(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 108353078 A
(43)申请公布日 2018.07.31

(21)申请号 201680062961.2

(22)申请日 2016.10.11

(30)优先权数据
14/935,522 2015.11.09 US

(85)PCT国际申请进入国家阶段日
2018.04.26

(86)PCT国际申请的申请数据
PCT/US2016/056438 2016.10.11

(87)PCT国际申请的公布数据
WO2017/083043 EN 2017.05.18

(71)申请人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 S·A·艾哈迈德扎德赫
N·伊斯兰 M·克里斯托多雷斯库
R·古普塔 S·M·达斯

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

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/56(2006.01)
G06F 21/55(2006.01)
G06F 21/57(2006.01)

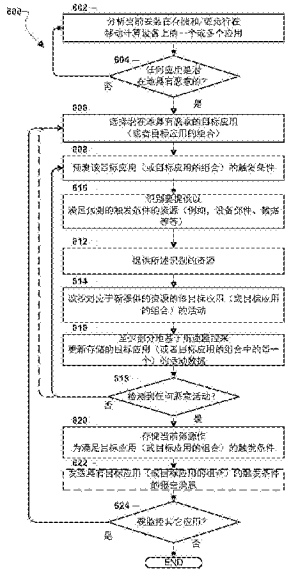
权利要求书4页 说明书16页 附图5页

(54)发明名称

动态蜜罐系统

(57)摘要

各个实施例包括配置为使用行为分析算法和动态资源提供触发恶意应用的恶意活动的蜜罐系统。一种由计算设备的处理器执行的方法(该计算设备可以是移动计算设备)可以包括至少部分地基于分析确定当前运行在该计算设备上的目标应用是否是潜在地具有恶意的,预测该目标应用的触发条件作为对确定该目标应用潜在地具有恶意的响应,至少部分地基于所述预测的触发条件提供一个或多个资源,监听该目标应用对应于所提供的一个或多个资源的活动,并且至少部分地基于所述监听的活动确定该目标应用是否为恶意软件。所述资源可以是设备部件(例如,网络接口、传感器等等)和/或数据(例如,文件等)。



CN 108353078 A

1.一种实现在蜜罐系统中用于触发由应用进行的恶意活动的方法,包括:

响应于确定目标应用潜在地具有恶意,经由计算设备的处理器来预测所述目标应用的触发条件;

至少部分地基于所预测的触发条件,经由所述处理器来提供一个或多个资源;

经由所述处理器来监控与所提供的一个或多个资源相对应的所述目标应用的活动;以及

至少部分地基于所监控到的活动,经由所述处理器来确定所述目标应用是否是恶意应用。

2.如权利要求1所述的方法,其中,经由所述处理器监控所述目标应用的活动包括监控可能具有相同触发条件的一组应用。

3.如权利要求1所述的方法,还包括:

经由所述处理器来确定当前运行在所述计算设备上的应用是否是潜在地具有恶意的;以及

响应于确定所述应用潜在地具有恶意,指定所述应用为所述目标应用。

4.如权利要求3所述的方法,其中,经由所述处理器来确定当前在所述计算设备上执行的所述应用是否是潜在地具有恶意的包括:

经由所述处理器,分析以下各项中的至少一项:对与访问所述计算设备的资源相对应的所述应用的许可,以及存储的指示所述应用的先前活动的活动数据。

5.如权利要求1所述的方法,其中,所述一个或多个资源包括一个或多个设备部件和数据中的一项或两项。

6.如权利要求5所述的方法,其中,所述一个或多个设备部件包括由已安装应用、操作系统、网络接口、处理单元、数据存储单元、耦合的设备、输出单元、输入单元和传感器组成的群组中的至少一个成员。

7.如权利要求5所述的方法,其中,所述数据包括由联系人列表、存储的文件、个人信息、网络状况数据、订阅信息、位置信息、系统信息、已知易损性信息和传感器数据组成的群组中的至少一个成员。

8.如权利要求1所述的方法,其中,响应于确定所述目标应用潜在地具有恶意,经由所述处理器来预测所述目标应用的所述触发条件包括:

经由所述处理器,评估以下各项中的至少一项:对所述目标应用的许可、先前对于所述目标应用可访问的任何资源和存储的指示所述目标应用的先前活动的活动数据。

9.如权利要求1所述的方法,其中,至少部分地基于所预测的触发条件经由所述处理器来提供所述一个或多个资源包括以下各项中的至少一项:

至少部分地基于所预测的触发条件,经由所述处理器来调整先前对于所述目标应用可见的资源;以及

经由所述处理器来配置先前对于所述目标应用不可见的资源,从而使所述资源变得对于所述目标应用可见。

10.如权利要求1所述的方法,其中,至少部分地基于所预测的触发条件经由所述处理器来提供所述一个或多个资源包括:

至少部分地基于所预测的触发条件,经由所述处理器来创建虚拟资源,其中,所述虚拟

资源代表并非实际存在于所述计算设备中或由所述计算设备支持的模拟的设备部件或数据。

11.如权利要求1所述的方法，其中，经由所述处理器来监控与所提供的一个或多个资源相对应的所述目标应用的活动包括：

经由所述处理器来检测由所述目标应用进行的应用程序接口(API)调用。

12.如权利要求1所述的方法，其中，至少部分地基于所监控到的活动经由所述处理器来确定所述目标应用是否是恶意应用包括：

经由所述处理器来评估所监控到的活动和存储的指示所述目标应用的先前活动的活动数据。

13.如权利要求1所述的方法，还包括经由所述处理器来更新存储的所述目标应用的活动数据，所述活动数据包括关于响应于确定所述目标应用是恶意应用而提供的资源的信息。

14.如权利要求1所述的方法，还包括响应于确定所述目标应用是恶意应用，来发送指示针对所述目标应用的所述触发条件的报告消息。

15.一种计算设备，包括：

存储器；以及

处理器，其被耦合到所述存储器的并且被配备有处理器可执行指令，以执行包括以下各项的操作：

响应于确定目标应用潜在地具有恶意，预测所述目标应用的触发条件；

至少部分地基于所预测的触发条件，提供一个或多个资源；

监控与所提供的一个或多个资源相对应的所述目标应用的活动；

以及

至少部分地基于所监控到的活动，确定所述目标应用是否是具有恶意的。

16.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而监控所述目标应用的活动包括：监控可能具有相同触发条件的一组应用。

17.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行还包括以下各项的操作：

确定当前运行在所述计算设备上的应用是否是潜在地具有恶意的；以及

响应于确定所述应用潜在地具有恶意，指定所述应用为所述目标应用。

18.如权利要求17所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而确定当前在所述计算设备上执行的应用是否是潜在地具有恶意的包括：

分析以下各项中的至少一项：对与访问所述计算设备的资源相对应的一个或多个目标应用的许可，以及存储的指示所述一个或多个目标应用的先前活动的活动数据。

19.如权利要求15所述的计算设备，其中，所述一个或多个资源包括一个或多个设备部件和数据中的一项或两项。

20.如权利要求19所述的计算设备，其中，所述一个或多个设备部件包括由已安装应用、操作系统、网络接口、处理单元、数据存储单元、耦合的设备、输出单元、输入单元和传感器组成的群组中的至少一个成员。

21.如权利要求19所述的计算设备，其中，所述计算设备是移动计算设备，并且所述数

据包括由联系人列表、存储的文件、个人信息、网络状况数据、订阅信息、位置信息、系统信息、已知易损性信息和传感器数据组成的群组中的至少一个成员。

22.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而响应于确定所述目标应用潜在地具有恶意来预测所述目标应用的所述触发条件包括：

评估以下各项中的至少一项：对所述目标应用的许可、先前对于所述目标应用可访问的任何资源，以及存储的指示所述目标应用的先前活动的活动数据。

23.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而至少部分地基于所预测的触发条件来提供所述一个或多个资源包括以下各项中的至少一项：

至少部分地基于所预测的触发条件，调整先前对于所述目标应用可见的资源；以及

配置先前对于所述目标应用不可见的资源，从而使所述资源变得对于所述目标应用可见。

24.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而至少部分地基于所预测的触发条件来提供所述一个或多个资源包括：

至少部分地基于所预测的触发条件来创建虚拟资源，其中，所述虚拟资源代表并非实际存在于所述计算设备中或由所述计算设备支持的模拟的设备部件或数据。

25.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而监控与所提供的一个或多个资源相对应的所述目标应用的活动包括：

检测由所述目标应用进行的应用程序接口(API)调用。

26.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作从而至少部分地基于所监控到的活动来确定所述目标应用是否具有恶意包括：

评估所监控到的活动和存储的指示所述目标应用的先前活动的活动数据。

27.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作还包括：更新存储的所述目标应用的活动数据，所述活动数据包括关于响应于确定所述目标应用具有恶意而提供的资源的信息。

28.如权利要求15所述的计算设备，其中，所述处理器被配备有处理器可执行指令以执行操作还包括：响应于确定所述目标应用具有恶意来发送指示针对所述目标应用的所述触发条件的报告消息。

29.一种其上存储有处理器可执行指令的非暂时性处理器可读存储介质，所述处理器可执行指令被配置为使计算设备的处理器执行包括以下各项的操作：

响应于确定一个或多个目标应用潜在地具有恶意，预测所述一个或多个目标应用的触发条件；

至少部分地基于所预测的触发条件，提供一个或多个资源；

监控与所提供的一个或多个资源相对应的所述一个或多个目标应用的活动；以及

至少部分地基于所监控到的活动，确定所述一个或多个目标应用中的任何目标应用是否是具有恶意的。

30.一种计算设备，包括：

用于响应于确定一个或多个目标应用潜在地具有恶意，预测所述一个或多个目标应用

的触发条件的单元；

用于至少部分地基于所预测的触发条件，提供一个或多个资源的单元；

用于监控与所提供的一个或多个资源相对应的所述一个或多个目标应用的活动的单元；以及

用于至少部分地基于所监控到的活动，确定所述一个或多个目标应用中的任何目标应用是否具有恶意的单元。

动态蜜罐系统

背景技术

[0001] “蜜罐系统”(或简称“蜜罐”)是有目的地被部署以用于由恶意软件探测、攻击和盗用,以便发现、识别和特征化这种软件的计算机系统。典型的蜜罐系统被锁住以便将恶意软件限制在该系统的控制的功能,而不会使该恶意软件能够发出进一步的、不可控制的攻击。典型的蜜罐系统是能够进行广泛的系统和应用监听和登录的。蜜罐系统经常很容易被恶意软件通过网络访问(例如,在局域网(LAN)上是可发现的等等)。蜜罐系统的监听和控制功能被很好地伪装以避免被配置为识别和避免蜜罐的恶意软件检测到。有了这些特性,蜜罐系统经常用于在网络中吸引或隔离攻击,以及用于生成指示恶意软件如何工作的有用数据。例如,蜜罐系统能够提供指示恶意软件形成的潜在威胁的数据,该数据能够与其它设备共享以便用作早期预警系统。一般来讲,成功的蜜罐系统提供受控制的时机以向恶意软件学习而不用担心对数据、网络和该网络上的计算设备的实际损害。

