(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 104025635 A
(43)申请公布日 2014.09.03

(21)申请号 201280053818.9
(22)申请日 2012.10.16
(30)优先权数据
61/548,194 2011.10.17 US
61/548,224 2011.10.18 US
13/339,221 2011.12.28 US
(85)PCT国际申请进入国家阶段日
2014.04.30
(86)PCT国际申请的申请数据
PCT/US2012/060455 2012.10.16
(87)PCT国际申请的公布数据
WO2013/059210 EN 2013.04.25
(71)申请人 迈克菲公司
地址 美国加利福尼亚
(72)发明人 P·G·巴萨瓦帕特纳 S·K·加达拉 S·施雷克 D·M·戈尔德施拉格
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英 张立达
(51)Int.Cl.
H04W 12/08(2006.01)
H04W 24/00(2006.01)

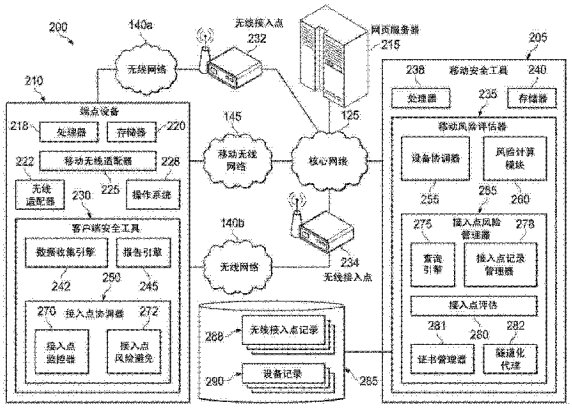
权利要求书2页 说明书19页 附图9页

(54)发明名称

移动风险评估

(57)摘要

从特定端点设备接收识别由所述特定端点设备遇见的特定无线接入点的查询。识别针对所识别的特定无线接入点的预存在的风险评估数据，并且将以与所述特定无线接入点相关联的预评估风险为特征的查询结果数据发送到所述特定端点设备。在一些实例中，基于所述预存在的风险评估数据生成所述查询结果数据。在一些实例中，预存在的风险评估数据可以是至少部分地由端点设备执行的较早风险评估的结果，所述端点设备与所述特定无线接入点连接并且测试所述特定无线接入点。



CN 104025635 A

1. 一种方法，包括：

从特定端点设备接收识别由所述特定端点设备遇见的特定无线接入点的查询；

识别针对所识别的特定无线接入点的预存在的风险评估数据；并且

向所述特定端点设备发送以与所述特定无线接入点相关联的预评估的风险为特征的查询结果数据。

2. 如权利要求 1 所述的方法，进一步包括利用所述特定端点设备参与所述特定无线接入点的风险评估。

3. 如权利要求 2 所述的方法，进一步包括结合由所述特定端点设备执行的至少一个评估任务而从所述端点设备接收风险评估反馈数据。

4. 如权利要求 3 所述的方法，进一步包括使用所接收的风险评估反馈数据来确定针对所述特定无线接入点的风险概要。

5. 如权利要求 4 所述的方法，其中，在所述风险概要的确定中考虑与所述特定无线接入点相关联的所述预评估的风险。

6. 如权利要求 3 所述的方法，其中，所述反馈数据包括服务集标识符 (SSID)、描述由所述无线接入点使用的加密的数据、醒目页面信息以及无线接入点密码信息中的至少一个。

7. 如权利要求 2 所述的方法，其中，所述风险评估包括：

所述特定端点设备尝试通过所述特定无线接入点与受信端点进行通信；并且

监控所尝试的通过所述特定无线接入点与所述受信端点的通信以便评估与所述特定无线接入相关联的风险。

8. 如权利要求 7 所述的方法，其中，尝试与所述受信端点进行通信包括尝试在所述特定端点设备和所述受信端点之间建立安全连接，并且建立所述安全连接包括从所述受信端点接收期望的信任验证数据；

其中，除了所述期望的信任验证数据以外的数据的接收被认为指示所述特定无线接入点是不可信的，表明与所述特定无线接入点相关联的较高风险。

9. 如权利要求 8 所述的方法，其中，参与所述特定无线接入点的所述风险评估包括，在所述特定端点设备尝试通过所述特定无线接入点与所述受信端点进行通信之前，促成所述期望的信任验证数据到所述特定端点设备的传送。

10. 如权利要求 7 所述的方法，其中，参与所述特定无线接入点的所述风险评估包括，在所述特定端点设备尝试通过所述特定无线接入点与所述受信端点进行通信之前，对于所述特定端点设备，从多个可用的受信端点设备中识别所述受信端点设备。

11. 如权利要求 1 所述的方法，其中，结合由端点设备与所述特定无线接入点的至少一个先前遇见来生成针对所识别的特定无线接入点的预存在的风险评估数据。

12. 如权利要求 11 所述的方法，其中，与所述特定无线接入点的所述先前遇见由除了所述特定端点设备以外的端点设备完成。

13. 如权利要求 1 所述的方法，其中，从包括针对由无线使能的端点设备识别的多个无线接入点的预存在的风险评估数据的风险评估记录中识别针对所识别的特定无线接入点的所述预存在的风险评估数据。

14. 如权利要求 1 所述的方法，其中，所述查询包括指示所述特定端点设备和所述特定无线接入点中的至少一个的位置的地理位置数据。

15. 如权利要求 14 所述的方法，进一步包括至少部分地以针对所识别的特定无线接入点的所述预存在的风险评估数据以及在所述地理位置数据中识别的位置为基础来生成所述查询结果数据。

16. 如权利要求 1 所述的方法，进一步包括以包括与由所述特定端点设备接入的无线接入点相关联的风险的一组设备属性为基础来计算针对所述特定端点设备的风险概要。

17. 如权利要求 1 所述的方法，进一步包括使与所述特定无线接入点相关联的风险的图形指示符呈现在所述特定端点设备处。

18. 如权利要求 1 所述的方法，其中，通过除了与所述特定无线接入点相关联的无线网络以外的安全连接发送所述查询。

19. 如权利要求 18 所述的方法，其中，所述安全连接通过无线移动宽带连接和 VLAN 隧道中的至少一个实现。

20. 编码在非暂态介质中的逻辑，包括用于执行的代码并且当由处理器执行时操作为执行包括下列方面的操作：

从特定端点设备接收识别由所述特定端点设备遇见的特定无线接入点的查询；

识别针对所识别的特定无线接入点的预存在的风险评估数据；以及

向所述特定端点设备发送以与所述特定无线接入点相关联的预评估的风险为特征的查询结果数据。

21. 一种系统，包括：

至少一个处理器设备；

至少一个存储器元件；以及

无线接入点风险评估器，当由所述至少一个处理器设备执行时，所述无线接入点风险评估器适于：

从特定端点设备接收识别由所述特定端点设备遇见的特定无线接入点的查询；

识别针对所识别的特定无线接入点的预存在的风险评估数据；并且

向所述特定端点设备发送以与所述特定无线接入点相关联的预评估的风险为特征的查询结果数据。

22. 如权利要求 21 所述的系统，进一步包括设备风险评估工具，所述设备风险评估工具适于以包括与由所述特定端点设备接入的无线接入点相关联的风险的一组设备属性为基础来计算针对所述特定端点设备的风险概要。

移动风险评估

[0001] 本专利申请按照U.S.C.§120要求享有2011年10月17日递交的发明名称为“MOBILE RISK ASSESSMENT”的美国临时专利申请序列号61/548,194以及2011年10月18日递交的发明名称为“MOBILE RISK ASSESSMENT”的美国临时专利申请序列号61/548,224的优先权,这里以引用的方式分别将其整体并入。

技术领域

[0002] 本公开通常涉及计算机安全的领域,并且更加具体地涉及移动计算设备的安全。

背景技术

[0003] 互联网已经实现了使全世界范围内不同计算机网络的互连。然而,有效地保护和维持稳定的计算机和系统的能力,为组件制造商、系统设计者及网络运营商提出了巨大阻碍。由于恶意软件作者所采用的系列手段的不断进步,这一阻碍变得更加复杂。此外,随着移动计算设备的迅速增长和普及,计算环境本身也在发展,所述移动计算设备包括能够使用无线或移动通信网络连接到互联网的智能电话、平板电脑、膝上型电脑,该无线或移动通信网络采用诸如WiFi、WiMAX、3G、4G、CDMA、GSM、LTE等等的技术。随着移动或无线使能的计算设备的数量的激增,计算机安全提供方正尝试开发程序和工具用于管理这些设备上的安全并且使计算机安全服务适应新发展的移动计算设备所具有的安全问题,包括基于网络的威胁、移动操作系统和移动应用特有的漏洞等等。此外,移动计算设备的快速部署已经引入了连接无线或移动网络的新一代用户,在一些情况下,引入了该部分设备用户的较低安全意识。

附图说明

[0004] 图1是根据一个实施例包括一个或多个移动计算设备的示例通信系统的简化示意图;

[0005] 图2是根据一个实施例包括示例移动风险评估引擎的示例系统的简化框图;

[0006] 图3是受危害的无线接入点的示例使用的表示;

[0007] 图4A-4D说明了根据至少一些实施例评估无线接入点的示例;

[0008] 图5是根据至少一些实施例的多个无线接入点的评估的示意性表示;

[0009] 图6是根据至少一些实施例的示例用户界面的至少局部截屏的说明;

[0010] 图7A-7B是说明与所述系统的至少一些实施例相关联的示例操作的简化流程图;

[0011] 在各幅图中相似的附图标记和名称指示相似的元素。

具体实施方式

[0012] 概述

[0013] 通常,本说明书中描述的主题的一个方面可以体现在包括一些行为的方法中,这些行为包括从特定端点设备接收识别由该特定端点设备遇见的特定无线接入点的查询,识

别针对所识别的特定无线接入点的预存在的风险评估数据，并且向所述特定端点设备发送以与所述特定无线接入点相关联的预评估的风险为特征的查询结果数据。

[0014] 进而，在另一通常的方面，可以提供一种系统，该系统包括至少一个处理器设备、至少一个存储器元件以及无线接入点风险评估器。当由所述处理器执行时，所述无线接入点风险评估器能够从特定端点设备接收识别由所述特定端点设备遇见的特定无线接入点的查询，识别针对所识别的特定无线接入点的预存在的风险评估数据，并且向所述特定端点设备发送以与所述特定无线接入点相关联的预评估的风险为特征的查询结果数据。在一些实例中，所述系统也可以包括适于以包括与由该特定端点设备接入的无线接入点相关联的风险的一系列设备属性为基础来计算针对该特定端点设备的风险概要的设备风险评估工具。

[0015] 这些和其它实施例能够分别可选地包括下列特征中的一个或多个。特定无线接入点的风险评估可以利用特定端点设备完成。可以结合由该特定端点设备执行的至少一个评估任务来从该端点设备接收风险评估反馈数据。所接收的风险评估反馈数据可以用于确定针对该特定无线接入点的风险概要。在确定风险概要时可以考虑与该特定无线接入点相关联的预评估风险。所述反馈数据可以包括服务集标识符 (SSID)、描述由无线接入点使用的加密的数据、醒目页面信息和无线接入点密码信息中的至少一个。所述风险评估可以包括特定端点设备尝试通过特定无线接入点与受信端点进行通信并且监控所尝试的通过特定无线接入点与受信端点的通信以便评估与特定无线接入相关联的风险。尝试与受信端点进行通信可以包括尝试在特定端点设备和受信端点之间建立安全连接，并且建立所述安全连接可以包括从该受信端点接收期望的信任验证数据。可以假设除了期望的信任认证数据以外的数据的接收指示该特定无线接入点是不可信的，表明与该特定无线接入点相关联的较高风险。参与特定无线接入点的风险评估可以包括：在特定端点设备尝试通过该特定无线接入点与受信端点进行通信之前，促成期望的信任验证数据到该特定端点设备的传送。参与特定无线接入点的风险评估可以包括：在特定端点设备尝试通过该特定无线接入点与受信端点进行通信之前，对于该特定端点设备，从多个可用的受信端点设备中识别该受信端点设备。

[0016] 进而，实施例可以分别可选地包括下列特征中的一个或多个。可以结合端点设备与特定无线接入点的至少一个先前遇见来生成针对所识别的特定无线接入点的预存在的风险评估数据。与特定无线接入点的先前遇见可以例如由除了该特定端点设备以外的端点设备实现。针对所识别的特定无线接入点的预存在的风险评估数据可以根据风险评估记录进行识别，所述风险评估记录包括针对由无线使能的端点设备识别的多个无线接入点的风险评估数据。所述查询可以包括指示特定端点设备和特定无线接入点中的至少一个的位置的地理位置数据。所述查询结果数据可以至少部分地以针对所识别的特定无线接入点的预存在的风险评估数据和在地理位置数据中识别的位置为基础来生成。可以基于一组设备属性来计算针对特定端点设备的风险概要，所述风险概要包括与由特定端点设备接入的无线接入点相关联的风险。可以使与特定无线接入点相关联的风险的图形指示符呈现在特定端点设备处。可以通过除了与特定无线接入点相关联的无线网络以外的安全连接来发送查询。所述安全连接可以通过无线移动宽带连接和 VLAN 隧道中的至少一个实现。

[0017] 所述特征中的一些或者全部可以是计算机实现的方法或者进一步包括在用于执

行这一所描述的功能的各自的系统或其它设备中。在附图和下文的描述中阐述了本公开的这些和其它特征、方面和实现的细节。根据说明书和附图并且根据权利要求书，本公开的其它特征、目标及优点将是显而易见的。

[0018] 示例实施例

[0019] 图 1 是说明计算系统 100 的示例实现的简化框图，该系统 100 包括能够接入一个或多个核心网络（例如，125）、至少部分为有线的网络、互联网等等，的多个端点计算设备（例如，105、110、115、120），包括机器（例如，网页服务器 130、135）和核心网络 125 中的托管资源。例如，端点计算设备可以通过一个或多个无线接入网络（例如，无线接入网络 140a、140b、140c、140d、145）来接入核心网络 125，包括使用各种无线网络技术和协议的网络，该无线网络技术和协议包括 WiFi 网络、移动宽带网络（包括 GSM、CDMA、3G、4G、LTE 等等）、WiMAX 网络、蓝牙等等。在一些实例中，端点设备 105、110、115、120 能够在多种不同的无线通信环境中进行通信。例如，端点设备可以适于在移动宽带网络和 WiFi 网络中进行通信。

