(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102132594 A
(43)申请公布日 2011.07.20

(21)申请号 200980133794.6

(22)申请日 2009.06.12

(30)优先权数据
12/163,517 2008.06.27 US

(85)PCT申请进入国家阶段日
2011.02.24

(86)PCT申请的申请数据
PCT/US2009/047182 2009.06.12

(87)PCT申请的公布数据
WO2009/158214 EN 2009.12.30

(71)申请人 微软公司
地址 美国华盛顿州

(72)发明人 C·E·赫雷

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 黄嵩泉

(51)Int.Cl.
H04W 12/06(2006.01)
G06F 21/00(2006.01)

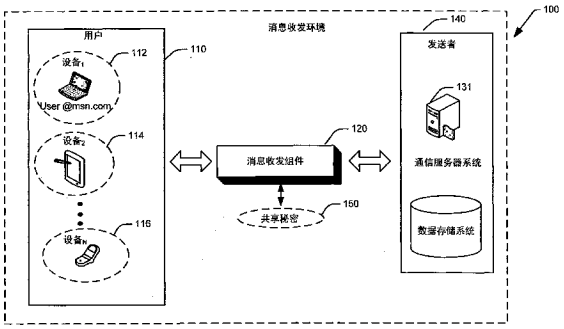
权利要求书 2 页 说明书 9 页 附图 9 页

(54)发明名称

通信认证

(57)摘要

各系统和方法通过展示共享秘密的知识但不揭露这一秘密来认证消息发送者从而在消息接收者(例如,用户)和消息发送者之间建立信任。消息收发组件可以按共享秘密所指导地将消息传达给受用户控制的通信系统。因此,用户可以容易地确定消息发送者是该发送者所声称的人,因为发送者已经通过将消息发送给由用户确定的通信系统来展示共享秘密的知识。此外,通常通过在通信期间不实际揭示共享秘密来确保秘密的稳健性。



CN 102132594 A

1. 一种计算机实现的方法，包括：

定义消息的发送者 (140) 和接收者 (110、612) 之间的共享秘密 (150、250)；所述共享秘密 (150、250) 与所述接收者 (110、612) 访问第一通信帐户 (212) 和第二通信帐户 (214) 的能力相关联；以及

在将消息发送给所述第一通信帐户 (212) 时，提示发送者对所述第二通信帐户 (214) 的知识。

2. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述提示动作还采用揭示所述第一或第二通信帐户的部分信息的散列函数。

3. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述提示动作还包括使得所述接收者能够推断发送者具有所述共享秘密的知识。

4. 如权利要求 1 所述的计算机实现的方法，其特征在于，还包括将语音转换为文本。

5. 如权利要求 2 所述的计算机实现的系统，其特征在于，还包括在不揭示所述共享秘密的情况下展示所述共享秘密的知识。

6. 如权利要求 1 所述的计算机实现的系统，其特征在于，还包括所述发送者在发送电子邮件消息之后留下语音邮件、或发送即时消息、或其组合。

7. 如权利要求 2 所述的计算机实现的系统，其特征在于，还包括配对所述第一和第二通信帐户。

8. 如权利要求 2 所述的计算机实现的系统，其特征在于，还包括将一个电子邮件帐户指定为主帐户。

9. 如权利要求 1 所述的计算机实现的系统，其特征在于，还包括验证与所述共享秘密的一致性。

10. 如权利要求 1 所述的计算机实现的系统，其特征在于，还包括在所述消息的一部分中包括所述消息已经被发送至两个通信帐户的指示。

11. 一种计算机实现的系统，包括以下计算机可执行组件：

接收在消息的发送者 (140) 和接收者 (110、612) 之间定义的共享秘密 (150、250) 的用户界面组件，所述共享秘密 (150、250) 与所述接收者 (110、612) 访问第一通信帐户 (212) 和第二通信帐户 (214) 的能力相关联；以及

向所述接收者 (110、612) 提示知道关于所述共享秘密 (150、250) 的消息收发组件 (120、325、660)。

12. 如权利要求 11 所述的计算机实现的系统，其特征在于，所述第一通信帐户和所述第二通信帐户是从电子邮件、语音邮件、传真、即时消息收发、文本消息收发或电话的组中选择的。

13. 如权利要求 11 所述的计算机实现的系统，其特征在于，还包括揭示所述第一或第二通信帐户中的一个的部分信息的映射函数。

14. 如权利要求 11 所述的计算机实现的系统，其特征在于，所述用户界面组件带有为所述消息指定的重要性级别。

15. 一种计算机实现的系统，包括以下计算机可执行组件：

用于通过在不揭示共享秘密 (150、250) 的情况下展示共享秘密 (150、250) 的知识来将消息传达给通信系统 (212、214) 的装置；以及

用于接收所述通信系统 (212、214) 中的消息的装置。

通信认证

[0001] 背景

[0002] 通信技术的发展已经改变了常见的商业协议。随着人们通过替代媒介进行通信，人与人之间的直接交流越来越少。例如，电子邮件 (e-mail) 允许个人实际上瞬时地进行通信。实时通信允许个人就像是他们在一起一样进行通信，即使他们在物理上不在同一个位置。例如，员工可以在不离开他们的桌子或个人计算机的情况下通过即时信使服务来进行通信。

[0003] 随着因特网作为业务媒介的不断普及，用户在线参加越来越多样的交易。这些交易中的某些，诸如与金融机构或在线零售商的交易，可能涉及敏感的个人信息，诸如银行帐号或信用卡信息。为保护这些信息，可以采用各种方法。例如，许多在线机构要求用户在在线交易任何业务之前向该机构注册并获得唯一的用户名和口令。

[0004] 网络钓鱼一般可以被描述为第三方企图通过假冒用户已知且信任的实体来欺骗用户向该第三方透露其用户名和口令。一般而言，网络钓鱼攻击可以通过向用户发送精心炮制的看上去源自已知且受信实体的电子邮件消息来发起。这些电子邮件消息常常通知接收者该实体必须通过让用户输入其用户名和口令来验证用户的信息。用户可能在看上去属于该已知且受信实体但实际上由第三方控制的网站处输入这一信息。一旦用户在第三方的网站（有时被称为网络钓鱼站点）处输入这一信息，则第三方可以在其假冒的实体的真实网站处使用所输入的用户名和口令来执行交易或者甚至从用户夺取对于已知且受信实体的帐户的控制。

[0005] 从计算机安全观点出发，若干因素使得网络钓鱼成为一个挑战性的问题。首先，在网络钓鱼攻击中，受害者在不知不觉或者无意中通过自愿向攻击者提供诸如用户名和口令之类的其安全凭证来协助攻击者。其次，使用固定算法来标识网络钓鱼站点可能是困难的，因为攻击者不但能快速适应安全措施，而且即使可能也难以用一组固定的规则来预测所有未来攻击者的独创性。再者，用户往往忽略有关安全危险的警告。如果用户不注意警告，那么即使呈现最好的警告也是没有用的。本文公开和描述的组件和方法将这些因素考虑在内以提供用于保护以防网络钓鱼攻击的手段。

[0006] 概述

[0007] 以下提出了简化概述以便提供对在此描述的某些方面的基本理解。此概述不是所要求保护的主题的详尽的概述。它既不旨在标识出所要求保护的主题的关键或重要的要素，也不描绘其范围。其唯一的目的是以简化形式呈现一些概念，作为稍后呈现的更详细描述的序言。

[0008] 本发明提供了通过用消息收发组件展示共享秘密的知识但不揭露这一秘密（例如，提示）来认证消息发送者从而在用户和消息发送者之间建立信任。该消息收发组件可以如共享秘密所指导地将消息传达给受用户控制的通信系统和 / 或通信帐户（例如，由用户控制的两个电子邮件、由用户控制的电话号码和电子邮件等等）。因此，用户可以容易地确定消息发送者是该发送者所声称的人，因为发送者已经通过将消息发送给由用户确定的通信系统来展示共享秘密的知识，其中通常通过在通信期间不揭露该共享秘密来确保秘密

的稳健性。

[0009] 在一相关方面，用户可以建立多个独立通信帐户（例如，两个电子邮件帐户），其中建议消息发送者：如果消息被发送到第一通信帐户，则在用户将该消息作为真实的来对待之前，必须将相同的消息发送到其他通信帐户。例如，共享秘密可以包括在将该消息传送到第一电子邮件帐户之后将消息传送到第二电子邮件帐户。因此，一旦发送者将消息发送到第一电子邮件帐户，该消息的一部分还可以包括本消息也被发送到了第二电子邮件（不需要实际指定整个地址，例如 xxxx@hotmail.com）。此外，发送者将消息发送到第二电子邮件帐户。这种与发送消息的方式的一致性通常可以确保发送者的真实性，因为恶意实体不容易得到共享秘密。

[0010] 在一相关方面，消息收发组件还可以包括可以存储由共享秘密定义的通信方式的注册组件。该注册组件可以向消息收发组件提供将消息传达给受用户控制的通信系统（例如，由用户控制的两个电子邮件、由用户控制的电话号码和电子邮件等等）的方式，如共享秘密所指导的。消息收发组件还可以包括将消息彼此独立地且如共享秘密所指导地发送的发送组件。该共享秘密对恶意实体要获得关于非公众可用的帐户的信息（例如，电子邮件别名）提出了巨大的挑战。

