(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107209818 B
(45)授权公告日 2020.09.29

(21)申请号 201680006328.1
(22)申请日 2016.01.11
(65)同一申请的已公布的文献号
申请公布号 CN 107209818 A
(43)申请公布日 2017.09.26
(30)优先权数据
14/616,046 2015.02.06 US
(85)PCT国际申请进入国家阶段日
2017.07.19
(86)PCT国际申请的申请数据
PCT/US2016/012851 2016.01.11
(87)PCT国际申请的公布数据
WO2016/126379 EN 2016.08.11
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 陈茵 尹曼奇 维纳伊·斯里达拉
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 杨林勳
(51)Int.Cl.
G06F 21/31(2013.01)
(56)对比文件
US 2014150100 A1,2014.05.29
US 2013304677 A1,2013.11.14
WO 2010105249 A1,2010.09.16
US 2009199296 A1,2009.08.06
US 2013247187 A1,2013.09.19
CN 103797492 A,2014.05.14
审查员 李华芳

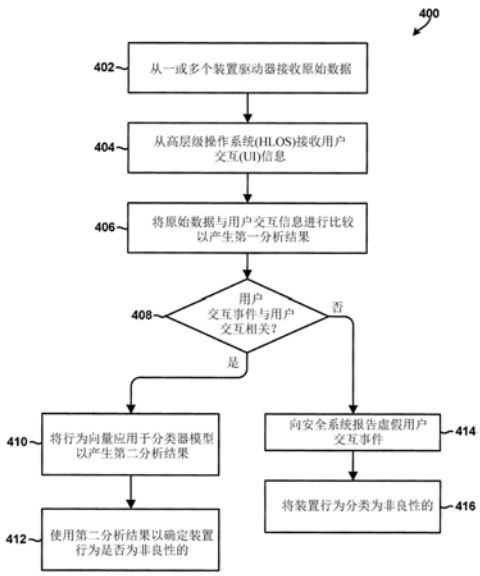
权利要求书4页 说明书23页 附图10页

(54)发明名称

用于检测与移动装置的虚假用户交互以用于改进的恶意软件防护的方法和系统

(57)摘要

一种计算装置处理器可以处理器可执行指令配置以实施检测和响应于虚假用户交互UI事件的方法。所述处理器可通过与由高层级操作系统产生或接收的用户交互事件信息结合而分析由一或多个硬件驱动器产生的原始数据来确定用户交互事件是否为虚假用户交互事件。另外，所述处理器可以处理器可执行指令配置以实施使用行为分析和机器学习技术以基于所检测用户交互事件是真实还是虚假用户交互事件而识别、防止、校正或以其它方式响应于计算装置的恶意或性能降级的行为的方法。



CN 107209818 B

1.一种分析在计算装置上操作的软件应用程序的活动的方法,其包括:

监视在所述计算装置上操作的软件应用程序的活动;

确定所监视的所述活动是否直接或固有地涉及某一形式的用户交互;

响应于确定所监视的所述活动涉及用户交互而确定是否存在对应于所监视的所述活动的用户交互事件;

从所述计算装置的传感器收集原始数据;

与关联于所检测用户交互事件的用户交互事件信息结合而分析所收集的所述原始数据以产生分析结果;

基于所产生的所述分析结果而确定所述所检测用户交互事件是否与所述计算装置的用户相关;

响应于基于所产生的所述分析结果确定所述所检测用户交互事件与所述计算装置的所述用户相关而将所述所检测用户交互事件分类为真实用户交互事件;

响应于基于所产生的所述分析结果确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述所检测用户交互事件分类为虚假用户交互事件;以及

基于所述所检测用户交互事件的所述分类而确定所述软件应用程序的所监视的所述活动是否为非良性的。

2.根据权利要求1所述的方法,其中接收所述用户交互事件信息包括从所述计算装置的高层级操作系统接收所述用户交互事件信息。

3.根据权利要求1所述的方法,其中基于所述所检测用户交互事件的所述分类而确定所述软件应用程序的所述活动是否为非良性的包括:

响应于确定所述所检测用户交互事件被分类为所述虚假用户交互事件而将所述软件应用程序的所述活动分类为非良性的。

4.根据权利要求1所述的方法,其进一步包括:

产生表征所述软件应用程序的所述活动的行为向量;

响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述行为向量应用于包含决策节点的分类器模型,所述决策节点评估是否存在对应于所述活动的用户交互事件;以及

基于将所述行为向量应用于所述分类器模型的结果而确定所述软件应用程序的所述活动是否为非良性的。

5.根据权利要求1所述的方法,其进一步包括:

产生表征所述软件应用程序的所述活动的行为向量;

响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而选择不包含决策节点的分类器模型,所述决策节点测试是否存在对应于所述活动的用户交互事件;

将所述行为向量应用于选定的所述分类器模型以产生额外分析结果;以及

基于所述额外分析结果而确定所述软件应用程序的所述活动是否为非良性的。

6.根据权利要求1所述的方法,其进一步包括:

响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而选择一系列稳健分类器模型;以及

将多个行为向量应用于选定的所述一系列稳健分类器模型中的一或多个分类器模型

以确定所述软件应用程序的所述活动是否为非良性的。

7.根据权利要求1所述的方法，其进一步包括将从所述计算装置的第一传感器接收的所述原始数据与从所述计算装置的第二传感器接收的所述原始数据进行比较以确定从所述第一传感器接收的所述原始数据是否与从所述第二传感器接收的所述原始数据一致，其中基于所收集的所述原始数据和所接收的所述用户交互事件信息而产生分析结果的所述操作是响应于确定从所述第一传感器接收的所述原始数据与从所述第二传感器接收的所述原始数据一致而执行。

8.根据权利要求7所述的方法，其中将从所述第一传感器接收的所述原始数据与从所述第二传感器接收的所述原始数据进行比较包括比较将行为向量应用于分类器模型的结果。

9.根据权利要求1所述的方法，其中：

从所述计算装置的所述传感器收集所述原始数据包括从用户输入传感器收集所述原始数据；且

接收所述用户交互事件信息包括从用于所述用户输入传感器的驱动器接收数据。

10.根据权利要求1所述的方法，其进一步包括：

产生表征所述软件应用程序的所述活动的行为向量；

响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述行为向量应用于不包含决策节点的分类器模型，所述决策节点评估涉及与所述计算装置的用户交互的条件；以及

基于将所述行为向量应用于所述分类器模型的结果而确定所述软件应用程序的所述活动是否为非良性的。

11.一种计算装置，其包括：

用于监视在所述计算装置上操作的软件应用程序的活动的装置；

用于确定所监视的所述活动是否直接或固有地涉及某一形式的用户交互的装置；

用于响应于确定所监视的所述活动涉及用户交互而确定是否存在对应于所监视的所述活动的用户交互事件的装置；

用于从所述计算装置的传感器收集原始数据的装置；

用于与关联于所检测用户交互事件的用户交互事件信息结合而分析所收集的所述原始数据以产生分析结果的装置；

用于基于所产生的所述分析结果而确定所述所检测用户交互事件是否与所述计算装置的用户相关的装置；

用于响应于基于所产生的所述分析结果确定所述所检测用户交互事件与所述计算装置的所述用户相关而将所述所检测用户交互事件分类为真实用户交互事件的装置；

用于响应于基于所产生的所述分析结果确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述所检测用户交互事件分类为虚假用户交互事件的装置；以及