[0020] 在该示例计算系统 100 中，端点计算设备 105、110、115、120 能够通过无线接入网络（例如，140a、140b、140c、140d），使用能够促成通过相对应的无线接入网络（例如，140a、140b、140c、140d、145）到核心网络 120 的接入的特定无线接入点（如 150、155、160、165）来接入核心网络 125。无线接入点可以包括适于通过无线电信号与一个或多个端点设备进行无线通信并且将端点设备连接到有线网络连接、路由器或其它网络元件或网络的一个或多个设备。无线接入点 150、155、160、165 本身可以包括无线路由器、通用中继器、WiFi 阵列、无线桥、无线以太网适配器、移动接入点等等。

[0021] 随着在用户家中、部署地点、学校、零售店、餐馆、咖啡厅、机场、社区等等中无线使能的端点设备的激增以及无线接入点的类似扩展，正在引入新的计算机安全威胁和漏洞。在计算系统 100 的一些实现中，还提供移动安全工具 170 以便辅助促成无线使能的端点设备的安全。移动安全工具 170 可以包括一个或多个计算设备和软件模块，包括使用经过移动安全工具 170 提供的安全功能和服务的远离端点设备或和 / 或在该端点设备附近的设备和软件。在一些实例中，移动安全工具 170 可以通过包括无线网络的网络连接与端点设备进行通信。在一些实例中，这样的连接可以被加密或者以其它方式被保护并且允许移动安全工具 170 将安全信息和服务上传、发送、推送或以其它方式传送到客户端端点设备。在一些实例中，移动安全工具 170 可以与客户端端点设备进行交互并且接收包括安全请求、设备属性数据、威胁数据、反馈数据以及移动安全工具 170 能够使用的其它信息的数据，并且结合经过移动安全工具 170 提供到无线使能的计算设备（例如，105、110、115、120）的安全服务和功能而做出响应。

[0022] 通常，“服务器”、“客户端”以及包括用于实现移动安全工具 170 的设备的“计算设备”，可以包括可操作用于接收、传输、处理、存储或管理与软件系统 100 相关联的数据和信息的电子计算设备。如在本文档中使用的，术语“计算机”、“计算设备”、“处理器”或“处理设备”意在包含任何合适的处理设备。例如，系统 100 可以使用除了包括服务器池的服务器的计算机实现。进而，该计算设备的任意一个、所有或者一些可以适于执行包括 Linux、UNIX、Windows Server 等等的任何操作系统以及适于虚拟化包括定制和专有操作系统的特定操作系统的执行的虚拟机。

[0023] 服务器、客户端和计算设备（例如，105、110、115、120、150、155、160、165、170）可以分别包括一个或多个处理器、计算机可读存储器以及一个或多个接口的其它特征和硬件。服务器可以包括任何合适的软件组件或模块，或者能够托管和/或服务软件应用或服务（例如，移动安全工具 170 的服务）的计算设备，包括分布式的、基于企业的或基于云的软件应用。例如，服务器可以配置为托管、服务或以其它方式管理诸如基于 SOA 的服务或者企业网络服务的网络服务或应用，或者与其它企业服务接口、协调或者取决于该其它企业服务的包括集中于安全的应用的应用。在一些实例中，服务器、系统、子系统或计算设备，包括移动安全工具 170，可以实现为服务器的某种组合，该组合能够被托管在公共计算系统、服务器、服务器池或云计算环境上并且共享包括共享存储器、处理器和接口的计算资源。

[0024] 端点设备 105、110、115、120 可以包括台式机、膝上型电脑和平板计算设备以及诸如智能电话、个人数字助理、视频游戏控制台、互联网使能的电视机和能够通过一个或多个无线技术和协议无线地连接到至少部分为有线的网络的其它设备的其它计算设备。端点设备 105、110、115、120 的属性在不同设备之间变化很大，包括操作系统和加载的、安装的、执行的、操作的或对于设备可访问的软件程序的集合。设备的程序集可以包括操作系统、应用、插件、小应用程序、虚拟机、机器图像、驱动器、可执行文件以及能够由各自的设备（例如，105、110、115、120）运行、执行或以其它方式使用的其它基于软件的程序。其它设备属性也可以包括连接到设备或者对于设备可访问的外围设备，以及设备适于的网络技术的类型。

[0025] 每一个端点设备可以包括至少一个图形显示设备和用户界面，允许用户浏览系统 100 中提供的应用和其它程序的图形用户界面并且与之进行交互。通常，端点设备可以包括可操用于接收、传输、处理和存储与图 1 的软件环境相关联的任何合适数据的任何电子计算设备。可以理解，可以存在与系统 100 相关联的任意数量的端点设备以及位于系统 100 外部的任意数量的端点设备。进而，不偏离本公开的范围的情况下，可以适当可互换地使用术语“客户端”、“端点设备”和“用户”。而且，尽管按照由一个用户使用来描述每一个端点设备，但是本公开预期许多用户可以使用一台计算机或者一个用户可以使用多台计算机。

[0026] 尽管将图 1 描述为包含多个元件或者与多个元件相关联，但是并不是在本公开的每一个可选实现中都会利用在图 1 的系统 100 内说明的所有元件。此外，本文描述的一个或多个元件可以位于系统 100 的外部，而在其它实例中，某些元件可以包括在其它描述的元件和在所说明的实现中没有描述的其它元件中的一个或多个内或者作为该其它描述的元件和没有描述的其它元件中的一个或多个的一部分。进而，图 1 中说明的某些元件可以与其它组件进行组合，并且用于除了本文描述的目的以外的可选或附加目的。

[0027] 转到图 2。图 2 示出了包括移动安全工具 205 的示例实现的示例系统的简化框图 200。在图 2 中，将移动安全工具 205 表示在计算环境内，该计算环境包括适于经由一个或多个无线接入网络 140、145 接入一个或多个至少部分为有线的网络 125 的至少一个移动端点设备 210，该至少部分为有线的网络 125 包括诸如互联网或 LAN 的核心网络，并且该至少一个移动端点设备 210 包括存在于网络 125 上的诸如网页服务器 215 的其它计算设备。

[0028] 无线使能的端点设备 210 可以包括一个或多个处理器 218 和存储器元件 220，用于执行存储的、下载的或对于设备 210 可访问的软件。在一些实例中，端点设备 210 可以进一步包括移动无线适配器 222、无线适配器 225、操作系统 228、各种程序、应用以及包括实现

客户端安全工具 230 的软件的其它软件。无线适配器 222 可以包括实现无线网络接口控制器的软件组件和硬件组件，所述无线网络接口控制器能够将端点设备 210 连接到一个或多个无线的、基于无线电的通信网络，例如基于 WiFi 的网络（例如，IEEE802.11）、蓝牙网络、WiMAX 网络等等。此外，在一些实现中，端点设备 210 可以进一步包括允许该端点设备连接到无线的基于无线电的移动宽带网络的移动无线适配器 225，所述网络例如使用蜂窝电话联网基础设施等等，包括采用 GSM、CDMA、3G、4G、LTE 及其它技术和协议的移动网络。适配器 222、225 可以包括用于向并且从接入网络 140 中的无线接入网络元件，特别是无线接入点（例如，232、234），发送和接收无线电信号的天线和其它硬件。

[0029] 移动安全工具 205 也可以包括一个或多个处理器设备 238 以及存储器元件 240。移动安全工具 205 可以包括适于计算无线使能的端点设备（例如，210）的风险的移动风险评估器 235，所述端点设备包括配置用于通过移动接入网络进行通信的端点设备。移动安全工具 205 可以结合有助于计算针对特定端点设备的暴露风险的一个或多个计算机风险评估任务的性能而与一个或多个无线使能的端点设备（例如，210）进行交互。例如，移动安全工具 235（例如，使用移动风险评估器 235）能够与客户端安全工具 230 进行交互以便协调端点设备 210 处的数据收集，用于由移动风险评估器 235 进行的评估。实际上，移动风险评估器 235 可以包括适于利用由移动风险评估器 235 提供的风险评估服务来识别端点设备 210 并且与之进行通信的设备协调器 255。在一些实例中，移动风险评估器 235 可以为多个或成组的无线使能的端点设备提供风险评估服务，例如，基于计算机风险评估服务的提供方与设备所有者、管理员、操作者、互联网或移动服务提供方、设备制造商和 / 或与特定无线使能的计算设备相关联的其它实体之间的协议或合同。

[0030] 移动风险评估器 235 可以基于各种因素或输入来计算暴露于特定端点设备的风险。实际上，可以针对特定端点计算不同类型的风险和风险情境，包括动态改变的风险。风险可以在无线端点设备 210 上动态地改变，特别是在给定它们的便携式属性下，当它们从一个物理的、网络或计算环境移动到另一个时。可以使用风险计算模块 260，例如用于计算包括暴露于特定端点设备的多种类型的风险的计算机风险。

[0031] 作为示例，可以从端点设备 210 收集数据，例如，经过描述设备 210 的属性的端点设备 210 的安全扫描，例如，使用客户端安全工具 230 的数据收集引擎 242 以及结合该设备使用的其它数据收集工具。例如，特定操作系统（例如，228），对应于操作系统 228 的补丁和更新，以及结合操作系统 228 操作的其它程序和应用（包括“移动应用”），可以连同与操作系统 228 和在端点设备 210 上执行、安装或访问的其它程序相关的信息一起被检测。这样的信息可以通过移动客户端设备 210 与移动安全工具 205 进行共享或通信，例如，通过至少部分为安全的网络连接，为移动风险评估器 235 提供用于在确定针对端点设备 210 的一个或多个风险概要时使用的数据。例如，继续当前示例，端点设备（例如，210）操作系统的属性可以被评估，例如安装在操作系统上的补丁或更新，例如，通过发现针对操作系统的更新和 / 或补丁的最新集，通过确定针对操作系统的理想版本或更新并且将这些与实际安装在端点设备上的进行比较，或者通过识别针对特定操作系统装置的已知漏洞，等等。在一些实例中，从端点设备 210 收集（通过数据收集引擎 242）的数据可以描述过期的、易受安全威胁攻击的或者以其它方式次优的并且将端点设备暴露于特定已知安全威胁的操作系统属性，定义针对端点设备的漏洞。

[0032] 取决于所识别的安全风险或漏洞的严重性和确定为使设备面对特定的所识别的属性（或漏洞）集的威胁的严重性，风险计算模块 260 能够确定针对端点设备 210 的风险概要。所述风险概要可以涉及端点设备的功能的特定子系统或类别，或者代表面向端点设备的合计风险。可以将这样的风险评估计算和结果的至少一部分传送到端点设备 210，并且可以由端点设备 210 或者在该端点设备上执行的程序（例如，客户端安全工具 230 的报告引擎 245）渲染，以便向具有补救面向设备的威胁和漏洞的任务的用户或管理员呈现并且传送风险评估得分、预测或其它结果。在一些示例中，可以将使用移动风险评估器 235 生成的风险评估结果传送到第三方设备，例如由具有管理针对特定设备或者设备的子集的安全和风险的任务的 IT 人员和其它管理员使用的管理员系统。

[0033] 客户端安全工具 230 和移动安全工具 205 可以相互作用并且协同地操作以便实现用于在评估端点设备 210 的风险时使用的一个或多个安全任务。这样的任务可以包括计算机风险和威胁的检测以及用于处理和减轻所检测的风险的对策的识别和发起。多个安全风险潜在地威胁无线使能的端点设备（例如，210），包括不安全的网络连接、恶意软件、病毒、未授权的接入、身份和数据窃取等等许多其它威胁。进而，面向无线使能的设备的一些安全风险对于在包括无线接入网络（例如，140、145）的无线网络环境中进行通信的设备可以是特定的。例如，随着 WiFi 热点以及其它无线接入网络的激增，作为不讲道德的用户进行传染、钓鱼或者以其它方式危害无线使能的端点设备的流行工具，流氓无线接入点已经出现，使这些端口设备足够不幸以便尝试通过流氓无线接入点接入诸如互联网的网络。

[0034] 在一些实现中，移动安全工具 205 的移动风险评估器 235 可以包括适于辅助识别和评估涉及无线接入点（例如，232、234）的风险的接入点风险管理器 265，所述无线接入点能够由一个或多个无线使能的端点设备（例如，210）接入。接入点风险管理器 265 可以包括提供用于评估特定无线接入点（例如，232、234）的风险的功能的一个或多个模块。例如，接入点风险管理器 265 可以包括查询引擎 275、接入点记录管理器 278、接入点评估模块 280、证书管理器 281、隧道化代理 282 等等的其它模块及其组合。在一些实现中，接入点风险管理器 265 能够与接入点协调器 250 进行交互并且协同地操作，该接入点协调器 250 例如包括有客户端安全工具 230。示例接入点协调器 250 可以在特定的无线使能的端点设备（例如，210）附近操作并且包括由诸如接入点监控器 270、接入点风险避免模块 272 等等的其它模块和实现的模块提供的功能。

[0035] 客户端安全工具 230 的接入点协调器 250 可以用于监控和收集关于特定端点设备与一个或多个无线接入点（例如，232、234）的交互的数据。例如，无线端点设备（例如，210）可以通过从相对应的无线接入点（例如，232、234）接收信号来检测特定无线接入网络（例如，140a-b）的可用性。在识别给定位置内的无线接入点时，接入点协调器 250 可以例如使用接入点监控器 270 与无线接入点进行通信，并且甚至尝试通过无线接入点连接到有线网络 125 上的服务器 215 以便收集与所发现的无线接入点相关的数据。接入点监控器 270 可以使从各种无线接入点（例如，232、234）收集的数据被转发到移动安全工具 205，用于例如由接入点风险管理器 265 进行处理和评估。

[0036] 接入点风险管理器 265 可以接收由在多个不同的无线使能的端点设备（例如，210）上操作的接入点协调器收集的描述多个不同的无线接入点（例如，232、234）的属性和行为的数据。根据从接入点协调器 250 接收到的数据（例如，由接入点监控器 270 收集），

接入点风险管理器 265 可以使用接入点记录管理器 278 来构建描述并记载由端点设备（例如，210）发现的无线接入点的属性的数据记录（例如，无线接入点（WAP）记录 288）。