[0011] 根据本发明的方法，共享秘密最初可以由用户指定。该共享秘密可以涉及标识与用户通信的方式（例如，消息必须被发送到两个电子邮件地址，在发送一个电子邮件消息之后还需要联系一个电话号码，等等）。接着，用户可以接收到据称从发送者发送的消息。为了验证发送者的真实性，用户检查与共享消息的一致性。如果验证了一致性，则用户将所接收的消息作为真实的来对待。否则，用户可以忽略所接收的消息。在一相关方面，用户访问注册组件以获得关于共享秘密的更新。

[0012] 为实现上述及相关目的，在此结合以下描述和附图描述了所要求保护的主题的某些说明性方面。这些方面指示可实践本主题的各种方式，它们均落在所要求保护的主题的范围之内。当结合附图阅读以下详细描述时，本发明的其他优点和新颖特征将变得显而易见。

[0013] 附图简述

[0014] 图 1 示出根据本发明的一个方面的展示共享秘密的知识但不揭露共享秘密的系统的框图。

[0015] 图 2 示出根据本发明的一个方面的用于信任建立的特定系统。

[0016] 图 3 示出根据本发明的一个方面的认证消息发送者和用户 / 接收者之间的信任的系统的特定方面。

[0017] 图 4 示出根据本发明的又一方面的在用户和发送者之间建立信任的方法。

[0018] 图 5 示出根据本发明的又一方面的发送者认证的方法。

[0019] 图 6 示出根据本发明的又一方面的包括通知组件的系统的特定框图。

[0020] 图 7 示出根据本发明的又一方面的示例性图形用户界面。

[0021] 图 8 是根据本发明的一个方面的可被用作信任建立的一部分的示例计算环境 1000 的示意性框图。

[0022] 图 9 示出了用于实现本发明的各方面的示例性环境。

[0023] 详细描述

[0024] 现在将参考附图描述本发明的各方面，全部附图中相同的标号指的是相同或相应的元素。然而应该了解，附图及其相关详细描述不旨在将所要求保护的主题限于所公开的具体形式。相反，其意图是覆盖落在所要求保护的主题的精神和范围内的所有修改、等效和替换方案。

[0025] 图 1 示出能够通过用消息收发组件 120 展示共享秘密 150（例如，预先确定的）的知识但不揭示这一秘密 150 来认证消息发送者 140 以实现用户 110 和发送者 140 之间信任的建立。例如，发送者 140 可以是金融机构、电子商务企业、并且一般可以是用户 110 是其客户的任何实体，而来自发送者的消息可能遭受攻击。此外，共享秘密 150 可以涉及消息发送者应该与用户 116 进行通信的方式，例如，在将消息发送到电子邮件帐户 User@msn.com 之后，还要将消息发送到共享秘密所指定的另一因特网服务提供商上的电子邮件帐户，该帐户已经由用户为发送者 140 设置。

[0026] 如图 1 所示，用户侧 110 可以包括多个设备 112、114、116（1 到 N，其中 N 是一个整数），这些设备受用户 110 的控制并且可以从发送者 140 接收消息。设备 112、114、116 也可以是诸如系统区域网络或其他类型的网络等网络（例如，无线网络）的一部分，并且可包括若干主机（未示出），这些主机可以是个人计算机、服务器或其他类型的计算机。这些主机一般能够运行或执行一个或多个应用级（或用户级）程序，以及发起 I/O 请求（例如，I/O 读取或写入）。另外，网络可以是例如，以太网 LAN、令牌环 LAN 或其他 LAN、或广域网 (WAN)。此外，该网络还可包括硬连线和 / 或光学和 / 或无线连接路径。

[0027] 例如，通过将消息发送给由共享秘密 150 指导的设备 112、114、116，用户可以容易地确定消息发送者是该发送者所声称的人。换言之，因为发送者 140 已经通过将消息发送给由用户 110 早先标识的所选择的通信系统 / 设备来展示共享秘密 150 的知识，消息的真实性被证实。

[0028] 可以在设备 112、114、116 之间共享连接，这些设备还可以包括 :个人计算机、工作站、电视机、电话以及类似的设备。此外，网络还可包括一个或多个输入 / 输出单元 (I/O 单元），其中这些 I/O 单元可包括与其连接的一个或多个 I/O 控制器，并且每一个 I/O 都可以是若干种类型的 I/O 设备中的任一种，诸如存储设备（例如，硬盘驱动器、磁带驱动器）或其他 I/O 设备。主机和 I/O 单元及其附连的 I/O 控制器和设备可被组织成诸如群集等多个组，且每一群集都包括一个或多个主机并且通常包括一个或多个 I/O 单元（每一个 I/O 单元都包括一个或多个 I/O 控制器）。这些主机和 I/O 单元可经由连接一个或多个群集中的一组节点（例如，连接一组主机和 I/O 单元）的路由器、交换机和通信链路（诸如导线、连接器、电缆等）的集合来互连。可以理解，无线通信网络可以是蜂窝或 WLAN 通信网络 ;诸如全球移动通信系统 (GSM) 网络、通用移动电信系统 (UMTS) 网络、以及诸如网际协议语音 (VoIP) 和网际协议 (IP) 数据网络等无线 IP 网络。

[0029] 例如，用户 110 用来从发送者 140 接收消息的便携式设备可以是手持式无线通信设备，该手持式无线通信设备可以与无线通信网络（例如，无线通信网络）进行通信以便经由诸如蜂窝基站、移动交换中心、802.11x 路由器、802.16x 路由器等蜂窝接入点和 / 或无线接入网络 (WLAN) 接入点来上传和下载数字信息。便携式用户设备的其他示例可包括蜂窝通信设备、多模蜂窝设备、多模蜂窝电话、双模蜂窝设备、双模蜂窝 /WiFi 电话、或类蜂窝和 / 或组合蜂窝 / 固定网际协议 (IP) 接入设备。

[0030] 因此，系统 100 可以使得用户 110 能够容易地确定消息的发送者 140 是该发送者所声称的人，因为发送者已经通过将消息发送给由用户确定的通信系统来展示共享秘密的知识，其中通常通过在通信期间不揭露该共享秘密来确保秘密的稳健性。例如，发送者可以用间接建议或暗示的形式来提供提示（例如，该消息的副本已被发送至电子邮件帐户 snoop*****@hotmail.com，而不实际指示这一电子邮件地址）；和 / 或用使得用户能够推断消息发送者知道该共享秘密的形式来提供提示（例如，两次呼叫用户的蜂窝电话并挂断，在预定时间联系第一或第二通信帐户，在用户的语音邮件帐户上留下秘密的语音邮件，发送即时消息给用户或接收者）。

[0031] 图 2 示出示例性通信系统 200，其中用户可以建立多个通信帐户，诸如两个电子邮件账户形式的两个通信系统 212、214 和 / 或通信帐户。共享秘密 250 可以包括用户提供给消息发送者的指令，该指令指示如果将消息发送给第一通信系统 212，则必须将同一个消息发送给第二通信系统 214，其中两个通信系统 212 和 214 都受用户的控制。因此，在用户将这些消息作为真实的来对待之前，用户验证两个通信系统 212 和 214 的内容。

[0032] 例如，共享秘密可以包括在将该消息传送到第一电子邮件帐户之后将消息传送到第二电子邮件帐户。因此，一旦发送者将消息发送到第一电子邮件帐户，该消息的一部分还可以包括本消息也被发送到了第二电子邮件（不需要实际指定整个地址，例如 xxxx@hotmail.com）。此外，发送者将消息发送到第二电子邮件帐户。这种与发送消息的方式的一致性通常可以确保发送者的真实性，因为恶意实体不容易得到共享秘密。

[0033] 与发送者相关联的发送组件 204 准备要发送给路由器组件 206 并最终要发送给分别与通信系统 212、214 相关联的接收组件 218、228 的消息。例如，消息可以行进至耦合到存储介质 232 的路由器组件 206，其中路由器组件 206 处理到接收组件 216 和 218 的正确的发送。每一接收组件 218、228 可以从路由器组件 206 和 / 或发送组件 204 接收信息，并且通过例如解码器（未示出）来解压所接收的信息。此外，验证组件 280 可以验证该消息实际上是由通信系统 212 和 214 接收的。该验证组件可以在预定事件发生之后和 / 或周期性地检查通信系统 212、214 来确定实际上是否已经接收到消息。

[0034] 图 3 示出根据本发明的一个特定方面的认证消息发送者（例如，金融机构）和消息接收者（例如，金融机构的用户或客户）之间的信任的系统 300 的特定方面。例如，如果共享秘密要求消息发送者按预定次数留言（在将电子邮件发送给用户的主电子邮件帐户之后），系统 300 能够实现将该语音邮件转换成被发送到用户的主电子邮件帐户的附加电子邮件。因此，用户可以在从系统 300 接收到后续电子邮件之后验证早先的电子邮件的真实性。换言之，系统 300 可以通过按共享秘密所指示地转换金融机构（消息发送者）发送的语音和 / 或传真来提供附加电子邮件。