发明内容

[0002] 各个实施例提供用于触发应用的恶意活动的蜜罐系统的方法、设备、系统和永久性处理器可读存储介质。各个实施例方法可以由实现该蜜罐系统的计算设备的处理器执行。实现各个实施例的计算设备可以是移动计算设备。各个实施例可以包括预测一个或多个目标应用的触发条件,作为对确定该一个或多个目标应用潜在地具有恶意的响应。各个实施例还可以包括至少部分地基于所述预测的触发条件提供一个或多个资源,并且监听该一个或多个目标应用对应于所提供的一个或多个资源的活动。各个实施例还可以包括至少部分地基于所监听到的活动确定所述一个或多个目标应用是否是具有恶意的。一些实施例还可以包括确定当前在该计算设备上运行的应用是否是潜在地具有恶意的,并且指定该应用作为一个或多个目标应用之一作为对确定该应用潜在地具有恶意的响应。在一些实施例中,确定当前在该计算设备上运行的应用是否是潜在地具有恶意的可以包括分析该对应于对该计算设备的资源的访问的对一个或多个目标应用的许可中的至少一个。在一些实施例中,确定当前运行在该计算设备上的应用是否是潜在地具有恶意的可以包括分析存储的指示一个或多个目标应用的先前活动的活动数据。

[0003] 在一些实施例中,所述一个或多个资源可以包括一个或多个设备部件和数据之一或二者。在一些实施例中,所述一个或多个设备部件包括由已安装应用、操作系统、网络接口、处理单元、数据存储单元、耦合的设备、输出单元、输入单元和传感器组成的群组中的至少一个成员。在一些实施例中,所述数据包括由联系人列表、存储的文件、个人信息、网络状况数据、订阅信息、位置信息、系统信息、已知易受攻击信息和传感器数据组成的群组的至少一个成员。

[0004] 在一些实施例中,预测所述一个或多个目标应用的所述触发条件可以包括评估对所述一个或多个目标应用的许可、先前对于所述一个或多个目标应用可访问的任何资源和存储的指示所述一个或多个目标应用的先前活动的活动数据中的至少一个。

[0005] 在一些实施例中,至少部分地基于所述预测的触发条件提供所述一个或多个资源

可以包括至少部分地基于所述预测的触发条件调整先前对于所述一个或多个目标应用可见的资源。在一些实施例中，至少部分地基于所述预测的触发条件提供所述一个或多个资源可以包括配置先前对于所述一个或多个目标应用不可见的资源使所述资源变得对于所述一个或多个目标应用可见。在一些实施例中，至少部分地基于所述预测的触发条件提供所述一个或多个资源可以包括至少部分地基于所述预测的触发条件创建虚拟资源，其中，所述虚拟资源代表并非实际存在于所述计算设备中或由所述计算设备支持的模拟的设备部件或数据。

[0006] 在一些实施例中，监听对应于所述提供的一个或多个资源的所述一个或多个目标应用的活动可以包括检测所述一个或多个目标应用进行的应用程序接口(API)调用。在一些实施例中，至少部分地基于所述监听的活动确定所述一个或多个目标应用是否是具有恶意的可以包括评估所述监听到的活动和存储的指示所述一个或多个目标应用的先前活动的活动数据。

[0007] 一些实施例还可以包括更新存储的所述一个或多个目标应用的活动数据，所述活动数据包括关于在监听的所述一个或多个目标应用的活动导致确定所述一个或多个目标应用是具有恶意的时提供的资源的信息。一些实施例可以还包括发送指示所述一个或多个目标应用的所述触发条件的报告消息，作为对确定所述一个或多个目标应用具有恶意的响应。

[0008] 其它实施例包括配置有用于执行上面描述的方法的操作的处理器可执行指令的计算设备。其它实施例包括非暂时性处理器可读介质，其上存储有处理器可执行指令，配置为使计算设备执行上面描述的方法的操作。其它实施例包括一种系统，其包括配备有用于执行上述方法的操作的处理器可执行指令的计算设备。

附图说明

[0009] 合并在本申请中的并且组成这一说明书的一部分的附图示出各个实施例，并且与上面给出的一般描述和下面给出的详细描述一起用于解释说明权利要求的属性。

[0010] 图1是根据各种实施方式包括配置为用作蜜罐系统的移动计算设备的系统示意图。

[0011] 图2-5是根据各种实施方式示出与配置为用作蜜罐系统的移动计算设备的资源相关联的动态数据的示意图。

[0012] 图6是根据各种实施方式用于由计算设备蜜罐执行动态提供资源的操作以便吸引或激起应用程序的恶意活动的方法的处理流程图。

[0013] 图7是适合用于一种实现中的移动计算设备的部件框图。

具体实施方式

[0014] 下面将参照附图详细描述各个实施例和实施方式。相同的参考编号将会在贯穿附图中尽可能地用于引用相同或相似的部分。针对特定示例和实施方式进行的参考是为了解释说明的目的，而非意在限制实施方式或权利要求的范围。

[0015] 各个实施例和实施方式包括在计算设备中实例化的动态蜜罐系统，其被配置为通过以预测的引出恶意行为的方式向应用呈现资源和功能的各种组合，从而识别处理器上运

行的应用的恶意行为。该计算设备可以是但并不仅限于移动计算设备。针对每个潜在的恶意应用，该蜜罐系统可以观察该应用的活动和状态并且使用观察到的数据执行分析。该蜜罐系统可以预测诸如可用的设备功能性和该系统的运行状态之类的状况，这些是使每个潜在恶意应用执行恶意动作可能需要的。该蜜罐系统可以相应地提供资源，诸如通过使各种设备部件(例如，传感器、网络接口、存储器位置、处理器、无线单元等等)和/或数据(例如，联系人列表、文件、消息内容等等)可访问或可见。该蜜罐系统可以继续监听潜在的恶意应用并迭代地调整可用资源，直到该潜在恶意应用展现出恶意活动为止。通过使移动计算设备(诸如智能电话)中常见的设备部件可访问或可见，各种实施例和实施方式可以用作评估可能将移动计算设备的常见文件和功能用于恶意目的的应用的移动蜜罐系统。

[0016] 术语“计算设备”在本申请中用于指代配备有至少一个处理器的电子设备。计算设备的示例可以包括移动计算设备(例如，蜂窝电话、可穿戴设备、智能电话、网络pad、平板计算机、互联网功能的蜂窝电话、Wi-Fi功能的电子设备、个人数字助理(PDA)、膝上型计算机等等)、个人计算机和服务器计算设备。例如，移动计算设备可以包括异构的或同种类的多核智能电话。在各种实施方式中，计算设备可以配备有内存和/或存储器以及网络功能，诸如被配置为建立广域网(WAN)连接(例如，蜂窝网络连接等等)和/或局域网(LAN)连接(例如，通过Wi-Fi路由器的到互联网的有线/无线连接等等)的网络收发机和天线。

[0017] 术语“恶意行为”、“恶意活动”和“恶意动作”在本申请中交替使用，用于指代由计算机设备上运行的应用(例如，恶意软件)执行的可能针对该计算设备和/或相关联的用户导致攻击、危害、失败、数据丢失和/或其它不需要的或未授权的状况的任意一个或多个操作。例如，恶意活动可以包括未授权或不需要的数据访问(例如，读、复制等等)、数据传输(例如，向远程设备转移的敏感数据等等)和/或数据交换(例如，重命名、写、覆写、删除、损坏、加密、解密、改变许可等等)。举另一个例子，恶意活动可以包括未授权的或不需要的设备部件变化，诸如重启系统或子系统、处理器过载、去激活传感器、断开存储器设备连接等等。恶意活动可以包括只有在组合执行时才造成不需要的或未授权的结果的多个操作。例如，恶意活动可以包括典型的对耦合的外部存储设备的良性调查与典型的对复制敏感数据的良性请求的组合。

[0018] 有各种不同类型的典型蜜罐系统。“主动的”蜜罐系统可以被配置为监听并响应从恶意应用检测到的威胁。“被动的”蜜罐系统可以被配置为简单地收集监听数据(例如，检测到的应用程序接口(API)调用等等)用于对采用和恶意活动的分析。一些蜜罐系统被设计为只提供对特定恶意应用可能感兴趣的计算系统的功能的访问。例如，一种蜜罐系统可以通过重新创建公知的易受攻击的子系统而不是提供全功能的系统来将公知恶意应用的活动作为目标。这些蜜罐系统技术可以将恶意应用的交互限制在公知的易受该特定恶意应用攻击的子系统。其它蜜罐系统技术可以采用重新创建全功能系统的高交互设计，诸如通过以高开销为代价来模仿常规特性和资源。

[0019] 由于需要资源以便为评估恶意活动提供适当环境，蜜罐系统通常实现在具有定义好的操作条件和/或设备部件的服务器或静态计算系统中。一些蜜罐系统还可以实现在移动计算系统中，但是通常由于移动系统有限的处理能力、内存和功率而具有更小的范围。例如，大量的或持续的监控操作可能由于有限的电池寿命和处理马力而难以在移动设备上在更长时间段完成。

[0020] 一些复杂的恶意应用能够选择性地决定何时攻击计算系统以及确定用于攻击的各种资源。例如，恶意应用可以不显露恶意活动(例如，从移动电话发送安全数据等)直到该恶意应用被下载并安装到系统上之后很久。举另一个例子，该恶意应用可以在运行时间的大部分内执行无害操作，只在满足主机计算系统的某些运行条件时才参与恶意活动(例如，删除文件等等)。不知道恶意活动何时可能发生或者什么资源可能被用于所述恶意活动，典型的蜜罐系统被迫采用代价很高的、对应用活动的持续监听。

[0021] 一些恶意应用的复杂属性是实现在移动计算设备上的蜜罐系统的另外的问题，因为移动设备通常包括可以用于恶意活动的很大范围的设备部件、功能和系统状态。例如，移动电话上的恶意应用可以利用或者依赖于多个通信接口、大范围的设备配置和操作场景(例如，可用的无线接入技术、信道条件)、不同用户行为(例如，提供输入等等)和同时运行的应用的任意组合。恶意应用可以被设计为利用某些资源，使得恶意活动只在给定时间处满足计算设备的高度专用和一套复杂运行条件时才被触发。例如，恶意软件可以使用智能电话的当前位置与一个或多个其它因素组合以确定是否发起恶意活动。移动系统中的恶意活动的如此多选择使得蜜罐的设计很复杂，该蜜罐能够吸引并触发这些恶意活动，从而留下这些流行的移动计算环境尤其易受攻击。

[0022] 各个实施例提供使用因果分析和/或行为预测来触发恶意应用的恶意活动的方法、设备和永久性处理器可读存储介质。一般而言，计算设备(例如，图1中示出的移动计算设备102)可以配置为用作蜜罐系统。在一个示例性实施方式中，该蜜罐系统可以是配置为在网络上可见的(例如，可发现的)的并且具有一些外部实体/用户可用的受控制的功能的智能电话等等。蜜罐系统可以分析通过该计算设备的处理器(例如，图1中的处理器121)运行的各个应用的各个特性、优先活动和准许。蜜罐系统还可以监听对该应用的所有请求、消息、调查、复制/写入、访问和其它活动。至少部分地基于这些分析和监听，该蜜罐系统可以预测可以触发该应用的恶意活动的条件(例如，某些设备部件的存在、计算设备的系统状态和/或其它运行条件)。然后，该蜜罐系统可以提供新的资源并且继续监听以确定所述应用是否开始恶意地活动。该蜜罐系统可以迭代地继续进行这些操作以便找到成功暴露恶意应用的资源的组合。有了至少部分地基于行为分析的这些预测，可以利用减少的系统监听和检测开销来识别出先前未知的威胁和弱点。