[0037] 由接入点监控器 270 收集的数据可以描述特定无线接入点的属性或行为，所述属性或行为可以用作预测性地确定特定无线接入点是被危害的、有危险的或流氓接入点的基础，换言之，该接入点是操作为、看起来操作为或者对作为用于向端点设备执行恶意行为的机制的操作敏感的无线接入点。类似地，由接入点监控器 270 收集的记载与特定无线接入点的一个或多个遇见的数据也可以用于预测性地确定特定无线接入点是理应安全的、可靠的、合法的或以其它方式可信的接入点。

[0038] 在一些实例中，评估由一个或多个端点设备收集的数据以便确定特定无线接入点的风险概要可以在端点设备 210 本身处、在移动安全工具 205 处（例如，使用接入点评估模块 280）或者端点设备 210 和移动安全工具 205 的组合处执行。进而，针对特定无线接入点确定的风险概要不需要是二值的（即，危险或安全）。实际上，在一些实现中，取决于针对特定无线接入点收集的数据和所收集的数据的量（即，来自几个监控实例），以及所收集的数据的一致性，特定无线接入点的风险概要可以被更细致地分级或打分，例如，如从“确定性流氓”到“确定性安全”的连续变化。

[0039] 在一些实现中，客户端安全工具 230（使用接入点协调器 250）和移动风险评估器 235（使用接入点风险管理器 265）可以协调为执行与特定无线接入点的精心设计的交互以便收集来自特定无线接入点的数据并且评估该特定无线接入点的安全。例如，端点设备 210 可以使用无线适配器 222 来识别特定无线接入点。为了建立用于执行对无线接入点的检查的受控环境，客户端安全工具 230 可以与接入点风险管理器 265 协调（在一些情况中，是远程的）以便识别核心网络 125 上的受信服务器或端点。例如，受信服务器或端点可以例如是由移动安全工具 205 或移动安全工具 205 的操作者控制的设备，对于所述移动安全工具 205 或移动安全工具 205 的操作者，特定安全令牌、密钥、证书等等是已知的，以便识别不讲道德的行为者是否正在使用所测试的无线接入点来攻击或危害使用该无线接入点的端点设备，例如，使用中间人攻击。进而，证书、令牌、哈希函数、加密密钥等等可以被管理用于受信服务器，例如，使用证书管理器 281。

[0040] 在尝试通过处于测试中的特定无线接入点与受信服务器建立通信时，客户端安全工具 230（例如，使用接入点监控器）可以监控被测试的无线接入点的行为。客户端安全工具 230 可以向移动风险评估器 235 报告所收集的数据。在一些实例中，接入点监控器 270 可以包括用于识别特定无线接入点有可能是流氓或被危害的逻辑，并且接入点监控器 270 的评估可以被传送到移动安全工具 205 并且由其进行记录。在其它实例中，接入点风险管理器 265 可以使用由客户端安全工具 230 报告的数据以便访问（例如，使用接入点评估模块 280）被测试的无线接入点的安全或者确认安全工具 230 的评估。进而，在一些实例中，接入点风险管理器 265 可以使用从与特定的被测试的无线接入点的多个遇见报告的数据来实现无线接入点的安全的特定确定或评估。

[0041] 在一些示例实现中，移动安全工具 205 可以帮助保护参与特定无线接入点的监控或评估的移动客户端设备 210 以使其免受由流氓无线接入点造成的潜在威胁。除了协调用于估计无线接入点的受控环境（例如，使用受信服务器以便通过无线接入点建立初始通信），移动安全工具 205 也可以用于进一步帮助使移动客户端设备 210 与威胁隔离。例如，

如果确定特定无线接入点受到危害，则移动安全工具 205，例如使用隧道化代理 282，可以帮助在受危害的无线接入点上协调和建立安全 VPN 隧道，用于由端点设备 210 使用。经过使用 VPN 隧道，端点设备 210 在享受某一级别的安全的同时，仍然可以使用具有受危害的或流氓无线接入点的无线接入网络。此外，也可以建立 VPN 隧道用于由端点设备 210 使用用于在与移动安全工具 205 进行通信时使用。例如，流氓无线接入点将具有高的动机来阻止或改变在接入点上拦截的来自移动客户端设备的数据，所述移动客户端设备尝试向移动安全工具 205 传送接入点的流氓状态。因此，能够对这样的关于特定无线接入点（包括受信无线接入点）的状态和行为的数据的通信进行加密。例如使用 VPN 隧道，或者经过使用不同的无线接入网络，包括确定为比其它可用的无线接入网络更加安全的或受信的无线移动接入网络。

[0042] 除了促成安全通信信道，例如经过结合特定无线接入点的特定安全或者风险评估的用于由参与的端点设备使用的 VPN 连接的建立，移动安全工具 205 和移动客户端设备 210 也可以基于特定无线接入点的评估来使其它行为和功能变得合适。例如，在一些实现中，由移动安全工具 205 维持的记载与各种无线接入点（例如，232、234）的先前遇见的记录 288 可以用于执行特定无线接入点的预评估查询。作为说明性示例，端点设备 210 可以检测第一无线接入点 232 并且向移动安全工具 205 发送识别无线接入点 232 的数据，例如所检测的 SSID 或者针对无线接入点 232 的其它标识符，以及在一些情况中与无线接入点 232 和 / 或端点设备 210 的地理位置相对应的地理位置数据。根据识别无线接入点 232 的数据，接入点风险管理器 265 可以例如使用查询引擎 275 来执行 WAP 记录 288 的查询，以便确定先前收集的数据是否针对所识别的无线接入点 232 存在，以及先前收集的数据是否指示无线接入点 232 是否可能是可信的。然后，可以将查询的结果转发到端点设备 210。进而，基于该查询结果，端点设备可以执行相对应的动作，如，在不检查无线接入点 232 的情况下连接到无线接入点 232（例如，基于指示无线接入点 232 可能是可信的查询结果），尝试评估（例如，与上文所述的移动安全工具 205 进行协作和协调）无线接入点的安全（例如，当查询结果指示还没有针对无线接入点生成记录时或者当存在关于无线接入点 232 的可信性的一些问题时），阻碍端点设备 232 连接到无线接入点 232 的能力（当查询结果指示无线接入点最可能是流氓接入点时），以及其它示例。实际上，在一些实例中，移动安全工具 205 可以评估 WAP 记录 288 的查询结果并且向端点设备 210 发送关于端点设备 210 针对所检测的无线接入点 232 应该采取的动作的建议或指令。

[0043] 能够在给定设备的风险暴露或安全的更加通常的评估中考虑通过各种无线接入点的评估以及端点设备与特定无线接入点的交互所收集到的数据。例如，例如使用数据收集引擎 242 从端点设备 210 收集到的数据可以与移动安全工具 205 共享并且例如由该移动安全工具 205 维持在设备记录 290 中。可以在包括端点设备与特定的已知无线接入点的交互的其它设备专用数据中考虑从端点设备 210 收集到的描述设备属性的数据，以便作为整体生成设备的合计风险评估（例如，使用风险计算模块 260）。这样的数据可以例如经过由客户端安全工具 230 进行的设备的扫描进行收集。在一些实例中，客户端安全工具（以及移动安全工具 205）可以适于支持各种不同的移动操作环境，包括 RIM 黑莓 (QNX)、谷歌安卓、苹果 iOS、微软 Windows 电话、诺基亚塞班 OS 及其它。在一些示例中，客户端安全工具 230 可以实现为从受信站点下载或者经由应用商店发布的应用，例如安卓市场或 iTunes。客户

端安全工具 230（例如，使用数据收集引擎 242）能够扫描该设备。扫描可以包括密钥库的完整性检查、端点设备内并且基于无线接入点的声誉信息的文件 / 变化控制或受信代码执行、认证方法的弱化、安全连接协议、加密方法以及涉及设备风险或漏洞评估的其它安全任务。

[0044] 由客户端安全工具 230 收集的数据可以用于设备的风险评估中。这样的评估可以例如进一步确定特定端点设备（或者成组的端点设备）是否、哪里和 / 或如何处于危险状态。除了暴露于受危害的无线接入点，无线使能的设备的风险可以考虑许多其它源，包括网络威胁、操作系统专用（如 228）或应用专用的漏洞、弱数据加密、不安全连接、钓鱼网站等等。此外，在某些条件下针对具有某些属性的某些设备记录各种威胁和风险的设备记录 290 可以例如在其它端点设备、多端点系统、各类特定端点设备及其它示例的风险评估中由风险计算模块 260 使用。此外，特定端点设备的风险评估也可以包括存在于端点设备上或者对于该端点设备可用的可能对策的考虑和分解。在一些情况中，相关对策的存在可以在针对端点设备的风险评分的计算中使用。进而，与移动安全工具 205 协同操作的客户端安全工具 230 也可以用于补救在端点设备上检测到的其它威胁和漏洞，包括目标对策的引入、恶意软件的去除、软件更新以及其它工具和动作。

[0045] 转到图 3，显示了受危害的无线接入点 310 的示例恶意使用的框图 300。例如，说明了一种示例中间人攻击。示例端点设备 305 可以通过无线接入网络 308 与示例无线接入点 310 进行通信以便接入由核心网络 312 上的示例服务器 315 提供的资源和 / 或服务。在图 3 的特定示例中，端点设备 305 可以尝试参与与服务器 315 的事务，所述事务涉及在与服务器 315 已经建立了安全会话的帮助下，例如，使用安全套接层（SSL）保护，通过无线接入点 310 发送诸如信用卡信息的敏感数据。因而，端点设备 305 可以期望证书或来自服务器 315 的某一其它令牌以便建立安全会话。恶意的计算设备 320 可以控制或以其它方式使用无线接入点 310 以便窥探无线接入点 310 上的业务。实际上，恶意设备 320 可以拦截并且检测来自端点设备 305 的请求与服务器 315 的安全连接的请求 322。进而，恶意设备 320 不是发送从服务器 315 发送的证书 325，而是可以发送其自己的代理证书 330 并且通过与端点设备 305 建立安全会话来模仿服务器，诱使设备 305 的用户确信地通过该安全连接共享敏感的个人数据。恶意设备 320 可以拦截传输这样的数据的通信（例如，335）（并且在一些情况中，代理到服务器 315 的数据以便不引起设备 305 的用户的怀疑）并且偷窃包括在敏感数据 335 中的信息以便在其它潜在的不法行为中使用。

[0046] 图 4A-4D 说明了根据至少一些实施例评估无线接入点的示例。实际上，在图 4A-4D 的示例中描述的示例方案和技术可以用于缓解如在图 3 的示例中描述的示例攻击的攻击。在图 4A 中，显示了说明涉及端点设备 402、无线接入点 310、恶意设备 320、接入点监控器 420 和受信服务器设备 405 的示例通信的流程图 400a。端点设备 402，例如被预定、使用或者以其它方式适于消费由一个或多个安全工具提供的安全服务的端点设备 402，可以检测特定无线接入点 310 并且尝试使用无线接入点 310 以便评估无线接入点 310 的安全。端点设备与无线接入点 310 的交互可以例如与无线接入点 310 的任何其它典型的端点设备的使用类似地发展，例如，以便使无线接入点 310 或者结合该无线接入点 310 操作的设备（例如，320）不能够警觉到该无线接入点 310 的安全正在被分析和评估。例如，端点设备 402 可以向特定服务器，服务器 A405，发送请求，并且尝试与特定服务器 405 建立安全连接。

[0047] 结合无线接入点 310 的评估，端点设备 402 能够以服务器 A 作为受信装置的预识别为基础，在使用无线接入点 310 开始其它通信之前刻意地与服务器 A405 进行交互。此外，与受信服务器 A405 的交互可以被精心设计以便在至少稍微受控的环境下接入无线接入点 310 的风险。例如，将由受信服务器 A405 结合与端点设备 402 的安全连接的建立而发送的特定证书、令牌、加密密钥、数字签名、水印及其它数据，能够在端点设备 402 尝试发起与受信服务器 405 的安全会话之前，被预协商、预接入、兑现或以其它方式对于端点设备 402 已知。实际上，在一些实例中，受信服务器 405 可以在控制之下，或者甚至由与端点设备 402 相关联的移动安全工具（例如，图 2 中的 205）托管。

[0048] 因此，端点设备 402 可以发送请求以便通过无线接入点 310 与受信服务器 405 建立安全连接，在这种情况下，例如基于与受信服务器 405 的关系或者熟悉度而期望特定安全证书 410 将由受信服务器 405 返回。继续图 4A 的示例，期望的证书 410 可以被恶意设备 320 利用受危害的无线接入点 310 拦截，并且所述恶意设备 320 可以尝试使用其自己的证书 330 替代期望的证书 410 以便诱使端点设备 402 与恶意设备建立安全连接并且通过恶意设备 320（例如，如图 3 中的示例中）错误地路由安全业务。然而，在图 4A 中的示例中，端点设备 402 对证书 330 而非期望的证书 410 的接收可以提示该端点设备怀疑无线接入点 310 是流氓接入点或者已经以其它方式受到危害。因而，端点设备 402 可以向接入点风险管理器 265 报告它的发现 415，用于在对可能受危害的或流氓接入点的入侵编目录时使用。这样的报告或反馈数据可以通过诸如 VPN 隧道或者移动宽带连接的安全连接 425 传送到接入点风险管理器 265。在端点设备能够收集并且传送到接入点风险管理器 265 的报告和反馈数据当中，端点设备 402 可以传送无线接入点 310 的身份（例如，SSID 或其它标识符）、所提出的报告 415 的行为或特性的类型、在其附近检测到无线接入点 310 的地理位置、无线接入点是否使用加密以及使用了何种类型的加密、是否需要密码、在与接入点进行连接时是否生成和接收了醒目页面以及描述相关无线接入点的属性和行为的其它数据。

[0049] 转到图 4B 的示例，在一种实现中，在部分特定无线接入点 310 上的可疑的或不可信行为的发现，例如在图 4A 的示例中，可以引起制定对策以便保护受影响的端点设备并且抵抗由无线接入点 310 造成的威胁。例如，如上所述，确定特定无线接入点 310 是不可信的、流氓的或以其它方式受危害的可以触发对策，所述对策包括用于在通过特定受危害的无线接入点 310 的随后通信 435 中由端点设备使用的 VPN 隧道的建立 430。实际上，在一些实例中，能够至少部分地经过与受信服务器 405（和 / 或接入点风险管理器 265）的通信来建立 430 所述 VPN 隧道。通过受危害的无线接入点 310 的隧道化可以提供用于特定的情形中，例如，当在给定时间没有其它无线接入点对于特定端点设备 402 可用时。在其它实例中，可以提供其它对策，例如阻挡特定的受危害的无线接入点、禁用到被确定为具有较低可信度的无线接入点的自动连接或者到被确定为不太有危险的可选的无线接入点的自动连接。

