(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 107533619 A
(43)申请公布日 2018.01.02

(21)申请号 201680019962.9

(22)申请日 2016.02.04

(30)优先权数据
62/112,503 2015.02.05 US
62/114,744 2015.02.11 US
62/135,990 2015.03.20 US
15/015,482 2016.02.04 US

(85)PCT国际申请进入国家阶段日
2017.09.29

(86)PCT国际申请的申请数据
PCT/US2016/016612 2016.02.04

(87)PCT国际申请的公布数据
WO2016/126971 EN 2016.08.11

(71)申请人 费施莱恩有限责任公司
地址 美国威斯康辛

(72)发明人 M·T·查普曼

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 21/62(2013.01)
H04L 29/06(2006.01)

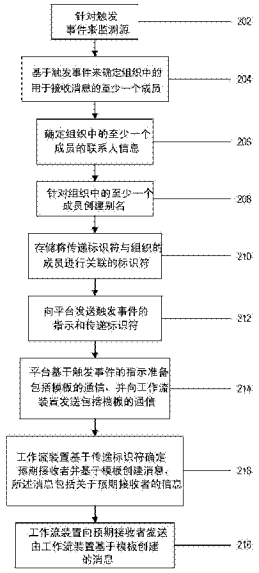
权利要求书3页 说明书15页 附图3页

(54)发明名称

社交工程模拟工作流装置

(57)摘要

提供了一种用于评估组织对社交工程的易感性的系统，所述组织具有多个源和使用电子设备的多个成员。该系统包括与多个源通信的装置，其被配置为取回成员的联系人信息并从多个源中检测触发事件。该系统包括远离装置的平台，该平台被配置为从装置接收指示触发事件的信号，并且基于每个触发事件准备包括模板的通信并向装置发送包括模板的通信。在接收到通信时，装置被配置为取回预期接收者成员的联系人信息、基于所述模板来创建消息、并将所述消息发送到所述预期接收者成员。平台不从装置接收多个成员的联系人信息。



CN 107533619 A

1.一种用于评估组织对社交工程的易感性的系统，所述组织具有多个源和使用电子设备的多个成员，所述系统包括：

与所述多个源进行通信的装置，所述装置被配置为从所述源中的至少一个接收所述多个成员的联系人信息，并且检测来自所述多个源的触发事件；以及

平台，其远离所述装置并且被配置为从所述装置接收指示检测到的触发事件的信号、基于所述触发事件中的每一个准备包括模板的通信、并且向所述装置发送所述通信；

其中，当接收到所述通信时，所述装置被配置为取回预期接收者成员的所述联系人信息、基于所述模板来创建消息、并且向所述预期接收者成员发送所述消息。

2.根据权利要求1所述的系统，其中，所述平台不从所述装置接收所述多个成员的所述联系人信息。

3.根据权利要求1所述的系统，其中，所述平台被配置为对关于触发事件的信息进行编译，并且基于所述触发事件对所述组织对社交工程的易感性进行评估。

4.根据权利要求1所述的系统，其中，所述源包括多个数据库和消息传送系统。

5.根据权利要求1所述的系统，其中，所述装置被配置为在所述消息中包括所述预期接收者成员的个人信息。

6.根据权利要求1所述的系统，其中，由所述装置向所述预期接收者成员发送的消息征求所述预期接收者成员来采取动作。

7.根据权利要求6所述的系统，其中，由所述消息征求的所述动作是以下中的一个：点击链接、提供机密信息以及下载文件。

8.根据权利要求6所述的系统，其中，所述平台被配置为监测所述预期接收者成员是否采取由所述消息征求的所述动作。

9.根据权利要求1所述的系统，其中，所述装置被配置为定期地从所述多个源中的至少一个源确定所述联系人信息中的任何一个是否已被更新或新联系人信息是否已被添加。

10.根据权利要求1所述的系统，其中，所述装置被配置为仅与所述平台进行输出连接。

11.根据权利要求1所述的系统，其中，所述装置被配置为充当专用SMTP服务器并且基于被包括在所述模板中的标签来对所述消息进行个性化。

12.根据权利要求1所述的系统，其中，所述装置是内置的、组织托管的或外部托管的SMTP服务器中的一个的SMTP客户端。

13.根据权利要求1所述的系统，还包括从所述组织外部托管的并且与所述平台分开的安全的SMTP服务器。

14.根据权利要求13所述的系统，其中，所述安全的SMTP服务器由与所述组织不同的第二组织托管，并且其中，所有消息和日志都定期地从所述安全的SMTP服务器中被删除。

15.根据权利要求1所述的系统，其中，所述消息包括到登录页面的链接，并且其中，所述装置包括被配置为服务所述登录页面的登录页面服务器。

16.根据权利要求15所述的系统，其中，所述登陆页面征求访问者输入信息，并且其中，所述装置被配置为收集独立于所述平台的信息。

17.根据权利要求1所述的系统，其中，所述消息包括到登录页面的链接，并且其中，服务所述登录页面的所述服务器是独立于所述平台的。

18.根据权利要求1所述的系统，其中，所述消息包括到由所述平台托管的登录页面的

链接，并且其中，所述平台被配置为定期被重置以移除关于点击所述链接的预期接收者成员的信息。

19.根据权利要求1所述的系统，其中，所述消息征求来自所述预期接收者成员的电子邮件响应，所述电子邮件响应被配置为由所述平台不能够访问的SMTP服务器来传递，其中，所述装置被配置为：回顾来自所述预期接收者成员的所述电子邮件响应、对所述消息进行别名化以移除识别信息、并且将别名化的消息转发到所述平台。

20.根据权利要求19所述的系统，其中，所述别名化是使用种子或非种子密码散列函数来执行的。

21.根据权利要求1所述的系统，其中，所述联系人信息包括电话号码，并且其中，所述装置被配置为利用电话标识符替换所述电话号码、向所述平台发送所述电话标识符，并且当从所述平台接收到所述通信时，所述装置被配置为基于所述模板针对每个预期接收者成员创建定制的消息，并且针对所述消息中的每一个拨打所述预期接收者成员的电话号码。

22.一种减少对社交工程的组织的易感性的方法，所述组织具有多个源，所述方法包括：

接收所述组织的多个成员的联系人信息；

针对触发事件来监测所述源中的每一个；

基于检测到的触发事件，将所述组织中的至少一个成员识别为预期接收者；

基于所述检测到的触发事件的特性来准备到所述预期接收者的消息，所述消息征求由所述预期接收者进行的动作；

向所述预期接收者发送所述消息；

确定所述预期接收者是否如由所述消息征求的那样来行动；并且

对所述预期接收者的所述动作进行评估。

23.根据权利要求22所述的方法，其中，所述源包括至少一个目录、至少一个数据库以及至少一个消息传送系统。

24.根据权利要求22所述的方法，其中，联系人信息包括电子邮件地址簿，所述电子邮件地址簿包括所述组织的成员的电子邮件地址，所述方法还包括定期地从所述源中的至少一个确定所述组织的成员的电子邮件地址簿是否已被更新。

25.根据权利要求22所述的方法，其中，联系人信息包括以下中的至少一个：用于语音网络钓鱼测试的所述组织的成员的电话号码、SMS文本消息通过其能够被发送到所述组织的成员的移动电话号码、以及所述组织的成员的社交媒体标识符。

26.一种用于评估对组织的社交工程的易感性的系统，所述组织具有目录、多个数据库和消息传送系统，所述系统包括：

装置，其被配置为从所述目录接收具有所述组织的成员的联系人信息的地址簿，并且被配置为连接到所述多个数据库和所述消息传送系统，所述装置被配置为针对触发事件来监测所述多个数据库和所述消息传送系统；以及

平台，其被配置为从所述装置接收指示由所述装置识别出的触发事件的信号、基于所述信号创建模板、以及向所述装置发送所述模板；

其中，所述装置被配置为基于所述模板创建到预期接收者的消息；

其中，所述平台被配置为确定所述预期接收者响应于所述消息是否采取预定动作；以

及

其中，所述平台被配置为响应于所述消息对关于所述触发事件、所述消息和所述预期接收者的动作的统计进行编译。

27.根据权利要求26所述的系统，其中，所述装置被配置为在所述组织的防火墙内，并且其中，所述平台被配置为在所述组织的防火墙外。

28.根据权利要求26所述的系统，其中，所述平台被配置为针对具有不同特性的触发事件来创建不同的模板。

29.根据权利要求26所述的系统，其中，所述平台被配置为在所述模板中的至少一个中包括标签，并且其中，所述装置被配置为基于所述标签将信息添加到关于所述消息的所述预期接收者的所述消息中的每一个中。

30.根据权利要求26所述的系统，其中，所述平台被配置为对一时间段内的对所述组织的社交工程的易感性进行分析，并且向所述装置发送所述分析，并且其中，所述装置被配置为将关于所述组织的成员的身份的信息并入到所述分析中。

31.根据权利要求26所述的系统，其中，所述装置被配置为通过所述组织的电子邮件服务器将所述消息转发到所述预期接收者。

32.一种用于评估组织对社交工程的易感性的系统，所述组织具有多个源和使用电子设备的多个成员，所述系统包括：

装置，其被配置为从所述源中的至少一个接收地址簿，所述地址簿包括关于所述组织的多个成员中的每一个的识别信息和联系人信息，所述装置被配置为对所述识别信息中的至少一些进行别名化并且利用标识符来替换所述联系人信息以创建别名化的地址簿，将要被别名化的所述信息是基于预定算法来确定的；