[0035] 系统 300 包括获取语音通信的分支交换组件 310，并且可以包括内联网协议 (IP) 分支交换 (IPBX)。此外，分支交换组件 310 可以是公共的（例如，中心局交换服务）或专用的 (PBX)。因此，分支交换组件 310 可以从常规电话系统接收通信，或者经由电话协议、IP 协议（例如，H.323、SIP 等）或任何其他公共或专用协议通过因特网等来接收通信。在接收到通信之后，分支交换组件 310 可以将该通信路由至转换组件 320。例如，分支交换组件 310 可以将无应答的呼叫或者被配置为应答传真的电话号码转发给转换组件 320。转换组件 320 可以从分支交换组件 310（或经由其提供的连接）接收通信，并且该转换组件 320 可以将所

接收的通信转换为电子邮件。例如，该通信可以在随后或者并发地被变换为 SMTP（简单邮件传输协议）消息。如图所示，系统 300 可以遵循用户和消息发送者之间的共享秘密中指定的方向来与消息收发组件 325 交互。

[0036] 在一相关方面，还可以记录或保存语音或传真消息，并将其提供为由系统 300 生成的电子邮件的附件。此外，该消息内容的一部分可以在正文中用例如 MIME（多用途因特网邮件扩展）格式来编码。还可以在正文中捕捉附加信息，诸如消息类型（例如，语音、传真）、呼叫电话号码、语音消息持续时间、语音消息发送者名、附件名和传真页数，等等。此外，MIME 消息随后可被转换成可以用消息分类的内部表示来存储的内部表示。

[0037] 在一相关方面，转换组件 320 还可以是可扩展的来采用第三方和 / 或非本机功能，例如，插件组件（未示出）所提供的功能。例如，这种插件组件可以提供算法来便于将语音到文本的转换或用于光学字符识别，并且因此转换组件 320 不需要单独提供所有功能。因此，可以更新转换组件 320 从而使得它可以例如将与电子邮件生成相关联的合适的技术或机制用作系统 300 的一部分。

[0038] 在一方面，可以将所生成的电子邮件或 SMTP 消息从转换组件 320 发送到消息服务器 330。消息服务器 330 可以处理消息以便传递给预期收件人邮箱等，从而使得这些消息可由电子邮件应用程序（例如，查看器 / 编辑器以及 POP 或 IMAP 客户端）接收或检索。例如，服务器 330 可以对应于邮箱、SMTP 和 / 或桥头服务器。还应认识到转换组件 320 可以是与 SMTP 服务器通信的 SMTP 客户端。除了将消息转发到收件人的一个或多个邮箱之外，消息服务器 330 还可以过滤这些消息。

[0039] 消息服务器可以采用音频代理 332 来扫描音频而非消息的文本预览。这些音频代理 332 可以基于语音音调、音量和 / 或词检查等等来进行评估。类似地，传真代理 334 可以扫描与所转换的结构化文档或预览分开的电子邮件的结构。还应注意到，这些代理 332 和 334 可以是由服务器厂商或第三方厂商等等生产的插件或附件。如早先所解释的，可以通过用消息收发组件 325 展示共享秘密（例如，预先确定的）的知识但不揭露这一秘密来认证消息发送者从而在用户和消息发送者之间建立信任。

[0040] 图 4 示出根据本发明的一个方面的在消息发送者和消息接收者（例如，用户）之间建立信任的相关方法 400。虽然该示例性方法此处被示出并描述为表示各种事件和 / 或动作的一系列框，但本发明并不受所示出的这些框的排序的限制。例如，根据本发明，除了在此示出的次序之外，某些动作或事件可以按不同的次序发生和 / 或与其他动作或事件同时发生。此外，不是所有示出的框、事件或动作都是实施根据本发明的方法所必需的。此外，将会认识到根据本发明的该示例性方法和其他方法可以与在此图示并描述的方法相关联地实现，也可与未示出或描述的其他系统和装置相关联地实现。

[0041] 根据本发明的方法 400，在 410 处，用户可以与消息发送者共享预定的通信方式。如早先所解释的，消息发送者可以是这样一个机构，用户或消息接收者可以是该机构的客户。消息发送者和用户之间的这种预定的通信方式可以被认为是用户和发送者之间的共享秘密。随后在 420 处，用户可以接收消息。在接收到该消息之后，随后在 430 处执行验证来检查是否与共享秘密一致。如果一致，则方法 400 继续至动作 440，其中将所接收的消息作为真实的来对待。否则，在 435 处忽略该消息。可以认识到，用户可以更新共享秘密（例如，经由向消息发送者注册新的共享秘密）。

[0042] 图 5 示出根据本发明的又一方面的发送者认证的相关方法 500。最初在 510 处，用户例如用因特网服务提供商建立电子邮件帐户。因此，在该特定方面，本发明基于具有一个以上电子邮件帐户的用户，其中恶意方不能容易地确定这两个电子邮件帐户属于同一个人。由此，用户向消息发送者（例如，金融机构）记录两个电子邮件帐户，即主电子邮件帐户（帐户 A）和副电子邮件帐户（帐户 B），而非只记录一个电子邮件帐户，其中随后在发送者侧可以基于共享秘密将这些电子邮件配对在一起用于联系用户。

[0043] 因此，为发送受信消息，机构将电子邮件发送给帐户 A 和 B 两者。在发送给 A 的消息的主题行（例如作为消息的片段的一部分）中，机构可以嵌入消息“该消息的一个副本已经被发送至 h(B)”，而在发送给 B 的消息的主题行中，机构可以嵌入消息“该消息的副本已经被发送至 h(A)”。此处，h() 是表示地址的一部分的函数（例如，散列函数，或通过映射获得的函数）。例如，如果 A = snoopy2314@hotmail.com，则电子邮件可以使 h(A) = snoop*****@hotmail.com。在不揭示地址本身的情况下，这样做揭示了发送者知道其他的电子邮件地址。此外，接收者可以检查副本是否已经被发送到所涉及的帐户。由此，重放变得困难，其中观察 A 的收件箱中的消息的攻击者知道的足够多来伪造主题行，但不足以使得消息还出现在 B 的邮箱中。因此，即使 A 和 B 都存在于垃圾邮件发送者正使用的列表上，这些恶意方在不知道哪些邮件被配对在一起的情况下无法模拟来自真正机构的邮件。在 530 处，在接收到主电子邮件帐户 A 中的消息之后，用户能够验证发送者知道秘密，但不揭示秘密本身。接着在 540 处，可以验证在副电子邮件帐户中的消息的接收，其中用户可以检查邮箱 B 包含该消息的副本。或者，用户可以将电子邮件从 B 转发至 A 从而使得两个邮件到达同一个邮箱；由此，用户能够验证发送者知道秘密，同时不向观察传送中的两个消息中的任一个的任何人揭示秘密。

[0044] 图 6 示出包括与本发明的消息收发组件 660 相关联的通知组件 610 的系统 600 的特定框图。根据本发明的一个方面，通知组件 610 可以向用户 612 和 / 或端点发送关于从消息发送者接收到电子邮件和 / 或通信的警告。另外，通知组件 610 可以基于消息发送者对用户的重要性来设置各个重要性级别 620。可以用同步的方式按照即时消息的形式来提供这种通知，该通知向用户指示已经接收到电子邮件。关于在电子邮件收件箱中接收到消息的通知可以是电话呼叫发起、即时消息等形式，其中向用户通知关于消息的接收。

[0045] 图 7 示出在发送者侧的示例性图形用户界面 (GUI)700，该图形用户界面 700 显示由稍后接收消息的用户所指定的所需通信方式和 / 或共享秘密。如图所示，用户可以选择选项 710，并进而指令消息收发组件联系两个电子邮件帐户并将消息发送给两个帐户。如以上详细解释的，共享秘密可以包括在将该消息传送到第一电子邮件帐户之后将消息传送到第二电子邮件帐户。同样，选项 720 使得用户能够将共享秘密指定为将预期消息发送给主电子邮件并且还呼叫移动电话。

[0046] 类似地，选项 730 提供了将共享秘密指定为联系用户的主电子邮件，并且按预定次数在用户的语音邮件上留下消息。因此，取决于这些所指定的上下文和 / 或共享秘密，向用户通知即将到来的通信，该通信由用于验证正被发送的消息的真实性的上下文和一个或多个策略 / 规则来定义。换言之，通信所采用的决策策略一般根据用户（接收这些消息的人）最初定义的一组标定设置来细化和个性化。

[0047] 此外，这种个性化能力增加了这些系统的价值，其中用户可以容易地操纵、控制并

进而个性化通信过程的方式。可以认识到，还可以提供默认设置来实现符合特定类型的用户（例如，忙碌的办公室工作者、道路工作者、居家工作者）的预定设置。随着用户越来越习惯通信和相关通知的量和/或频率，还可以提供调整系统（未示出）来修改和调整消息收发变量的特定上下文和/或子集来便于通信系统的个性化和细化。