[0050] 现在转到图 4C 的示例，在某些实例中，使用特定无线接入点时固有的风险可以被评估以便确定无线接入点可能是安全的、合法的或以其它方式可信的。采取措施之前，可能端点设备 402 不知道特定无线接入点针对可信性的声誉，并且由于它可能是任何其它情况，该端点可以接近无线接入点的评估。例如，端点设备可以尝试通过穿过与受信服务器 405 的安全连接的建立而评估无线接入点 438。这样的评估可以如图 4A 中的示例进行，然而，在这一示例中，期望的证书 410 被从受信服务器 405 返回到端点设备 402，向端点设备

402 表明无线接入点 435 潜在地不是流氓或受危害的接入点。实际上，与在图 4A 的示例中相同，在图 4C 的示例中的端点设备 402 可以向接入点风险管理器 265 报告它关于无线接入点 438 的发现，例如，用于由接入点风险管理器 265 在辅助对与特定无线接入点 438 的未来遇见的评估时使用（例如，在下面的图 5 的示例中更加详细描述的）。

[0051] 转到图 4D，在一些实现中，在可靠地确定特定无线接入点是安全的或可信的之前，可以确定，对于特定无线接入点的评估（例如，在图 4C 的示例中）返回单一的“清晰”结果是不充分的。例如，在图 4D 的示例中，更加复杂的无线接入点 460（结合无线接入点 460 或者恶意设备 465 的用户执行的恶意设备 465）可以预期一些端点设备将在发送恶意设备 465 实际上感兴趣捕获的“现场”数据之前尝试利用“测试”连接来评估无线接入点的可信性。这样的智能性可以由恶意设备 465（或者用户）收集，例如，基于关于这样的系统或者该系统的其它熟悉度的先前经验。因此，恶意设备 465 可以等待发起中间人或其它攻击，直到端点设备与无线接入点 460 的连接成熟。例如，恶意设备可以允许建立特定安全连接的一个或多个第一尝试以便在没有干扰的情况下进行，以诱使端点设备和 / 或接入点风险管理器假定无线接入点 460 是安全的。实际上，如在图 4D 的示例中所示，初始反馈数据 445 可以从端点设备 402 报告到接入点风险管理器 265，报告期望的证书 410 平安无事地从受信服务器 405 返回。

[0052] 继续图 4D 的示例，恶意设备 465 可以尝试钓鱼由端点设备 402 参与的其它安全通信，假定这样的尝试将不被监控。例如，代替返回服务器 B470 的合法证书 450，恶意设备 465 可以尝试模仿服务器 B470 并且用其自己的证书 330 替换证书 450。然而，这样的尝试也可以利用端点设备 402 和接入点风险管理器 265 进行处理。例如，端点设备（结合接入点风险管理器 265）可以在无线接入点 460 的端点 402 的使用期间进行无线接入点 460 的多个、周期性评估，而不是仅单次评估特定无线接入点 460 的可信性。例如，可以对端点设备通过网络 312 在现场（不涉及评估）事务中建立安全连接的尝试做出响应并且在该尝试之前发起新的风险评估。进而，在这些多个风险评估期间可以采用多个不同的受信服务器，以使得恶意设备 465 不识别与相同受信服务器的重复通信并且期望风险评估尝试。例如，服务器 B470 可以是由风险评估系统使用的受信服务器的第二实例。实际上，在一些实例中，风险评估系统可以使用技术以便动态且随机地循环所使用的特定受信服务器，动态地改变受信服务器的标识、地址或名称，开发与诸如电子商务平台的第三方服务器的受信关系，可以预期与该电子商务平台的现场事务，使用诸如由僵尸网络系统所使用的技术以便使受信服务器的身份不可预测，以及其它示例。因此，能够检测并且缓解恶意设备 465 通过受危害的无线接入点 460 对参与的端点设备 402 的干扰或发起对参与的端点设备 402 的攻击的延迟的尝试。进而，描述无线接入点 460 的这样的行为和特性的反馈数据 455 可以由接入点风险管理器 265 报告或维持。

[0053] 也可以使用如上所述的无线接入点评估技术内的其它技术。利用受危害的无线接入点的更加复杂的恶意设备可以利用其它技术来识别和预期并且躲避无线接入点风险评估。例如，恶意设备也可以跟踪和识别在结合风险评估的与受信服务器的精心设计的交换中使用的循环的证书或令牌。为了防止无线接入点评估的检测，在一些实现中，用于建立在端点设备 402 和受信服务器 405 之间交换的数据的连续认证的证书、令牌、签名等等的值或类型可以本身是动态改变的以便不具有重复值。例如，关于在特定无线接入点上风险评估

的发起，端点设备 402 可以协调（例如，利用接入点风险管理器 265）将在评估中使用的特定受信服务器的身份和地址以及应该被期望来自受信服务器的特定的期望证书（或其它令牌等）。按照这一方式，受信服务器的身份和证书的本质可以不断地改变以便隐藏其在特定无线接入点的风险评估中的参与。与远程接入点风险管理器 265 或其它协调工具的这样的协调可以例如通过不涉及将要被评估的无线接入点的连接而发生。例如，特定无线接入点的风险评估的协调可以在无线宽带信道或其它安全连接上完成。进而，尽管特定无线接入点的端点的评估可以是不具有直接移动宽带或其它连接性的端点的结果，但是可以提前协调风险评估的协调，例如，当这样的可选接入网络可用时。进而，在一些实现中，在这样的协调是不可能的情况下（例如，由于到安全信道的连接，或者在预协调的受信服务器处的故障），基于不能够可靠地评估无线接入网络的可信性的确定，可以自动地拒绝到特定无线接入网络的接入。

[0054] 尽管图 3、4A-4D 的示例集中于中间人类型的攻击并且基于不期望的证书、令牌或其它数据的接收来识别流氓接入点，但是可以意识到，这些示例是非限制性示例，在一些情况中，提供这些示例用于说明更加通常的原理。例如，除了基于不期望的证书的接收来评估无线接入点风险，可以基于在通过无线接入点的通信中识别的不一致性，例如不期望的加密类型、不期望的醒目页面数据、不期望的密码要求及其它示例，来识别特定无线接入点的风险性。进而，也可以考虑用于评估无线接入点的风险性的数据集在精确度或完整性方面的置信度。例如，如果描述无线接入点的数据集本身是不完整的，或者风险评估的结果是非决定性的，则评估的可靠性可能具有很小的置信度，并且可以抑制可用于减轻与无线接入点相关联的风险的行为。

[0055] 转到图 5，示出了说明示例移动安全工具 510 与一个或多个无线使能的端点计算设备 505 的示例交互的框图 500，该端点计算设备 505 用于评估一个或多个无线接入点 515、520 处的风险。一个或多个无线接入点（例如，515）可以是流氓无线接入点 515，例如，由恶意设备（如 535）用于钓鱼或窥探通过无线接入点发送的数据。

[0056] 在一个示例中，无线使能的端点设备 505 可以在特定位置内识别多个无线接入点并且发起对每一个的风险评估。例如，端点设备 505 可以首先评估无线接入点 515 并且通过向移动安全工具 510 发送识别第一无线接入点 515 的数据来开始该评估。数据可以包括标识符数据，例如，无线接入点 515 的 SSID 以及其它信息。例如，在一些实现中，SSID 可以跨越多个无线接入点被再利用，例如分配到即装即用的无线接入点的默认或通用的 SSID。此外，在一些无线接入点中，SSID 可以改变，并且可选的识别数据可以用于识别无线接入点。作为示例，其它标识符数据以及描述无线接入点的属性的数据可以被识别并且包括在发送到移动安全工具 510 的数据中，例如与无线接入点的位置相对应的地理位置数据、无线接入点被接入的一天的时间、由无线接入点使用的醒目页面数据、由无线接入点使用的签名或握手协议、由无线接入点使用的加密方法等等。除了或者代替上述数据，也可以使用多种其它数据，以便识别特定无线接入点，例如包括接入点的通信信道、BSSID、供应商、支持的数据率、类型（例如，管理的、未管理的等等）、密钥等等。

[0057] 移动安全工具 510 可以使用来自由端点设备 505 提供的数据的第一无线接入点 515 的识别，以便执行针对大量无线接入点评估记录 288 和 / 或其它数据（例如，存储在一个或多个存储器元件或数据结构（例如，285）中，例如数据库、数据对象和文件系统等等）

的查询 540，以利用端点设备 505 或者某一其它端点设备来识别第一无线接入点 515 在之前是否已经被评估，以及风险评估的结果是什么。查询结果 545 可以返回到端点设备 505，例如，通过安全连接或通信信道，包括通过无线移动宽带网络 145 的通信，以便在端点设备 505 连接到无线接入点 515 之前向端点设备 505 提供关于无线接入点 515 的智能。查询结果 545 可以识别在无线接入点 515 的先前风险评估中收集的数据，这允许端点设备处理该数据并且确定无线接入点 515 的风险性。在其它示例中，移动安全工具 510 可以结合 WAP 记录 288 的查询来确定或识别无线接入点 515 的风险得分或初步风险评估，并且向端点设备 505 提供该初步风险评估。

[0058] 此外，由端点设备识别的每一个无线接入点（例如，515、520）可以被识别并传送到移动安全工具，以便触发 WAP 记录 288 的各自查询 540。例如，除了发送关于与无线接入点 515 的遇见的数据 538，端点设备 505 也可以发送识别无线接入点 520 的数据 538。因此，可以针对由端点设备 505 检测并且对于该端点设备 505 可用的多个不同的无线接入点（例如，515、520）返回查询结果 545。在一些实例中，查询数据 545 可以用于识别所遇见的无线接入点 505 的相对安全或可信性。在一些实例中，查询数据 545 本身可以通信这样的信息，例如经过包括针对无线接入点 505 识别的风险得分或风险概要。在一些实例中，在遇见（并且评估）无线接入点时，这样的风险概要（以及查询结果 545 本身）可以基于由各种端点设备向移动安全工具提供的潜在地成百上千的评估数据点。

[0059] 在接收到来自移动安全工具 510 的初步风险评估数据或其它查询结果 545 时，端点设备可以继续进行所遇见的无线接入点 515、520 的评估，在一些情况中，与移动安全工具 510、一个或多个受信服务器 405 以及其它组件协作。在一些实现中，所执行的风险评估的类型和范围将至少部分地基于针对无线接入点 515、520 返回的查询数据 545。也可以考虑其它原因和属性，例如，无线接入点 515、520 的识别位置。例如，如果与端点设备和 / 或所遇见的无线接入点的位置相对应的地理位置数据指示无线接入点正在公开的空间或位置中操作，该公开的空间或位置之前被识别为包含一个或多个恶意的或受危害的无线接入点，则可以仍然在每一个所检测的无线接入点 515、520 上执行大量的风险评估，即使一个或多个所检测的无线接入点 515、520 的查询结果 545 指示无线接入点的特定可信性。

[0060] 在一些实例中，指示无线接入点的特定可信性或安全的查询结果 545 可以导致较少量的对无线接入点的安全评估检查，例如以便确认可信的无线接入点（例如，520）的先前所识别的属性，或者完全地跳过风险评估。在关于无线接入点的可信性存在某种不确定性的实例中，例如基于指示相冲突的行为或者关于无线接入点的记录 288 的不足（或者完全缺乏）的查询结果 545。此外，如果查询结果 545 指示特定无线接入点（例如，515）被相信是受危害的，例如基于对无线接入点 515 的多个评估，则到无线接入点的连接可能被全部拒绝，或者可以执行其它评估，例如以便收集关于无线接入点 515 的附加的数据点并且进一步确认（或者可能质疑）无线接入点 515 的初步风险评估。

[0061] 在经过与所遇见的无线接入点 515、520 的交互而完成风险评估任务 525、530 时，端点设备 505 可以向移动安全工具 510 发送反馈数据（例如，如图 4A-4D 的示例中的反馈数据 415、440、445、455），传送从风险评估任务收集到的数据和结果。转而，移动安全工具 510 可以使用由端点设备 505 报告的最新反馈数据来增补其记录（例如 288）。实际上，在一些实例中，由端点设备 505 报告的由风险评估任务 525、530 产生的反馈数据可以改变涉

及所评估的无线接入点 515、520 的未来查询的结果。例如，无线接入点 515 可能基于之前的 WAP 记录 288 已经被识别为是潜在可信的，但是无线接入点 515 的最近风险评估（例如，结合端点设备 505 的遇见和评估）可能已经识别了产生被添加到 WAP 的属性或行为（例如所尝试的中间人攻击），作为妥协，所述反馈数据用作用于无线接入点 515 的随后预评估的基础。

[0062] 在一个说明性示例中，用户可以使用移动智能电话来尝试连接到机场或另一公共场所内的 WiFi 网络。可以检测到多个可用 WiFi 网络（或者接入点）并且显示给用户。在一些实例中，流氓移动接入点可以通过采取表明合法性的名字来引诱不怀疑的用户使用它们的连接。例如，在达拉斯、德克萨斯沃斯堡机场，流氓无线接入点可以采取名称“DFW WiFi”，以便（错误地）向潜在的用户表明该接入点由机场的官方人员或其它合法源维持。实际上在一些实例中，流氓无线接入点可以采取（例如，伪造）官方接入点或热点的精确名称，以便使用户通过实际的、发起的接入点选择（有时盲目地）流氓接入点。在流氓接入点检测和 / 或其它接入点风险评估功能对于端点设备可用的实例中，例如在一些先前描述的示例中，可以根据上述原理来评估由端点设备遇见的无线接入点的可信性。实际上，在其中两个不同的接入点呈现有相同 SSID 的示例中，可以确定存在该两个无线接入点中的一个是流氓的并且正在尝试模拟另一个的高可能性，产生无线接入点的更加勤奋的风险评估以及报告至少一个流氓接入点在检测到无线接入点的特定位置（例如，机场）处可能存在的反馈数据。实际上，对特定位置处流氓接入点的先前识别可以导致在该位置处（例如，如从 GPS 或端点设备的其它地理位置数据识别的）检测到的无线接入点的加强的监视。然而，在一些实例中，确定在不同距离处接入点的变化可信性也可以或代替地被确定为很差地反映针对特定接入点的风险评估的置信度。风险评估的精确性的低置信度也引起对接入点的肯定评估的怀疑，在一些实例中，低置信度促成了应该避免到无线接入点的连接的总体指示（即，因为在之前被评估为不可信之后，接入点现在是可信性的这种评估，引起对当前评估的可靠性的怀疑）。

