全声明是真实和准确的证明。在一个或多个实施例中,该证明是数字签名 208 的形式。信任机构在声明组 202 上生成数字签名并且将所生成的数字签名存储为数字签名 208。信任机构还典型地在信道类标识符 204 和 / 或信道标识符 206 上也生成数字签名。通过数字签名声明组和标识符 204 和 / 或 206,声明组和标识符被捆绑在一起。该捆绑在一起允许验证数字签名的设备被确保具有特定标识符的通信信道具有包括在声明组中的特定安全特性。

[0032] 数字签名 208 是使用特定实体的公 / 私钥对的私钥生成的数字签名。该实体还可以被称为信任机构，因为数字签名是由该实体给出的、关于被数字签名的信息可被信任的证明。每个数字签名 208 典型地还包括或具有与其相关联的（例如，被包括在包括数字签名的数字证书中）实体的标识符和 / 或用于生成数字签名 208 的公 / 私钥对的公钥。多种不同的实体可以生成数字签名，比如通信信道的制造商、建立通信信道的设备、另一个受信任的第三方（例如，证明机构）等等。不管生成数字签名的实体，由该实体负责验证正在被数字签名的信息（例如，声明、标识符等）是准确的。

[0033] 当计算设备期望对通信信道进行访问时，设备的访问控制模块（例如图 1 的访问控制模块 112）分析声明组 202 以及信道安全描述符 200 中的其他信息。该分析依照设备的安全策略（例如，图 1 的安全策略 114）来执行，该安全策略指示由设备的访问控制模块期望的安全防范。访问控制模块要使用的安全防范然后可以基于该分析来确定。由通信信道提供的安全防范（如由安全声明确定）不需要由访问控制模块来复制。例如，如果安全策略指示通信信道上的数据的加密是所期望的，并且安全声明指示通信信道加密它接收的数据，则访问控制模块不需要在将数据传输到通信信道之前加密它。然而，如果安全策略指示通信信道上的数据的加密是所期望的，而没有安全声明指示通信信道加密它接收的数据，则访问控制模块在将数据传输到通信信道之前加密它。

[0034] 各种分析可以由访问通信信道的设备的访问控制模块来执行。该分析可以包括例如分析声明组中的安全声明、分析信道类标识符、分析信道标识符、分析数字签名等等。

[0035] 在一个或多个实施例中，访问控制模块分析数字签名 208 并至少部分地基于该分析确定它要使用的安全防范。作为分析数字签名 208 的一部分，数字签名 208 可以被验证。该验证可以使用生成如上所讨论的数字签名的实体的公钥来执行。如果数字签名未得到验证，则已被签名的信息不是受信任的。然而，如果数字签名得到验证，则已被签名的信息可以被信任或不受信任，如下所讨论。

[0036] 此外，作为分析数字签名 208 的一部分，可以针对生成数字签名的实体是否受信任和 / 或生成数字签名的实体受信任到什么程度做出确定。访问控制模块可以将生成数字签名的实体与实体的列表或其他记录进行比较以确定实体的信任水平。不同的实体可以具有不同的信任水平。例如，一些实体可以足够受信任，以使得访问控制模块信任该实体已经数字签名的无论任何信息。作为另一个示例，其他实体可能不受信任，使得访问控制模块不信任该实体数字签名的任何信息。作为又一个示例，另外其他实体可以是部分受信任的，使得访问控制模块信任该实体已经数字签名的一些信息，但是不信任其他信息（例如，信任已被签名的信道标识符，但是不信任关于所执行的加密类型的签名的声明）。

[0037] 实体的列表或其他记录和它们的信任水平可以在多种不同位置保持。例如，所述列表或其他记录可以作为安全策略的一部分而被保持或者可替代地独立于安全策略而被保持。

[0038] 在一个或多个实施例中，访问控制模块分析信道类标识符 204 并至少部分地基于该分析确定它要使用的安全防范。作为分析信道类标识符的一部分，对于不同信道类可以期望不同的安全防范。这些不同的期望安全防范可以例如在由访问控制模块访问的安全策略中标识。例如，该安全策略可以指示一种加密类型对于无线 USB 闪存设备通信信道类的通信信道是期望的，而另一种加密类型对于有线 USB 闪存设备通信信道类的通信信道是期