平台，其被配置为从所述装置接收所述别名化的地址簿；

其中，所述装置被配置为检测来自所述源的触发事件并且向所述平台发送所述触发事件的指示；

其中，所述平台被配置为将通信提供到所述装置，所述通信包括基于所述触发事件的消息模板、传递模式的指示、由所述装置已知的用于映射到所述组织的成员中的一个的传递标识符、以及调度指令；

其中，所述装置被配置为基于针对来自所述地址簿中的信息的所述预期接收者中的每一个的模板来创建个性化的消息；

其中，所述装置被配置为基于所述消息的类型来向与所述平台分开的多个服务器中的一个发送所述消息，所述服务器中的一个被配置为向所述预期接收者发送所述消息；

其中，所述装置被配置为监测来自所述预期接收者的对所述消息的响应；以及

其中，所述装置被配置为对所述响应的部分进行别名化、使所述响应的其他部分未别名化、并且基于预定算法对所述响应的部分进行概述、并且向所述平台发送所述响应的别名化的、未别名化的以及概述的部分。

33.根据权利要求32所述的系统，其中，所述服务器包括电话服务器、文本消息服务器和电子邮件服务器。

34.根据权利要求32所述的系统，其中，所述装置充当所述多个服务器。

社交工程模拟工作流装置

技术领域

[0001] 本发明大体上涉及对社交工程(例如网络钓鱼)的易感性;并且更具体地涉及用作测试和/或减少组织对社交工程的易感性的系统和软件。

背景技术

[0002] 社交工程包括操纵(例如,心理操纵)人们来执行动作或泄露机密信息,例如人们通常不会公开的信息。这种信息可以用于各种恶意的目的,例如,电子盗窃、欺诈等。社交工程中的一种形式是网络钓鱼。网络钓鱼是一种欺诈性地获取机密信息的技术。例如,网络钓鱼者可以向接收者发送消息,例如电子邮件、文本、SMS、电话呼叫、语音邮件、预先记录的消息等。该消息可以请求接收者采取一些动作,例如,点击链接、打开和/或下载文件、提供机密信息等。就链接而言,链接可以将接收者带到基于虚假的名义请求接收者提供机密信息的网站。其他链接可以将接收者带到被设计为将恶意代码(例如,从电子设备捕获接收者的个人信息的代码等)下载到接收者的电子设备上的网站。网络钓鱼消息可以被设计为本身是难以识别的,例如,消息包括可能被写入为、包括信息等以看起来源于合法的源。

发明内容

[0003] 本发明的一个实施例涉及一种用于评估组织对社交工程的易感性的系统。所述组织具有多个源和使用电子设备的多个成员。所述系统包括与所述多个源进行通信的装置。所述装置被配置为从所述源中的至少一个接收所述多个成员的联系人信息。所述装置被配置为检测来自所述多个源的触发事件。所述系统包括远离所述装置的平台。所述平台被配置为从所述装置接收指示检测到的触发事件的信号。所述平台被配置为基于所述触发事件中的每一个来准备包括模板的通信。所述平台被配置为向所述装置发送通信。在接收到所述通信时,所述装置被配置为取回预期接收者成员的所述联系人信息,以基于所述模板来创建消息,并将向所述预期接收者成员发送所述消息。所述平台不从所述装置接收所述多个成员的所述联系人信息。

[0004] 本发明的另一实施例涉及一种减少对社交工程的组织的易感性的方法。所述组织具有多个源。所述方法包括接收所述组织的所述多个成员的联系人信息。所述方法包括针对触发事件监测所述源中的每一个。所述方法包括基于检测到的触发事件,将所述组织中的至少一个成员识别为预期接收者。所述方法包括基于所述检测到的触发事件的特性来准备到所述预期接收者的消息。所述消息征求由所述预期接收者进行的动作。所述方法包括向预期接收者发送所述消息。所述方法包括确定所述预期接收者是否如由所述消息征求的来行动。所述方法包括对所述预期接收者的动作进行评估。

[0005] 本发明的另一实施例涉及一种用于评估对具有目录、多个数据库和消息传送系统的组织的社交工程的易感性的系统。所述系统包括装置。所述装置被配置为从所述目录接收具有所述组织的成员的联系人信息的地址簿。所述装置被配置为连接到所述多个数据库和所述消息传送系统。所述装置被配置为针对触发事件监测所述多个数据库和所述消息传

送系统。所述系统包括平台。所述平台被配置为从所述装置接收指示由所述装置识别出触发事件的信号。所述平台被配置为基于所述信号来创建模板。所述平台被配置为向所述装置发送所述模板。所述装置被配置为基于所述模板来创建到预期接收者的消息。所述平台被配置为确定所述预期接收者响应于所述消息是否采取预定的动作。所述平台被配置为响应于所述消息而对关于所述触发事件、所述消息和所述预期接收者动作的统计进行编译。

[0006] 本发明的另一实施例涉及一种用于评估组织对社交工程的易感性的系统。所述组织具有多个源和使用电子设备的多个成员。所述系统包括装置。所述装置被配置为从所述源中的至少一个接收地址簿，所述地址簿包括关于所述组织的多个成员中的每一个的识别信息和联系人信息。所述装置被配置为对所述识别信息中的至少一些进行别名化，并且利用标识符替换所述联系人信息以创建别名化的地址簿。要被别名化的信息是基于预定算法来确定的。所述系统包括被配置为从所述装置接收别名化的地址簿的平台。所述装置被配置为检测来自所述源的触发事件，并且向所述平台发送所述触发事件的指示。所述平台被配置为向所述装置提供通信，所述通信包括基于所述触发事件的消息模板、传递模式的指示、由所述装置已知的用于映射到所述组织的成员中的一个的传递标识符、以及调度指令。所述装置被配置为基于针对来自所述地址簿中的信息的所述预期接收者中的每一个的模板来创建个性化的消息。所述装置被配置为基于所述消息的类型向与所述平台分开的多个服务器中的一个发送所述消息，所述服务器中的一个被配置为向所述预期接收者发送所述消息。所述装置被配置为监测来自所述预期接收者的对所述消息的响应。所述装置被配置为对所述响应的部分进行别名化、保留所述响应的其他部分未别名化，并且基于预定算法来对所述响应的部分进行概述，并且向所述平台发送所述响应的别名化的、未别名化的以及概述的部分。

[0007] 替代的示例性实施例涉及如通常可以在权利要求中记载的其他特征和特征的组合。

附图说明

[0008] 结合附图根据以下详细描述将更充分地理解本申请，在附图中类似的附图标记指代类似的元件，其中：

[0009] 图1是示出了根据示例性实施例的包括工作流装置的用于测试和/或减少组织对社交工程的易感性的系统的框图；

[0010] 图2是示出了根据示例性实施例的包括图1的工作流装置的用于测试和/或减少组织对社交工程的易感性的系统的操作的方法的流程图；以及

[0011] 图3是示出了根据示例性实施例的包括工作流装置的用于测试和/或减少组织对社交工程的易感性的系统的框图。

具体实施方式

[0012] 参考附图，通常许多组织(例如，公司、政府、协会等)都希望减少对社交工程的易感性。随着电子设备以及其在组织中的使用的激增，许多组织都具有提供对机会的指示的信息的多个源，所述机会的指示例如，可教导时刻，其可能是用于启动社交工程易感性评估和/或减少运动(campaign)、测试等的有效或适当的时间和/或情况。本文描述的系统的实

施例被配置为针对这种对机会的指示来监测信息的源，并且自动(例如，无需用户干预)启动社交工程易感性评估和/或减少运动、测试等。

[0013] 例如，源可以包括不同的联网的目录、数据库、管理系统、消息传送系统和事件响应系统。许多组织可以具有与组织的各个部分进行交互的多个成员，例如雇员等。成员中的许多成员使用电子设备，例如计算机、膝上型计算机、智能电话、PDA等。这样的电子设备可以被配置为例如通过因特网、蜂窝网络、组织网络、LAN、WAN、Wifi等与其他电子设备、组织等进行通信。这些设备中的许多可以与联网的目录、数据库、管理系统、消息传送系统、事件响应系统等中的至少一个进行通信，并且这些目录可以包含关于电子设备的使用的信息。通过遍及组织的成员进行的许多不同事件(例如在电子设备上的动作)可以提供机会，例如可教导时刻，如上面所讨论的。

[0014] 例如，当在组织中发生某些事件或雇员动作时，在这些事件或动作之后不久，是例如通过事件或雇员动作来自动启动或触发的测试或运动来减少组织的社交工程易感性，用于减少组织的社交工程易感性的动作的效力可以被提高。然而，并非组织中的目录、数据库、管理系统、消息传送系统和事件响应系统中的所有都可以感知到事件或雇员动作。因此，在一个实施例中，提供了与整个组织中的许多目录、数据库、管理系统、消息传送系统和事件响应系统进行通信的系统，并且所述系统被配置为基于来自跨组织的目录、数据库、管理系统、消息传送系统和事件响应系统的信息来采取各种动作。