[0063] 对现有的无线接入点评估记录的预评估查询和 / 或在特定位置内所检测的无线接入点的评估做出响应，可以向端点设备的用户呈现（例如，经过端点设备的显示实体）用户界面，该用户界面识别在某一位置中可用的无线接入点，以及所检测的无线接入点的相对安全或可信性，连同在对每一个所检测的无线接入点的评估中相对置信度的测度。用户可以例如使用这一信息，以便评估使用特定无线接入点的风险。例如，用户可能仅遇见单个可用的无线接入点，或者用户能够连接到的单个无线接入点（例如，因为用户不具有对于其它所检测的无线接入点的预订或密码），但是可以考虑通过未知的接入网络进行连接。

[0064] 为了帮助用户理解用户设备（并且通过关联性，用户自身）面临的风险，可以利用端点设备向用户呈现用户界面，例如图 6 中所示的示例图形用户界面 (GUI)605 的屏幕截图 600。例如，GUI605 可以包括由端点设备在给定时间和位置处检测到的可用无线网络（或接入点）610a-d 的列表。进而，可以在列表中呈现无线接入网络的名称以及无线接入网络的其它属性，包括无线接入点（例如，在 615a-d 处）的信号强度以及该接入点是否被保护或者需要密码等等（例如，在 620a-d 处）。此外，一个或多个状态指示符（例如，如 625a-d 的颜色编码的状态指示符）可以呈现在 GUI605 中以便指示在无线接入点的评估中所确定的可信性和 / 或置信度。

[0065] 如上面解释的，所确定的无线接入点的可信性，包括其显示的状态指示符 625a-d，可以根据在无线接入点上执行的风险评估的合计（例如，根据无线接入点评估记录的查询识别）和 / 或结合由每一个无线接入点的端点设备执行的风险评估（例如，如图 4A-4D 中的示例所示）来确定。在图 6 的示例中，状态指示符 625a-d 可以是颜色编码的，例如，采取交通灯模式，绿色指示符（例如，625a）表明特定无线接入点（例如，610a）是可信的，黄色指示符（例如，625c）表明无线接入点（例如，610c）的可信性正在讨论中（例如，610c 因为在无线接入点上执行了太少的、矛盾的评估或者没有执行评估），或者红色指示符（例如，625b、625d）表明无线接入点的可信性不可接受地低或存在质疑。确定将三个颜色编码的状态指示符中的哪一个分配给无线接入点可以基于针对无线接入点的风险评估得分超过一个或多个阈值。

[0066] 在一些实例中，无线接入得分的风险评估得分可以根据多个因素进行调整并且取决于特定因素的存在而改变。例如，在图 6 的示例中，可以检测到被称为“freenet_wifi”的第一无线接入点 625b，并且基于先前风险评估，通常被确定为具有低风险或高可信度得分（例如，通常向该无线接入点 625b 提供相对应的绿色状态指示符）。然而，在图 6 的示例中，也提供同样被称为 freenet_wifi”的第二无线接入点 625d。在这样的实例中，并且在一些实现中，两个具有相同名称的无线接入点的存在能够表明一种高可能性，即具有类似名称的无线接入点中的一个是尝试模仿已建立的受信无线接入点的流氓接入点。在一些实例中，流氓无线接入点（例如，625d）可能做了模拟另一无线接入点的足够好的工作，对于流氓接入点评估技术来说难于区分这两个接入点的身份。因此，假定可以存在具有类似名称的接入点是流氓的百分之五十的机会，则红色状态指示符 625b、625d 可以被分配给每一个无线接入点。

[0067] 其它示例和实现以及场景能够落入本文公开的主题的范围内。作为一个实例，并且继续图 6 的示例，显示给端点设备的用户的 GUI605 可以自动排序 GUI605 内无线接入点的列表，以便向用户表明哪一个无线接入点是最期望使用的。这样的列表可以例如基于哪一个无线接入点具有最高可信的信誉或风险评估得分。在排序列 GUI605 中的无线接入点时，除了风险评估得分，也可以考虑其它因素。例如，在排序所呈现的列表中的无线接入点时可以考虑信号强度、所使用的加密协议及其它属性，等其它示例。也可以生成使用无线接入点评估数据的其它 GUI，包括显示存在于给定端点设备上的合计风险的特性的 GUI。这样的基于设备的风险评估及附属的 GUI，可以包括对暴露于设备的无线接入点风险的考虑。

[0068] 图 7a 是说明用于监控由无线使能的端点设备遇见的无线接入点的示例技术的简化流程图 700a。至少一个可用无线接入点可以在特定位置中由端点设备识别 705。在一些实例中，在该位置处可以将多个无线接入点识别为可用。可以使用由端点设备识别的无线接入点来建立 710 连接，以便促成尝试 715 通过无线接入点与受信端点设备进行通信。可以出于创建用于评估与所识别的无线接入点的使用相关联的风险的至少一些受控环境的目的来建立与受信端点的通信。实际上，可以至少部分地通过端点设备来监控 720 与受信端点的所尝试的通信 715，以便促成所识别的无线接入点的风险评估 725。在一些实例中，促成风险评估 725 可以包括执行在监控 720 期间返回的数据的至少部分分析，或者通过向一个或多个后端工具发送在监控 720 期间所收集的数据，用于分析和风险评估，如在上述示例中描述的。

[0069] 图 7B 是说明用于预评估与所识别的无线接入点相关联的风险的示例技术的简化流程图 700b。可以从无线使能的端点设备接收 730 查询，所述无线使能的端点设备识别由该无线使能的端点遇见的至少一个无线接入点。在一些实例中，可以在端点设备尝试连接到无线接入点之前并且结合评估所识别的无线接入点是否安全以便进行连接的尝试来接收 730 所述查询。对接收 730 所述查询做出响应，可以识别 735 先前收集的或生成的与所识别的无线接入点相对应的风险评估数据。在一些实例中，这样的风险评估数据可以是通过对无线接入点多个不同的风险评估积累的数据的集合，例如，结合多个不同的端点设备的遇见。在其它示例中，可以识别 735 不存在关于所识别的无线接入点的风险评估数据（例如，因为还没有完成先前的风险评估或者 WAP 识别算法失败或具有低置信度等等）。在任何情况下，对查询做出响应，可以将查询结果数据发送 740 到端点设备，所述结果数据以与特定无线接入点相关联的预评估风险为特征。这样的查询结果数据可以包括所识别的先前风险评估数据本身，以先前风险评估数据的分析、总结或评估为特征的数据，并且甚至可以包括用于与所识别的无线接入点进行交互的指令（即，基于与无线接入点相关联的预评估的风险，根据所识别的先前风险评估数据确定）。端点设备然后可以结合与无线接入点的交互来使用这一查询结果数据，包括利用与在图 7A 的示例中和本说明书的其它部分中描述的那些技术类似的技术来监控无线接入点。

[0070] 尽管利用某些实现和通常相关联的方法描述了本发明，但是这些实现和方法的修改和变换对于本领域的技术人员来说是显而易见的。例如，本文描述的行为可以按照与所描述的顺序不同的顺序执行，并且仍然能够实现期望的效果。作为一个示例，在附图中阐释的处理不必要求所示的特定顺序或顺次顺序来实现期望的效果。在某些实现中，多任务和并行处理可能是有利的。此外，可以支持多种用户界面布局和功能。此外，尽管上面的描述集中于将上述原理应用于定制白名单的生成，但是类似的原理可以应用于生成在安全任务中使用的其它这样的名单，包括调整的黑名单。其它变形包括在下列权利要求的范围内。

[0071] 本说明书中描述的主题和操作的实施例可以在数字电子电路或计算机软件、固件或硬件中实现，包括在本说明书中公开的结构和它们的结构等同物，或者它们中的一个或多个的组合。在本说明书中描述的主题的实施例可以实现为一个或多个计算机程序，即，一个或多个计算机程序指令模块，在计算机存储介质上编码用于由数据处理装置执行或者用于控制数据处理的操作。可选地或者另外地，程序指令可以在人工生成的传播信号上编码，例如，机器生成的电、光或电磁信号，所述信号生成为编码用于传输到合适的接收机装置用于由数据处理装置执行的信息。计算机存储介质可以是或包括在计算机可读存储设备、计算机可读存储基板、随机或序列存取存储器阵列或设备、或它们中的一个或多个的组合中。而且，尽管计算机存储介质本身不是传播信号，但是计算机存储介质可以是编码在人工生成的传播信号中的计算机程序指令的源或目的地。所述计算机存储介质也可以是或包括在一个或多个分离的物理组件或介质中（例如，多个 CD、光盘或其它存储设备），包括分布式软件环境或云计算环境。

[0072] 包括核心和接入网络的网络，可以包括一个或多个网络元件，所述接入网络包括无线接入网络。“网络元件”可以包含各种类型的路由器、交换机、网关、桥、负载平衡器、防火墙、服务器、联机服务节点、代理、处理器、模块或任何其它合适的设备、组件、元件或可操作为在网络环境中交换信息的对象。网络元件可以包括合适的处理器、存储器元件、用于

支持（或以其它方式执行）与使用处理器用于屏幕管理功能相关联的活动的硬件和/或软件，如本文列出的。而且，网络元件可以包括促成其操作的任何合适的组件、模块、接口或对象。这可以包括允许数据或信息的有效交换的合适的算法和通信协议。

[0073] 本说明书中描述的操作可以实现为由数据处理装置对存储在一个或多个计算机可读存储设备上或者从其它源接收的数据执行的操作。术语“数据处理装置”、“处理器”、“处理设备”和“计算设备”可以包含用于处理数据的所有类型的装置、设备和机器，通过示例的方式包括可编程处理器、计算机、片上系统或前述的多个或组合。所述装置可以包括通用或专用逻辑电路，例如，中央处理单元 (CPU)、刀锋、专用集成电路 (ASIC) 或现场可编程门阵列及其它合适的选项。尽管已经将一些处理器和计算设备描述和/或说明为单个处理器，但是根据相关联的服务器的特定需求，也可以使用多个处理器。对单个处理器的引用意味着在可应用的情况下包括多个处理器。通常，处理器执行指令并且操控数据，以便执行某些操作。除了包括硬件，装置还可以包括对于正在讨论的计算机程序的执行环境的代码，例如，构成处理器固件、协议栈、数据库管理系统、操作系统、跨平台运行环境、虚拟机或它们中的一个或多个的组合的代码。所述装置和执行环境可以实现各种不同的计算模型基础架构，例如网络服务、分布式计算和网格计算基础架构。

[0074] 可以按照任意形式的程序语言来编写计算机程序（也被称为程序、软件、软件应用、脚本、模块、（软件）工具、（软件）引擎或代码），包括编译或解释语言、声明或程序语言，并且可以按照任何形式进行部署，包括作为单机程序或者作为适合于在计算环境中使用的模块、组件、子例程、对象或其它单元。例如，当执行以便至少完成本文描述的处理和操作时，计算机程序可以包括位于有形介质上的计算机可读指令、固件、有线或编程硬件或它们的任意组合。计算机程序可以但不需要与文件系统中的文件相对应。可以将程序存储在保持其它程序或数据（例如，存储在标记语言文档中的一个或多个脚本）的文件的一部分中，专用于正在讨论的程序的单个文件中，或者多个协调的文件中（例如，存储一个或多个模块、子程序或部分代码的文件）。计算机程序可以被部署以便在位于一个位置或跨越多个位置分别并且通过通信网络互连的一个计算机或多个计算机上执行。

[0075] 程序可以实现为经过各种对象、方法或其它处理实现各种特征和功能的单独模块，或者如何合适，可以代替地包括多个子模块、第三方服务、组件、库等等。相反，如果合适，可以将各种组件的特征和功能组合为单个组件。在某些情况中，程序和软件系统可以实现为复合的托管应用。例如，部分复合应用可以实现为企业 Java 组件 (EJB) 或设计时间组件，所述组件可以具有将运行时间实现生成到不同的平台中的能力，所述平台例如是 J2EE(Java2 平台、企业版）、ABAP（高级商业应用编程）对象或微软的 .NET 等等。此外，应用可以表示经由网络（例如，经过互联网）接入并执行的基于网络的应用。进而，可以远程地存储、引用或执行与特定托管的应用或服务相关联的一个或多个处理。例如，特定托管的应用或服务的一部分可以是与被远程调用的应用相关联的网络服务，而托管的应用的另一部分可以是被捆绑用于在远程客户端处进行处理的接口对象或代理。而且，在不偏离本公开的范围的情况下，所托管的应用和软件服务中的任意一个或全部可以是另一软件模块或企业应用（未示出）的孩子或子模块。另外，所托管的应用的部分可以由直接在托管该应用的服务器处工作的用户执行，并且在客户端处远程执行。

[0076] 本说明书中描述的处理和逻辑流可以由执行一个或多个计算机程序的一个或多

个可编程处理器执行，以便通过对输入数据的操作并且生成输出来执行动作。所述处理和逻辑流也可以由专用逻辑电路实现，并且装置也可以实现为专用逻辑电路，所述专用逻辑电路例如是 FPGA（场可编程门阵列）或 ASIC（专用集成电路）。

[0077] 适合于执行计算机程序的处理器通过示例的方式包括通用和专用微处理器，以及任意类型的数字计算机的任意一个或多个处理器。通常，处理器将从只读存储器或随机存取存储器或两者接收指令和数据。计算机的基本元件是用于根据指令执行动作的处理器以及用于存储指令和数据的一个或多个存储器设备。通常，计算机也将包括或有效地耦接为接收来自用于存储数据的诸如磁、磁光盘或光盘的海量存储器的数据，或者向该海量存储器发送数据，或两者。然而，计算机可以不具有这样的设备。而且，计算机可以嵌入在另一设备中，例如，移动电话、个人数据助理 (PDA)、平板电脑、移动音频或视频播放器、游戏控制台、全球定位系统 (GPS) 接收机或便携式存储设备（例如，通用串行总线 (USB) 闪存驱动），仅举几例。适用于存储计算机程序指令和数据的设备包括所有形式的非易失性存储器、介质和存储器设备，通过示例的方式包括半导体存储器设备，例如 EPROM、EEPROM 和闪存设备；磁盘，例如内部硬盘或可移除盘；磁光盘；以及 CD ROM 和 DVD-ROM 盘。处理器和存储器可以由专用逻辑电路补充或者结合在该专用逻辑电路中。