[0048] 在此使用词语“示例性”意指用作示例、实例或说明。在此被描述为“示例性”的任何方面或设计并不一定要被解释为相比其他方面或设计更优选或有利。类似地，在此提供的示例只是出于清楚和理解的目的并且并不意味着以任何方式限制本发明或其部分。可以理解，本可呈现多个其他或替换示例，但已出于简明的目的而省略了。

[0049] 此外，本发明的全部或部分可以使用产生控制计算机以实现所公开的发明的软件、固件、硬件或其任意组合的标准编程和/或工程技术而被实现为方法、装置或制品。例如，计算机可读介质可以包括，但不仅限于，磁存储设备（例如，硬盘、软盘、磁条）、光盘（例如，紧致盘（...CD）、数字多功能盘（DVD）…）、智能卡，以及闪存设备（例如，卡、棒、键驱动器...）。另外，应该理解，可以使用载波来携带计算机可读电子数据，诸如在传输和接收电子邮件或在访问诸如因特网或局域网（LAN）之类的网络时所使用的那些。当然，本领域的技术人员将会认识到，可在不背离所要求保护的主题的范围或精神的情况下对此配置进行许多修改。

[0050] 为了对所公开的主题的各个方面提供上下文，图 8 和 9 以及以下讨论旨在提供对其中可实现所公开的主题的各方面的合适的环境的简要、概括描述。尽管以上在运行在一台和/或多台计算机上的计算机程序的计算机可执行指令的一般上下文中描述了本主题，但本领域的技术人员将认识到，本发明也可结合其他程序模块实现。一般而言，程序模块包括执行特定任务和/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。而且，本领域的技术人员可以理解，本发明的方法可用其他计算机系统配置实现，包括单处理器或多处理器计算机系统、小型计算设备、大型计算机、以及个人计算机、手持式计算设备（例如，个人数字助理（PDA）、电话、手表...）、基于微处理器或可编程消费产品或工业电子设备等。所示各方面也可在任务由通过通信网络链接的远程处理设备中执行的分布式计算环境中实现。然而，即使不是本发明的全部方面，至少也有本发明的部分方面可以在独立计算机上实现。在分布式计算环境中，程序模块可以位于本地和远程存储器存储设备中。

[0051] 参考图 8，描述了用于实现本发明的各方面的示例性环境 910，其包括计算机 812。计算机 812 包括处理单元 814、系统存储器 816，以及系统总线 818。系统总线 818 将系统组件——包括但不仅限于系统存储器 816——耦合到处理单元 814。处理单元 814 可以是各种处理器中的任一种。还可以使用双微处理器及其他多处理器体系结构作为处理单元 814。

[0052] 系统总线 818 可以是若干类型的总线结构中的任一种，包括存储器总线或存储器控制器、外围总线或外部总线、和/或使用各种可用的总线体系结构中的任一种的局部总线，可用的总线体系结构包括，但不限于，11 位总线、工业标准体系结构（ISA）、微通道体系结构（MCA）、扩展 ISA（EISA）、智能驱动器电子接口（IDE）、VESA 局部总线（VLB）、外围部件互连（PCI）、通用串行总线（USB）、高级图形接口（AGP）、个人计算机存储卡国际协会总线（PCMCIA）以及小型计算机系统接口（SCSI）。

[0053] 系统存储器 816 包括易失性存储器 820 和非易失性存储器 822。基本输入/输出系统（BIOS）被存储在非易失性存储器 822 中，包含例如在启动过程中帮助在计算机 812 内

的元件之间传输信息的基本例程。作为说明而非限制，非易失性存储器 822 可以包括只读存储器 (ROM)、可编程 ROM(PROM)、电可编程 ROM(EPROM)、电可擦除 ROM(EEPROM) 或者闪存。易失性存储器 820 包括充当外部高速缓冲存储器的随机存取存储器 (RAM)。作为示例而非限制，RAM 以多种形式可用，诸如同步 RAM(SRAM)、动态 RAM(DRAM)、同步 DRAM(SDRAM)、双倍数据速率 SDRAM(DDR SDRAM)、增强型 SDRAM(ESDRAM)、同步链路 DRAM(SLDRAM) 以及直接存储器总线 (Rambus)RAM(DRRAM)。

[0054] 计算机 812 还包括可移动的 / 不可移动的，易失性 / 非易失性的计算机存储介质。图 8 示出了盘存储 824，其中这一盘存储 824 包括但不限于诸如磁盘驱动器、软盘驱动器、磁带驱动器、Jaz 驱动器、Zip 驱动器、LS-60 驱动器、闪存卡、或者记忆棒等设备。另外，磁盘存储器 824 可包括存储介质——分开地或与其他存储介质相结合——包括，但不限于，诸如紧致盘 ROM 设备之类的光盘驱动器 (CD-ROM)、CD 可记录驱动器 (CD-R 驱动器)、CD 可重写驱动器 (CD-RW 驱动器) 或数字多功能盘 ROM 驱动器 (DVD-ROM)。为便于磁盘存储设备 824 连接到系统总线 818，通常使用诸如接口 826 之类的可移动或不可移动接口。

[0055] 应该明白，图 8 描述了在用户和在合适的操作环境 810 中描述的基本计算机资源之间担当中介的软件。这样的软件包括操作系统 828。可以存储在磁盘存储器 824 上的操作系统 828 用于控制和分配计算机系统 812 的资源。系统应用程序 830 利用由操作系统 828 通过存储在系统存储器 816 或者存储在盘存储 824 上的程序模块 832 和程序数据 834 对资源的管理。应该明白，在此描述的各个组件可以用各种操作系统或操作系统的组合来实施。

[0056] 用户通过输入设备 836 向计算机 812 输入命令或信息。输入设备 836 包括，但不限于，诸如鼠标、跟踪球、指示笔、触摸板之类的指示设备、键盘、麦克风、游戏杆、游戏手柄、圆盘式卫星天线、扫描仪、TV 调谐器卡、数码相机、数字视频摄像机、网络摄像头等等。这些及其他输入设备通过系统总线 814 经由接口端口 838 连接到处理单元 818。接口端口 838 包括，例如，串行端口、并行端口、游戏端口，以及通用串行总线 (USB)。输出设备 840 与输入设备 836 使用一些相同类型的端口。如此，例如，可以使用 USB 端口来向计算机 812 提供输入，以及从计算机 812 向输出设备 840 输出信息。提供输出适配器 842 是为了示出存在如监视器、扬声器、和打印机以及其他输出设备 840 等需要特殊适配器的一些输出设备 840。输出适配器 842 包括，作为说明而不是限制，在输出设备 840 和系统总线 818 之间提供连接手段的视频卡和声卡。应该注意，其他设备和 / 或设备的系统提供诸如远程计算机 844 之类的输入和输出两种能力。

[0057] 计算机 812 可以使用到诸如远程计算机 844 之类的一个或多个远程计算机的逻辑连接来在联网环境中操作。远程计算机 844 可以是个人计算机、服务器、路由器、网络 PC、工作站、基于微处理器的电器、对等设备或其他公共网络节点等等，并且通常包括就计算机 812 所描述的许多或全部元件。出于简洁起见，与远程计算机 846 一起，只示出了存储器设备 844。远程计算机 844 通过网络接口 848 在逻辑上连接到计算机 812，然后，经由通信连接 850 在物理上连接。网络接口 848 涵盖诸如局域网 (LAN) 和广域网 (WAN) 这样的通信网络。LAN 技术包括光纤分布式数据接口 (FDDI)、铜分布式数据接口 (CDDI)、以太网 /IEEE 802.3、令牌环 /IEEE 802.5 等。WAN 技术包括，但不限于，点对点链路、电路交换网，如综合业务数字网 (ISDN) 及其变体，分组交换网络，以及数字订户线 (DSL)。

[0058] 通信连接 850 是指用来将网络接口 848 连接到总线 818 的硬件 / 软件。尽管为清楚起见通信连接 850 被示为在计算机 812 内部，但是，它也可以位于计算机 812 外部。连接到网络接口 848 所需的硬件 / 软件包括，只作示例，内部和外部技术，诸如，调制解调器，包括常规电话级调制解调器、电缆调制解调器和 DSL 调制解调器、ISDN 适配器，以及以太网卡。

[0059] 图 9 是根据本发明的一个方面的可被用作信任建立的一部分的示例计算环境 900 的示意性框图。系统 900 包括一个或多个客户机 910。客户机 910 可以是硬件和 / 或软件（例如，线程、进程、计算设备）。系统 900 还包括一个或多个服务器 930。服务器 930 也可以是硬件和 / 或软件（例如，线程、进程、计算设备）。服务器 930 可以容纳各线程以通过例如利用在此描述的各组件执行转换。在客户机 910 和服务器 930 之间的一种可能的通信能够以适合在两个或更多计算机进程之间传输的数据分组的形式进行。系统 900 包括通信框架 950，该通信框架 950 可以被用来促进客户机 910 和服务器 930 之间的通信。客户机 910 可在操作上连接至一个或多个客户机数据存储 960，客户机数据存储可用来存储对客户机 910 本地的信息。同样地，服务器 930 可在操作上连接到可以用来存储对服务器 930 本地的信息的一个或多个服务器数据存储 940。