望的。

[0039] 在一个或多个实施例中，访问控制模块分析声明组 202 并至少部分地基于该分析确定它要使用的安全防范。作为分析声明组的一部分，针对声明组中的安全声明是否满足期望的安全策略中的安全防范做出确定。如果安全声明指示由安全防范指示的特定安全由（或为）通信信道提供，则安全声明满足安全防范。如果安全声明组满足期望的安全策略中的安全防范，则访问控制模块知道该安全防范由（或另外地，为）通信信道处理并且因此不需要由访问控制模块来执行。

[0040] 作为分析声明组的一部分，声明组的数字签名被分析，包括被验证，如上所讨论的。此外，作为分析的一部分，访问控制模块获取通信信道的信道标识符，并且验证通信信道的信道标识符与信道标识符 206 相同和验证数字签名 208 将声明组 202 捆绑到信道标识符 206。该验证向访问控制模块确保声明组中的安全声明确实是用于该通信信道的正确的安全声明（被数字签名）。

[0041] 基于由访问控制模块执行的分析，访问控制模块可以容易地标识用于特定通信信道的期望的安全防范和特定通信信道已经满足的安全防范。那些特定通信信道尚未满足的安全防范然后由访问控制模块在向和 / 或从通信信道传输数据时使用。

[0042] 由访问控制模块执行的分析可以以不同方式执行。在一个或多个实施例中，访问控制模块以包括用于通信信道的所有期望安全防范的安全防范列表开始它的分析。声明组的安全声明被分析，并且对于满足期望安全防范的每个安全声明，满足的期望安全防范从列表中被移除。在声明组的安全声明被分析之后，安全防范的剩余列表是由访问控制模块在向和 / 或从通信信道传输数据时使用的安全防范列表。

[0043] 可替代地，由访问控制模块使用的安全防范可以以其他方式来标识。例如，访问控制模块可以以空的安全防范列表开始。期望的安全防范被分析，并且对声明组的安全声明不满足的每个安全防范，该期望的安全防范被添加到安全防范列表。在期望的安全防范被分析之后，安全防范列表是由访问控制模块在向和 / 或从通信信道传输数据时使用的安全防范列表。

[0044] 图 3 是图示根据一个或多个实施例用于创建信道安全描述符的示例过程 300 的流程图。过程 300 由一个或多个计算设备，比如图 1 的计算设备 102 和 / 或另一个计算设备来执行，并且可以在软件、固件、硬件或其组合中实现。过程 300 被示出为一组动作但不限于所示出的用于执行各种动作的操作的顺序。过程 300 是用于创建信道安全描述符的示例过程；创建信道安全描述符的附加讨论参考不同附图而包括在本文中。

[0045] 在过程 300 中，获取通信信道的标识符（动作 302）。该信道标识符可以如上所讨论的基于特定通信信道而以不同方式被获取。例如，该信道标识符可以是从可移动存储设备获取的标识符、基于一个或多个用作通信管道的一部分的加密密钥生成的标识符等等。

[0046] 也获取通信信道类的标识符（动作 304）。该信道类标识符可以如上所讨论的基于特定通信信道而以不同方式获取。例如，该信道类标识符可以是从可移动存储设备获取的标识符、通过确定用于建立通信管道的通信协议获取的标识符等等。

[0047] 也获取用于通信信道的一个或多个安全声明的组（动作 306）。这安全声明组可以以多种不同方式获取，比如由实现过程 300 的设备的当前用户指定、由实现过程 300 的设备的另一个组件或模块指定、由实现过程 300 的设备的当前安全策略指定、由另一个设备指

定，等等。

[0048] 从信任机构获取该安全声明组和标识符上的数字签名(动作 308)。该信任机构可以是实现过程 300 的设备，或可替代地可以是另一个设备。使用生成数字签名的设备(或其模块或组件)的公 / 私钥对的私钥生成该数字签名。

[0049] 生成包括信道标识符、信道类标识符、安全声明组和数字签名的信道安全描述符(动作 310)。动作 302-308 可以重复以生成包括在信道安全描述符中的安全声明的附加组。

[0050] 存储信道安全描述符(动作 312)以用于后续使用。该信道安全描述符可以存储在通信信道上，或可替代地单独存储，如上所讨论的。

[0051] 应当理解，过程 300 的一个或多个动作可以不被执行。例如，动作 304 可以不被执行，在此情况下，在信道标识符和安全声明组但没有信道类标识符上生成动作 308 中生成的数字签名。

[0052] 还应当注意，动作 306 和 308 可以(由相同的计算设备或不同的计算设备)重复多次，并且安全声明和数字签名的结果组存储在相同的信道安全描述符中。