[0023] 在一些实施方式中，蜜罐系统可以使用机器学习算法和应用的历史活动数据来识别潜在地具有恶意的应用。在一些实施方式中，应用可以至少部分地基于对该应用能够或者被放置为发布恶意活动的概率的计算被识别为潜在地具有恶意的。例如，蜜罐系统可以至少部分地基于该应用的当前许可和先前观察到的该应用的动作(例如，数据访问、连接请求等)的分析计算概率值。这样计算出的概率值可以与门限值比较，诸如至少部分地基于观察到的与可疑的或潜在地具有恶意的活动匹配的动作随着时间更新的预定义的门限或动态门限。

[0024] 使用潜在恶意应用的活动的分析，该蜜罐系统可以预测该潜在恶意应用要求在其将要显现恶意活动之前出现在该移动计算设备上的条件(即，触发条件)。例如，该蜜罐系统可以估计该潜在恶意应用可以等待的网络条件(例如，信号强度、带宽和连接类型)。这些估计的网络条件可以至少部分地基于在该计算设备的先前的操作条件内的该潜在恶意应用的记录的动作，诸如当不同网络接口可用或不可用时。预测的触发条件可以使该蜜罐系统

能够识别可用于促使该潜在恶意应用开始动作的准确的资源(例如,激活的设备部件、可用的网络接口等等)。此外,预测的触发条件还可以使该蜜罐系统识别适当地诱骗该潜在恶意应用开始动作所要求的间接条件(例如,系统状态、位置、配置参数等等)。

[0025] 该蜜罐系统可以提供识别出的资源,诸如通过激活设备部件和/或调整存储的数据值。一般来讲,提供可以包括禁用、激活、调整、配置、隐藏、显示、创建、删除和/或另外的使该移动计算设备的各种功能可用(或不可用)。提供的资源可以是独立于该蜜罐系统的其它元件(例如,沙箱的)或由该蜜罐系统模仿的真实资源。提供的资源可以是对于应用的群组在系统范围内可见的或者只对潜在恶意应用可见。

[0026] 在一些实施方式中,提供的资源或其它相关资源可以被配置为向所述潜在恶意应用隐藏该蜜罐系统的属性。例如,当该蜜罐系统正在移动(或模仿移动)时,假的Wi-Fi接入点可以被识别为来来回回。举另一个例子,该蜜罐系统可以用多种不同的区域码创建假的联系人列表以便类似于真实的联系人列表一样出现在实际用户的智能电话上。

[0027] 在各种实施方式中,可以提供的资源可以由提供该蜜罐系统的计算设备的规范来确定或者不由其确定。例如,在一些实施方式中,该蜜罐系统可以被配置为调整和/或模仿没有针对该计算设备实际出现或可用的功能(例如,全球定位系统(GPS)接收机、加速传感器、4G连接等等)。

[0028] 蜜罐系统可以密切地监听并且分析对应于任何提供的资源的潜在恶意应用的活动。例如,该蜜罐系统可以截获来自该潜在恶意应用的输出消息和/或应用程序接口(API)调用。

[0029] 如果该潜在恶意应用不对应于具有恶意活动的提供的资源,则该蜜罐系统可以迭代地继续至少部分地基于后续监听/预测来预测触发条件和提供新的(或调整的)资源。例如,该潜在恶意应用的活动的新的观察可以被转发给分析器以便识别该潜在恶意应用等待使用的可能资源。举另一个例子,作为对捕获来自该潜在恶意应用的输出消息和/或应用程序接口(API)调用的响应,该蜜罐系统可以用假的信息进行响应(例如,可用的网络连接、联系人列表数据、传输确认等等)。这一迭代处理可以继续针对该潜在恶意应用来定制该蜜罐系统的资源直到恶意活动被检测到或者被完全分析。

[0030] 如上所述,各个实施例的蜜罐系统在评估可能利用移动计算设备(诸如智能电话)的文件、部件和功能的移动应用中尤其有用。由于这一原因,各个实施例和实现是参考作为适用于实现实施例蜜罐系统的计算设备的示例的移动计算设备描述的。但是,对移动计算设备的参考仅仅是示例性的,而并不意在限制权利要求的范围。

[0031] 下面是根据各种实施方式在移动计算设备(例如,智能电话)上运行的蜜罐系统的非限制性示例。特定应用可以被设计为只在该蜜罐系统位于乌克兰时执行恶意活动(例如,泄漏密码等等)。换言之,在位于乌克兰之前,该应用将不会显示任何恶意活动。该蜜罐系统可以观察该应用具有对访问存储的数据、广域网(WAN)连接和位置服务的许可。所述资源可以是该蜜罐系统创建的实际资源或虚拟资源的任何组合。该蜜罐系统可以提供假的GPS坐标,其指示该移动计算设备处于加州的旧金山。在一段周期内,该蜜罐系统可以观察到该应用周期性地读取或访问位置数据(例如,GPS数据),但是只显现有限的或良性的网络活动。

[0032] 至少部分地基于所述许可,该蜜罐系统可以推断该应用有很高概率泄漏信息。该蜜罐系统可以预测该应用可以要求特定位置来触发恶意活动。作为响应,该蜜罐系统可以

生成各种假的位置数据以指示在全世界的不同位置。当生成指示当前位置是在乌克兰的定位数据时，该应用可以被触发并且可以开始执行泄漏敏感信息的操作，因此确认该应用是具有恶意的。该蜜罐系统可以如果有必要则阻止这一泄漏并且可以将该条件/可用的资源作为特定应用的准确触发条件来记录。

[0033] 在一些实施方式中，该蜜罐系统可以维护一段时间周期的所有应用的历史和状态，以便检测具有延迟的或具体触发器的恶意活动。在一些实施方式中，潜在恶意应用可以至少部分地基于后续活动被确定为不是具有恶意的。

[0034] 在各种实施方式中，可以由该蜜罐系统提供的资源可以包括各种设备部件(和/或相关联的设置)和数据(和/或相关联的设置)。例如，资源可以包括已安装的应用(例如，病毒保护软件、防火墙软件等等)、操作系统(例如，安卓、Windows等等)、网络接口(用于在各种网络局域网和/或广域网上建立通信的硬件和/或软件，诸如收发机、天线、控制器等等)、无线接入技术(RAT)(例如，长期演进(LTE)、3G、2G、Wi-Fi、蓝牙等等)、处理单元(例如，数字信号处理器(DSP)、中央处理单元(CPU)、图形处理单元(GPU)等等)、数据存储单元(例如，存储器、缓存、硬件驱动器等等)、耦合的设备(例如，通过通用串行总线(USB)连接的外部硬件驱动、USB优盘、安全数字(SD)卡等等)、输出单元(例如，显示器、扬声器等等)、输入单元(例如，键盘、触摸屏等等)和/或传感器(例如，摄像机、麦克风、加速计、陀螺仪等等)的一个或多个的任意组合。举另一个例子，资源可以是数据，包括联系人列表、存储的文件、安全或个人信息(例如，图片、视频、保存的密码、消息内容、电子邮件等等)、网络状况数据(例如，接入点名字(APN)、互联网协议(IP)地址、轮询时间(RTT)、可用吞吐量、开放可用端口、回程信息、移动性、信号强度、上传/下载速率、带宽等等)、订阅信息(例如，可用的订户识别/标识模块(SIM)卡、公共陆地移动网络(PLMN)、移动网络运营商(MNO)、跟踪区域等等)、位置信息(例如，全球定位系统(GPS)可用性、位置坐标等等)、系统信息(例如，可用存储、中央处理器(CPU)信息、CPU使用、运行服务、激活的屏幕/显示器、可用的触摸能力等等)、公知的易受攻击性信息(例如，诸如OS版本、OS已安装补丁之类的操作系统(OS)信息；诸如安全套接字层(SSL)版本、SSL实现之类的安全信息；诸如专家级AES之类的弱的或过期的安全算法等等)和传感器数据(例如，传感器可用性、传感器数据等等)的一个或多个的任意组合。

[0035] 在一些实施方式中，该蜜罐系统可以利用各种模块、部件、指令、操作、电路和/或例程来执行因果关系和/或行为分析操作、监听和/或其它操作以检测、控制和/或预测该移动计算设备内的活动。在一些实施方式中，该蜜罐系统可以通过蜜罐系统控制模块(例如，图1的蜜罐系统控制模块140)生效。例如，这一蜜罐系统控制模块可以是OS服务、软件、电路、模块、例程等等，其配置有对该移动计算设备中的系统级资源和/或信令的访问。在一些实施方式中，该蜜罐系统可以使用诸如高通公司的高通Snapdragon智能防护之类的实时分析平台识别潜在的恶意应用。

[0036] 各个实施例提供使用行为分析和预测以触发或诱发应用在受控制的移动环境中的隐藏恶意活动的动态蜜罐系统。具体来讲，公开的各种实现迭代地预测潜在恶意应用要求的触发条件并且持续调整可用资源直到观察到恶意活动为止。这些新颖技术适用于检测未知恶意软件或其它威胁的易攻击性，因为各种实施方式不要求预定义的触发条件而是分析应用行为和特性以便动态识别测试中要使用的资源。这些技术也可以降低监听和检测开销。

[0037] 各个实施例不同于监听应用以识别恶意软件的现有技术。例如，一些现有技术简单地提供已知恶意软件可以预期的设备输入(例如，虚拟按键)，但是并不动态地改变移动计算设备运行条件或环境。这些现有技术不是预测性的并且不会至少部分地基于观察到的应用的非恶意活动迭代地提供不同资源。各种实现可以使用移动计算设备的状态信息和系统资源信息，以引起未识别的或未知的恶意软件的恶意活动，并且因此不依赖于使用明显的致使已知恶意软件激活的输入机制。

[0038] 与其它现有技术不同，各种实现不仅仅采用软件或计算系统的静态配置。例如，本申请中公开的各种实施方式并不迭代地实现针对不同操作系统或架构的预定义软件安装(或系统镜像)的集合。相反，各种实施方式至少部分地基于对潜在恶意应用的行为分析(例如，当前许可、历史活动)动态地改变个体资源(例如，可用硬件设备部件、系统状态变量值等等)。这些动态改变并不基于已知的使用或已知造成恶意软件活动的具体场景。例如，基于未知应用的当前行为，用各种实现配置的移动设备可以评估所述行为并且迭代地改变任意数量的可用设备部件、设备部件配置或操作状态(例如，连接性)和/或系统条件(例如，电池功率水平等等)。

[0039] 一些现有技术监听计算机系统中的具体内容的移动(例如，输出传输中的数据)。各种实施方式不仅是水印或仅仅监听具体数据或文件是否已经移动了。相反，各种实施方式评估潜在恶意应用的各种活动，以预测促使恶意活动所需要的触发条件。换言之，各种实施方式并不简单地跟踪某些已经被泄漏出去的数据、提供水印或识别到敏感数据的访问路径。

[0040] 图1示出了根据各种实施方式的包括被配置为用作蜜罐系统的移动计算设备102的通信系统100。移动计算设备102可以通过有线或无线连接103(例如，Wi-Fi网络连接、蜂窝网络连接等等)在一个或多个网络105上交换通信。例如，移动计算设备102可以与一个或多个远程服务器110交换数据，所述远程服务器也通过有线或无线连接111连接到一个或多个网络105。在各种实施方式中，网络105可以包括局域网(LAN)和/或广域网(WAN)，并且可以与各种接入点(诸如，Wi-Fi路由器、蜂窝网络基站等等)相关联。