[0015] 另外，在一个实施例中，系统包括装置，例如工作流装置。工作流装置被配置为从源(例如，组织中的目录、数据库、管理系统、消息传送系统和事件响应系统)收集信息。然而，工作流装置在组织处维持收集到的信息，例如就物理硬件工作流装置而言，所述装置保持物理上位于组织处，并将收集到的信息维持在组织内；或者就虚拟和/或软件实现的工作流装置而言，收集到的信息被维持在系统、虚拟基础架构和/或组织的控制内。

[0016] 另外，在一个实施例中，所述装置被配置为与外部平台进行通信，所述外部平台诸如例如是作为服务平台的软件，所述服务平台被配置为提供社交工程测试或运动以降低组织对社交工程的易感性以及测试或运动的分析。所述装置收集识别信息和/或联系人信息，例如，来自诸如组织的目录、数据库、管理系统、消息传送系统和事件响应系统之类的例如组织的雇员的电子邮件地址、电话号码、移动电话号码、社交媒体标识符(诸如，FACEBOOOK帐户ID、TWITTER用户名等)。所述装置被配置为匿名联系人信息，并且当将要启动社交工程运动、测试等时，向所述平台传送匿名的联系人信息。因此，组织的成员的身份和/或联系人信息被维持在组织内，例如，未被传送到组织之外或组织的控制之外。当平台由所述装置触发以创建用于组织的预期接收者成员的模板时，该平台向所述装置发送包括与匿名的联系人信息相关联的模板的通信。所述装置根据匿名的联系人信息来确定实际的联系人信息、基于模板来创建消息、并向预期接收者发送消息。因此，实际的联系人信息未被传送到组织之外，这对于一些组织可能是期望的。

[0017] 参考图1，示出了系统100的实施例，系统100例如用于评估和/或减少组织对社交工程的易感性的系统。系统100包括远离组织的平台102。平台102是社交工程测试、改进和/或易感性评估平台，其被配置为测试组织对社交工程的易感性、评估、分析并且提供关于对组织的社交工程的易感性的度量、并训练组织的成员以减少对社交工程的易感性。平台102被配置为准备包括模板的通信，该模板可以用于创建可以经由各种格式、协议、设备等(诸

如例如，电子邮件、文本、SMS、电话、语音邮件等)被传递到组织的成员的消息。该消息征求接收者采取行动，例如点击链接、下载或上传文件、提供机密信息、手动回复消息、自动回复消息(例如“不在办公室”)，包括其中所征求的回复或交互是经由与通过其接收到消息的通信介质不同的通信介质来进行的回复或交互的情况，例如，电话消息征求电子邮件回复、电子邮件消息征求文本消息回复等。在一个实施例中，消息可以包括链接，该链接被配置为将接收者带到征求来自接收者的机密信息和/或将恶意代码下载到接收者的电子设备上的网站。平台102和/或工作流装置104被配置为监测和/或确定接收者是否采用所征求的动作。另外，平台102和/或工作流装置104可以被配置为对机密信息进行概述(例如，散列(hash)等)(或指导接收者的网络服务器这样做)、收集概述的信息、并丢弃机密信息，使得平台102不收集机密信息。例如，平台102可以收集机密信息中的字符的数量和/或类型，但是不收集机密信息本身。另外，平台102被配置为评估所收集的信息，例如执行基准测试等，以提供数据来通知进一步训练从而减少对社交工程的易感性。在一个实施例中，平台102作为软件被实现为服务平台，例如在云中、在远离客户端组织且不受该客户端组织控制的服务器上等等，组织获取许可来使用平台102。在其他实施例中，平台102可以以软件、硬件或软件和硬件的组合被提供到组织。

[0018] 在一个实施例中，系统100还包括被示为工作流装置104的装置。在一个实施例中，工作流装置104可以是虚拟装置，例如，在超级监督者服务器、VMWare、Microsoft Hyper-V、Citrix XenServer、Oracle VM Virtualbox、GNU/Linux KVM等上运行的软件中被实现的。在另一实施例中，工作流装置104可以是位于运行软件的客户端组织处的包括硬件处理器的物理装置，所述软件被配置为实现如下所述的工作流装置104的功能，所述物理装置例如，标准个人计算机硬件、PC或MAC、如Blackberry PI的小型装置、或者可以是服务器类的机架安装硬件。在任一情况下，在一个实施例中，工作流装置104在组织的控制中，例如，物理上位于组织处、以运行在由组织控制的服务器上的软件被实现、在由组织控制的虚拟基础架构上工作、在组织的环境内部等。

[0019] 工作流装置104与组织的源106进行通信。在一个实施例中，工作流装置104被给予对源106或源的一部分的有限的只读访问权。源106可以包括目录108，诸如例如，雇员联系人信息目录、可从MICROSOFT获得的活动目录(ACTIVE DIRECTORY)、轻量级目录访问协议(LDAP)目录、OpenLDAP目录、以及包括联合id系统的替代身份管理服务，等等。在一个实施例中，工作流装置104通过轻量级目录访问协议(LDAP)连接器110与目录中的每一个进行通信。源106还可以包括企业数据库112，诸如例如关联式系统，例如Oracle数据库、Sybase、Microsoft SQL、IBM DB2、Oracle MySQL;非关联式平面文件格式，例如逗号分隔值(CSV)或固定长度格式、非sql技术，例如HADOOP等。工作流装置104通过结构化查询语言(SQL)或类似连接器114与企业数据库112中的每一个进行通信。源106还可以包括学习管理系统116，诸如例如MOODLE、SCORM CLOUD、MEDIAPRO等。工作流装置104通过文件传输协议(FTP)或web服务连接器118与学习管理系统116中的每一个进行通信。源106还可以包括消息传送系统120，诸如例如，电子邮件系统、文本消息传送系统、即时通信系统例如Microsoft Exchange、IBM协作系统(Lotus)、使用IMAP或POP协议的其他电子邮件系统、其他非电子邮件系统网关例如SMS或电话网关等。工作流装置104通过IMAP/POP或web服务连接器122与消息传送系统120中的每一个进行通信。源106还可以包括事件响应源124，诸如系统或日志，

例如报告的组织的I.T.支持事件、给予组织的成员的帮助等的日志。事件响应源可以包括经由例如事件日志(Event Logs)、Syslog等提供事件日志的任何服务器或网络解决方案。工作流装置104通过连接器126(例如,SYSLOG、数据库或web服务)与事件响应源124中的每一个进行通信。

[0020] 在以上列出的将工作流装置104连接到源中的每一个的连接器是示例性的。在其他实施例中,可以使用其他合适的连接器。

[0021] 在一个实施例中,工作流装置104被配置为从源106中的至少一个接收组织的成员的联系人信息。例如,组织的电子邮件地址簿可以从源106中的至少一个传输到工作流装置104。在一个实施例中,组织的成员的电话号码、即时消息传送信息和/或其他联系人信息可以从源106传送到工作流装置104。然而,因为工作流装置104在组织的控制之下,所以联系人信息不被传输到组织之外和/或组织的控制之外。在一个实施例中,组织的成员的联系人信息可以包括例如组织的成员的电话号码(例如用于语音网络钓鱼测试的)、组织的成员的移动电话号码(例如通过其可以向组织的成员发送SMS文本消息以用于SMS网络钓鱼测试的)、和/或组织的成员的社交媒体标识符,例如FACEBOOK帐户标识符、TWITTER用户名等。

[0022] 在一个实施例中,识别信息可以包括属性或者与属性相关联,例如,基于风险的概述信息。例如,一个属性可以是雇员的部门、科室、位置、语言等的指示。另外,基于风险的属性可以包括雇员是否在预定时段期间多于一次呼叫帮助台重新设置密码、雇员以前是否在其电子设备上发现了病毒等的指示。这些属性可以由工作流装置104来使用,例如用于选择将成为社交工程运动和/或测试中的参与者的雇员、基于属性对社交工程和/或测试的结果进行分析和/或基准测试,例如,跨组织和/或在组织的一部分内进行基准测试。此外,在一个实施例中,对社交工程运动和/或测试的结果进行基准测试和/或分析可以相对于在与该组织相同的工业中或跨不同工业的其他组织来进行。

[0023] 在一个实施例中,工作流装置104被配置为定期地自动地(例如,无需用户干预)从源106确定是否已经对联系人信息进行了任何更新,例如,是否已经添加或移除了任何额外的雇员、是否更改了任何联系人信息等,并且相应地更新工作流装置104的联系人信息记录。

[0024] 在一个实施例中,如果工作流装置104确定存储在源106上的包括组织的成员的联系人信息的地址簿已经被更新,则工作流装置104将自动导入最新地址簿和/或最新联系人信息。在一个实施例中,工作流装置104监测地址簿的频率可以由用户来调整。另外,工作流装置104可以被配置为当检测到包括新雇员的更新的联系人信息时发起新雇员培训,例如社交工程易感性培训、组织特定的培训、基于风险的调查、模拟社交工程测试等。

[0025] 另外,在一个实施例中,工作流装置104被配置为定期地监测源106中的每一个以确定是否已经发生触发事件(例如基于风险的事件等)。参考图2,在步骤202中,工作流装置104被配置为针对触发事件来监测源。在步骤204中,当检测到来自源106中的一个的触发事件时,工作流装置104被配置为基于触发事件来确定组织的成员中的用于接收消息的成员或分组。然后,在步骤206中,工作流装置104确定组织的成员中的用于接收消息的成员或分组的联系人信息。