[0053] 图 4 是图示根据一个或多个实施例的用于确定要在向和 / 或从通信信道传输数据时使用的安全防范组的示例过程 400 的流程图。过程 400 由诸如图 1 的计算设备 102 之类的计算设备执行，并且可以在软件、固件、硬件或其组合中实现。过程 400 被示出为一组动作而不限于被示出的用于执行各种动作的操作的顺序。过程 400 是用于确定要在向和 / 或从通信信道传输数据时使用的安全防范组的示例过程；确定要在向和 / 或从通信信道传输数据时使用的安全防范组的附加讨论参考不同附图而包括在本文中。

[0054] 在过程 400 中，获取用于通信信道的安全声明组(动作 402)。该安全声明组可以从通信信道或如上所讨论的其他组件、模块或设备获取。

[0055] 将该安全声明组与实现过程 400 的计算设备的安全策略进行比较(动作 404)。该比较包括识别该安全声明组的安全声明满足安全策略的哪些安全防范。

[0056] 还标识已经数字签名该安全声明组的实体(动作 406)。该实体可以以不同方式标识，比如如上所讨论的根据数字签名来标识。

[0057] 基于安全声明组与实现过程 400 的计算设备的安全策略的比较以及数字签名了安全声明组的实体，确定要在向和 / 或从通信信道传输数据时使用的安全防范(如果有的话)(动作 408)。动作 408 中的确定还可以基于附加的分析，比如如上所讨论的对通信信道的信道类标识符的分析。

[0058] 本文所讨论的通信信道声明相关的安全防范提供了各种使用场景。例如，计算设备的安全策略可以指示特定加密类型将被用于通信信道。如果通信信道的声明组中没有安全声明指示通信信道使用该特定加密类型，则计算设备使用该特定加密类型来对向通信信道传输的数据进行加密(并且对从通信信道传输的数据进行解密)。然而，如果通信信道的声明组中的安全声明指示通信信道使用该特定加密类型，则计算设备不需要对向通信信道传输的数据进行加密(或对从通信信道传输的数据进行解密)。

[0059] 继续该示例，计算设备的安全策略可以进一步指示，如果通信信道受到特定个体或群体的控制，则不需要对通信信道使用加密。如果通信信道的声明组中的安全声明指示该特定个体或群体正在控制通信信道，则计算设备不需要对向通信信道传输的数据进行加密(和对从通信信道传输的数据进行解密)，而不管通信信道是否对数据进行加密。如果通

信信道的声明组中没有安全声明指示该特定个体或群体正在控制通信信道，则如上所述的那样基于声明组中的安全声明是否指示该特定加密类型被通信信道使用而对向通信信道传输的数据进行加密(和对从通信信道传输的数据进行解密)。

[0060] 作为另一个示例，计算设备的安全策略可以指示特定加密类型要被用于通信信道，并且指示用于该特定加密类型的密钥将由受信任源生成。如果通信信道的声明组中的安全声明指示该特定加密类型的被通信信道使用，并且进一步指示用于该加密的密钥由在被计算设备信任的实体列表上的源生成，则计算设备可以向和 / 或从通信信道传输数据，而无需加密向通信信道传输的数据(和解密从通信信道传输的数据)。否则，计算设备加密向通信信道传输的数据(并且解密从通信信道传输的数据)。

[0061] 作为又一个示例，计算设备的安全策略可以指示从通信信道传输的数据服从特定契约或协定，该契约或协定免除计算设备(和 / 或计算设备的用户) 由于查看通信信道上的数据而产生的任何影响(taint) 或其他倾向性(liability)。如果通信信道的声明组中的安全声明指示这样的契约或协定存在，则计算设备可以从通信信道传输数据(假设安全策略的剩余部分也得到满足)。然而，如果通信信道的声明组中没有安全声明指示这样的契约或协定存在，则计算设备不从通信信道传输数据。

[0062] 图 5 图示了根据一个或多个实施例的可被配置成实现通信信道声明相关的安全防范的示例计算设备 500。计算设备 500 可以是例如图 1 的计算设备 102 或实现本文所讨论的一个或多个技术的另一个计算设备。