[0041] 在各种实施方式中，移动计算设备102可以是各种类型的移动计算设备的任意一种，诸如平板电脑、智能电话和膝上型计算机。在一些实施方式中，一个或多个远程服务器110可以包括各种第三方服务器(例如，可以通过互联网访问的网络服务器、应用商店服务器等)和/或与蜜罐系统监听相关联的服务器计算设备(例如，管理关于恶意软件应用的数据的安全服务器等等)。

[0042] 在各种实施方式中，移动计算设备102可以包括一个或多个处理器121。例如，移动计算设备102可以包括一个或多个中央处理单元(CPU)(或应用处理器)、数字信号处理器(DSP)、图形处理单元(GPU)或它们的任意组合。移动计算设备102还可以包括能够存储处理器可执行指令(例如，应用、程序、例程、操作系统等等)、数据(例如，应用数据、消息、简档、图片、音频文件等)和/或其它用于执行如本申请中所描述的各种操作的其它信息的各种存储器/数据存储单元122(例如，RAM、缓存、硬件驱动、闪存驱动等等)。移动计算设备102的各种部件(例如，121-130)可以通过有线和/或无线连接(诸如通过总线132)耦合到一起。

[0043] 移动计算设备102还可以包括根据各种实施方式用于实现蜜罐系统所必须或不必须的可选部件。例如，移动计算设备102可以包括用于与其它设备和/或网络交换通信的一

个或多个网络接口130。为了简化的目的，所述网络接口可以指的是，或者包括用于根据各种无线接入技术、协议和或格式来交换无线信号的任何硬件(例如，收发机、天线、连接器等等)和/或软件(例如，逻辑、固件等等)。例如，所述网络接口可以包括Wi-Fi、蓝牙、RF和/或近场通信(NFC)无线单元。移动计算设备102可以包括一个或多个传感器124(例如，摄像机、麦克风、光传感器、加速计、陀螺仪等等)。移动计算设备102还可以包括各种输入设备126，诸如触摸屏输入、外设(例如，鼠标、键盘等等)。移动计算设备102还可以包括各种输出设备128，诸如触摸屏显示器、灯泡、扬声器等等。在一些实施方式中，移动计算设备102还可以包括全球定位系统(GPS)接收机。

[0044] 各个可选部件可以被认为是可选的，因为在一些实施方式中移动计算设备102可以配置为简单地模仿这些部件或相关功能，而无需要求实际的部件出现在移动计算设备102中。例如，移动计算设备102可以不包括实际的蓝牙无线单元，但是可以为了使蓝牙资源对于应用可用以便触发该处理器121上运行的应用的恶意活动的目的模仿蓝牙无线单元的出现。

[0045] 在各种实施方式中，移动计算设备102可以被配置有能够至少实现移动计算设备102(即，蜜罐系统)上的对恶意应用活动的监听、分析和预测的各种软件、服务、部件、模块、电路和/或其它功能。本质上，该蜜罐系统可以是对潜在恶意应用不可见的，但是能够控制该潜在恶意应用与所述移动设备102的各种系统部件、数据和能力的每次交互。在一些实施方式中，移动计算设备102的处理器121可以通过运行蜜罐系统控制模块140来使蜜罐系统生效。蜜罐系统控制模块140可以配置为继续生成、拦截和过滤该系统内的信号，以控制可由潜在恶意应用使用的信息和资源。例如，蜜罐系统控制模块140可以拦截或者检测API调用以及任何设备级或OS级消息发送，诸如从已安装应用向调查传感器请求或者从存储器或其它数据存储单元接收存储的数据。

[0046] 在一些实施方式中，蜜罐系统控制模块140可以包括和/或利用各种模块(例如，逻辑、软件、电路等等)以提供该蜜罐系统。例如，蜜罐系统控制模块140可以使用配置为评估系统信息(例如，状态变量、访问等等)并执行机器学习以便识别潜在恶意应用的出现的行为观察和分析模块144。例如，行为观察和分析模块144可以被配置为评估某个应用的应用许可、先前运行的API调用和/或资源访问(例如，存储器访问、网络连接查询等等)，以计算该应用是恶意软件或者不是的概率。至少部分地基于这一分析，该行为观察和分析模块144可以将该应用识别为潜在地具有恶意的或者不是。

[0047] 蜜罐系统控制模块140还可以利用应用行为预测模块146，后者被配置为预测可以使该目标应用呈现恶意活动的触发条件。例如，应用行为预测模块146可以执行目标应用、相关特性和先前观察到的活动的辅助分析以识别移动计算设备102的先前还没有可用但是如果可用则会使恶意软件激活的一个或多个资源或运行条件。

[0048] 蜜罐系统控制模块140可以利用动态资源选择模块148，后者被配置为选择可以使用和/或调整以便触发潜在恶意应用的恶意活动的各种资源和/或系统状态。对这些资源和/或系统状态的选择可以以设计为增加满足识别出的触发条件的可能性的方式来完成。

[0049] 蜜罐系统控制模块140还可以使用动态资源提供模块150，后者被配置为向潜在恶意应用提供所选择的资源。例如，该动态资源提供模块150可以创建和/或调整虚拟的(或模仿的)资源(例如，虚拟网络连接或接口，诸如Wi-Fi网络连接、向具体MNO的注册等等)。举另

一个例子，动态资源提供模块150可以配置实际资源可见但是只具有对应用的有限访问的(例如，使无法照相的摄像机传感器可见)。动态资源提供模块150可以使资源对应用的群组在系统范围内可见或者只对特定应用可见。

[0050] 蜜罐系统控制模块140还可以使用蜜罐系统监听模块152，后者被配置为监听和观察各种资源(例如，系统状态信息、设备状态等等)以及潜在恶意应用的任何操作和/或状态。例如，蜜罐系统监听模块152可以被配置为拦截并评估来自特定目标应用的任何API调用、OS请求、中断、信号和/或其它通信。

[0051] 蜜罐系统控制模块140还可以使用恶意活动检测模块154，后者被配置为将新的观察与先前观察到的对应于潜在恶意应用的信息组合起来以检测恶意活动。例如，恶意活动检测模块154可以检测目标应用在若干行为分析的迭代上的动作趋势并且确定动作组合可能表示恶意活动。

[0052] 图2-5是根据各种实施方式示出了可以由被配置为用作蜜罐系统的移动计算设备102使用的动态数据200的示例的示意图。动态数据200可以对应于移动计算设备102在根据本申请中描述的各种实施方式用于确定潜在恶意应用的触发条件的迭代行为分析算法的运行期间存储的信息。在一些实施方式中，动态数据200和迭代行为分析算法可以如上所述由蜜罐系统控制模块140更新、管理、执行或者控制。

[0053] 出于非限制性解释说明的目的，图2-5处理移动计算设备102已识别出目标应用250(或者目标“应用”)为潜在恶意应用的场景。这一识别可以至少部分地基于如上所述的通过行为观察和分析模块144对目标应用250的许可和/或先前活动的分析。动态数据200可以对应于移动计算设备102在关于目标应用250的迭代行为分析算法的运行期间存储的信息。动态数据200可以包括：指示在给定时间提供的或者“可见的”以便由目标应用250使用的当前资源(例如，设备部件、系统状态的数据)的资源数据分段202a-202d；指示对目标应用250的许可的许可数据分段204；以及指示当前目标应用250活动(例如作为对资源和/或状态信息的调整的相应的API调用等等)的活动数据分段206a-206d。出于在图2-5中示出的示例的目的，许可数据分段204可以指示目标应用250具有对访问各种网络功能(例如，蜂窝网络连接、Wi-Fi网络连接等等)，以及存储器和/或存储设备访问(例如，向存储器、硬盘、外部存储读取/写入数据等)的许可。

[0054] 在各种实施方式中，移动计算设备102可以使用用于存储、定义、显示(或使其可访问)和跟踪与目标应用250和/或行为分析算法相关联的数据的各种数据结构和记录方案。图2-5中示出的任何数据或数据结构仅仅是示例性的，而非限制数据管理的其它方式。

[0055] 图2示出了在行为分析算法的第一次迭代之后由移动计算设备102存储的动态数据200。具体来讲，动态数据200可以包括资源数据分段202a，其包括指示蜂窝网络接口存在于移动计算设备102中的数据。动态数据200还可以包括活动数据分段206a，其指示目标应用250还没有执行任何动作或者另外还没有执行与所述可用蜂窝网络连接的任何潜在恶意动作。具体来讲，目标应用250可能仅执行了对当前网络连接的检查，这可以是运行在移动计算设备上的很多良性应用的常见操作。

[0056] 由于在该行为分析算法的第一次迭代之后没有检测到恶意活动，移动计算设备102可以使用动态数据200中的数据的任意组合以执行该行为分析算法的第二次迭代，以便预测目标应用250的触发条件。具体来讲，移动计算设备102可以评估对目标应用250的许可

(例如,网络和存储/内存访问)与目标应用250的可用的当前资源(例如,蜂窝网络)的组合,以便预测目标应用250可以在执行恶意动作之前等待的条件和/或资源。可以如上所述使用应用行为预测模块146做出这些预测。

[0057] 例如,通过该行为分析算法,移动计算设备102可以观察目标应用250具有网络访问许可,具有对敏感数据的访问并且只执行与蜂窝网络连接的良性活动(例如,检查可用网络连接(例如,RAT可用性、对特定非公共地址的域名系统(DNS)查询等等))。作为对这一观察的响应,移动计算设备102可以推断目标应用250具有很高概率使用WAN连接来泄露敏感信息。移动计算设备102也可以预测目标应用250寻找不同类型的网络连接或RAT(例如,Wi-Fi),以用于泄漏敏感信息。

[0058] 至少部分地基于这些预测,移动计算设备102可以提供只对目标应用250可见的虚拟Wi-Fi网络连接或接口,诸如通过如上所述的动态资源选择模块148和动态资源提供模块150。虚拟Wi-Fi网络连接可以被紧密地监听并且具有受限的网络连接。移动计算设备102能够检测通过新的Wi-Fi网络连接发送的(或请求要发送的)任何通信,诸如通过如上所述的蜜罐系统监听模块152。

[0059] 图3示出了在这一示例的行为分析算法的第二次迭代和提供虚拟Wi-Fi网络连接之后由移动计算设备102存储的动态数据200。所述资源数据分段202b指示移动计算设备102提供Wi-Fi网络连接以取代如图2中所示的蜂窝网络连接。作为对改变目标应用250可用的网络连接类型的响应,动态数据200现在可以包括活动数据分段206b,其指示目标应用250执行操作以访问敏感数据(例如,密码文件、联系人列表等等),并且随后通过虚拟Wi-Fi网络连接操作外部数据转移。移动计算设备102可以确定目标应用250的这些动作是潜在地具有恶意的,诸如通过如上所述的恶意活动检测模块154。使用这一迭代的行为分析算法,移动计算设备102可能已经至少确定目标应用250可能被设计为只使用Wi-Fi网络连接(例如,不使用蜂窝网络)来进行盗取/散发敏感数据的恶意活动。