[0078] 为了提供与用户的交互，本说明书中描述的主题的实施例可以在具有用于向用户显示信息的显示设备的计算机上实现，所述显示设备例如是 CRT（阴极射线管）或 LCD（液晶显示器）监视器，以及用户可以通过其向计算机提供输入的键盘和诸如鼠标或轨迹球的指向设备。也可以使用其它类型的设备来提供与用户的交互；例如，提供给用户的反馈可以是任何形式的感官反馈，例如视觉反馈、听觉反馈或触觉反馈；并且可以按照任何形式接收来自用户的输入，包括声音、语音或触觉输入。此外，计算机可以通过向设备发送文档或从设备接收文档来与用户进行交互，所述设备包括由用户使用的远程设备。

[0079] 本说明书中描述的主题的实施例可以在计算系统中实现，所述计算系统包括后端组件，例如，作为数据服务器，或者包括中间件组件，例如，应用服务器，或者包括前端组件，例如，具有图形用户界面或网页浏览器的客户端计算机，通过所述图形用户界面或网页浏览器用户可以与本说明书中描述的主题的实现进行交互，或者一个或多个这样的后端、中间件或前端组件的任意组合。系统的组件可以由数字数据通信的任意形式或介质互连，例如，通信网络。通信网络的示例包括可操作为促成系统中各种计算组件之间的通信的任意内部或外部网络、网络、子网络或它们的组合。网络可以例如在网络地址之间通信互联网协议 (IP) 分组、帧中继帧、异步传输模式 (ATM) 信元、声音、视频、数据及其它合适的信息。所述网络也可以包括一个或多个局域网 (LAN)、无线接入网 (RAN)、城域网 (MAN)、广域网 (WAN)、所有或部分互联网、对等网络（例如，自组织对等网络）和 / 或位于一个或多个位置处的任意其它通信系统或系统。

[0080] 所述计算系统可以包括客户端和服务器。客户端和服务器通常是远离于彼此的并且通常经过通信网络进行交互。客户端和服务器的关系借助于在各自计算机上运行的并且彼此具有客户端 - 服务器关系的计算机程序而产生。在一些实施例中，服务器向客户端设备传输数据（例如，HTML 页面）（例如，用于向与客户端设备交互的用户显示数据或者从该用户接收用户输入）。在客户端设备处生成的数据（例如，用户交互的结果）可以在服务器处从客户端设备接收。

[0081] 尽管本说明书包含许多具体的实现细节，但是这些不应该被解释为对任何发明或请求保护的范围的限制，而是应该被解释为针对特定发明的特定实施例的特征的描述。本说明书中在分别的实施例的背景下描述的某些特征也可以在单个实施例中被组合实现。相反，在单个实施例的背景下描述的各种特征也可以分别在多个实施例中或者在任意合适的子组合中实现。而且，尽管上文中将特征描述为在某些组合中执行并且甚至初始被这样进行请求保护，但是所请求保护的组合的一个或多个特征在某些情况中可以被从该组合中剔除，并且所请求保护的组合可以涉及子组合或子组合的变形。

[0082] 类似地，尽管在附图中按照特定顺序描述了操作，但是这不应该被理解为要求按照所示出的特定顺序或顺次顺序来执行这样的操作或者要求执行所有示出的操作以便实现期望的结果。在某些情况下，多任务和并行处理可能是有利的。而且，在上述实施例中各种系统组件的分离不应该被理解为在所有实施例中均要求这样的分离，并且应该被理解为所描述的程序组件和系统通常可以被一起整合在一个单个软件产品中或被打包为多个软件产品。

[0083] 因而，已经描述了该主题的特定实施例。其它实施例在下列权利要求的范围内。在一些情况中，在权利要求中引述的动作可以按照不同的顺序执行并且仍然能够实现期望的结果。此外，在附图中描述的处理不必要求所显示的特定顺序或顺次顺序来实现期望的结果。

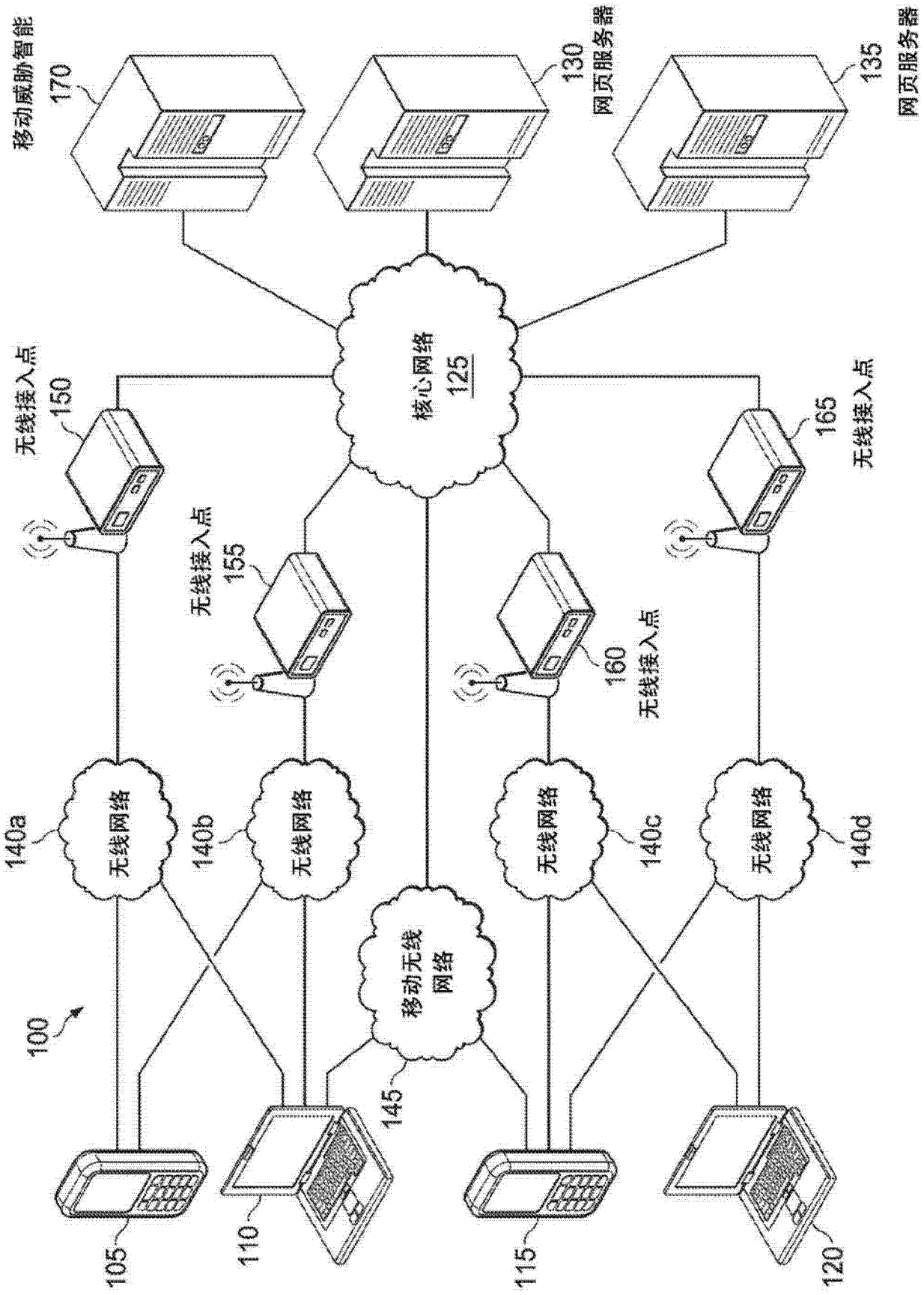

移动威胁智能
170
网页服务器
130
网页服务器
135
核心网络
125
无线接入点
150
无线接入点
155
无线接入点
160
无线接入点
165
无线网络
140a
无线网络
140b
无线网络
140c
无线网络
140d
移动无线
网络
145
100
105
110
115
120

图 1

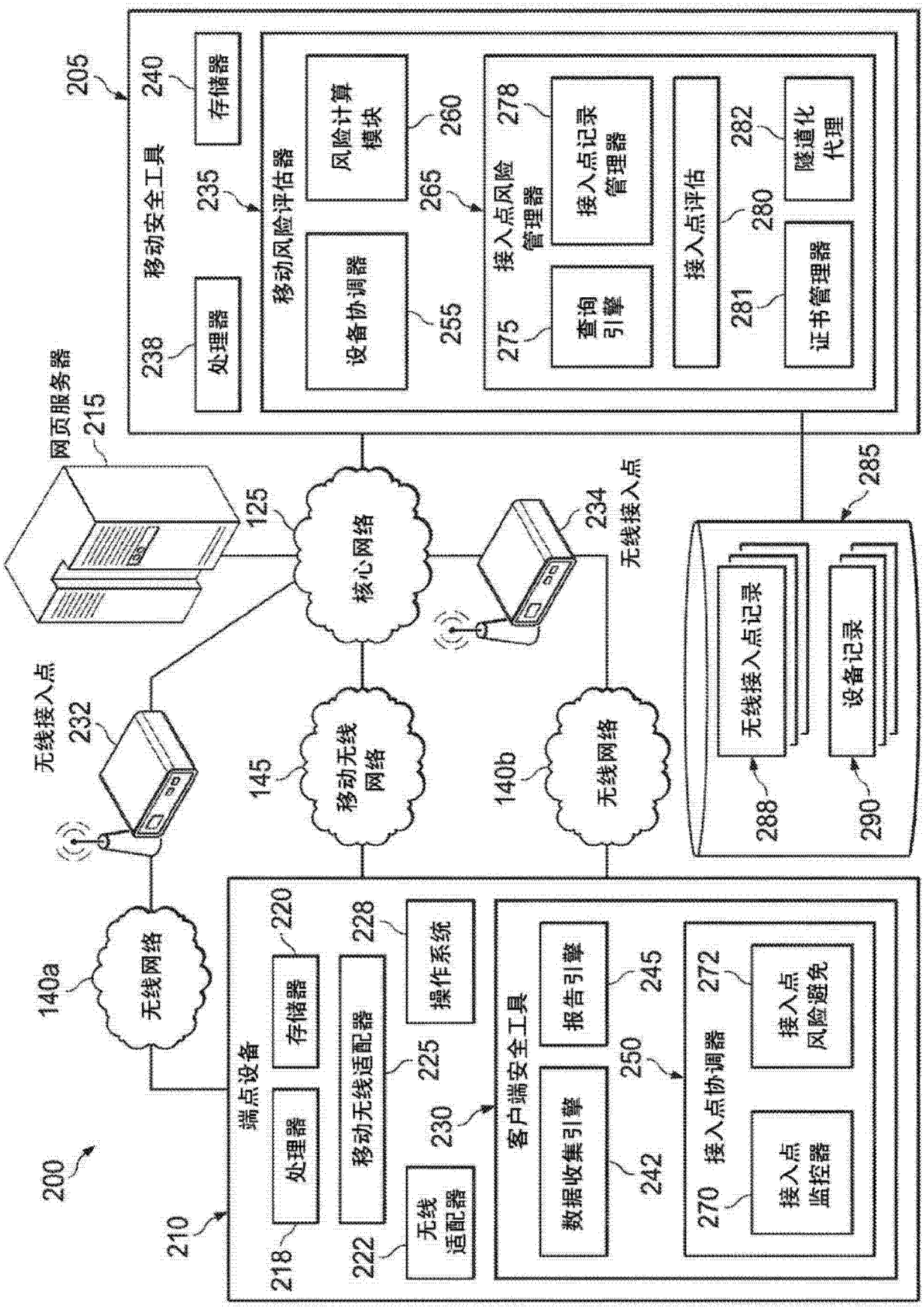

200
205
移动安全工具
240
存储器
235
移动风险评估器
风险计算模块
260
265
接入点风险管理器
278
接入点记录管理器
接入点评估
282
隧道化代理
280
238
处理器
设备协调器
255
275
查询引擎
281
证书管理器
网页服务器
215
125
核心网络
234
无线接入点
285
无线接入点记录
设备记录
288
290
无线接入点
232
145
移动无线网络
140b
无线网络
140a
无线网络
端点设备
220
存储器
228
操作系统
处理器
移动无线适配器
225
230
无线适配器
218
222
210
客户端安全工具
报告引擎
245
数据收集引擎
250
242
接入点协调器
272
接入点风险避免
270
接入点监控器