[0063] 计算设备 500 包括 :一个或多个处理器或处理单元 502 ;一个或多个计算机可读介质 504，其可以包括一个或多个存储器和 / 或存储组件 506 ;一个或多个输入 / 输出(I/O) 设备 508 ;以及总线 510，其允许各种组件和设备相互通信。存储器和 / 或存储组件 506 可以包括例如可移动存储设备(例如图 1 的通信信道 104)。计算机可读介质 504 和 / 或一个或多个 I/O 设备 508 可以作为计算设备 500 一部分而被包括在内，或可替代地可以耦合到计算设备 500。总线 510 表示一个或多个若干类型的总线结构，包括使用多种不同总线结构的存储器总线或存储器控制器、外围总线、加速图形端口、处理器或局部总线等等。总线 510 可以包括有线和 / 或无线总线。

[0064] 存储器 / 存储组件 506 表示一个或多个计算机存储介质。组件 506 可以包括易失性介质(比如随机存取存储器(RAM))和 / 或非易失性介质(比如只读存储器(ROM)、闪存、光盘、磁盘等等)。组件 506 可以包括固定介质(例如 RAM、ROM、固定硬盘驱动器等) 以及可移动介质(例如闪存驱动器、可移动硬盘驱动器、光盘等等)。

[0065] 本文所讨论技术可以在软件中利用由一个或多个处理单元 502 执行的指令来实现。应当理解，不同的指令可以存储在计算设备 500 的不同组件中，比如在处理单元 502 中、在处理单元 502 的各种高速缓存存储器中、在设备 500 的其他高速缓存存储器(未示出)中、在其他计算机可读介质上等等。此外，应当理解，指令存储在计算设备 500 中的位置可以随时间改变。

[0066] 一个或多个输入 / 输出设备 508 允许用户向计算设备 500 输入命令和信息，并且还允许将信息呈现给用户和 / 或其他组件或设备。输入设备的示例包括键盘、光标控制设备(例如鼠标)、麦克风、扫描器等等。输出设备的示例包括显示设备(例如监视器或投影仪)、扬声器、打印机、网卡等等。

[0067] 在本文中可以在软件或程序模块的大体上下文中描述各种技术。一般地，软件包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。这些模块和技术的实现可以存储在某种形式的计算机可读介质上或跨越某种形式的计算机可读介质传送。计算机可读介质可以是可被计算设备访问的任何可用介质或媒质。作为示例而非限制，计算机可读介质可以包括“计算机存储介质”和“通信介质”。

[0068] “计算机存储介质”包括以用于存储信息(比如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括但不限于，RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光学存储、盒式磁带、磁带、磁盘存储或其他磁存储设备、或可以用于存储期望信息并可以被计算机访问的任何其他介质。

[0069] “通信介质”典型地将计算机可读指令、数据结构、程序模块或其他数据体现在已调制的数据信号中，比如载波或其他传送机制。通信介质还包含任何信息传递介质。术语“已调制的数据信号”意指这样的信号，其将其一个或多个特性以使得信号中的编码信息的方式设置或改变。作为示例而不是限制，通信介质包含诸如有线网络或直接有线连接之类的有线介质和诸如声学、RF、红外和其他无线介质之类的无线介质。上述任意介质的组合也包括在计算机可读介质的范围内。

[0070] 一般地，本文所描述的任何功能或技术可以使用软件、固件、硬件(例如固定逻辑电路)、手动处理或这些实现方式的组合来实现。本文所使用的术语“模块”和“组件”大体表示软件、固件、硬件或其组合。在软件实现方式的情况下，模块或组件表示在处理器(例如一个或多个 CPU)上被执行时执行指定任务的程序代码。该程序代码可以存储在一个或多个计算机可读存储器设备中，其进一步的描述可以参考图 5 找到。本文所描述的通信信道声明相关的安全防范的特征是独立于平台的，这意味着所述技术可以在具有多种处理器的多种商业计算平台上实现。

[0071] 尽管已经以特定于结构特征和 / 或方法动作的语言描述了本主题，但是应当理解，所附权利要求中定义的主题不必限于上述特定特征或动作。相反，上述特定特征和动作是作为实现权利要求的示例形式而被公开的。