[0060] 在一些情况中,移动计算设备102可以执行行为分析算法的额外迭代以触发目标应用250的恶意活动。例如,如果目标应用250被配置为只在满足若干条件时执行恶意活动,则移动计算设备102可以重复地执行分析、预测和提供操作直到出现引起恶意活动的准确的因素组合为止。

[0061] 图4示出了响应于从蜂窝网络连接到Wi-Fi网连接的改变,目标应用250不开始执行恶意动作的示例性场景。具体来讲,图4示出了在行为分析算法的第二次迭代和提供资源数据分段202c所指示的虚拟Wi-Fi网络连接之后存储的动态数据200。在这一示例中,活动数据分段206c不指示响应于新提供的Wi-Fi网络连接目标应用250执行了潜在的恶意动作。

[0062] 由于正在该行为分析算法的第二次迭代之后没有检测到恶意活动,移动计算设备102可以使用动态数据200中的数据的任意组合来执行该行为分析算法的第三次迭代,以预测目标应用250的触发条件。移动计算设备102可以评估目标应用250的许可(例如,网络和存储/内存访问)与目标应用250可用的当前资源(例如,Wi-Fi网络连接)的组合。然后,移动计算设备102可以预测目标应用250在执行恶意动作之前可以等待的条件和/或资源。

[0063] 例如,通过行为分析算法,移动计算设备102可以观察目标应用250具有不同类型的网络访问加上对某些敏感数据的访问,但是只执行了良性的活动。作为响应,移动计算设备102可以推断目标应用250可能有很高概率盗取移动计算设备102可以访问敏感数据但是

不会本地存储任何数据的信息。在这种环境中，移动计算设备102可以预测目标应用250可以等待包含该目标应用250被设计盗取的特定类型数据的新的数据源。至少部分地基于该预测，移动计算设备102可以创建到假的外部数据源(或驱动)的虚拟连接，诸如通过无线或有线连接(例如，蓝牙、NFC、电缆等等)连接的硬驱动或者通过通用串行总线(USB)连接来连接的优盘驱动等等。移动计算设备102能够检测向所述新的假的外部数据源的任何数据访问(例如，复制、写入、读取等等)。

[0064] 图5示出了在该行为分析算法的第三次迭代和提供到所述假的外部数据源的连接之后由移动计算设备102存储的动态数据200。资源数据分段202d指示移动计算设备102除了先前提供的Wi-Fi网络连接之外还提供到外部数据源(或驱动)的连接。作为对所提供资源的改变的响应，动态数据200现在包括活动数据分段206d，它指示目标应用250开始操作以访问外部驱动(例如，复制数据等等)，然后操作在该Wi-Fi网络连接上的外部数据转移；可能是具有恶意的活动。换言之，使用迭代行为分析算法，移动计算设备102在这一示例中确定目标应用250被设计为至少使用Wi-Fi网络连接以进行从移动计算设备102外部的数据源盗取和散发数据的恶意活动。

[0065] 图6示出了根据各种实施方式用于移动计算设备使用行为分析和动态资源提供来触发应用的恶意活动的方法600。在一些实施方式中，方法600的各种操作可以由蜜罐系统控制模块140和各种模块(例如，模块144-154)来执行，每个通过该移动计算设备的处理器(例如，移动计算设备102的处理器121)来运行。

[0066] 在方框602中，移动计算设备的处理器可以分析安装在该移动计算设备的存储上和/或运行在该移动计算设备的处理器上的一个或多个应用以估计该应用可能具有恶意的概率。例如，该移动计算设备可以评估运行在该处理器上的每个应用的许可，以识别该移动计算设备的可以由该应用访问的潜在子系统和/或其它功能。该移动计算设备可以至少部分地基于先前观察到的并且存储的每个应用的数据(例如，该应用的历史活动、当前许可等等)来计算所述一个或多个应用中的每一个潜在地具有恶意的概率。在一些实施方式中，某些许可、先前的动作或它们的任意组合可以指示一个应用具有更高可能性是恶意软件。例如，该移动计算设备可以由于一个应用访问该移动计算设备的特定部件(例如，网络接口)和/或敏感数据的能力而计算该应用有很高概率能够执行恶意数据泄漏操作。举另一个例子，该移动计算设备可以基于将恶意应用的已知行为与在该移动计算设备上运行期间观察到的该应用的当前(或最近)行为匹配，而计算该应用有很高概率能够执行恶意数据泄漏操作。

[0067] 在判定方框604中，该移动计算设备的处理器可以确定当前安装在该移动计算设备的存储上和/或在该移动计算设备的处理器上运行的一个或多个应用的任何一个是否是潜在地具有恶意的。例如，该移动计算设备可以将计算出的该应用具有恶意的概率与门限值比较，以确定一个应用是否应该被归类为潜在地具有恶意的。在一些实施方式中，方框602-604的操作可以使用如上参考图1描述的行为观察和分析模块144来执行。

[0068] 作为对确定当前在该移动计算设备的处理器上运行的一个或多个应用中没有一个潜在地具有恶意(即，判定框604＝“否”)的响应，该移动计算设备可以继续进行块602中的分析操作，或者如果所有应用都已经被分析并发现很可能是良性的则结束。

[0069] 作为对确定该移动计算设备的处理器上当前运行的一个或多个应用潜在地具有

恶意(即,判定框604＝“是”)的响应,该移动计算设备的处理器可以在块606中选择潜在地具有恶意的目标应用。例如,所选择的目标应用可以简单地是多个识别出的潜在恶意应用中的下一个。在一些实施方式中,该移动计算设备可以选择多个(或组合)目标应用以评估方框606-622的操作。换言之,由该移动计算设备进行的方框606的选择可以不仅限于一个目标应用,而是该蜜罐系统可以针对可能具有相似(或者相同)触发参数的一组应用来运行。

[0070] 在方框608中,该移动计算设备的处理器可以预测可以激起或触发该目标应用(或目标应用的组合)的恶意活动的触发条件(例如,可用资源、系统状态等等)。例如,该移动计算设备可以预测该目标应用要求Wi-Fi网络连接以开始恶意动作,即使Wi-Fi网络连接实际上并不可用。在一些实施方式中,该移动计算设备可以通过评估对目标应用(或目标应用的组合)的许可、先前对于该目标应用可访问的任何资源和存储的指示该目标应用的先前活动的活动数据,做出对触发条件的这些预测,以便识别该目标应用可以在开始恶意行为之前等待的状况。在一些实施方式中,方框608的操作可以使用如上参考图1所描述的应用行为预测模块146执行。例如,该移动计算设备可以基于在该目标应用执行中直到当前时间观察到的相关动作,做出关于未来可能由该目标应用访问的动作或资源(例如,蓝牙通信)的预测,诸如针对该移动计算设备的蓝牙部件的出现或状态的查询。

[0071] 在方框610中,该移动计算设备的处理器可以识别要提供的可以满足所述预测出的触发条件的资源(例如,设备部件、系统状态数据)。例如,至少部分地基于预测出的指示该目标应用要求Wi-Fi网络连接以开始恶意动作的触发条件,该移动计算设备可以识别应该模仿假的Wi-Fi网络接口或者使其对该目标应用可见。在一些情况中,该移动计算设备可以识别已经可用的资源应该被调整或重新配置以满足所述预测的触发条件。例如,信号强度读取可能需要被人为地增加或减少。在一些实施方式中,该移动计算设备可以迫使可用资源进入例外条件以便向该目标应用(或目标应用的组合)显示可能触发额外的恶意行为的极端案例。

[0072] 如上所述,可以被识别为用于提供的资源可以包括设备部件和数据中的一个或多个(例如,系统变量、OS级别数据、寄存器数据等等)。例如,设备部件可以包括已安装的应用、操作系统、网络接口、处理单元、数据存储单元、耦合的设备、输出单元、输入单元和传感器。举另一个例子,资源数据可以包括联系人列表、存储的文件、个人信息、网络状况数据、订阅信息、位置信息、系统信息、已知易受攻击信息和传感器数据。

[0073] 为了触发特定的复杂恶意应用,动态提供资源和/或对资源的调整应该尽可能实际地呈现给目标应用(或目标应用的组合)。例如,该目标应用应该不能从实际存在于该移动计算设备的网络中的真实网络条件来区分出假的或模仿的网络条件。举另一个例子,现实的电话联系人列表可以包括具有多于一个区域码的电话号码。举另一个例子,消息日志可以指示该移动计算设备已经与该联系人列表中的一些而不是全部联系人交换过多个短消息服务(SMS)消息。此外,动态资源应该以与实际资源一致的随机性水平来出现、改变和消失。例如,由于Wi-Fi网络连接无法在典型Wi-Fi传输范围之外维持,因此单个Wi-Fi接入点在其它数据指示该移动计算设备远超过典型Wi-Fi接入点可达到范围时不应该被报告为活动的。

[0074] 因此,在方框610中,该移动计算设备可以识别与预测的该目标应用(或目标应用

的组合)的触发条件直接和/或间接相关的资源。例如,为了避免恶意应用检测到蜜罐系统环境的出现,该移动计算设备可以呈现或模仿移动信息(例如,传感器或改变GPS数据)和不同连接的接入点的提供(例如,SSID、媒体接入控制(MAC)地址、RSSI)二者。举另一个例子,为了提供更真实的可由该目标应用访问的假的联系人列表,该移动计算设备可以确定更多不同联系人需要被添加到该假的联系人列表中(例如,来自不同区域码的电话号码、各种数量的SMS消息的不同接收方/发送方等等)。在一些实施方式中,方框610的操作可以使用如上参考图1所描述的动态资源选择模块148来执行。

[0075] 在方框612中,该移动计算设备的处理器可以提供识别出的资源。在一些情况中,提供可以包括至少部分地基于预测的触发条件调整已经可用的(或可见的)资源,诸如通过改变设备部件的运行特性(例如,吞吐量、处理速度、温度读数等等)和/或调整可以由该目标应用调查的系统数据的值。例如,该移动计算设备可以调整该目标应用可请求以指示特定信号强度、接入点名称、接入网络等等的网络连接状态数据。举另一个例子,该移动计算设备可以改变GPS数据以指示该移动计算设备已经重新定位到新的城市。提供还可以包括配置对该目标应用(或目标应用的组合)可见的资源,即使在这些资源通常不存在于该移动计算设备上时。例如,该移动计算设备可以激活特定网络接口和/或传感器,用于由该目标应用的潜在使用。举另一个例子,该移动计算设备可以至少部分地基于预测出的触发条件来调整先前对目标应用可见的资源(例如,调整运行参数或配置)。举另一个例子,该移动计算设备可以配置先前对目标应用不可见的资源,使其变得对该目标应用可见或者可访问。

[0076] 在一些实施方式中,提供可以包括至少部分地基于预测出的触发条件创建虚拟资源。这些虚拟资源可以代表没有实际出现在该移动计算设备中或者由其支持的模拟的设备部件和/或数据。例如,该移动计算设备可以生成对于该目标应用可见并且可访问的虚拟(或假的)Wi-Fi网络接口、假的蓝牙无线单元、假的SIM卡、耦合的外部设备(例如,USB优盘驱动等等)和/或假的DSP。在一些实施方式中,方框612的操作可以使用如上参考图1描述的动态资源提供模块150执行。