[0060] 以上描述的内容包括各个示例性方面。当然，出于描绘这些方面的目的而描述每一个可以想到的组件或方法的组合是不可能的，但本领域内的普通技术人员应该认识到，许多进一步的组合和排列都是可能的。因此，在此描述的各方面旨在包括所有这些属于所附权利要求书的精神和范围内的改变、修改和变型。

[0061] 此外，就在说明书或权利要求书中使用术语“包括”而言，这一术语旨在以与术语“包含”在被用作权利要求书中的过渡词时所解释的相似的方式为包含性的。

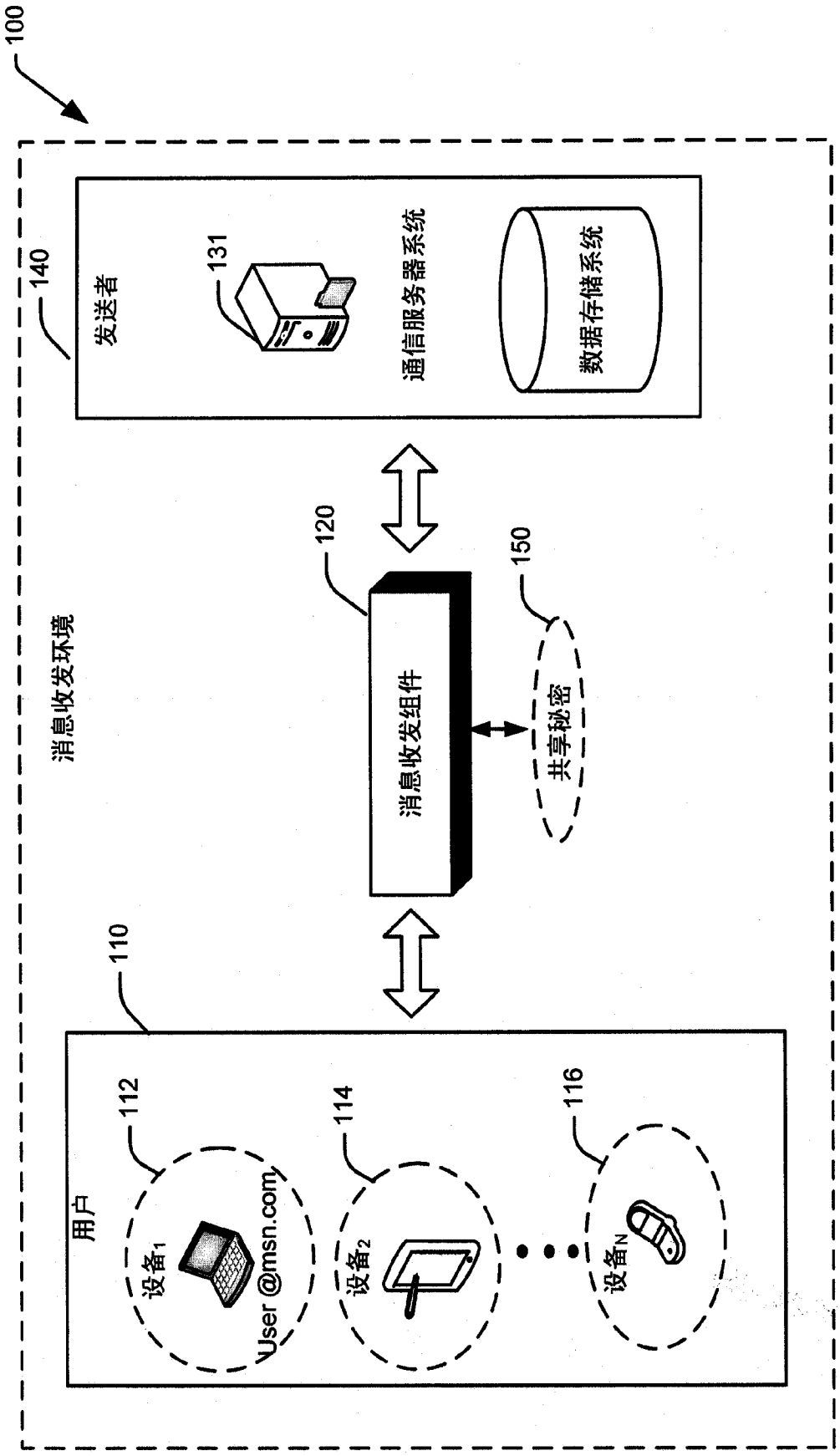

100
消息收发环境
140
发送者
131
通信服务器系统
数据存储系统
120
消息收发组件
150
共享秘密
110
用户
112
设备1
User @msn.com
114
设备2
116
设备N

图 1

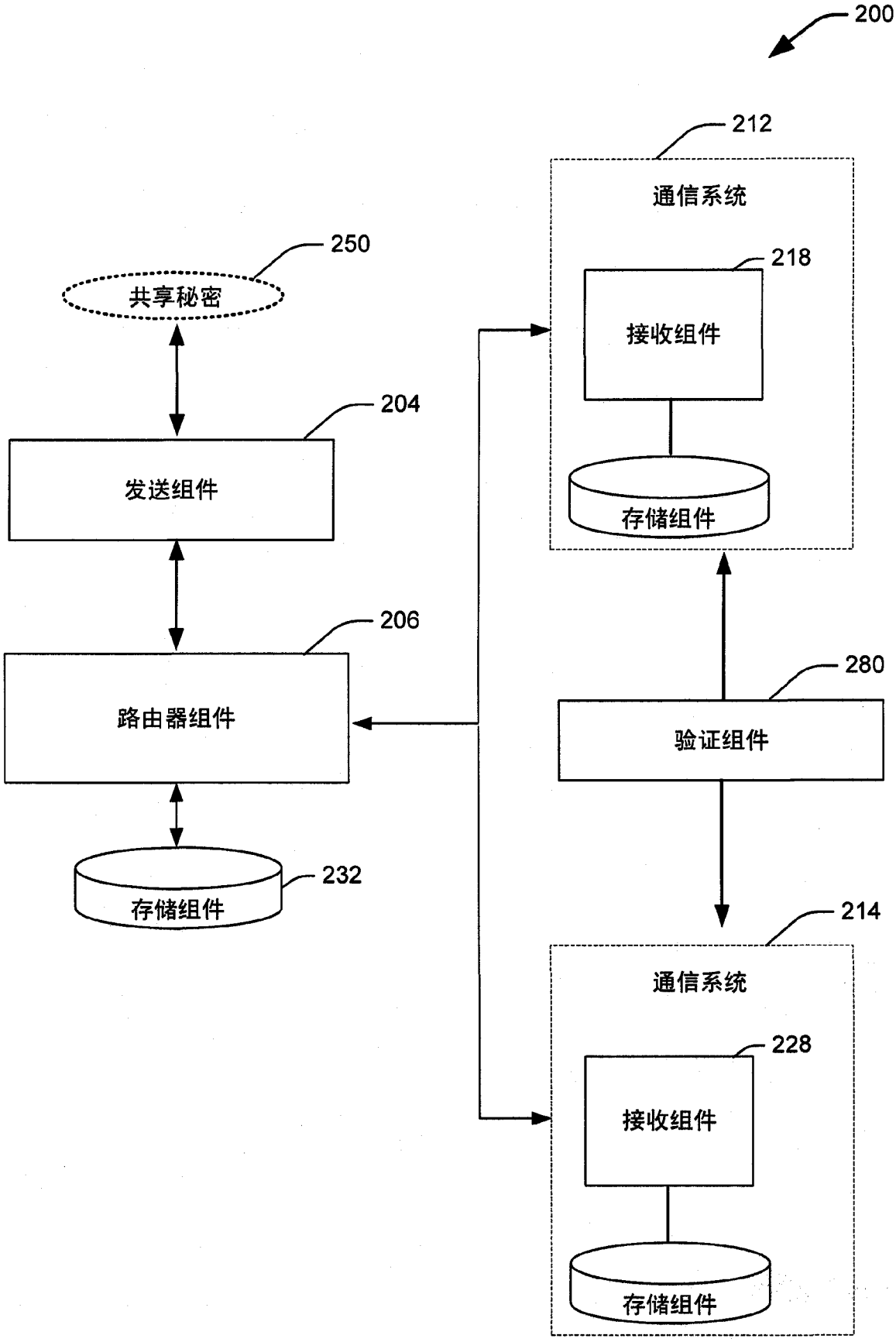

200
212
通信系统
250
共享秘密
218
接收组件
204
发送组件
存储组件
206
路由器组件
280
验证组件
232
存储组件
214
通信系统
228
接收组件
存储组件