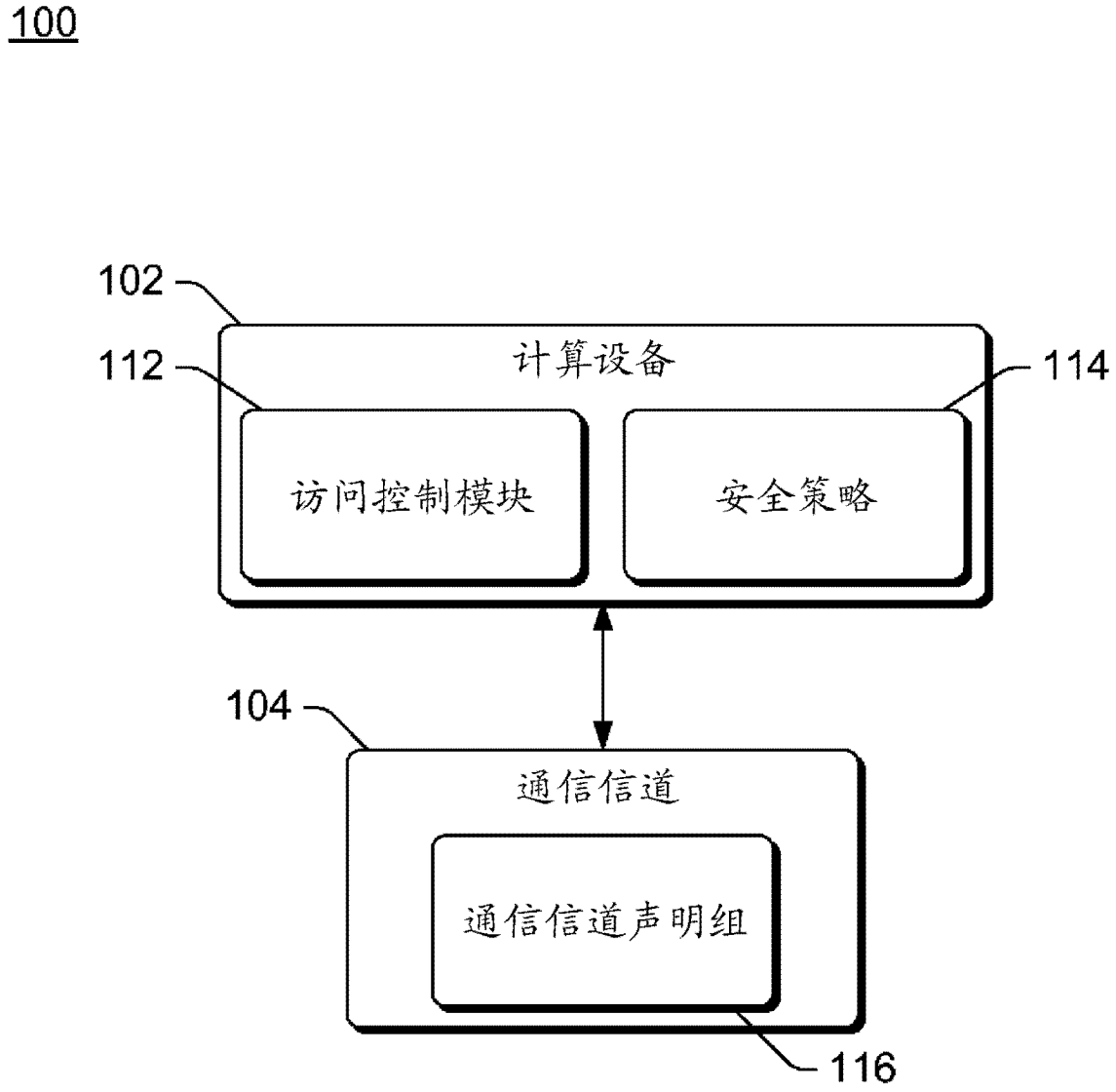


图 1

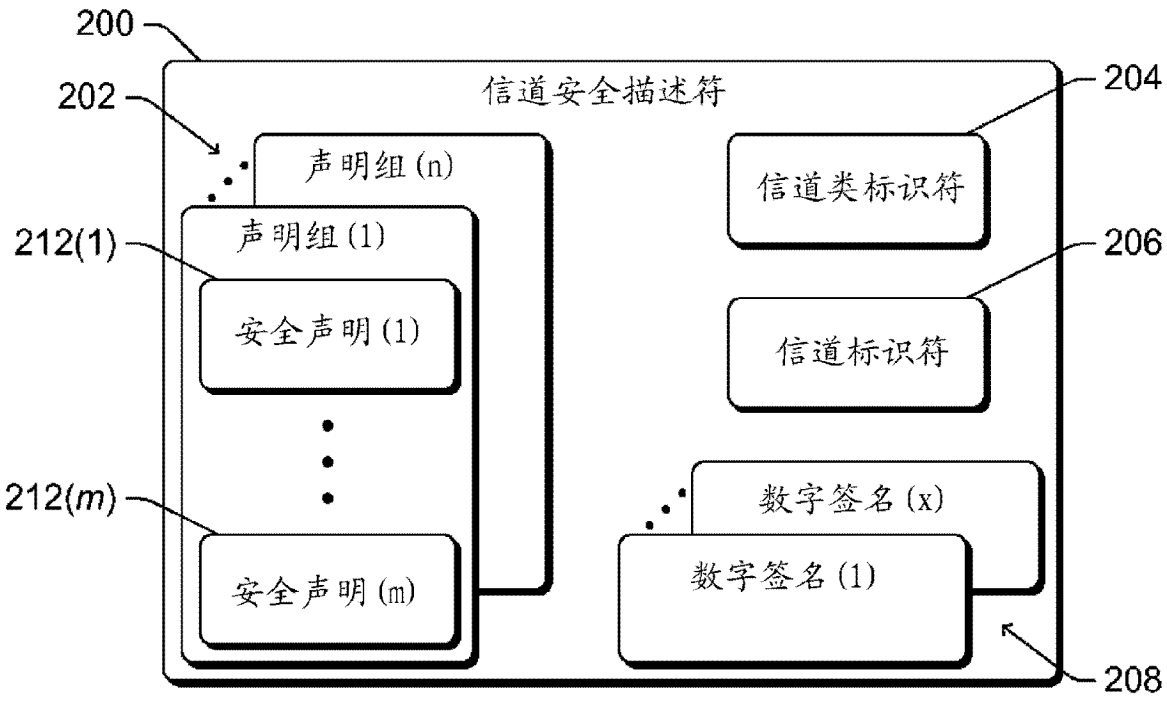

200
信道安全描述符
202
204
声明组 (n)
信道类标识符
212(1)
声明组 (1)
206
安全声明 (1)
信道标识符
212(m)
数字签名 (x)
安全声明 (m)
数字签名 (1)
208