图 2

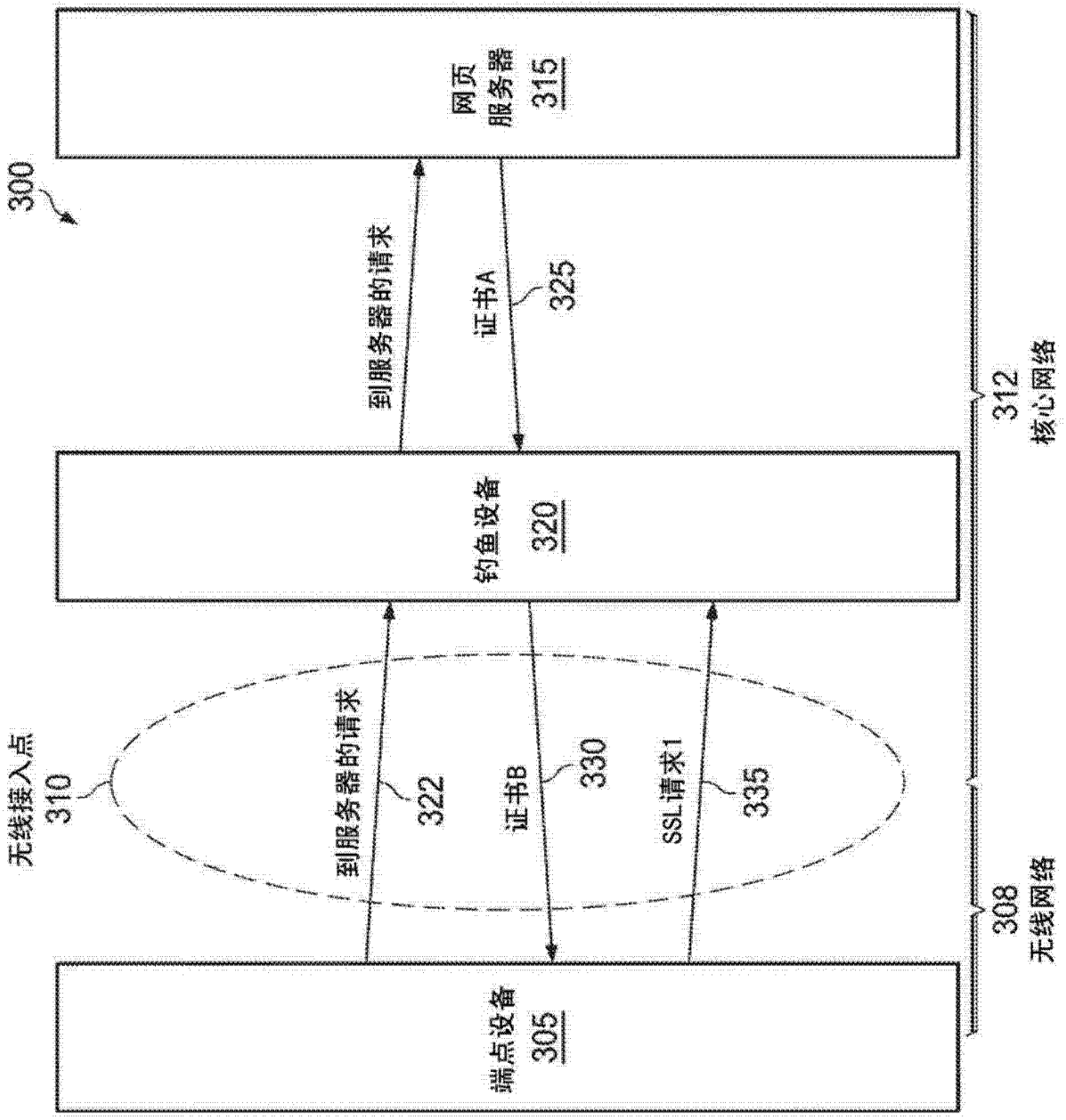

300
网页
服务器
315
到服务器的请求
证书A
325
312
核心网络
钓鱼设备
320
无线接入点
310
到服务器的请求
322
证书B
330
SSL请求1
335
308
无线网络
端点设备
305

图 3

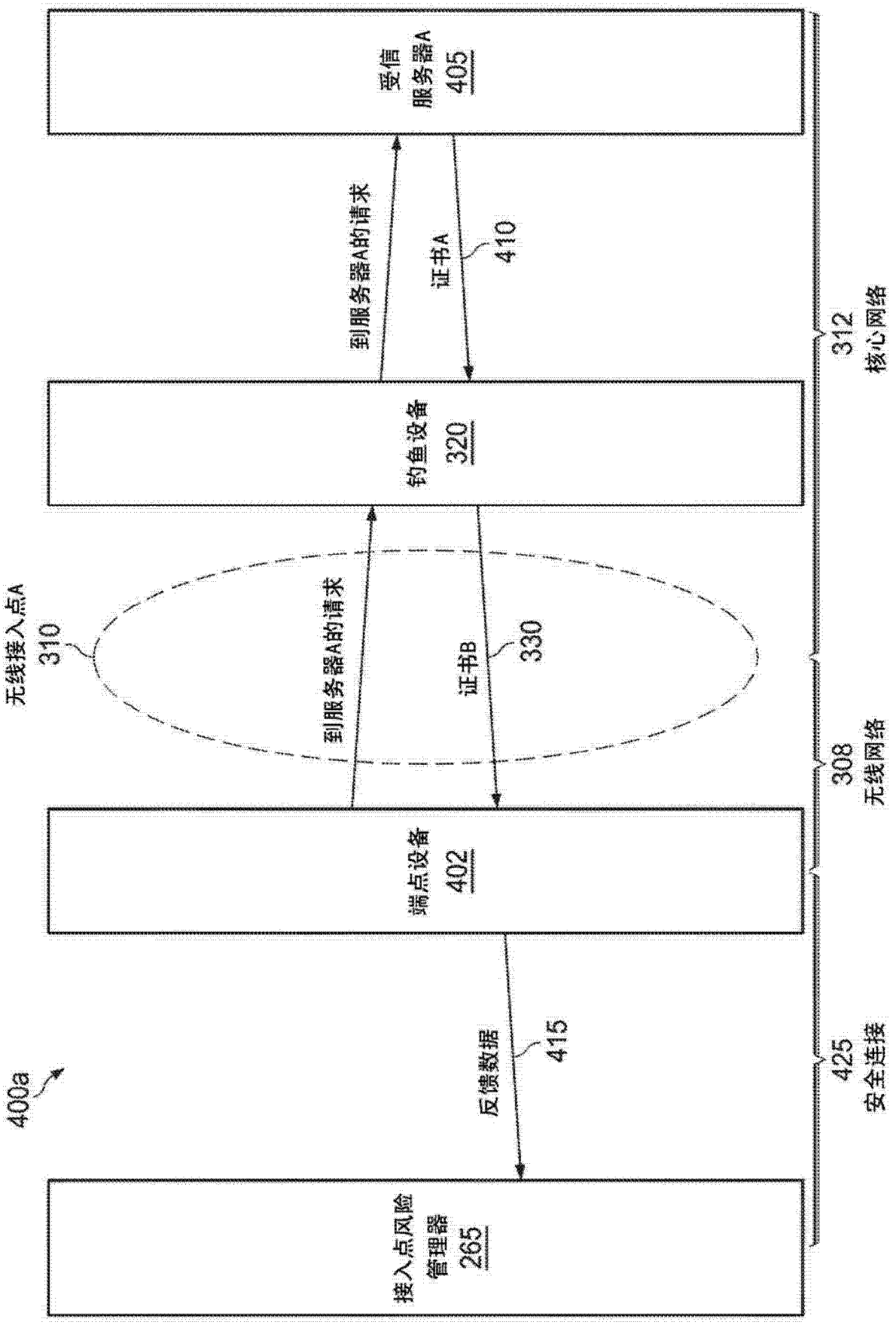

受信
服务器A
405
到服务器A的请求
证书A
410
钓鱼设备
320
312
核心网络
无线接入点A
310
到服务器A的请求
证书B
330
308
无线网络
端点设备
402
400a
反馈数据
415
425
安全连接
接入点风险
管理器
265

图 4A

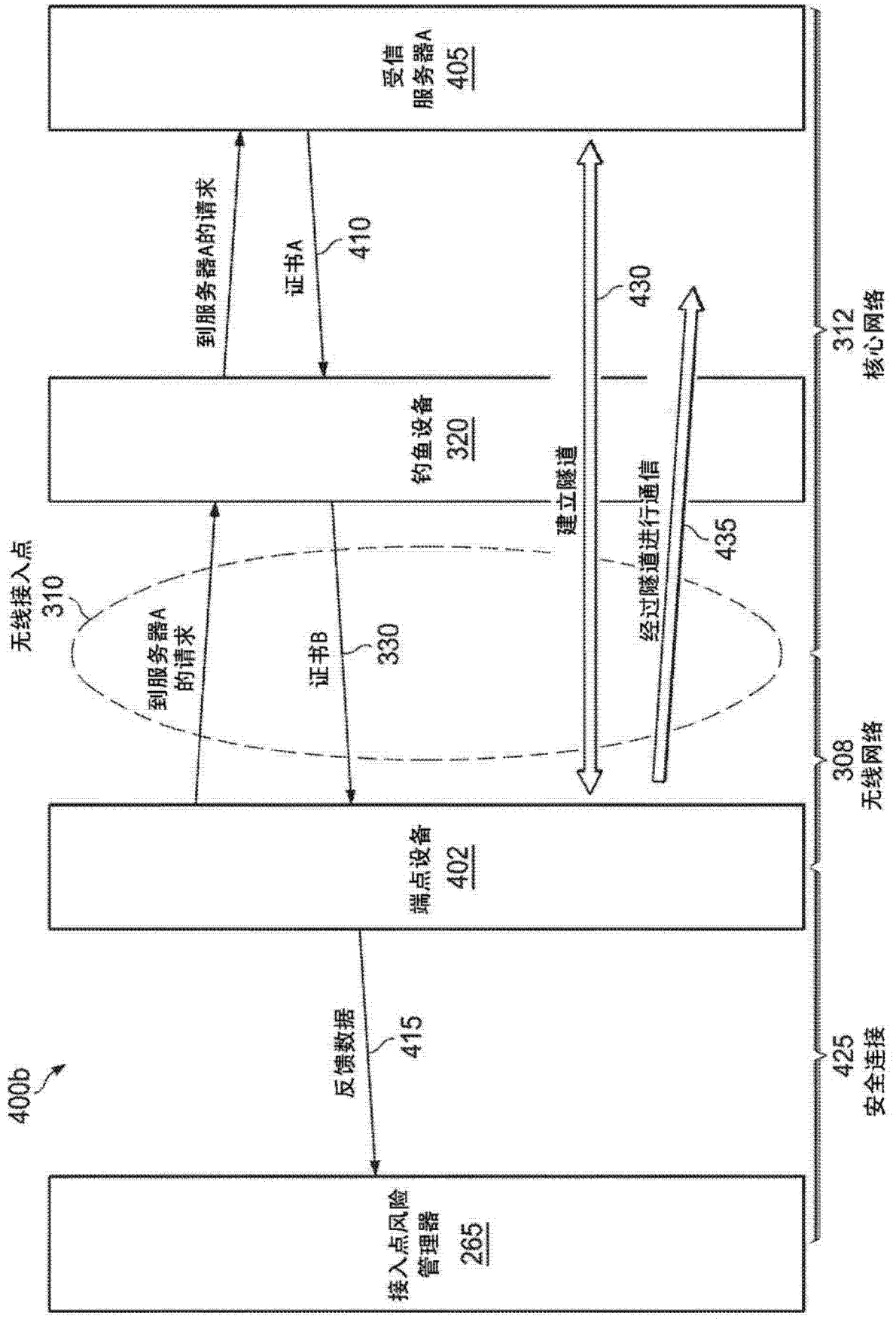

受信服务器A 405
到服务器A的请求
证书A
410
430
312 核心网络
钓鱼设备 320
建立隧道
经过隧道进行通信
435
无线接入点 310
到服务器A的请求
证书B
330
308 无线网络
端点设备 402
反馈数据
415
400b
425 安全连接
接入点风险管理器 265

图 4B

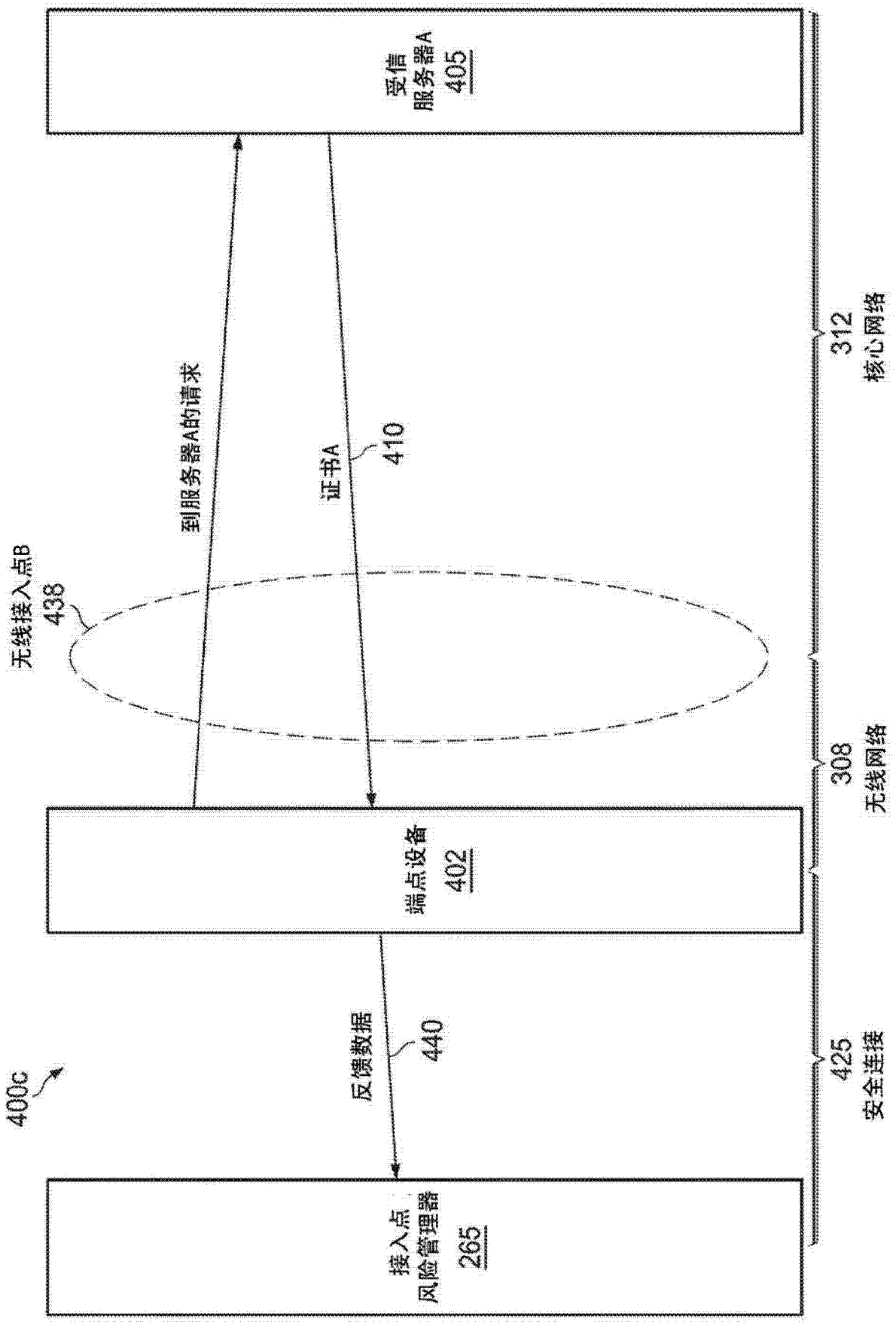

受信
服务器A
405
到服务器A的请求
证书A
410
无线接入点B
438
312
核心网络
308
无线网络
端点设备
402
反馈数据
440
400c
425
安全连接
接入点
风险管理器
265