图 2

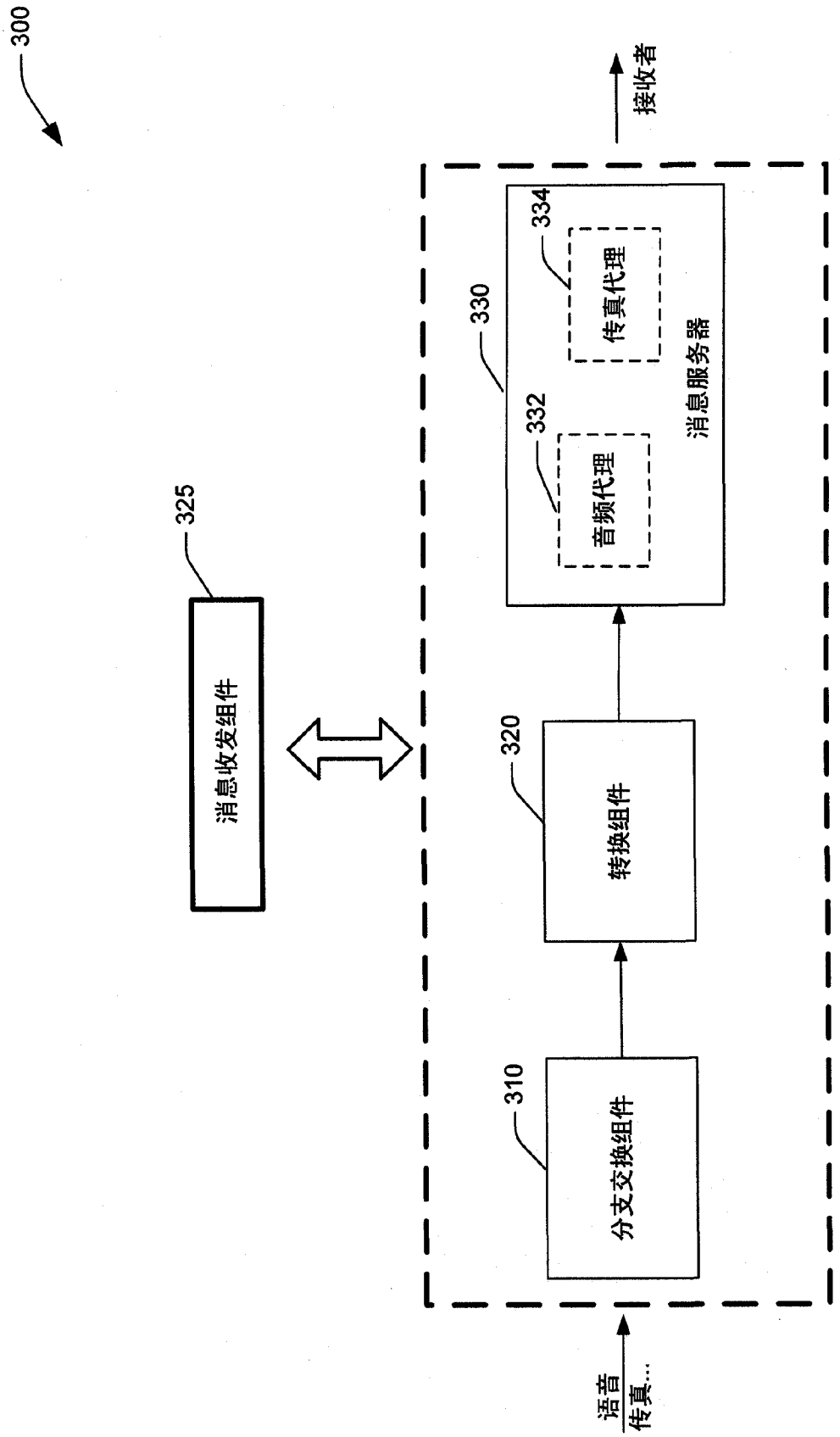

300
接收者
334
传真代理
330
消息服务器
332
音频代理
325
消息收发组件
320
转换组件
310
分支交换组件
语音
传真...