图 2

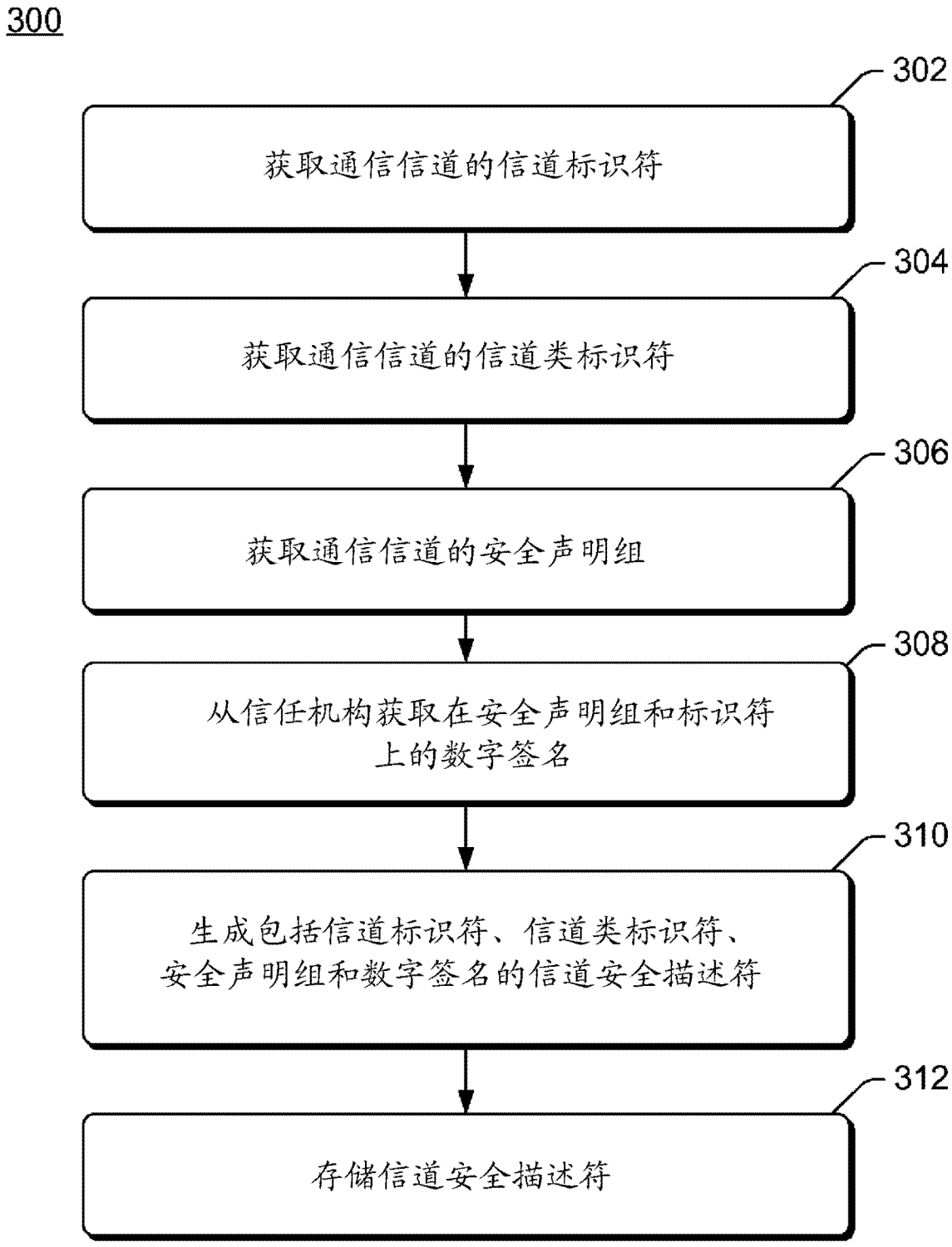

300
302
获取通信信道的信道标识符
304
获取通信信道的信道类标识符
306
获取通信信道的安全声明组
308
从信任机构获取在安全声明组和标识符上的数字签名
310
生成包括信道标识符、信道类标识符、安全声明组和数字签名的信道安全描述符
312
存储信道安全描述符