图 4C

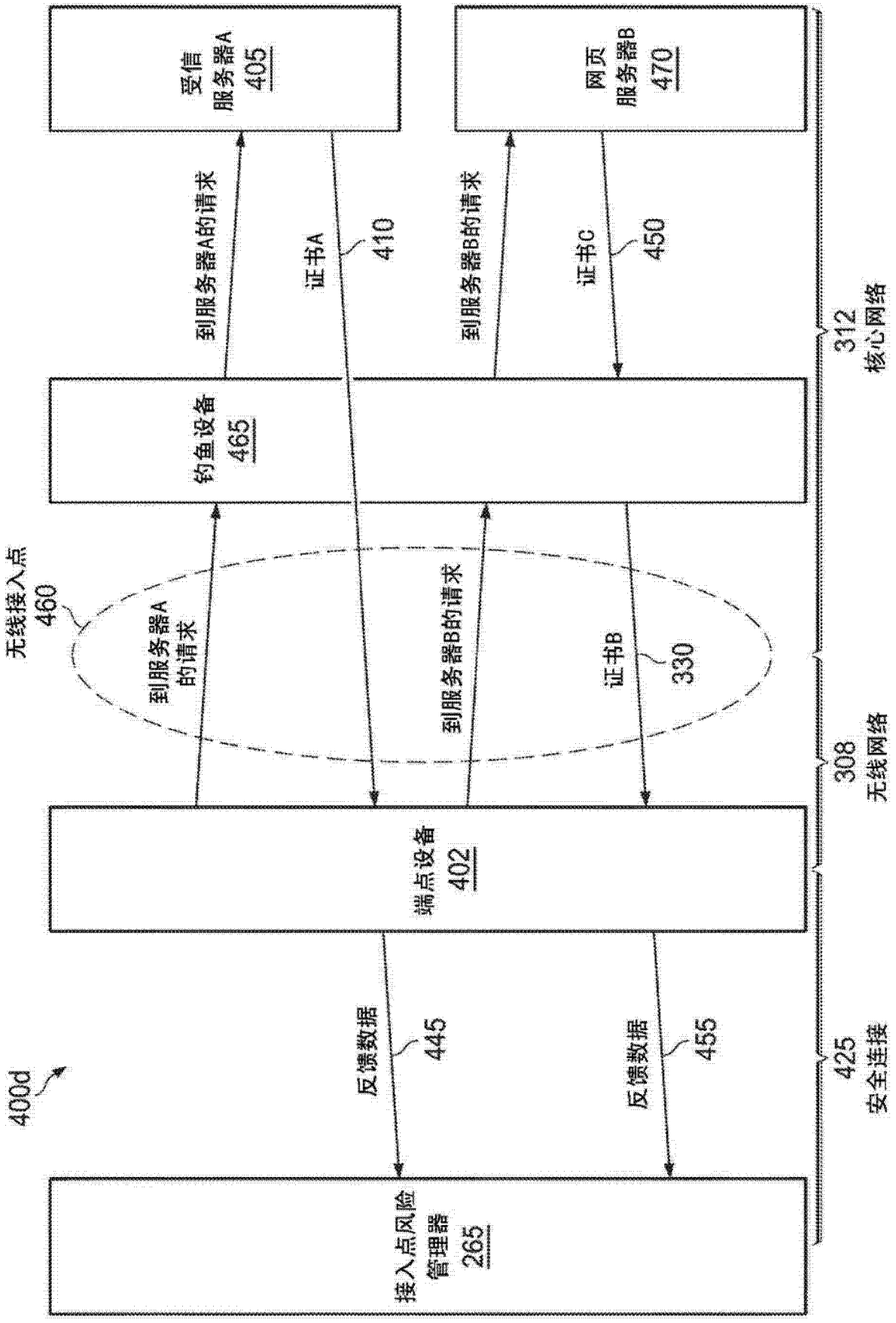

400d
无线接入点
460
受信
服务器A
405
网页
服务器B
470
到服务器A的请求
证书A
410
到服务器B的请求
证书C
450
312
核心网络
钓鱼设备
465
到服务器A
的请求
到服务器B的请求
证书B
330
308
无线网络
端点设备
402
反馈数据
445
反馈数据
455
425
安全连接
接入点风险
管理器
265

图 4D

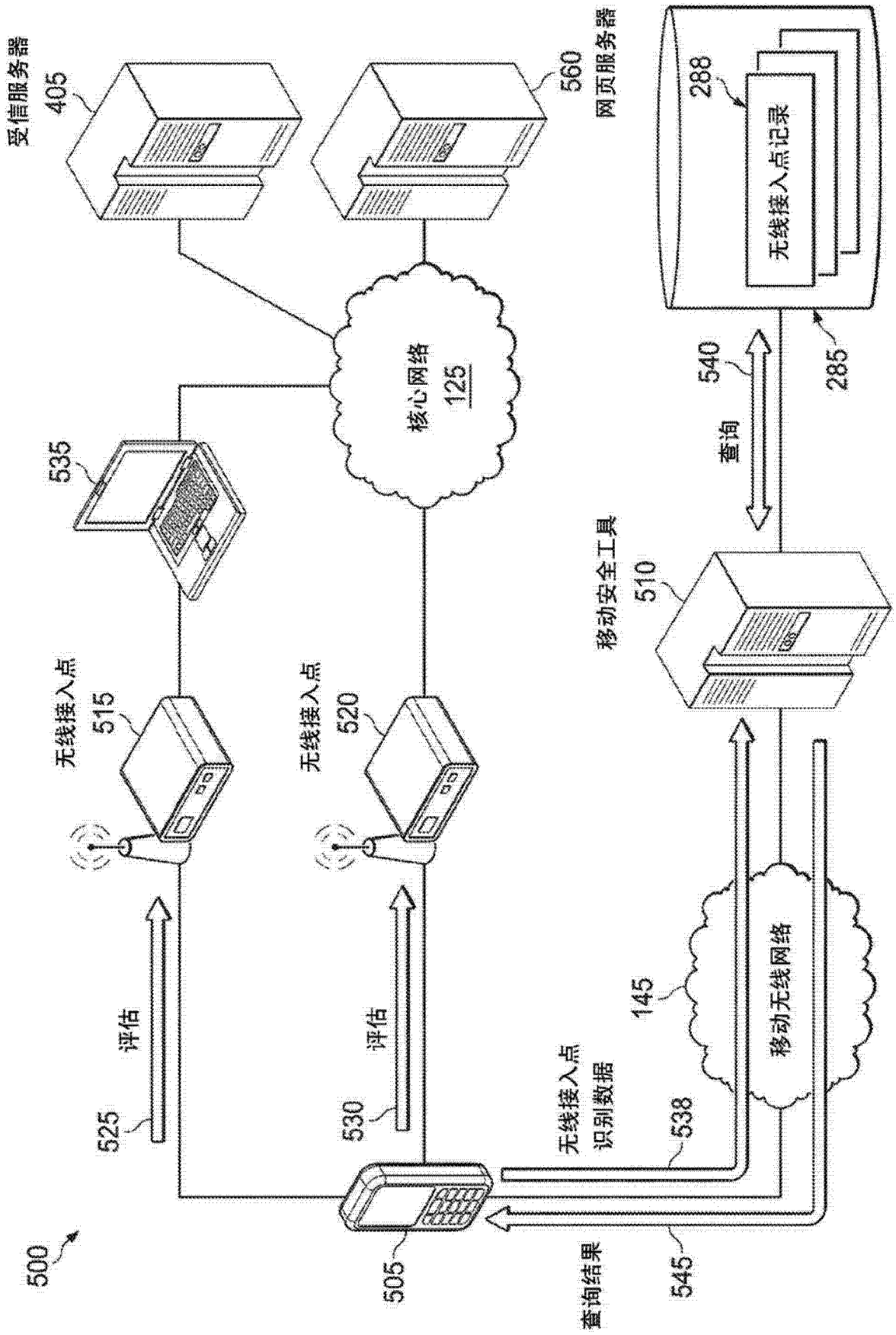

受信服务器
405
560
网页服务器
288
无线接入点记录
核心网络
125
540
查询
285
535
移动安全工具
510
无线接入点
515
无线接入点
520
评估
评估
525
530
145
移动无线网络
无线接入点
识别数据
538
500
505
查询结果
545

图 5

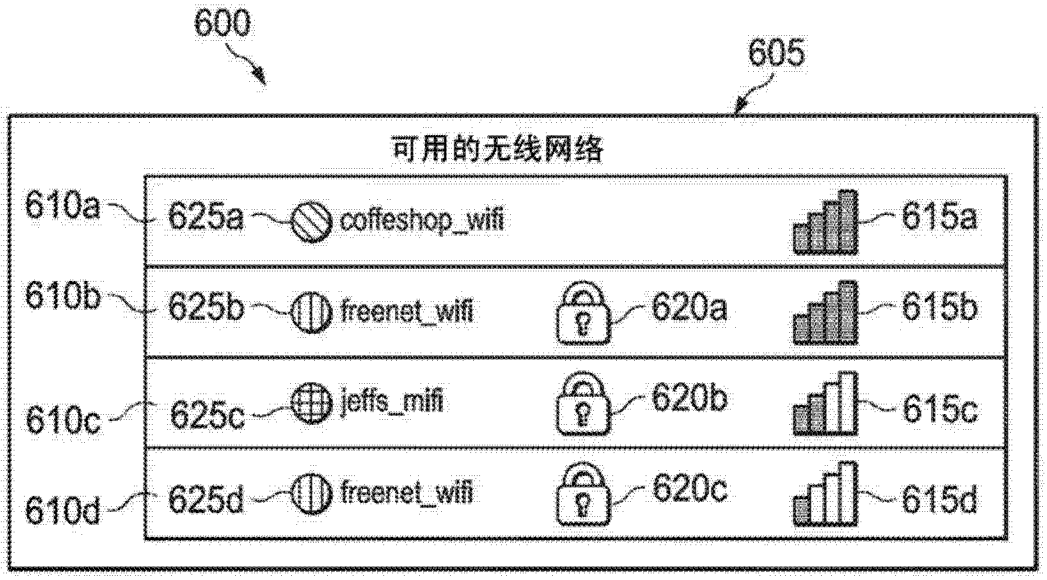

600
605
可用的无线网络
610a
625a
coffeshop_wifi
615a
610b
625b
freenet_wifi
620a
615b
610c
625c
jeffs_mifi
620b
615c
610d
625d
freenet_wifi
620c
615d

图 6

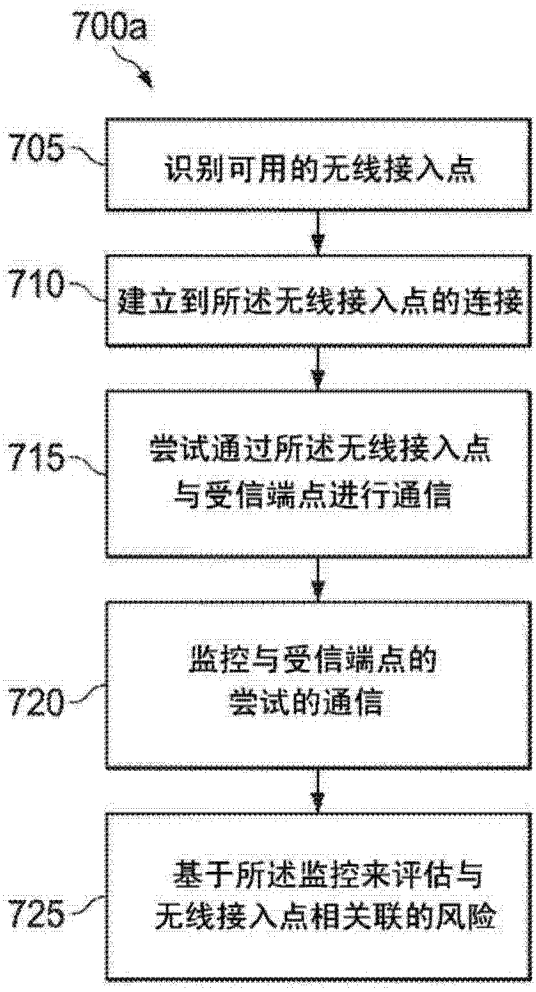

700a
705
识别可用的无线接入点
710
建立到所述无线接入点的连接
715
尝试通过所述无线接入点
与受信端点进行通信
720
监控与受信端点的
尝试的通信
725
基于所述监控来评估与
无线接入点相关联的风险

图 7A

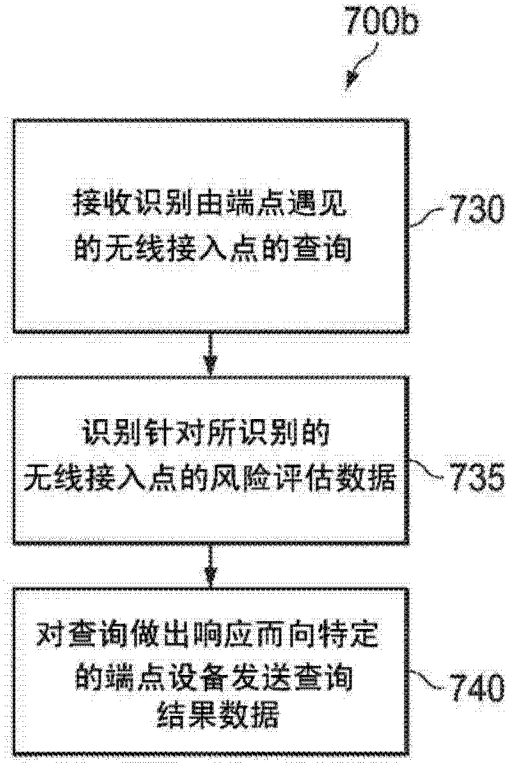

700b
接收识别由端点遇见
的无线接入点的查询
730
识别针对所识别的
无线接入点的风险评估数据
735
对查询做出响应而向特定
的端点设备发送查询
结果数据
740

图 7B