[0026] 在一个实施例中,工作流装置104被配置为将地址簿中的组织的成员中的每一个的联系人信息(例如,电子邮件地址等)映射到传递标识符。在一个实施例中,传递标识符是

十六进制数字，例如随机生成的，等等。在一个实施例中，传递标识符不是实际联系人信息并且不是电子邮件地址，这可以是有利的，因为如果传递标识符是电子邮件地址，则拥有该电子邮件地址的第三方可能会向组织的成员(例如，不是网络钓鱼模拟服务提供商也不是该组织)发送电子邮件，这可能是不期望的。另外，传递标识符不是转发电子邮件地址别名。

[0027] 在步骤208中，工作流装置104针对组织的预期接收者成员中的每一个创建传递标识符。传递标识符被配置为使组织的成员的联系人信息和/或身份模糊，使得该信息不会离开组织的控制，并且使得平台102不能基于传递标识符确定组织的成员中的每一个的联系人信息和/或身份。在步骤210中，工作流装置104被配置为将传递标识符与组织的将要成为消息的预期接收者的成员中的每一个进行关联，例如，在查找表中等，使得工作流装置104可以基于传递标识符确定组织中的用于接收消息的成员中的每一个成员的联系人信息和/或身份。在步骤212中，工作流装置104被配置为向平台102发送与传递标识符相关联的触发事件的指示和/或向平台102传递标识符。在步骤214中，平台102基于触发事件的指示准备模板，并向工作流装置104发送包括模板的通信。在一个实施例中，模板是基于触发事件的指示而准备的电子邮件模板。

[0028] 在一个实施例中，使用密码散列函数来创建传递标识符。在其他实施例中，传递标识符可以包括唯一的、非电子邮件地址标识符。在另一实施例中，随机生成传递标识符以避免信息泄漏，例如，如果组织的成员的身份是按字母顺序组织的，则非随机传递标识符例如用户1(“user1”)可能指示用户1是按字母顺序的组织的第一成员。通过提供不将信息提供到平台102的传递标识符，工作流装置104可以避免将关于组织成员的身份或联系人信息的信息泄漏到平台102。

[0029] 在一个实施例中，工作流装置104被配置为基于从平台102接收到的模板来创建到预期接收者的消息，并且工作流装置104将经由电子邮件向预期接收者发送所创建的消息，如下面进一步描述的。平台102被配置为在模板中插入标签。标签将指示工作流装置104在消息中创建消息位置，在该消息中包括联系人信息和/或识别信息以及所要包括的联系人信息和/或识别信息的类型，例如，对消息进行个性化。

[0030] 例如，电子邮件模板可以包括“Hello{emailFirstName:user1@pva}”。平台102不具有预期接收者的联系人信息或识别信息。基于“Hello{emailFirstName:user1@pva}”，工作流装置104可以被配置为创建以下电子邮件：以“Hello”开始接着是预期接收者的名字，工作流装置104具有对该预期接收者的名字的访问权，但是平台102不具有对该预期接收者的姓的访问权。

[0031] 模板还可以包括征求预期接收者采取动作的指示。工作流装置104可以基于例如在电子邮件模板中的征求被配置为在电子邮件中包括到网站的链接。链接包含识别信息，该识别信息向工作流装置104指示点击链接并被带到网站的成员的传递标识符。在一个实施例中，平台102可以被配置为向工作流装置104报告统计和/或分析，其中关于传递标识符来报告所述统计和/或分析，并且工作流装置104可以被配置为基于传递标识符利用组织的成员的实际身份和/或联系人信息来补充所报告的统计和/或分析。

[0032] 在步骤216中，当从平台102接收到包括模板的通信时，工作流装置104基于传递标识符来确定预期接收者。工作流装置104基于模板创建消息(例如电子邮件消息)，该电子邮件消息包括关于预期接收者的信息。例如，如果电子邮件模板包括“{emailFirstName:

user1@pva}”，则工作流装置104可以被配置为创建在电子邮件消息的正文中具有预期接收者的名字的电子邮件消息。工作流装置104可以从预期接收者的电子邮件地址、从组织的目录等获取预期接收者的名字，然而，平台102不具有对预期接收者的名字的访问权。此外，在电子邮件模板的示例中，工作流装置104基于联系人信息添加电子邮件报头并将电子邮件消息定址到预期接收者。在步骤218中，工作流装置104向预期接收者发送基于电子邮件模板所创建的电子邮件消息。电子邮件消息可以由接收者通过接收者的电子设备(例如计算机、智能电话、平板计算机等)进行访问和/或交互。

[0033] 在一个实施例中，工作流装置104被配置为从发送到平台102的信息中移除接收到的关于组织的成员的所有信息或信息的子集。例如，如果工作流装置104接收到组织的成员的电话号码，则工作流装置104被配置为利用电话传递标识符来替换电话号码，并向平台102发送电话传递标识符而不是实际的电话号码。工作流装置104将电话传递标识符与组织的成员中的每一个进行关联，例如在查找表中，使得工作流装置104可以根据电话传递标识符确定组织的实际成员和/或组织的成员的实际电话号码。然后，如果将要启动电话网络钓鱼感知运动，则工作流装置104向平台102发送用于组织中的预期参与该运动的成员中的每一个的电话传递标识符。作为响应，平台102准备模板(例如电话消息模板)，并且向工作流装置104发送包括具有电话传递标识符内容的模板的通信。工作流装置104根据电话传递标识符识别每个预期接收者的电话号码、基于模板创建个性化的电话消息、并拨打电话号码以传递个性化的消息，例如，文本消息、电话呼叫、语音邮件、记录的消息等。因此，平台102不接收组织的成员的实际电话号码。在一个实施例中，平台102能够独立于工作流装置104来调度和配置运动。该消息被配置为从组织的成员征求对工作流装置104(而不是平台102)的回复，例如，在消息中包括联系工作流装置104的电话号码等。工作流装置104接收独立于平台102的对由组织的成员发送的消息的回复。工作流装置104被配置为从回复中移除可以用于识别或联系组织的成员的信息和/或任何机密信息，并向平台102发送将信息移除后的回复以用于分析、评估等。因此，平台102也不从由组织的成员进行的回复中接收组织的成员的识别信息和/或联系人信息。在无需识别信息/联系人信息或机密信息的情况下，平台102仍然能够调度和报告整体结果。

[0034] 在一个实施例中，工作流装置104被配置为从组织接收关于组织的成员的按字段组织的信息。各种字段可以包括例如姓名、电子邮件地址、电话号码、移动电话号码、社交媒体标识符、组织中的部门、职位头衔等。工作流装置104被配置为创建标识符以与在这些字段中的预定字段中的信息进行关联，而使在这些字段中的其他预定字段中的信息未受影响。标识符用于发送到平台102代替实际信息，并且不包含组织的成员的任何识别信息和/或联系人信息。例如，工作流装置104可以将组织的成员的姓名、电子邮件地址、电话号码、移动电话号码、社交媒体标识符和职位头衔中的每一个与标识符进行关联，而使组织中的成员的部门未受影响，例如，平台102将接收成员的在组织中的实际部门但仅是标识符，平台102不能根据该标识符针对其他字段确定个人或联系人信息。可以由工作流装置104向平台102发送标识符以及组织信息中的部门。部门或在其它实施例中不被工作流装置104改变的其他信息可以由平台102使用用于社交工程测试的结果的分析/评估。在一个实施例中，工作流装置104被配置为接收输入，以在向平台102传送标识符之前，基于组织的偏好、策略等，确定针对哪些字段信息将与标识符进行关联或不进行关联。

[0035] 在一个实施例中，装置104被配置为通过组织内的各种应用接口进行连接以发送消息，这允许“发送消息”功能从平台102扩展到装置104，而无需平台102对组织不希望其离开组织或离开组织的控制的组织信息具有访问权，并且无需平台104具有对组织内的应用接口的直接访问权。

[0036] 在一个实施例中，工作流装置104和平台102使用应用程序接口(例如，web服务调用、远程程序调用等)进行通信。因此，平台102可以通过工作流装置104在组织中传送消息而无需知道工作流装置104连接到的组织的网络的细节。在一个实施例中，工作流装置104扩展平台“发送消息”功能并充当SMTP客户端，并与组织的SMTP服务器进行通信以使修改的消息传递到预期接收者。

[0037] 当由工作流装置104检测到触发事件时，工作流装置104向平台102发送关于触发事件的信息以及传递标识符，工作流装置104可以根据该传递标识符确定消息的预期接收者的联系人信息，但是平台102不能根据该传递标识符确定预期接收者的身份或联系人信息。基于关于触发事件的信息，平台102生成包括模板的通信。通信不是电子邮件消息。通信包括模板(诸如例如，电子邮件消息模板)和消息请求。消息请求包括关于传递标识符和时间帧的信息。该通信通过安全的(例如通道传输)非电子邮件连接被传送到工作流装置104。

[0038] 工作流装置104接收该通信并且基于从平台102接收到的模板创建消息，例如电子邮件消息，例如具有报头的，等等。在一个实施例中，工作流装置104被配置为基于关于预期接收者的信息来对每个消息进行个性化。然后，在一个实施例中，工作流装置104使用自包含的SMTP服务器来传递基于从平台102接收到的模板所创建的消息。