图 3

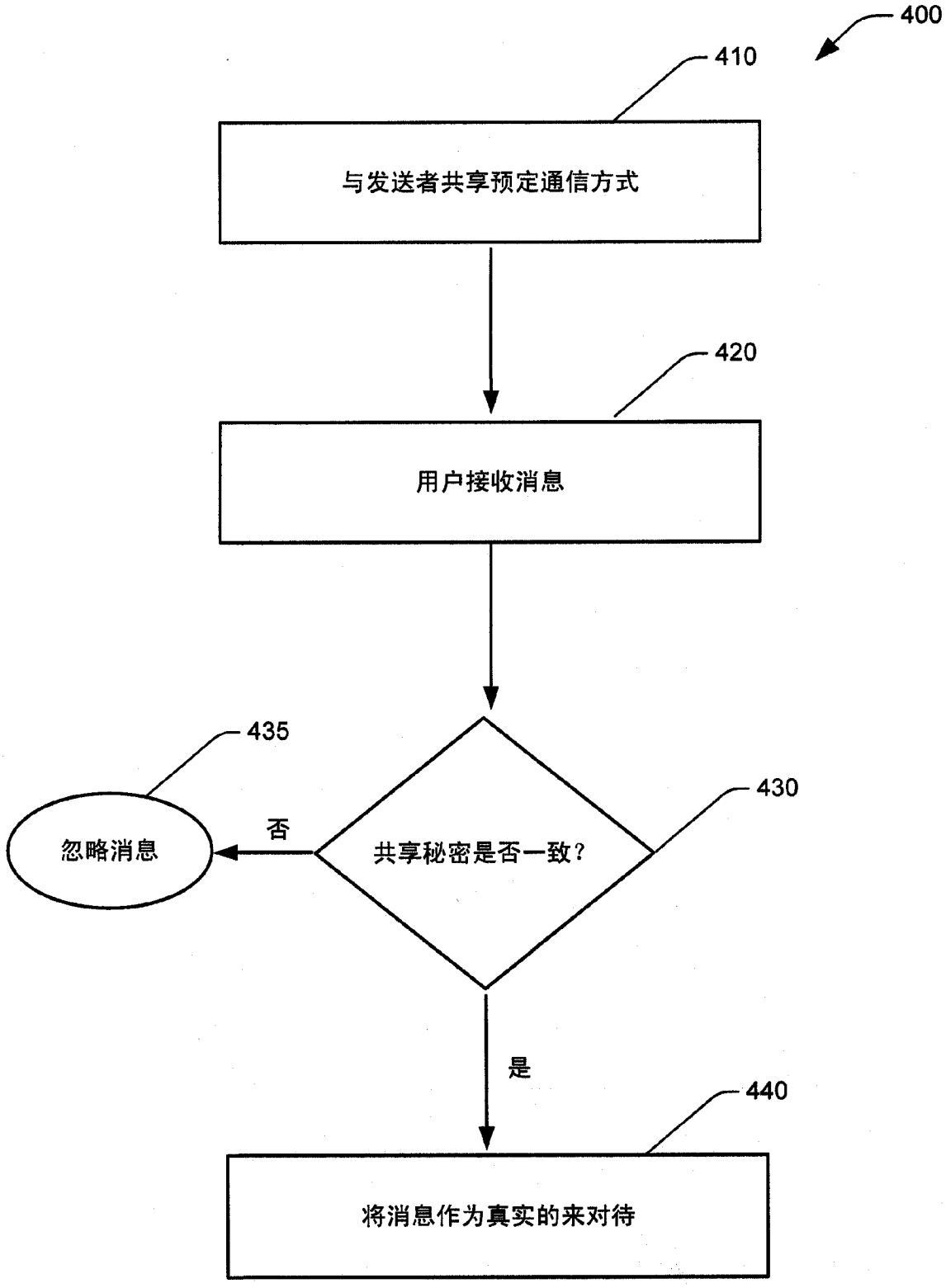

400
410
与发送者共享预定通信方式
420
用户接收消息
435
忽略消息
否
共享秘密是否一致?
430
是
440
将消息作为真实的来对待

图 4

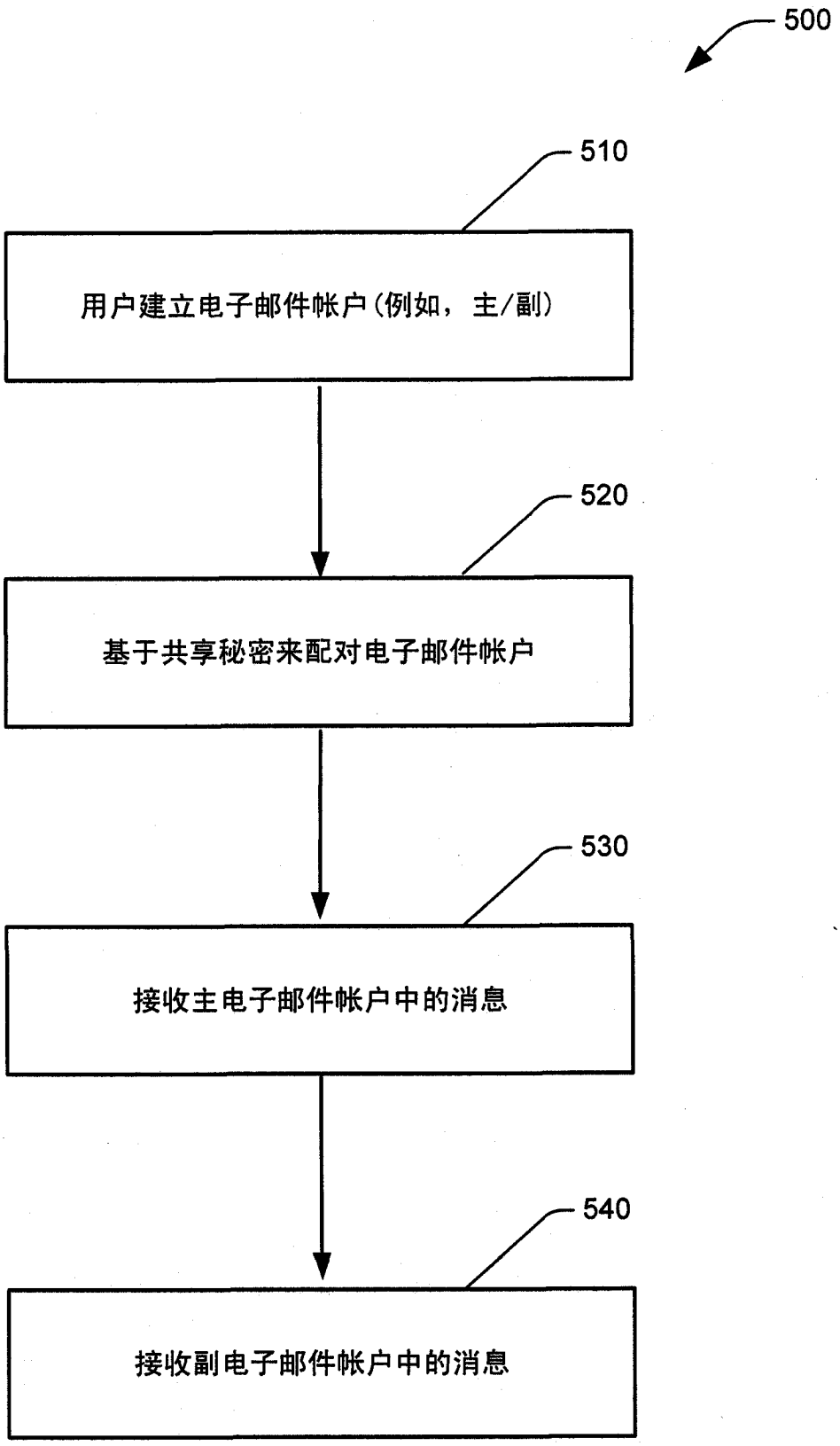

500
510
用户建立电子邮件帐户(例如，主/副)
520
基于共享秘密来配对电子邮件帐户
530
接收主电子邮件帐户中的消息
540
接收副电子邮件帐户中的消息