图 3

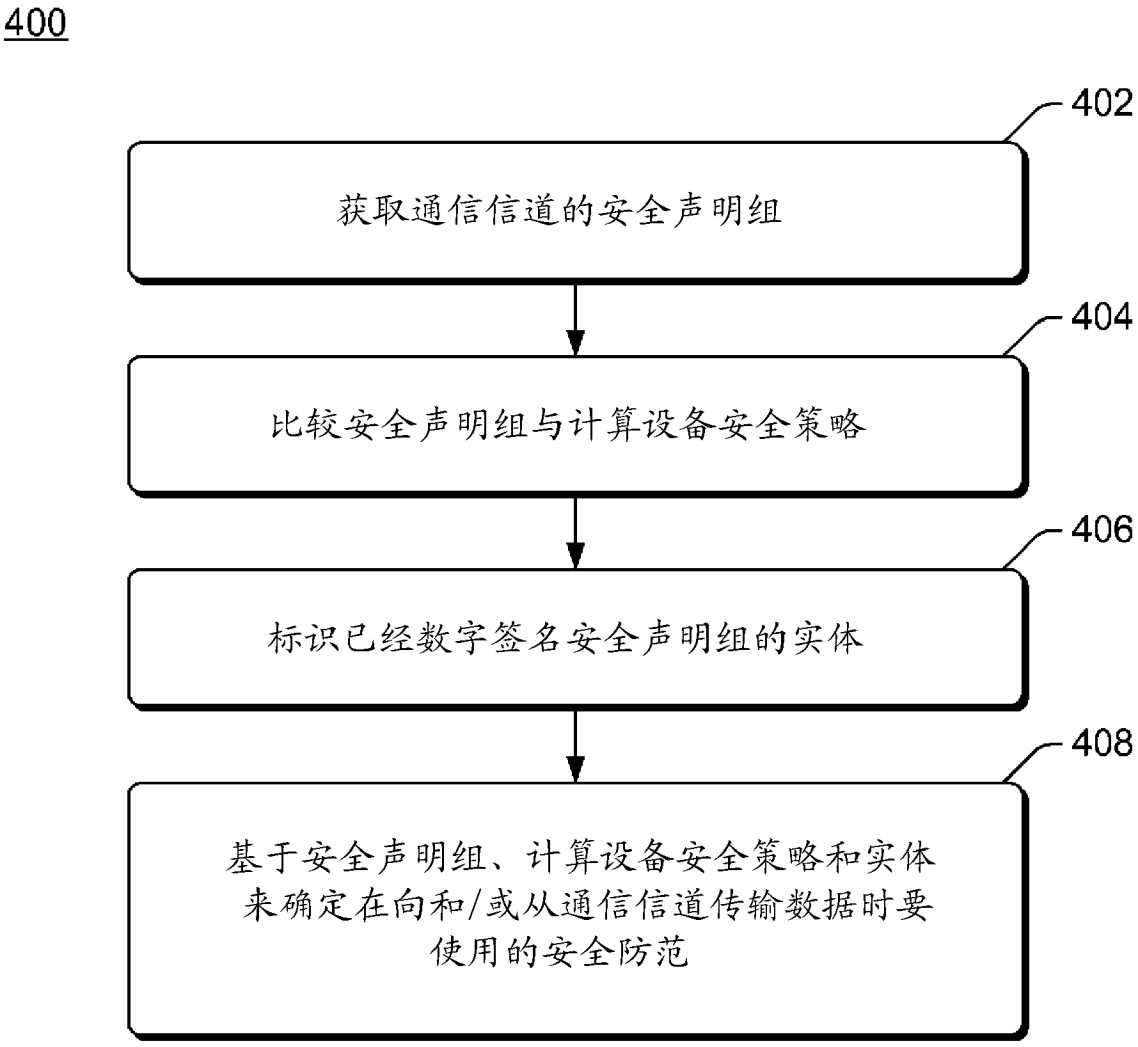

400
402
获取通信信道的安全声明组
404
比较安全声明组与计算设备安全策略
406
标识已经数字签名安全声明组的实体