[0039] 在一个实施例中，托管平台102的公司还将安全的电子邮件服务器托管在组织之外。工作流装置104被配置为使用安全的电子邮件服务器来向组织中的接收者发送由工作流装置104基于从平台102接收到的电子邮件模板所创建的电子邮件消息。由工作流装置104从平台102接收到的通信不是电子邮件消息，例如，不是通过SMTP接收到的，等等。安全的电子邮件服务器不是由平台102直接可访问的。在一个实施例中，所有消息和日志定期从安全的电子邮件服务器中删除。

[0040] 在一个实施例中，工作流装置104被配置为向组织的成员发送电子邮件消息，例如由工作流装置104基于从平台102接收到的电子邮件模板准备的电子邮件消息。电子邮件消息包括用于通过电子邮件进行回复的征求。来自组织的成员的电子邮件响应被配置为被引导到不由平台102访问的SMTP服务器。SMTP服务器将电子邮件响应引导到工作流装置104，该工作流装置使用IMAP/POP或其他类似协议来回顾和/或读取电子邮件响应。工作流装置104被配置为从电子邮件响应中移除组织的成员的任何识别信息或联系人信息，以便概述(例如，散列等)电子邮件中的机密和/或其他信息，并且向平台102发送概述的电子邮件响应，联系人信息和/或识别信息被移除以用于评估、分析等。因此，平台102不从由组织的成员对电子邮件消息的回复中接收识别信息、联系信息或机密信息。

[0041] 在一个实施例中，工作流装置104被配置为向组织中的预期接收者发送包括链接的电子邮件消息。当由预期接收者点击链接时，预期接收者被带到由与平台102分开的和/或由平台102不可访问的登录页面服务器所服务的网页。在一个实施例中，工作流装置104包括和/或充当登录页面服务器。在另一实施例中，登录页面服务器与工作流装置104分开并与平台102分开。该链接被配置为发送与包含被点击的链接的电子邮件消息关联的标识

符，例如十六进制数，等等。工作流装置104被配置为确定(或根据登录页面服务器确定)电子邮件消息包含被点击的链接。然后，工作流装置104确定组织中的接收到具有被点击的链接的电子邮件的成员的身份、利用平台102不能根据其确定关于组织的成员的任何识别信息的标识符来替换身份、并且向平台102发送关于被点击的链接的标识符以用于分析、评估等。因此，平台102不获取关于组织中的点击链接的成员的实际身份或联系人信息的信息。在一个实施例中，当组织的成员点击电子邮件中的链接时到达的登陆网页可以征求组织的成员将信息输入到网页中，例如，网页可以包含在其中可以输入信息的字段等。组织可能希望收集成员输入到网页中的信息，但可能不希望信息离开组织的控制。工作流装置104被配置为收集(如果工作流装置104充当登录页面服务器，或者如果登录页面服务器与工作流装置104分开，则工作流装置104从登录页面服务器收集)由组织的成员输入的信息。然后，信息可以被概述(例如，散列等)，并且可以由工作流装置104向平台102发送关于例如输入的字符的量/类型等的指示符和概述的信息以用于评估、分析等，而无需实际的底层信息本身离开组织的控制。

[0042] 描述了各种示例性触发和工作流装置/平台响应。例如，在一个实施例中，当组织的成员从组织的帮助台请求新密码和/或重置密码时，工作流装置104确定触发事件已经发生了，例如，帮助台可以具有在其中记录了针对新密码的所有请求等等的数据库。工作流装置104在检测到来自源106中的一个的密码重置时，(或在一个实施例中，根据在预定时间段内针对所有检测到的密码重置进行处理的预定调度定期地)，联系平台102并且指示这种类型的触发事件已经发生。平台102基于这种类型的触发事件创建包括电子邮件模板的通信。通信还包括消息请求，该消息请求包括关于传递标识符的信息，工作流装置104可以根据该传递标识符确定预期接收者和时间帧。工作流装置104基于电子邮件模板创建电子邮件消息，以由工作流装置104向组织中的其密码被重置的成员发送该电子邮件，请求该组织的成员点击电子邮件中的链接并输入新密码信息以用于验证。由工作流装置104创建的电子邮件消息是基于包含在从平台102发送到工作流装置104的通信中的电子邮件模板和消息请求(包括关于传递标识符和时间帧的信息)来创建的。

[0043] 由平台102向工作流装置104发送的通信包括电子邮件模板和包括传递标识符的消息请求，工作流装置104可以基于该传递标识符确定将要由工作流装置104创建的电子邮件消息的预期接收者的身份和时间帧信息，例如，关于何时将要向预期接收者发送由工作流装置104创建的电子邮件消息的信息。由平台102通过安全的通道连接(例如，不是通过SMTP电子邮件)向工作流装置104发送包括电子邮件模板的通信。工作流装置104基于从平台102接收到的通信来创建将被发送到组织的预期接收者成员的电子邮件消息。如果接收者点击包含在电子邮件消息中的链接并将接收者的密码输入到登录页面网站，则登录页面通知接收者该电子邮件消息和登录页面是测试，当电子邮件是真正的网络钓鱼攻击电子邮件而不是测试时接收者将是网络钓鱼攻击的受害者，并且在一个实施例中，登录页面针对接收者建议培训机会。工作流装置104对由接收者输入的密码信息进行概述例如，散列(或指导网站对其进行概述)，并丢弃(或指导网站丢弃)机密密码信息。工作流装置104利用标识符来记录概述的信息，工作流装置104可以根据该标识符确定接收者的提供机密信息的身份和/或联系人信息，但是平台102不能根据该标识符确定接收者的身份和/或联系人信息。

[0044] 在另一实施例中，当组织的成员从组织的帮助台请求新密码和/或重置密码时，工作流装置104确定该触发事件已经发生，例如，帮助台可以具有在其中记录了针对新密码的所有请求等等的数据库。工作流装置104在检测到来自源106中的一个的密码重置时，(或在一个实施例中，根据在预定时间段内针对所有检测到的密码重置进行处理的预定调度定期地)，联系平台102并且指示已经发生了这种类型的触发事件。平台102创建包括用于这种类型的触发事件的电子邮件模板和包括传递标识符的消息请求的通信，工作流装置104可以基于该传递标识符确定将由工作流装置104创建的电子邮件消息的预期接收者的身份和时间帧信息，例如，关于何时将要向预期接收者发送由工作流装置104创建的电子邮件消息的信息。工作流装置104使用电子邮件模板来创建由工作流装置104向组织中的其密码被重置的成员发送的电子邮件消息，请求组织的成员点击电子邮件中的链接并输入新密码信息以用于验证。平台102向工作流装置104发送包括电子邮件模板的通信。工作流装置104根据电子邮件模板创建电子邮件消息，并向组织的预期接收者成员发送电子邮件消息。如果接收者点击链接并输入密码，则网站通知接收者该电子邮件和网站是测试，当电子邮件是真正的网络钓鱼攻击电子邮件而不是测试时，接收者将是网络钓鱼攻击的受害者，并且在一个实施例中针对接收者建议培训机会。工作流装置104对由接收者输入的密码信息进行概述例如，散列(或指导网站对该密码信息进行概述)，并丢弃(或指导网站丢弃)机密密码信息。工作流装置104记录概述的信息并利用标识符替代识别信息，平台102不能根据该标识符确定接收者的身份和/或联系人信息。在该情况下，平台102使用工作流装置104来提供更新的信息并触发平台动作。

[0045] 在一个实施例中，工作流装置104被配置为定期地和/或基于来自用户的请求来联系平台102以接收匿名的(例如，无需识别信息)关于对社交工程的组织的易感性和/或社交工程测试结果的报告和/或分析。在一个实施例中，工作流装置104被配置为基于报告中的标识符利用识别信息和/或联系人信息来补充匿名的报告和/或分析。

[0046] 示例性触发事件可以包括：例如，将新联系人信息添加到地址簿中、将组织的成员移动到组织的不同科室、组织的成员具有组织中的成员资格周年(例如，雇员具有工作周年等)、组织的成员请求重置密码、组织的成员违反数据丢失预防规则、组织的成员将可疑电子邮件转发到帮助台、用户完成培训、用户改变工作状态或角色、管理员基于其下属触发了事件、用户因太多次尝试登陆而被锁定在系统外、用户从工作中抽出时间、用户由于人力资源违规而被控告、安全警告/事故、公司的重组、裁员、分包商入职/退出等。其他示例性的触发事件可以包括个人访问或尝试用于访问已知的网络钓鱼web站点、访问或尝试用于访问可疑的网络钓鱼web站点、接收网络钓鱼电子邮件或通信、或是成为由入站消息过滤器拦截的网络钓鱼电子邮件或通信的预期接收者。特别地，对被引导到特定个人的鱼叉式网络钓鱼电子邮件或通信的识别可以作为触发事件。额外的触发事件可以包括个人忽略或未能响应于培训邀请、对咨询或就业合同或状态的先前或未决更改、或在可识别分组中基于个性、IQ、物理或可客观测试的其他个人属性进行的分类。