[0077] 在方框614中,移动计算设备的处理器可以监听该目标应用(或目标应用的组合)对应于新提供的资源的活动(例如,对所提供的资源的访问)。例如,该移动计算设备可以拦截和/或检测所有应用程序接口(API)调用、中断、消息和/或该目标应用发出的其它信令。所监听的活动可以包括诸如请求OS级别服务、对内存或其它存储的读取/写入、使用更多功率和/或处理器时间、对系统变量或数据的查询或改变、经由网络接口发起通信、调查设备部件(例如,传感器)和/或使用该移动计算设备的一个或多个资源执行任何其它操作之类的动作。

[0078] 在方框616中,该移动计算设备的处理器可以至少部分地基于方框614的监听操作更新针对目标应用(或目标应用的组合)存储的活动数据。在一些实施方式中,该移动计算设备可以将所有评估的应用的历史和状态维护一段时间。这些历史活动数据可以被保存在与个体目标应用相关联的各种数据结构中,诸如应用简档。例如,该移动计算设备可以更新与该目标应用相关联的简档数据以指示任何API调用、内存访问和/或由该目标应用发起的其它动作,作为对各种提供操作的响应。在一些实施方式中,该移动计算设备可以将历史活动数据存储在与目标应用的组合相关联的各种数据结构或简档中。在一些实施方式中,方框614-616的操作可以使用如上参考图1所描述的蜜罐系统监听模块152执行。

[0079] 在判定框618中，该移动计算设备的处理器可以确定该目标应用(或目标应用的组合)是否进行任何恶意活动。这一判定可以包括对作为对使资源可用或调整资源的响应出现的监听到的该目标应用的活动进行评估。例如，作为对生成可用于由该目标应用访问的假的联系人列表的响应，该移动计算设备可以在当该联系人列表被传递以通过该目标应用可访问的出站连接(例如，Wi-Fi连接、蜂窝网络连接等等)传输时确定发生恶意活动。在一些实施方式中，这一确定还可以包括评估存储的指示该目标应用的先前活动的活动数据。例如，当该目标应用先前复制了敏感数据并且重复地检查可用Wi-Fi连接但是没有尝试发送所述复制的数据时，该移动计算设备可以在该目标应用稍后被观察到请求与远程数据源建立连接时，确定在发生恶意活动。在各种实施方式中，该移动计算设备可以至少部分地基于观察到的活动数据(例如，拦截的API调用、中断和/或由该目标应用生成或者发起的其它信号)识别恶意活动，所述观察到的数据被转发给分析器作为对方框612的提供操作的响应。在一些实施方式中，判定框618的操作可以使用如上参考图1所描述的恶意活动检测模块154执行。

[0080] 作为对确定没有检测到对应于该目标应用的恶意活动(即，判定框618＝“否”)的响应，该移动计算设备可以继续进行方框608中的预测操作。换言之，该移动计算设备可以迭代地确定如何提供资源和相应地重新提供资源直到该目标应用响应为止。例如，至少部分地基于新观察到的该目标应用的行为，该移动计算设备可以更新行为预测并且识别要模仿的或者要调整的新的资源以触发该目标应用。不同资源和/或系统状态数据可以替代和/或添加到先前可用的资源和/或提供给该目标应用的系统状态数据。

[0081] 在一些实施方式中，该移动计算设备可以使用蜜罐系统观察，以更新方框602中由该目标应用进行恶意活动的概率，并且因此可以确定该目标应用可能不具有恶意。例如，在方框608-618的操作的若干次迭代之后，该移动计算设备可以确定该目标应用是恶意软件的概率低于门限，并且将该目标应用从潜在恶意应用列表中移除。当这种情况发生时，该移动计算设备可以在方框606中选择下一个目标应用并且继续进行聚焦在该目标应用上的方法600的操作。

[0082] 作为对确定在目标应用中检测到恶意活动(即，判定框618＝“是”)的响应，该移动计算设备的处理器可以确定所预测出的触发条件是准确的，或者记录当前提供的资源，并且在方框620中将关于当前提供的资源的信息存储为满足该目标应用(或目标应用的组合)的触发条件。

[0083] 在一些实施方式中，该移动计算设备可以执行各种操作，作为对检测到该目标应用(或目标应用的组合)的恶意活动的响应。例如，基于检测到的恶意行为，该移动计算设备可以阻止目标应用访问某些资源和/或禁用该目标应用。作为对检测恶意活动的响应执行的操作的另一个非限制性示例，该移动计算设备可以执行报告操作。因此，在可选框622中，该移动计算设备的处理器可以发送指示该目标应用(或目标应用的组合)的触发条件的报告消息。例如该移动计算设备可以与服务器通信，该服务器被配置为登记关于在该移动计算设备上提供的促使该目标应用呈现恶意行为的部署的资源的恶意软件数据以及观察的恶意行为的类型(例如，泄漏敏感数据的应用)。举另一个例子，该移动计算设备可以警告其它移动计算设备(例如，在该移动计算设备附近的或者通过通信介质可到达的设备等等)关于部署的资源和相应恶意行为。这些其它设备可以选择针对类似的这些设置监听各自的本

地应用。

[0084] 在判定框624中，该移动计算设备的处理器可以确定是否存在要监听的任何其它潜在恶意应用。作为对确定存在要监听的其它潜在恶意应用(即，判定框624＝“是”)的响应，该移动计算设备可以在方框606中选择另一个目标应用来监听并且聚焦在该应用上继续进行方法600的操作。作为对确定没有其它潜在恶意应用要监听(即，判定框624＝“否”)的响应，该移动计算设备可以结束方法600。

[0085] 各种形式的移动计算设备，包括个人计算机和膝上型计算机，可以用于实现各种实现。这些计算设备典型地包括图7中示出的部件，其示出示例性智能移动计算设备700。

[0086] 在各种实施方式中，该移动计算设备700可以包括耦合到触摸屏控制704和内部存储器702的处理器701。该处理器701可以是针对一般或专用处理任务指定的一个或多个多核IC。内部存储器702可以是易失性和/或非易失性存储器，并且也可以是安全的和/或加密的存储器，或者不安全的和/或未加密的存储器，或者它们的任意组合。该触摸屏控制器704和处理器701也可以耦合到触摸屏面板712，诸如电阻传感触摸屏、电容传感触摸屏、红外传感触摸屏等等。

[0087] 移动计算设备700可以具有相互耦合和/或耦合到该处理器701的一个或多个无线信号收发机708(例如，蓝牙、ZigBee®、Wi-Fi、射频(RF)收发机)和天线710，用于发送和接收。收发机708和天线710可以与上述电路一起使用以便实现各种无线传输协议栈和接口。该移动计算设备700可以包括能够通过蜂窝网络通信并且耦合到该处理器的蜂窝网络无线调制解调器芯片716。

[0088] 该移动计算设备700可以包括耦合到该处理器701的外围设备连接接口718。该外围设备连接接口718可以唯一地配置为接受一个类型的连接，或者多重地配置为接受各种类型的公共的或私有的物理和通信连接，诸如USB、火线接口、闪电接口或PCI。该外围设备连接接口718也可以耦合到类似配置的外围设备连接端口(未示出)。

[0089] 该移动计算设备700还可以包括用于提供音频输出的扬声器714。该移动计算设备700还可以包括由塑料、金属或合成材料构造的外壳720，用于容纳本申请中讨论的所有或一些部件。该移动计算设备700可以包括耦合到处理器701的电源722，诸如一次性的或可充电的电池。可充电电池也可以耦合到外围设备连接端口以便从该移动计算设备700外部的电源接收充电电流。

[0090] 示出和描述的各个实现仅仅是作为示例提供的，以便解释说明权利要求的各个属性。但是，关于任何给定实现示出并描述的属性并不必须仅限于相关联的实现，而是可以示出和描述的其它实现一起使用或组合起来。此外，权利要求并不意在受到任何一个示例性实现的限制。

[0091] 本申请中描述的各种处理器可以是能够由软件指令(应用)配置为执行各种功能(包括本申请中描述的各个实现的功能)的任何可编程微处理器、微计算机或多处理器芯片或芯片组。在各个设备中，可以提供多个处理器，比如专用于无线通信功能的一个处理器和专用于运行其它应用的一个处理器。通常，软件应用可以在它们被访问并载入到处理器中之前存储在内部存储器中。在一些设备中，所述处理器可以包括足够存储该应用软件指令的内部存储器。在很多设备中，该内部存储器可以是易失性的或非易失性的存储器，比如闪存或它们的混合。为了这一说明书的目的，对存储器的一般引用指的是可由处理器访问的

存储器，包括内部存储器或插入到各种设备的移动存储器和处理器内部的存储器。

[0092] 上述方法描述和处理流程图仅仅作为示例性示例提供，而并不意在要求或暗示各个实现的操作必须以示出的顺序执行。本领域的技术人员应该了解的是，上述实现中的操作顺序可以用任何顺序执行。比如像“之后”、“然后”、“接下来”等术语并不意在限制操作的顺序；这些术语仅仅用于贯穿方法描述引导读者。此外，任何以单数形式对声明单元的引用，例如使用冠词“a”、“an”或“the”并不能解释为将该单元限制为单数。

[0093] 结合本申请中公开的实现所描述的各种示例性的逻辑框、模块、电路和算法操作可以实现成电子硬件、计算机软件或其组合。为了清楚地示出硬件和软件之间的可交换性，上面对各种示例性的部件、方框、模块、电路和操作已经围绕其各自功能进行了总体描述。至于这种功能是实现成硬件还是实现成软件，取决于特定的应用和对整个系统所施加的设计约束条件。熟练的技术人员可以针对每个特定应用，以变通的方式实现所描述的功能，但是，这种实现决策不应解释为背离本发明权利要求的保护范围。

[0094] 用于执行本申请所述功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑设备、分立门或者晶体管逻辑器件、分立硬件部件或者其任意组合，可以实现或执行用于实现结合本申请公开实现描述的各种示例性的逻辑、逻辑框图、模块和电路的硬件。通用处理器可以是微处理器，或者，该处理器也可以是任何处理器、控制器、微控制器或者状态机。处理器还可以实现为计算设备的组合，例如，DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合，或者任何其它此种结构。另外，一些操作或方法可以由专用于给定功能的电路执行。

[0095] 在包括方法600的各种实现中，所描述的功能可以用硬件、软件、固件，或其任意结合来实现。如果在软件中实现，功能可以作为一条或多个指令或代码存储在永久性处理器可读、计算机可读或服务器可读介质或永久性处理器可读存储介质上或通过其发送。本申请中公开的方法或算法的操作可以实现在处理器可执行软件模块或处理器可执行软件指令中，其可以驻留在永久性计算机可读存储介质、永久性服务器可读存储介质和/或永久性处理器口存储介质上。在各个实现中，这些指令可以是存储的处理可执行指令或存储的处理器可执行软件指令。有形的、永久性计算机可读存储介质可以是计算机可访问的任何可用存储介质。举个例子，但是并不作为限制，这种永久性计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储器、磁盘存储器或其它磁存储设备，或可以用于以指令或数据结构的形式存储期望的程序代码并可以由计算机访问的任何其它介质。本申请中所用的磁盘和光盘，包括压缩光盘(CD)、激光盘、光盘、数字多功能光盘(DVD)、软盘和蓝光盘，其中，磁盘通常磁性地复制数据，而光盘则用激光光学地复制数据。上述的结合也应该包含在永久性计算机可读介质的范围内。另外，方法或算法的操作可以作为永久性处理器可读介质和/或有形的永久性处理器可读存储介质和/或计算机可读介质上的代码和/或指令的一个或任何组合或集合，其可以整合到计算机程序产品中。