408
基于安全声明组、计算设备安全策略和实体来确定在向和/或从通信信道传输数据时要使用的安全防范

图 4

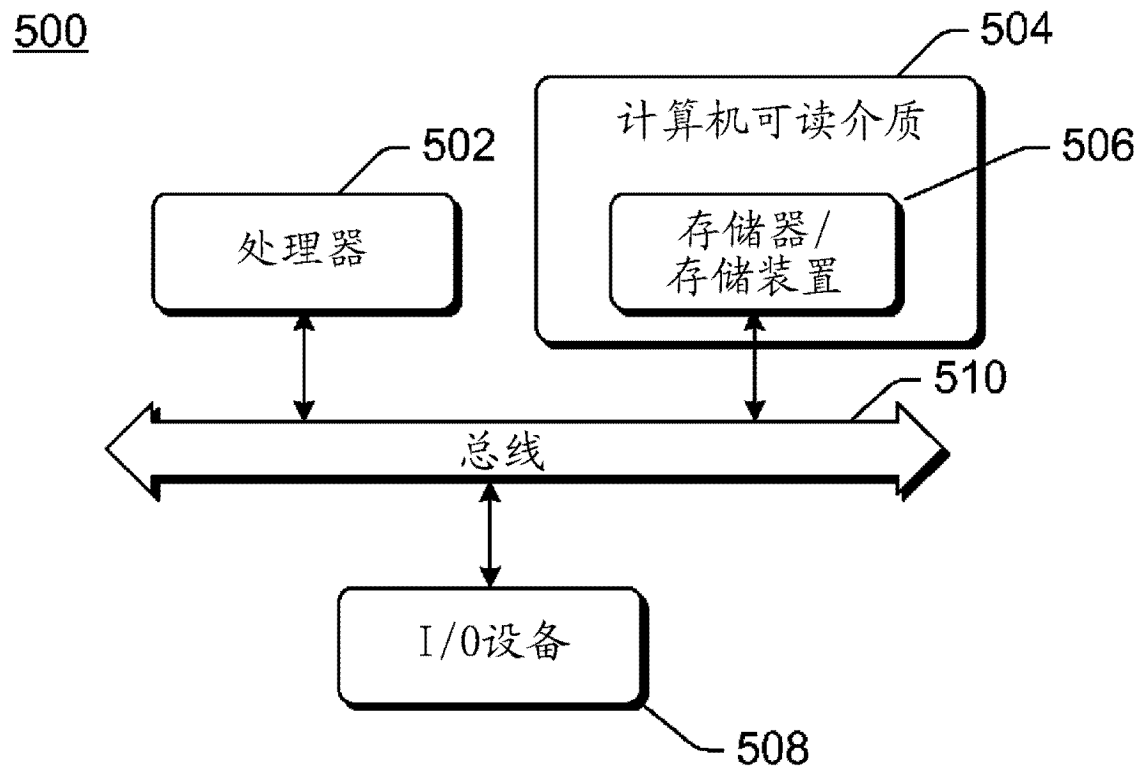


图 5