[0047] 监测源106的工作流装置104允许基于风险的用户属性从多个数据库源被合并。例如，人力资源数据库可以包括组织的所有成员的联系人信息，帮助台数据库可以包括针对新密码的所有请求、IT问题的报告、发现的新病毒的列表，并且这样的工作流装置104可以使用来自帮助台数据库的信息，例如，针对新密码的请求，其用于自动触发工作流装置104

来联系平台102从而启动用于减少对社交工程的易感性的运动。由于各种不同的源106正由工作流装置104来监测，所以可以由工作流装置104来观察各种不同的触发，工作流装置104可以自动地(例如，无需用户干预)引导平台102基于观察到的触发类型通过工作流装置104来启动对组织的不同成员的不同的运动、测试等。

[0048] 在一个实施例中，工作流装置104被配置为与平台102进行出站连接，例如，无需组织打开任何输入端口，并因此不需要对组织的防火墙进行任何修改。在一个实施例中，工作流装置104被配置为使用加密通道技术(例如，VPN、SSH等)与平台102进行输出连接和/或通道。然后，工作流装置104和平台102能够通过通道安全地传送通信，其中在工作流装置104和平台102之间发送的数据被加密。由平台102通过通道而不是例如通过电子邮件等向工作流装置104发送消息。

[0049] 在一个实施例中，可以针对组织提供如上所述的多个工作流装置，例如，不同工作流装置用于组织的不同科室，等等。

[0050] 在一个实施例中，工作流装置104可以包括被配置为用于缓存来自平台102的信息的存储器。例如，大型文件(例如，多媒体训练文件等)可被缓存在工作流装置104的存储器中以用于在组织内部对其进行快速和/或容易地访问，而无需在每次使用和/或访问大型文件时均从例如平台102下载大型文件。

[0051] 在一个实施例中，如上所述的工作流装置充当用于在组织的虚拟基础架构上的组织的网络内运行的组织的黑盒。

[0052] 在一个实施例中，平台102被配置为创建网站，到所述网站的链接在电子邮件模板中被发送到工作流装置104。网站可以包括向被链接到该网站的某人指示该网站是合法的信息。此外，网站可以包括被配置为接收来自用户的信息(例如，机密信息)和用户提供机密信息的请求的字段。

[0053] 参考图3，示出了系统300的另一实施例，例如用于评估和/或减少组织对社交工程的易感性的系统。系统300允许在作为服务环境(例如，远离客户端组织)的软件中对来自组织成员的测试的数据进行分析和评估，而无需用于对数据进行分析和评估的算法和源代码被给予给组织，而且也无需使任何机密信息、敏感信息、联系人信息或成员识别信息离开组织的控制。系统300具有与上述系统100的许多相似之处，因此其他特征是下面描述的重点。

[0054] 在一个实施例中，系统300包括远离组织(例如不在组织的控制之下)的平台302。平台302包括处理器，该处理器被编程为生成和/或取回用于社交工程测试的消息并且评估和分析对消息的响应和测试结果。系统300还包括工作流装置304。在一个实施例中，工作流装置304位于组织的物理位置处，在组织的基础架构上运行，或者在组织的控制之下。工作流装置304与组织的信息的源306(例如类似于上述的源106)进行通信。工作流装置304从组织接收到地址簿。地址簿包括组织的成员的识别信息，例如姓名、部门、组织内的职位等。此外，地址簿包括组织的成员的联系人信息，例如，电子邮件地址、电话号码、移动电话号码、社交媒体标识符等。如果组织不希望机密信息(例如，地址簿中的信息)离开组织的控制，则装置304被配置对地址簿的识别信息的至少部分进行别名化，并针对地址簿的联系人信息创建传递标识符，而且还创建和保留足以根据别名化的信息和传递标识符来识别未别名化的地址簿中的条目的信息，例如创建查找表等。

[0055] 在一个实施例中，对地址簿中的信息进行别名化包括随机映射。因此，例如，如果

组织中的多于一个成员具有名字“John”，则组织中的每个“John”的别名化的名字将是不同的别名化值，例如，防止信息的泄漏的不同的30位十六进制数或任何其他合适的别名，例如，防止基于别名化的信息来确定关于组织的成员的实际身份或联系人信息的信息。

[0056] 装置304被配置为以安全的方式(例如，如上所述的通道传输等)通过因特网与平台302进行联系和通信。当装置304检测到来自组织中的源306的触发事件时，装置304被配置为向平台302发送关于触发事件的信息以及响应于该触发事件而被联系的组织的成员的传递标识符，例如，平台302不接收响应于触发事件而被联系的组织的成员的实际联系人信息。在一个实施例中，关于组织的成员中的被发送到平台302的任何识别信息在到平台302之前被别名化，使得平台302不能确定关于组织的成员的任何识别信息。联系人信息不被发送到平台302，而是传递标识符(平台302不能根据该标识符确定组织的成员的实际联系人信息)替代地被发送到平台302。在另一实施例中，仅对关于组织的成员的将被发送到平台302的识别信息中的一些进行别名化，而识别信息的其他部分可以不被别名化并且可由平台302来识别，例如成员在其中工作的组织的部门等可以不被别名化。

[0057] 基于关于从工作流装置304接收到的触发事件的信息，平台302取回和/或创建包括模板(例如电子邮件模板)的通信。在一个实施例中，平台302向工作流装置304发送包括模板的通信，该模板包括通用标签，所述通用标签向工作流装置304指示信息的类型，工作流装置304将所述信息的类型包括在由工作流装置304基于模板所创建的消息内，以针对预期接收者对消息进行个性化，例如，电子邮件模板可以包括“你好，电子邮件名”的问候语，基于该问候语工作流装置304将从地址簿中取回每个预期接收者的名字，并且将姓名插入到基于电子邮件模板针对预期接收者的预期而创建的每个电子邮件中。在另一实施例中，平台302被配置为将别名化的信息插入到模板中，例如，利用“你好，来自从装置接收到的别名化的地址簿的电子邮件名字的别名值”替换“你好，电子邮件名”的电子邮件模板问候语。

[0058] 在各种实施例中，可以由平台302创建其他类型的模板(例如，用于可听消息的脚本模板、用于文本消息的模板等)并且将其发送到工作流装置304，并且工作流装置304可以被配置为基于其他类型的模板来创建其他类型的消息，例如，可听消息、书面消息、文本消息等。

[0059] 装置304从平台302接收包括模板的通信，并且确定将要基于模板被创建的消息的预期接收者。然后，装置304找到并替换消息中的标签，或者在由平台302插入别名化的信息的情况下，利用关于来自地址簿的预期接收者的实际信息来替换别名化的信息。在其中平台302已将别名化的信息插入到模板的实施例中，一旦装置304确定消息的预期接收者，则装置304查找模板中的别名化的信息的每个部分，并将来自地址簿的相对应的实际信息输入到由装置304基于模板创建的消息中，例如，将“别名化的名字”变为“实际的名字”、将“别名化的姓”变为“实际的姓”、将“别名化的职称”变为“实际的职称”等。如果别名化的值中的一个与查找表中的别名化的值不匹配，则装置304将识别和/或补救该错误，其中查找表是将用于预期接收者的别名化的值与地址簿中的实际信息进行关联的表。例如，如果装置304确定消息的预期接收者是“John Smith”，并且在查找表中John Smith的名的别名化的值是“XYZ”，并且平台302已将别名化的名字替代为“ABC”来插入到消息中，则装置304将识别出别名化的值与预期接收者不对应，并且将不会插入具有别名化的名字“ABC”的不同接收者的名字。

[0060] 一旦装置304使用来自地址簿的信息基于模板创建了个性化的消息，装置304就被配置为例如通过因特网、通过安全连接等基于消息的类型向多个服务器350中的一个发送个性化的消息。例如，如果消息是电子邮件消息，则装置304被配置为向电子邮件服务器352发送消息。然后，电子邮件服务器352将电子邮件提供到预期接收者的电子邮件账户353。如果消息是文本消息，则装置304被配置为向文本消息服务器354发送消息。然后，文本消息服务器将文本消息提供到预期接收者的文本消息帐户。如果消息是可听消息，例如语音邮件等，或者如果消息的文本版本由计算机化的文本到语音转换器说出，则装置304被配置为向电话服务器356发送消息。然后，电话服务器356将可听消息提供到预期接收者的电话357。

[0061] 在一个实施例中，服务器352、354、356包含于工作流装置304中，例如，工作流装置304本身包括和/或充当服务器352、354、356。在另一实施例中，服务器352、354、356与工作流装置304分开，但与工作流装置304进行通信，并且也与平台302分开但不可由平台302访问。

[0062] 在一个实施例中，消息征求来自接收者的响应。所征求的响应可以在与初始消息的介质相同的介质(例如，可听、文本、电子邮件)上，或者可以在不同的介质上。工作流装置304被配置为例如通过服务器350等监测和收集接收者对消息的响应。装置304被配置为回顾每个接收到的响应、将组织不希望离开组织的控制的响应所接收到的预定信息进行别名化、使组织不要求被保留在组织的控制之下的响应所接收到的其他预定信息保持未别名化、并且对在响应中接收到的一些预定信息进行概述，例如在一个实施例中，信息不能被别名化。然后，装置304被配置为向平台402发送每个响应的别名化的部分、未别名化的部分和概述的部分以用于分析和/或评估。因此，机密信息被保持在组织的控制之下而不被呈现给平台302。平台302分析响应并准备社交工程测试和/或培训的报告，例如，关于结果、有效性等的报告。装置304接收具有别名化的信息和概述的信息的报告，并且更新该报告以利用例如来自地址簿的实际信息替换别名化信息，并例如利用实际信息替换概述的信息，使得该报告可以由组织的特定成员来回顾。因此，由装置向组织提供的报告可以包括平台不可用的个人识别信息。