[0096] 提供前面对公开实现的描述以便使本领域的任何技术人员能够制作或使用本权利要求的技术。对这些技术的修改对于本领域的技术人员来说是显而易见的，并且本申请中定义的一般原则可以在不脱离本发明的精神或范围的前提下应用于其它实现。因此，本公开内容并不意在限制本申请中示出的实现，而是与下面的权利要求和本申请中公开的原则和新颖性特征保持最广泛范围的一致。

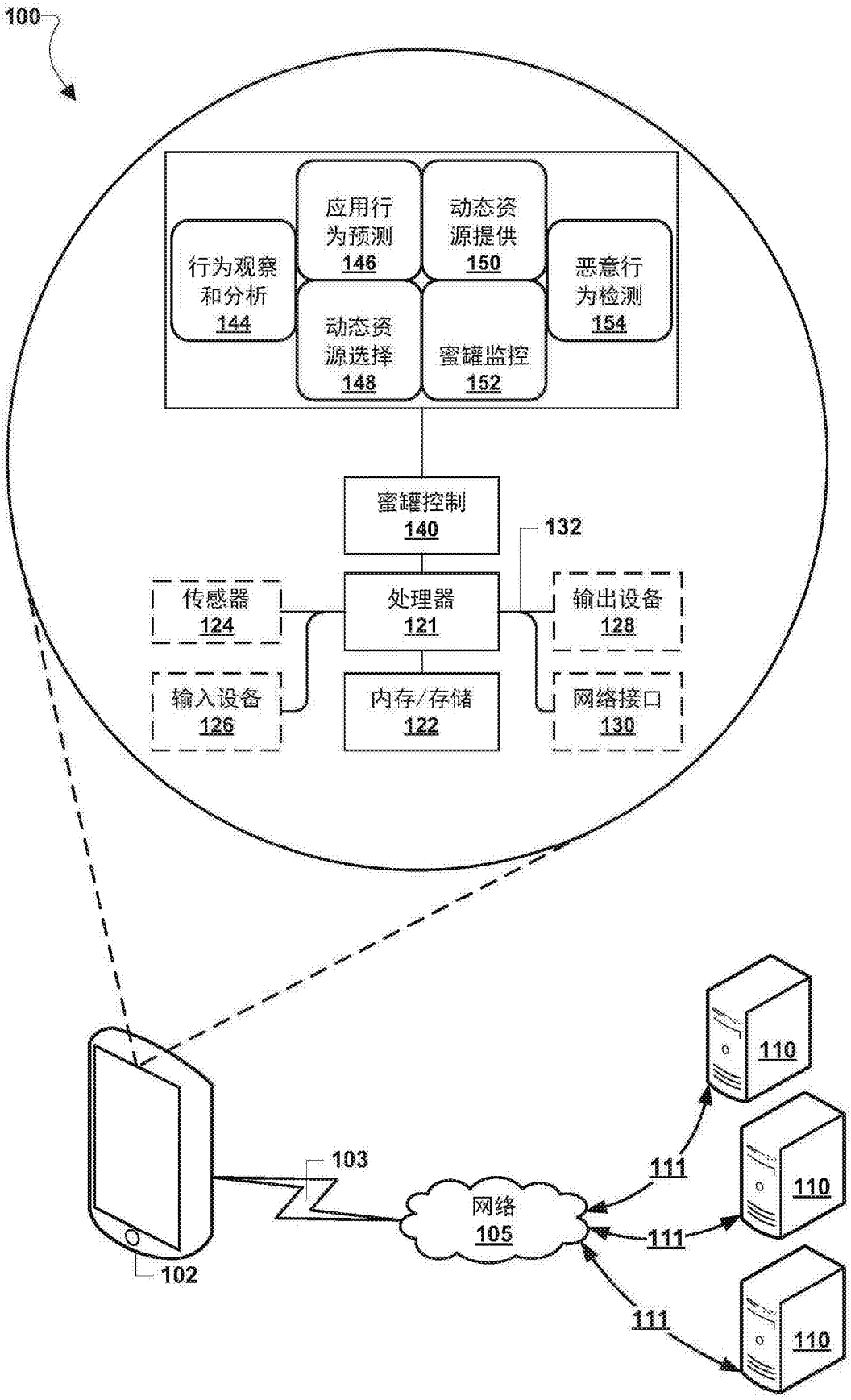

100
应用行为预测 146
动态资源提供 150
行为观察和分析 144
恶意行为检测 154
动态资源选择 148
蜜罐监控 152
蜜罐控制 140
132
传感器 124
处理器 121
输出设备 128
输入设备 126
内存/存储 122
网络接口 130
110
110
110
111
111
111
103
网络 105
102

图1

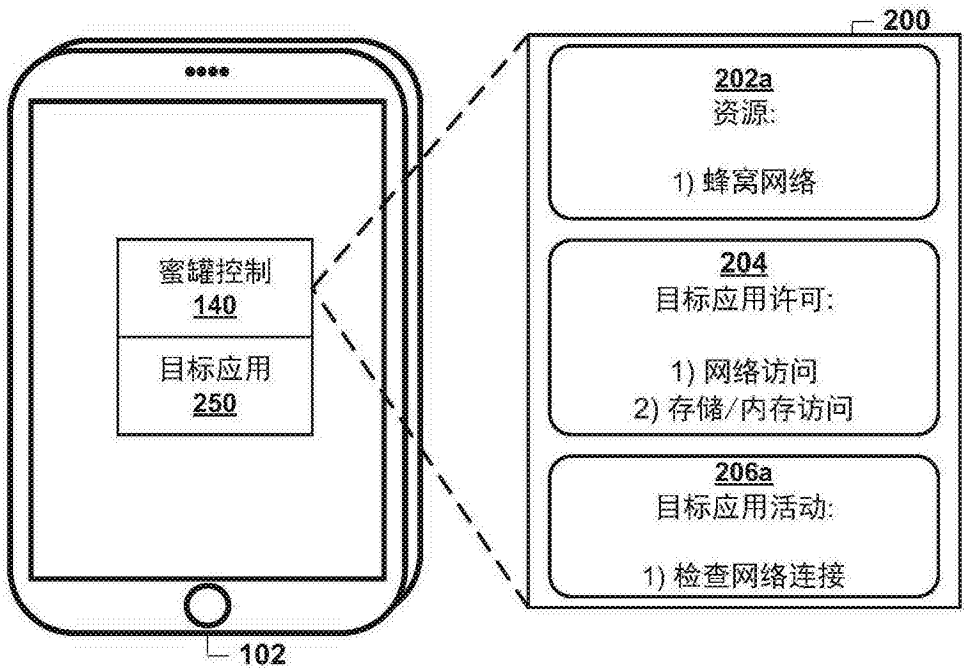

200
202a
资源:
1) 蜂窝网络
204
目标应用许可:
1) 网络访问
2) 存储/内存访问
206a
目标应用活动:
1) 检查网络连接
蜜罐控制
140
目标应用
250
102

图2

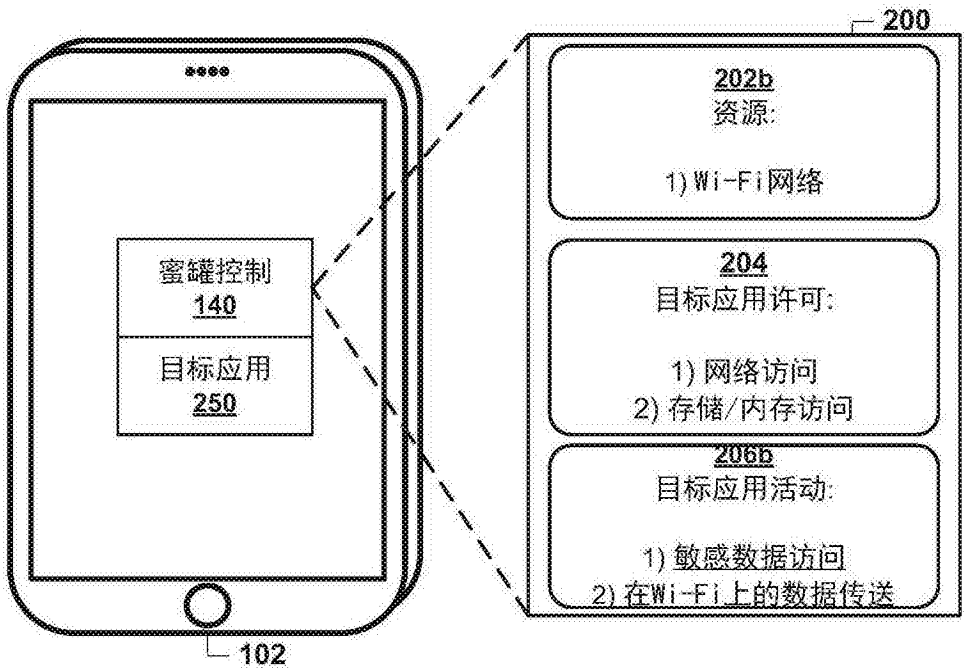

200
202b
资源:
1) Wi-Fi网络
204
目标应用许可:
1) 网络访问
2) 存储/内存访问
206b
目标应用活动:
1) 敏感数据访问
2) 在Wi-Fi上的数据传送
蜜罐控制
140
目标应用
250
102

图3

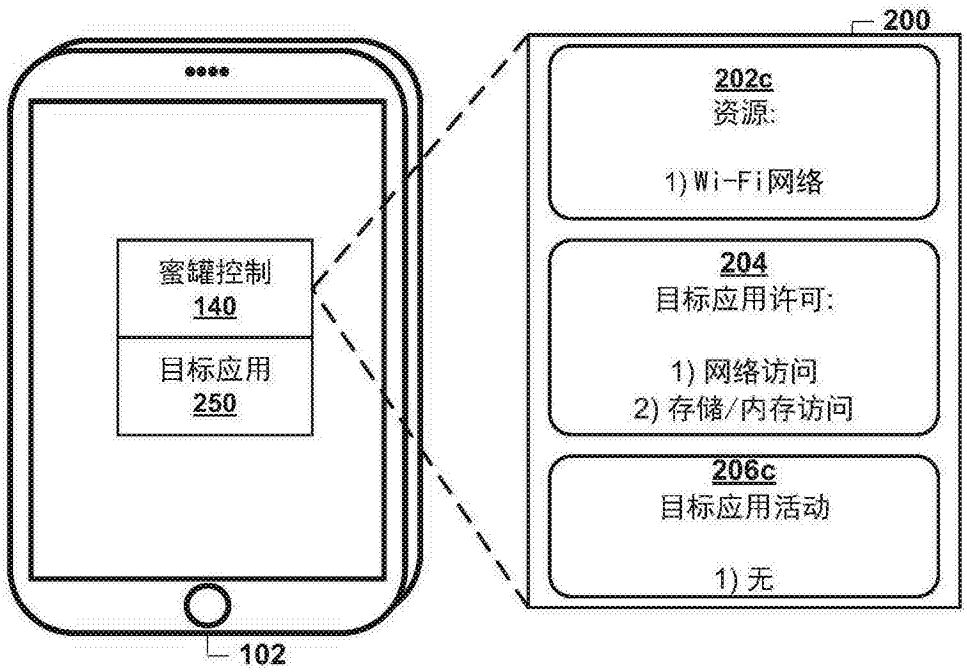

200
202c
资源:
1) Wi-Fi网络
204
目标应用许可:
1) 网络访问
2) 存储/内存访问
206c
目标应用活动
1) 无
蜜罐控制
140
目标应用
250
102