用于基于所述所检测用户交互事件的所述分类而确定软件应用程序的所监视的所述活动是否为非良性的装置。

12.根据权利要求11所述的计算装置，其中用于接收所述用户交互事件信息的装置包括用于从高层级操作系统接收所述用户交互事件信息的装置。

13.根据权利要求11所述的计算装置,其中用于基于所述所检测用户交互事件的所述分类而确定所述软件应用程序的所述活动是否为非良性的装置进一步包括用于响应于确定所述所检测用户交互事件被分类为所述虚假用户交互事件而将所述软件应用程序的所述活动分类为非良性的装置。

14.根据权利要求11所述的计算装置,其进一步包括:

用于产生表征所述软件应用程序的所述活动的行为向量的装置;

用于响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述行为向量应用于包含决策节点的分类器模型的装置,所述决策节点评估是否存在对应于所述活动的用户交互事件;以及

用于基于将所述行为向量应用于所述分类器模型的结果而确定所述软件应用程序的所述活动是否为非良性的装置。

15.根据权利要求11所述的计算装置,其进一步包括:

用于产生表征所述软件应用程序的所述活动的行为向量的装置;

用于响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而选择不包含决策节点的分类器模型的装置,所述决策节点测试是否存在对应于所述活动的用户交互事件;

用于将所述行为向量应用于选定的所述分类器模型以产生额外分析结果的装置;以及

用于基于所述额外分析结果而确定所述软件应用程序的所述活动是否为非良性的装置。

16.根据权利要求11所述的计算装置,其进一步包括:

用于响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而选择一系列稳健分类器模型的装置;以及

用于将多个行为向量应用于选定的所述一系列稳健分类器模型中的一或多个分类器模型以确定所述软件应用程序的所述活动是否为非良性的装置。

17.一种计算装置,其包括:

处理器,其以处理器可执行指令配置以进行以下操作:

监视在所述计算装置上操作的软件应用程序的活动;

确定所监视的所述活动是否直接或固有地涉及某一形式的用户交互;

响应于确定所监视的所述活动涉及用户交互而确定是否存在对应于所监视的所述活动的用户交互事件;

从所述计算装置的传感器收集原始数据;

与关联于所检测用户交互事件的用户交互事件信息结合而分析所收集的所述原始数据以产生分析结果;

基于所产生的所述分析结果而确定所述所检测用户交互事件是否与所述计算装置的用户相关;

响应于基于所产生的所述分析结果确定所述所检测用户交互事件与所述计算装置的所述用户相关而将所述所检测用户交互事件分类为真实用户交互事件;

响应于基于所产生的所述分析结果确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述所检测用户交互事件分类为虚假用户交互事件;以及

基于所述所检测用户交互事件的所述分类而确定软件应用程序的所监视的所述活动是否为非良性的。

18.根据权利要求17所述的计算装置，其中所述处理器以处理器可执行指令配置以通过从高层级操作系统接收所述用户交互事件信息而接收所述用户交互事件信息。

19.根据权利要求17所述的计算装置，其中所述处理器以处理器可执行指令配置以通过响应于确定所述所检测用户交互事件被分类为所述虚假用户交互事件将所述软件应用程序的所述活动分类为非良性的而基于所述所检测用户交互事件的所述分类确定所述软件应用程序的所述活动是否为非良性的。

20.根据权利要求17所述的计算装置，其中所述处理器以处理器可执行指令配置以进行以下操作：

产生表征所述软件应用程序的所述活动的行为向量；

响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而将所述行为向量应用于包含决策节点的分类器模型，所述决策节点评估是否存在对应于所述活动的用户交互事件；以及