[0063] 例如，如果将语音邮件消息发送到组织的成员，请求接收者呼叫电话号码“XXX-XXX-XXX”，输入代码“YYYY”，并留下提供该人的新计算机密码的语音邮件，则装置304被配置为针对电话呼叫来监测电话服务器356。当接收到来自组织成员的呼叫时，装置304被配置为使用地址簿来识别该成员正在根据其进行呼叫的电话号码。装置304将对该电话号码信息进行别名化，使得平台302不接收该成员的实际电话号码。装置304还将收集由该组织的成员输入的“YYYY”代码。然而，由于该信息不是机密的(例如是由系统生成的，例如当消息初始生成时是由平台302生成的)，所以该信息可以被传递到平台302，并且不被装置304别名化。装置304还收集组织的成员的可听消息，例如，作为.wav文件或任何其他合适类型的文件。可听消息可以包含机密信息，但不被别名化(在其他实施例中，可以使用自动或手动的语音识别技术将可听消息转换成文本，并且装置304可以被配置为对所得到的文本进行别名化)。相反，装置304被配置为对关于可听消息的信息(例如，消息长度、非静音记录的秒数、音量级别、音频文件中的音节的估计的数量、其组合等)进行概述，以保存消息本身而不是向平台302发送消息本身。概述的信息可以被传递到平台302，使得机密信息不离开组织。因此，装置304被配置为回顾来自组织的成员的收集到的响应并且对来自响应的一些信

息进行别名化、使来自响应的其他信息未别名化、并根据预定算法对来自响应的其他信息进行概述而无需用户干预。在一个实施例中，装置304被配置为接收来自组织的指令，用于确定哪些信息将被别名化、哪些信息将保持不被别名化、以及哪些信息将根据组织的规范来进行概述。

[0064] 在一个实施例中，由平台302提供到工作流装置304的通信包括传递模式指示符，例如，指示工作流装置304将基于模板和/或介质所创建的消息的类型(例如，电话、电子邮件、SMS等)，工作流装置将通过其传递基于模板创建的消息。在一个实施例中，由平台302提供的通信包括调度指令，例如，指示工作流装置304何时创建和发送消息，如果消息不可传递(例如忙信号、反弹通知等)则该做什么(例如，通信包括有效的信息使得工作流装置304知道应该回拨或重试多少次、在一天中的什么时间、一周中的哪天等被允许或不允许发送消息、以及如何询问平台302进一步的指示)。

[0065] 应当理解，附图详细地示出了示例性实施例，并且应当理解，本申请不限于在说明书中阐述或在附图中示出的细节或方法。还应当理解，术语仅用于描述的目的而不应被视为限制。

[0066] 鉴于本描述，对于本领域技术人员而言，本发明的各个方面的进一步修改和替代实施例将是显而易见的。因此，本描述仅被解释为说明性的。在各种示例性实施例中示出的构造和布置仅仅是说明性的。虽然在本公开中仅详细描述了几个实施例，但是在实质上不背离本文所述的主题的新颖教导和优点的情况下，可以进行许多修改(例如，尺寸、维度、结构、参数的值、布置、材料的使用等中的变化)。显示为整体形成的一些元件可以由多个部件或元件构成，元件的位置可以颠倒或另外是变化的，并且分立的元件或位置的本质或数量可以被改变或变化。根据替代实施例，任何过程、逻辑算法或方法步骤的次序或序列可以被改变或重排序。在不背离本发明的范围的情况下，也可以在各种示例性实施例的设计、操作条件和布置中进行其他替换、修改、改变和省略。

[0067] 在各种实施例中，本文描述的平台和工作流装置可以包括通用处理器、专用处理器、包含一个或多个处理组件的电路、一组分布式处理组件(例如，被配置为用于处理的分布式计算机)等等。平台和工作流装置的实施例可以是或包括用于进行数据处理和/或信号处理的任何数量的组件。根据示例性实施例，任何分布式和/或本地存储器设备可以与本公开的系统、方法、装置和平台一起来使用和/或被包括在其中。在一个实施例中，工作流装置或平台可以包括可通信地连接到处理器或工具(例如，经由电路或其他连接)的存储器，并且可以包括用于执行本文所述的一个或多个过程的计算机代码。

[0068] 在各种实施例中，平台和/或工作流装置可以以软件来实现。在另一实施例中，平台和/或工作流装置可以以计算机硬件和软件的组合来实现。在各种实施例中，实现本文讨论的平台和/或工作流装置的系统包括被配置为提供本文讨论的功能的一个或多个处理组件、一个或多个计算机存储器组件以及一个或多个通信组件。在各种实施例中，平台和/或工作流装置可以包括通用处理器、专用处理器(ASIC)、包含一个或多个处理组件的电路、一组分布式处理组件、被配置为用于处理的一组分布式计算机等。在各种实施例中，平台和/或工作流装置可以包括存储器组件，例如用于存储数据的一个或多个设备和/或用于完成和/或有利于本公开中描述的各种过程的计算机代码，并且可以包括数据库组件、目标代码组件、脚本组件和/或用于支持本公开中描述的各种活动的任何其他类型的信息结构。在各

种实施例中，本文描述的通信组件可以包括用于传送用于本文讨论的系统和方法的数据的硬件和软件。例如，通信组件可以包括用于如本文所讨论的接收和发送信息的电线、插孔、接口、无线通信硬件等。在各种具体实施例中，本文描述的平台、工作流装置和/或方法可以是包括用于提供各种功能并执行本文讨论的各种步骤的(例如，计算机编码的)指令的非暂时性的计算机可读介质中的实施例。在各种实施例中，计算机代码可以包括目标代码、程序代码、编译代码、脚本代码、可执行代码、指令、编程的指令、非暂时性编程的指令或其任何组合。在其它实施例中，本文描述的工作流装置和/或平台可以通过任何其它合适的方法或机制来实现。在一个实施例中，上述工作流装置可以是本地的，例如，在与组织相同的物理位置处的或者在组织的控制之下的计算机硬件上实现的。在其他实施例中，工作流装置和/或平台可以远离组织，例如不在与组织相同的物理位置处。

[0069] 在一个实施例中，本文描述的工作流装置可以以存储和/或本地托管在客户端组织的软件来实现。在各种实施例中，本文描述的工作流装置可以经由分布式计算在云中实现，如托管在远离客户端组织的服务器上的软件不与客户端组织处于相同的物理位置等。