图4

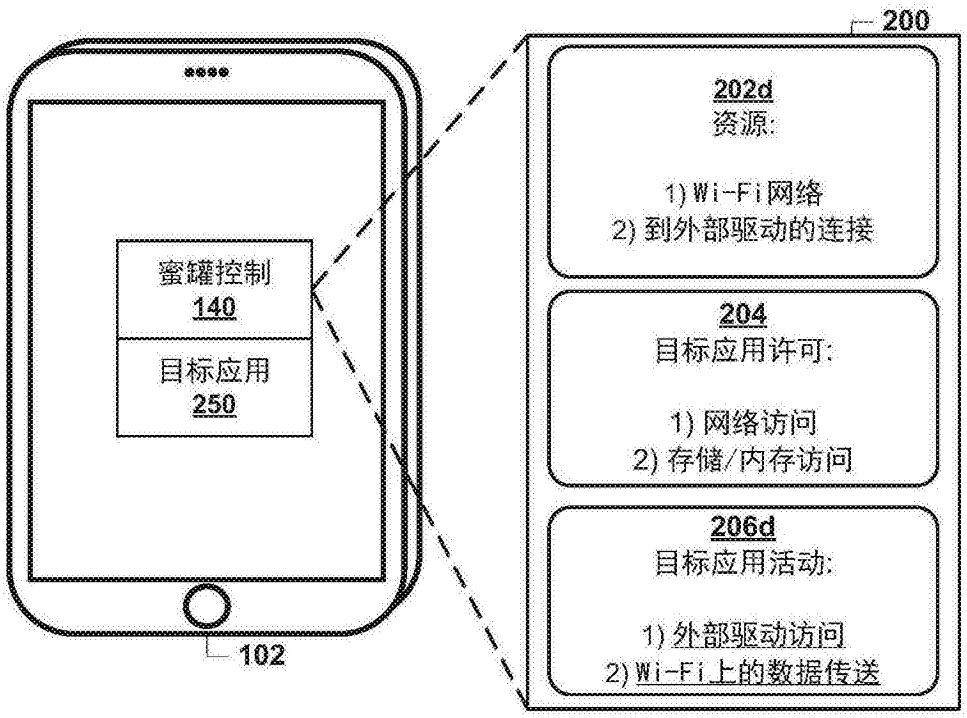

200
202d
资源:
1) Wi-Fi网络
2) 到外部驱动的连接
204
目标应用许可:
1) 网络访问
2) 存储/内存访问
206d
目标应用活动:
1) 外部驱动访问
2) Wi-Fi上的数据传送
蜜罐控制
140
目标应用
250
102

图5

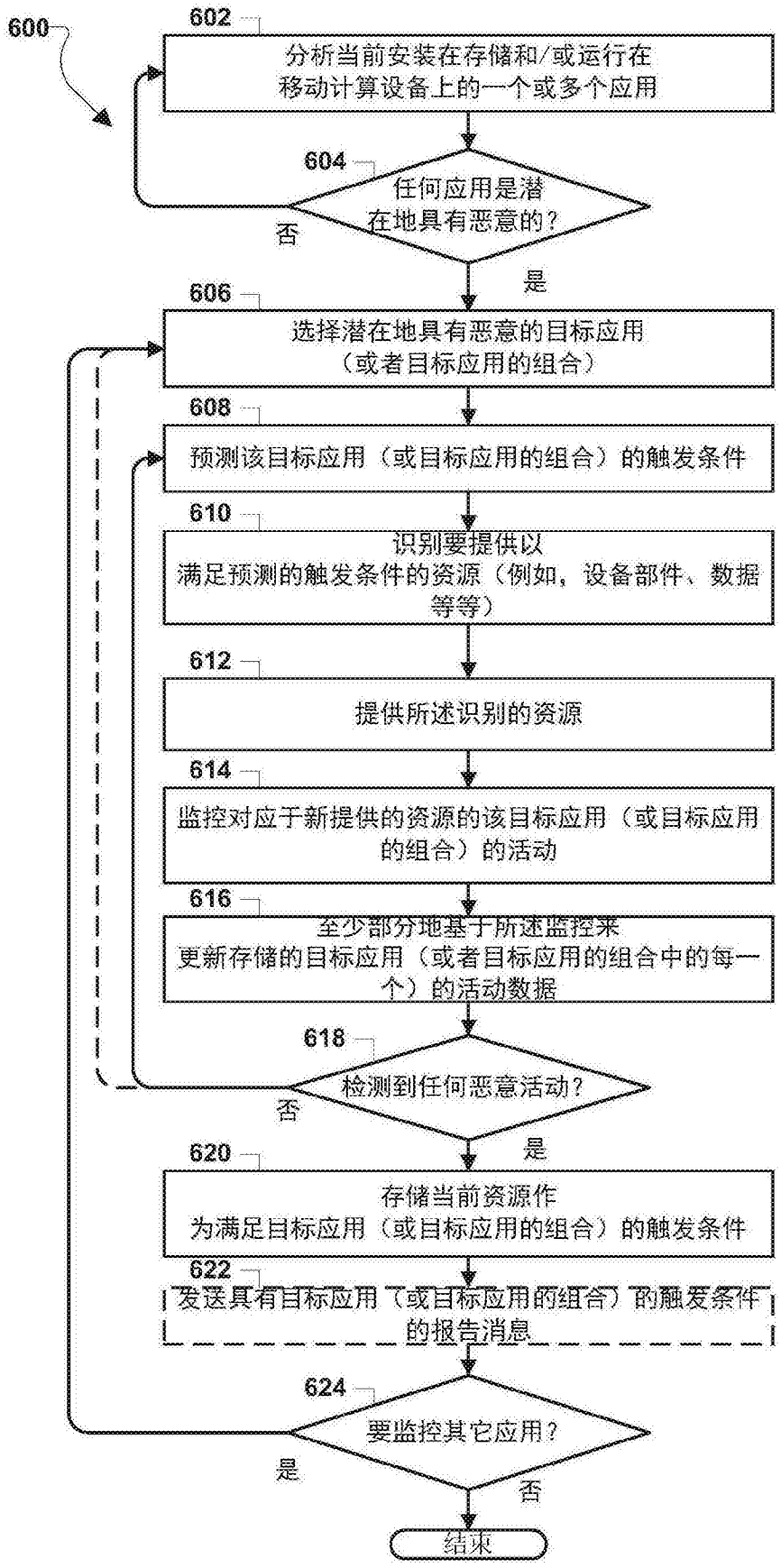

600
602
分析当前安装在存储和/或运行在移动计算设备上的一个或多个应用
604
任何应用是潜在地具有恶意的？
否
是
606
选择潜在地具有恶意的目标应用（或者目标应用的组合）
608
预测该目标应用（或目标应用的组合）的触发条件
610
识别要提供以满足预测的触发条件的资源（例如，设备部件、数据等等）
612
提供所述识别的资源
614
监控对应于新提供的资源的该目标应用（或目标应用的组合）的活动
616
至少部分地基于所述监控来更新存储的目标应用（或者目标应用的组合中的每一个）的活动数据
618
检测到任何恶意活动？
否
是
620
存储当前资源作为满足目标应用（或目标应用的组合）的触发条件
622
发送具有目标应用（或目标应用的组合）的触发条件的报告消息
624
要监控其它应用？
是
否
结束

图6

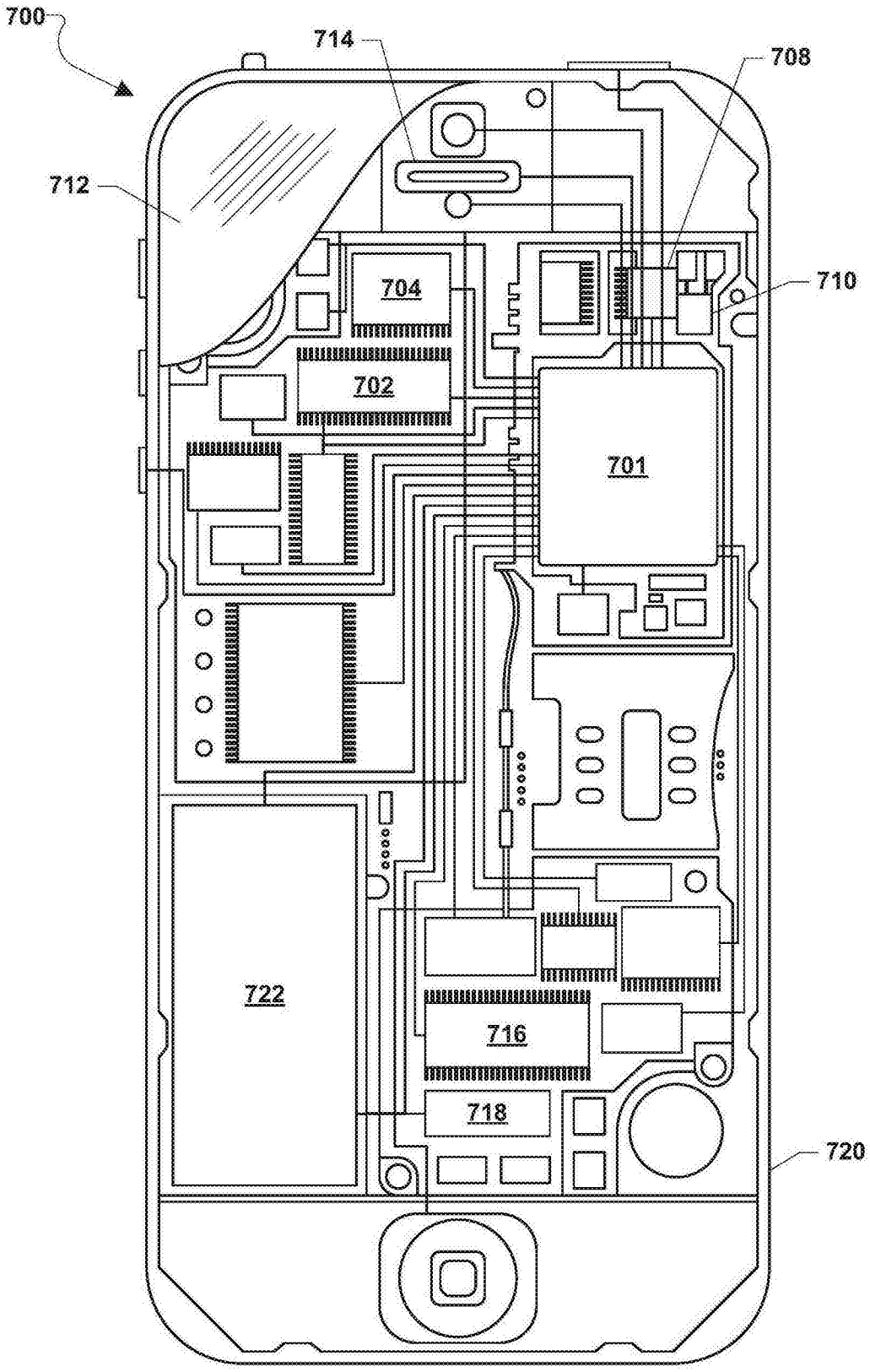


图7