基于将所述行为向量应用于所述分类器模型的结果而确定所述软件应用程序的所述活动是否为非良性的。

21.根据权利要求17所述的计算装置，其中所述处理器以处理器可执行指令配置以执行进一步包括以下各项的操作：

产生表征所述软件应用程序的所述活动的行为向量；

响应于确定所述用户交互事件不与所述计算装置的所述用户相关而选择不包含决策节点的分类器模型，所述决策节点测试是否存在对应于所述活动的用户交互事件；

将所述行为向量应用于选定的所述分类器模型以产生额外分析结果；以及

基于所述额外分析结果而确定所述软件应用程序的所述活动是否为非良性的。

22.根据权利要求17所述的计算装置，其中所述处理器以处理器可执行指令配置以执行进一步包括以下各项的操作：

响应于确定所述所检测用户交互事件不与所述计算装置的所述用户相关而选择一系列稳健分类器模型；以及

将多个行为向量应用于选定的所述一系列稳健分类器模型中的一或多个分类器模型以确定所述软件应用程序的所述活动是否为非良性的。

23.一种非暂时性计算机可读存储媒体，其具有存储于其上的处理器可执行指令，所述处理器可执行指令经配置以致使计算装置的处理器根据权利要求1-10中的任一项执行操作。

用于检测与移动装置的虚假用户交互以用于改进的恶意软件防护的方法和系统

背景技术

[0001] 近几年来，蜂窝技术和无线通信技术迅猛发展。无线服务供应商现在提供大量特征和服务，所述特征和服务向其用户提供对信息、资源及通信的前所未有的水平的存取。为了与这些增强保持同步，个人和消费型电子装置(例如，蜂窝式电话、手表、头戴受话器、远程控件等)变得前所未有的强大和复杂，且现在所述电子装置通常包括强力的处理器、大型存储器和允许在它们的装置上执行复杂和强力的软件应用程序的其它资源。

[0002] 由于这些和其它改进，个人和消费型电子装置在现代生活中变得普遍存在，且具有对由其用户产生或涉及其用户的信息的前所未有的存取水平。另外，人们频繁地使用其装置来存储敏感信息(例如，信用卡信息、联系人等)和/或实现安全性重要的任务。举例来说，移动装置用户频繁地使用他们的装置来购买货物、发送和接收敏感通信、支付账单、管理银行账户并且进行其它涉密交易。由于这些趋势，个人和消费型电子装置快速地变成恶意软件和网络攻击的下一前线。因而，更好的保护资源受限制的计算装置(例如，移动和无线装置)的新的且改进的安全解决方案将有利于消费者。

发明内容

[0003] 各种实施例包含一种分析在计算装置上操作的软件应用程序的活动的方法，其包含：将从所述计算装置的用户输入装置接收的原始数据与在所述计算装置中接收的用户交互事件信息进行比较以产生分析结果；以及使用所述产生的分析结果以确定用户交互(UI)事件是否与所述计算装置的用户相关。在另一实施例中，从所述用户输入装置接收的所述原始数据可包含从装置驱动器接收的原始数据，且在所述计算装置中接收的所述用户交互事件信息可包含从所述计算装置的高层级操作系统接收的交互信息。

[0004] 在另一实施例中，所述方法可包含响应于确定所述用户交互事件不与所述计算装置的用户相关而将所述软件应用程序的所述活动分类为非良性的。在另一实施例中，所述方法可包含：产生表征所述软件应用程序的所述活动的行为向量；响应于确定所述用户交互事件不与所述计算装置的用户相关而将所述产生的行为向量应用于可包含决策节点的分类器模型，所述决策节点评估是否存在对应于所述活动的用户交互事件；以及使用将所述产生的行为向量应用于所述分类器模型的结果以确定所述软件应用程序的所述活动是否为非良性的。

[0005] 在另一实施例中，所述方法可包含：产生表征所述软件应用程序的所述活动的行为向量；响应于确定所述用户交互事件不与所述计算装置的用户相关而选择不包含决策节点的分类器模型，所述决策节点测试是否存在对应于所述活动的用户交互事件；将所述产生的行为向量应用于所述选定分类器模型以产生额外分析结果；以及使用所述产生的额外分析结果以确定所述软件应用程序的所述活动是否为非良性的。

[0006] 在另一实施例中，所述方法可包含：响应于确定所述用户交互事件不与所述计算装置的用户相关而选择一系列稳健分类器模型；以及将多个行为向量应用于所述选定系列