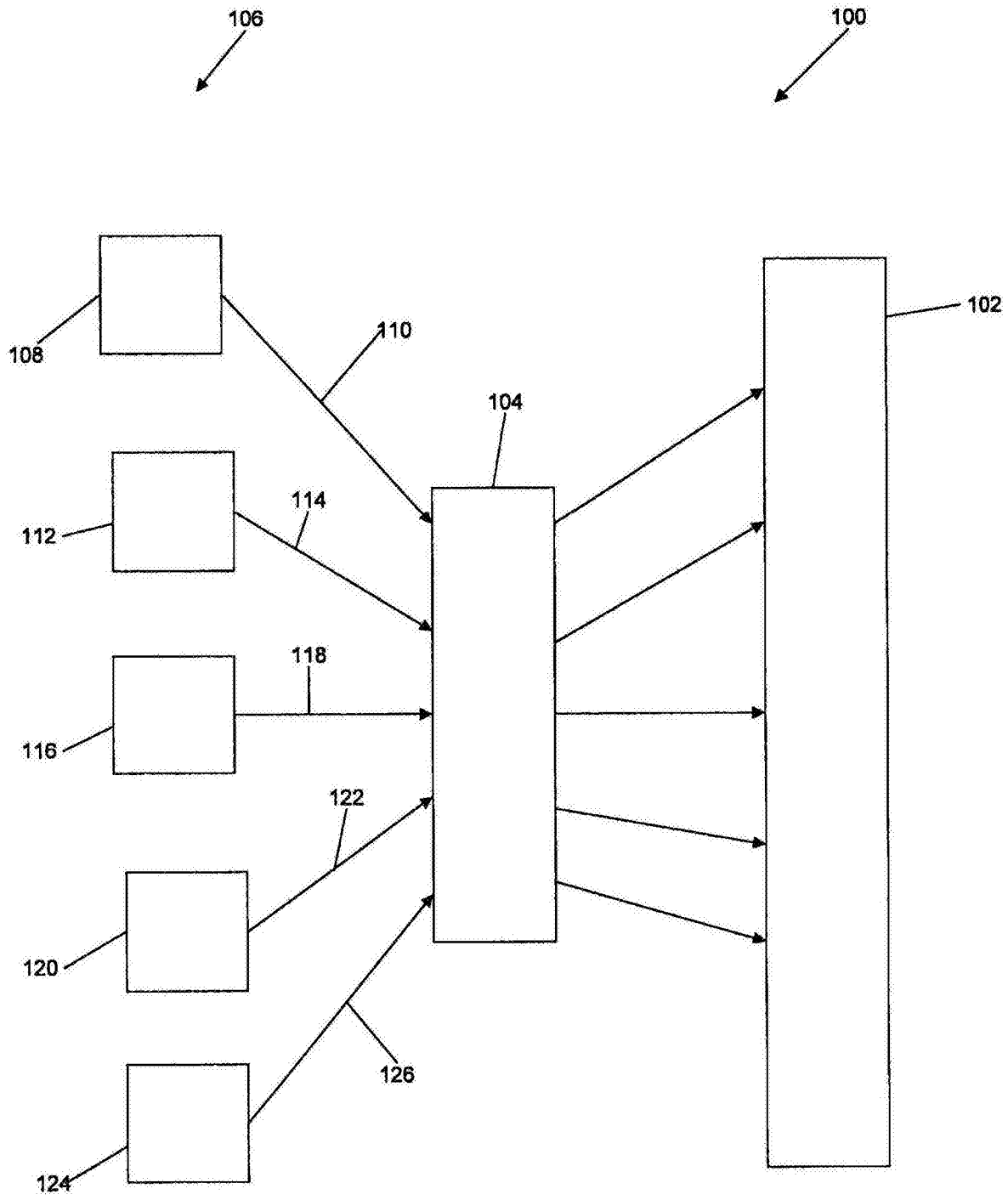


图1

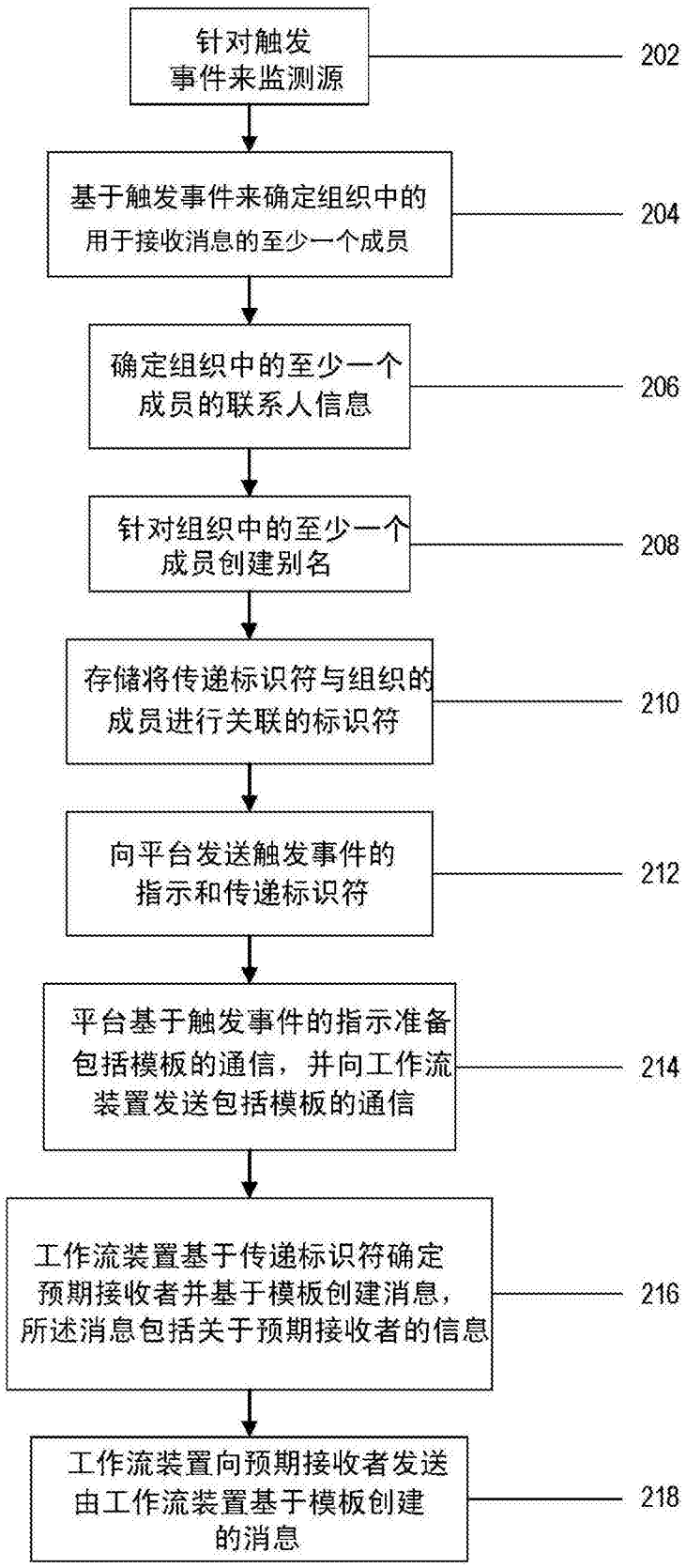

针对触发事件来监测源
202
基于触发事件来确定组织中的用于接收消息的至少一个成员
204
确定组织中的至少一个成员的联系人信息
206
针对组织中的至少一个成员创建别名
208
存储将传递标识符与组织的成员进行关联的标识符
210
向平台发送触发事件的指示和传递标识符
212
平台基于触发事件的指示准备包括模板的通信，并向工作流装置发送包括模板的通信
214
工作流装置基于传递标识符确定预期接收者并基于模板创建消息，所述消息包括关于预期接收者的信息
216
工作流装置向预期接收者发送由工作流装置基于模板创建的消息
218

图2

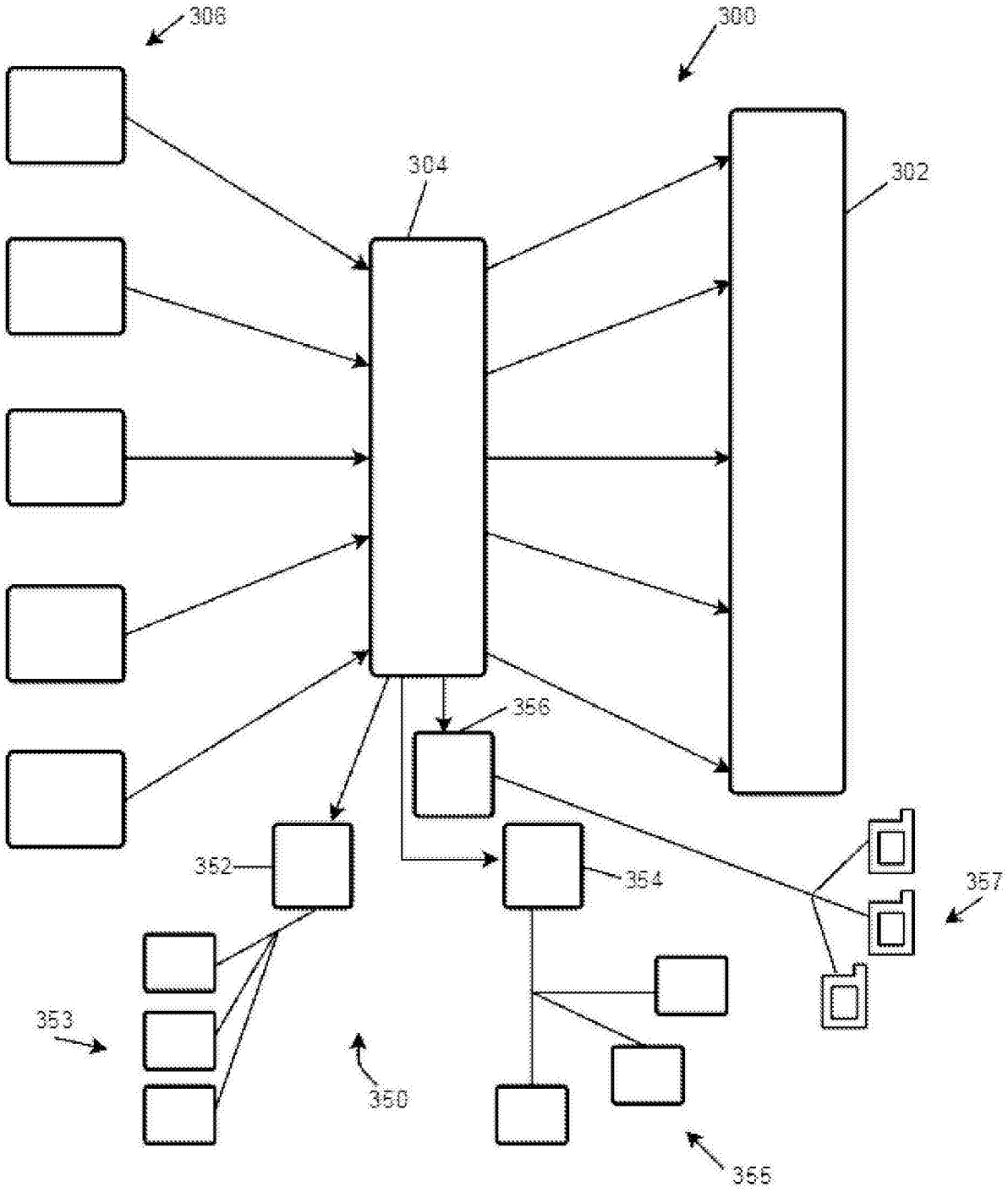


图3