图 5

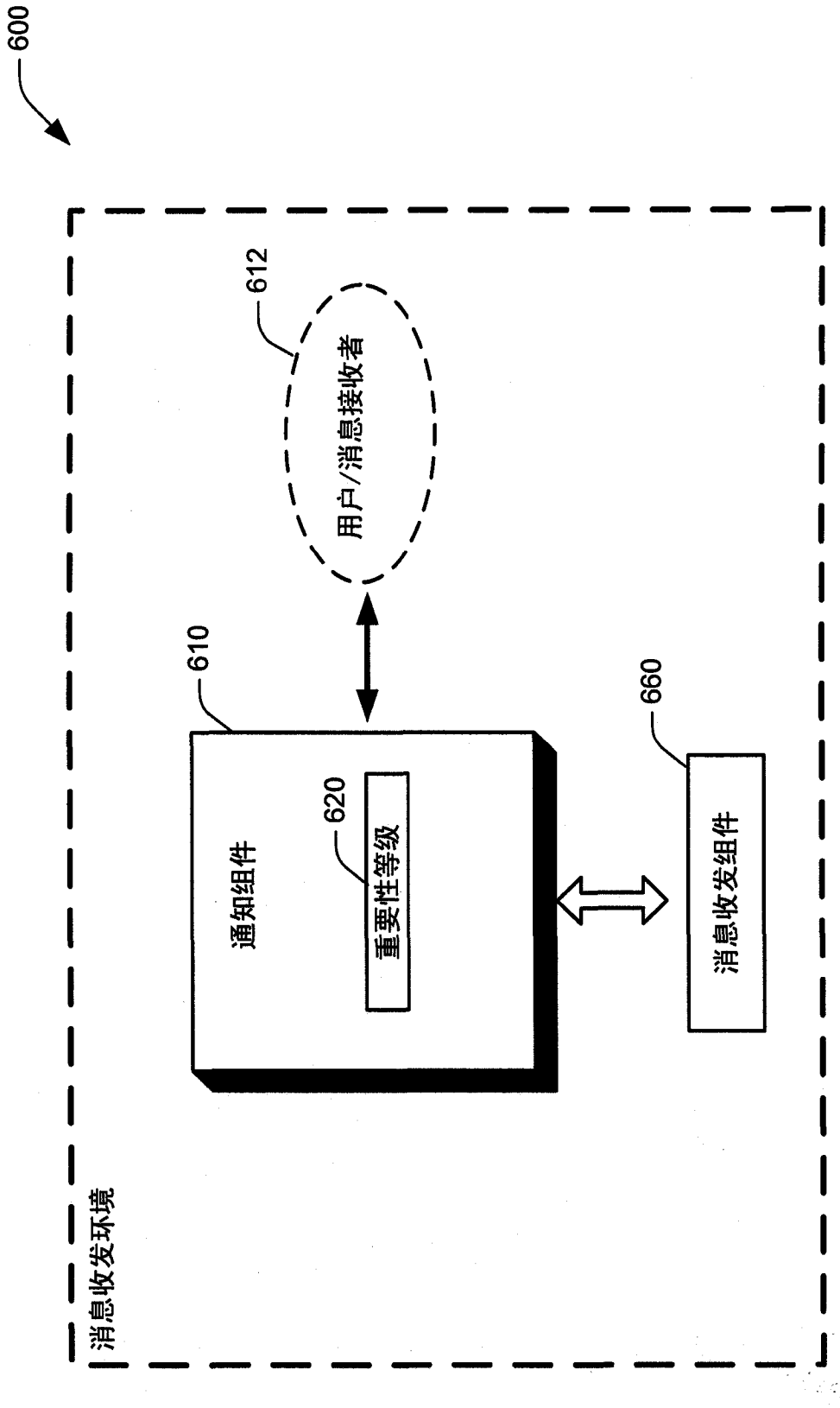


图 6

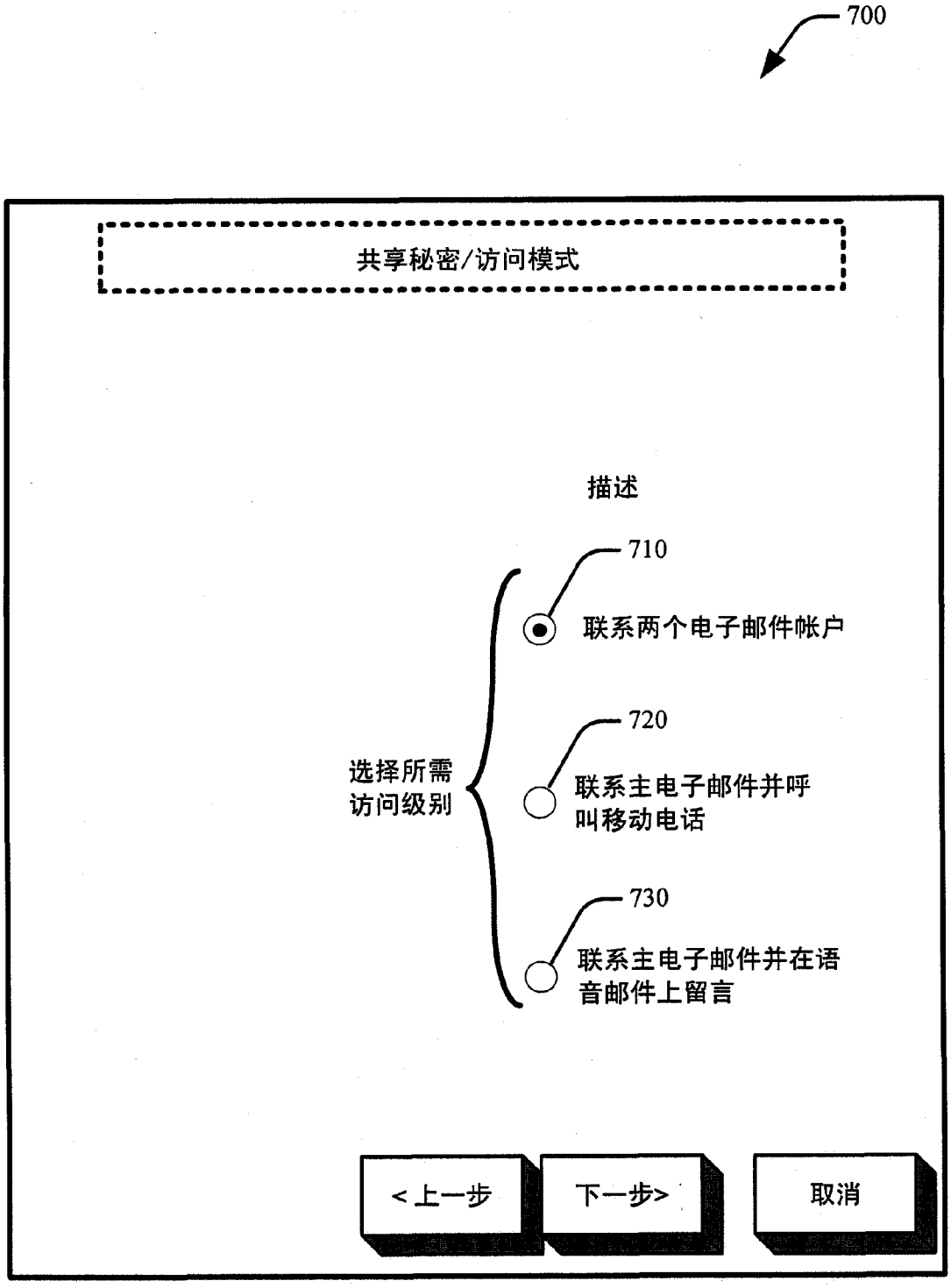

700
共享秘密/访问模式
描述
710
联系两个电子邮件帐户
720
联系主电子邮件并呼叫移动电话
730
联系主电子邮件并在语音邮件上留言
选择所需访问级别
< 上一步
下一步>
取消

图 7

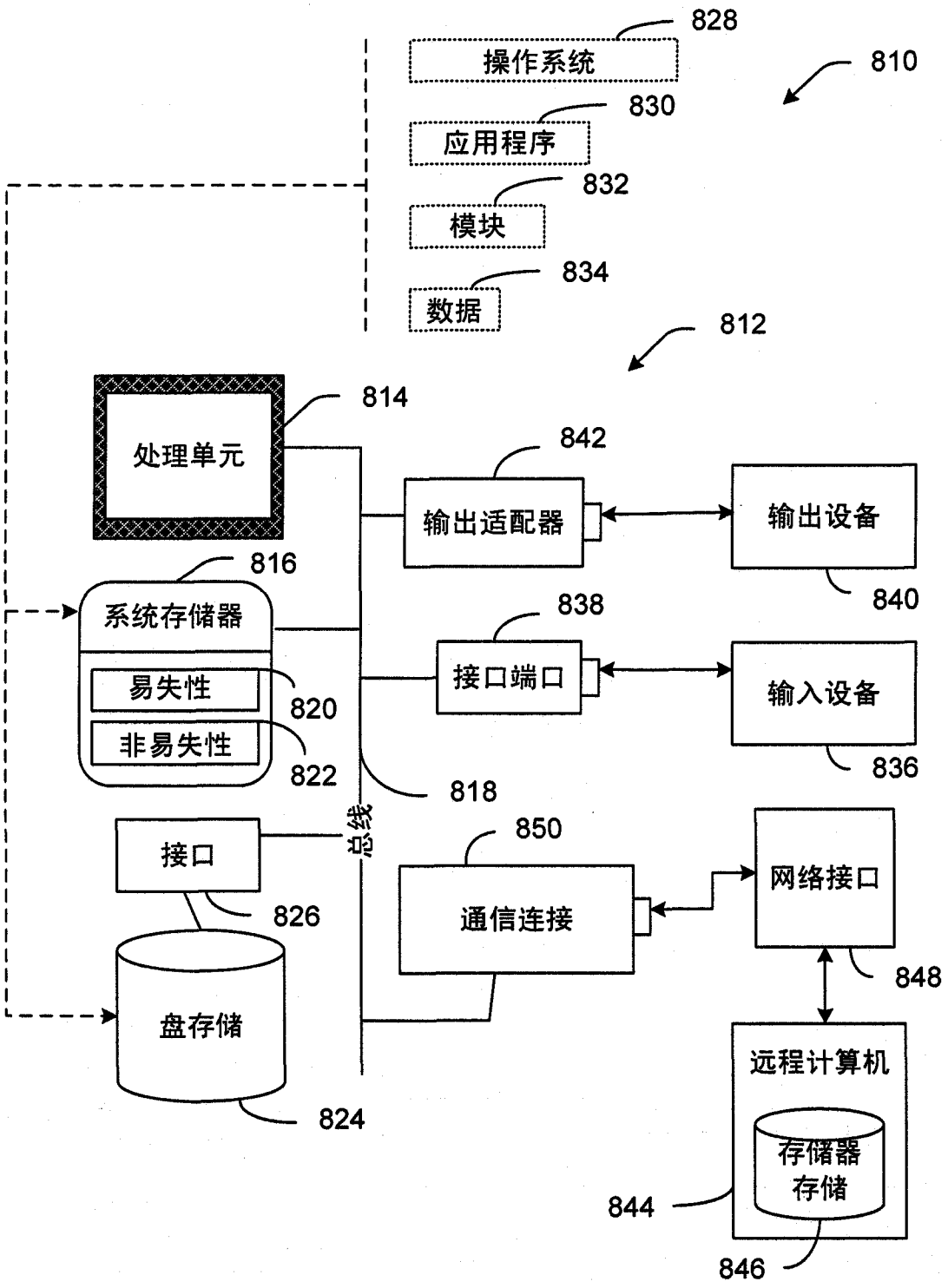

828
操作系统
810
830
应用程序
832
模块
834
数据
812
814
处理单元
842
输出适配器
输出设备
840
816
系统存储器
838
易失性
820
接口端口
输入设备
非易失性
822
836
818
总线
接口
850
826
通信连接
网络接口
848
盘存储
远程计算机
存储器
存储
844
824
846

图 8

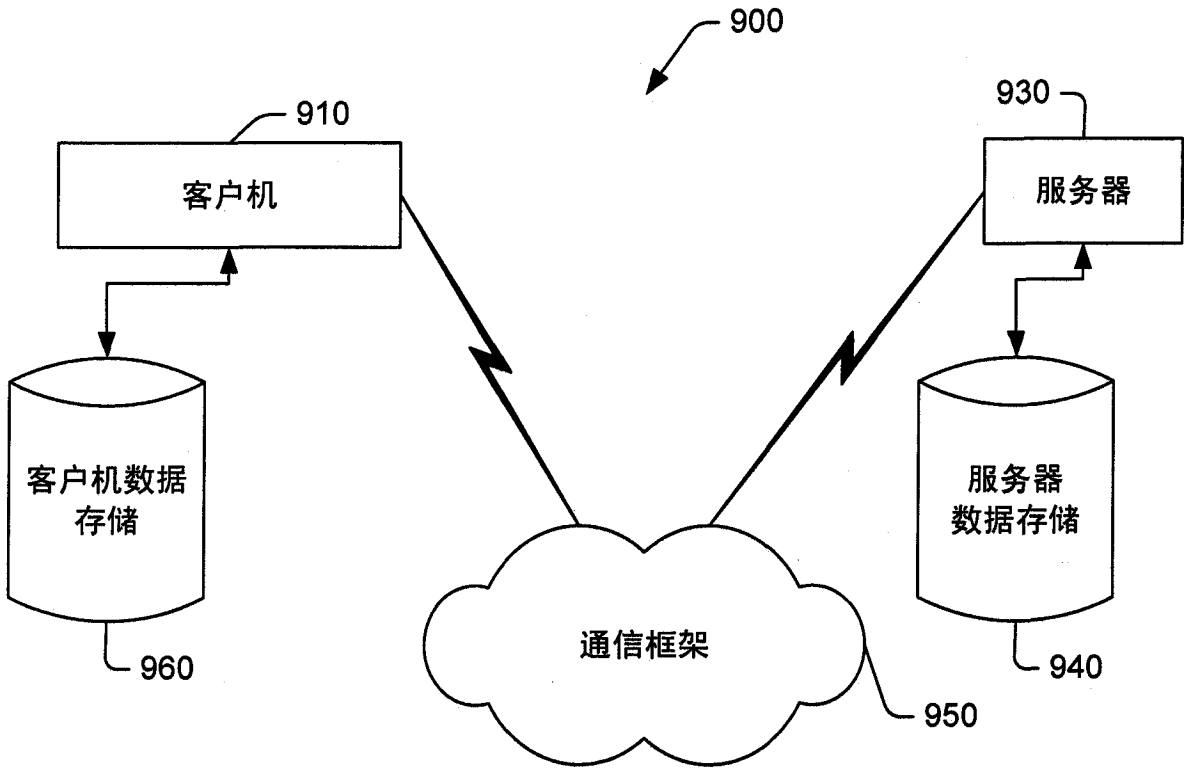


图 9