的稳健分类器模型以确定所述软件应用程序的所述活动是否为非良性的。在另一实施例中，所述方法可包含：将从所述计算装置的第一传感器接收的原始数据与从所述计算装置的第二传感器接收的原始数据进行比较以确定从所述第一传感器接收的所述原始数据是否与从所述第二传感器接收的所述原始数据一致，其中将从所述计算装置的所述用户输入装置接收的原始数据与在所述计算装置中接收的所述用户交互事件信息进行比较以产生所述分析结果是响应于确定从所述第一传感器接收的所述原始数据与从所述第二传感器接收的所述原始数据一致而执行的。

[0007] 在另一实施例中，将从所述第一传感器接收的原始数据与从所述第二传感器接收的所述原始数据进行比较可包含比较将行为向量应用于分类器模型的结果。在另一实施例中，从所述用户输入装置接收的所述原始数据可包含从用户输入传感器接收的原始数据；在所述计算装置中接收的所述用户交互事件信息可包含从用于所述用户输入传感器的装置驱动器接收的数据；且使用所述产生的分析结果以确定所述用户交互事件是否与所述计算装置的用户相关可包含响应于从所述用户输入传感器接收的所述原始数据不相关于从用于所述用户输入传感器的所述装置驱动器接收的所述数据而确定所述用户交互事件不与所述计算装置的用户相关。

[0008] 在另一实施例中，所述用户输入传感器可包含触摸屏，且所述装置驱动器可包含触摸屏装置驱动器。在另一实施例中，所述方法可包含响应于确定所述用户交互事件不与所述计算装置的用户相关而将所述软件应用程序的所述活动分类为非良性的。在另一实施例中，所述方法可包含：产生表征所述软件应用程序的所述活动的行为向量；响应于确定所述用户交互事件不与所述计算装置的用户相关而将所述产生的行为向量应用于不包含决策节点的分类器模型，所述决策节点评估涉及与所述计算装置的用户交互的条件；以及使用将所述产生的行为向量应用于所述分类器模型的结果以确定所述软件应用程序的所述活动是否为非良性的。

[0009] 另外的实施例可包含计算装置，其具有处理器，所述处理器以处理器可执行指令配置以执行对应于上文所论述的方法的各种操作。

[0010] 另外的实施例可包含具有用于执行对应于上文所论述的方法操作的功能的各种装置的计算装置。

[0011] 其它实施例可包含非暂时性处理器可读存储媒体，所述非暂时性处理器可读存储媒体在其上存储有处理器可执行指令，所述处理器可执行指令经配置以致使处理器执行对应于上文所论述的方法操作的各种操作。

附图说明

[0012] 并入本文中并且构成本说明书一部分的随附图式展示本发明的示范性实施例，并且与上文给出的一般描述和下文给出的详细描述一起用来解释本发明的特征。

[0013] 图1是适合于实施各种实施例的实例芯片上系统的架构图式。

[0014] 图2是说明根据各种实施例在一实施例计算装置中的实例逻辑组件和信息流的框图，所述计算装置包含经配置以识别且响应于虚假用户交互(UI)事件的虚假UI事件检测模块。

[0015] 图3是说明在一实施例计算装置中的实例逻辑组件和信息流的框图，所述计算装

置经配置以确定特定移动装置行为是否为良性或非良性的。

[0016] 图4A和4B是说明根据各种实施例检测且响应于虚假UI事件的方法的过程流程图。

[0017] 图4C是说明根据一实施例检测且响应于泄密的用户输入传感器装置驱动器的方法的过程流程图。

[0018] 图5是说明根据一实施例使用一系列分类器模型对装置行为进行分类的方法的过程流程图。

[0019] 图6是可产生且用以产生分类器模型的实例决策节点的图示。

[0020] 图7是说明根据一实施例执行自适应观测的方法的过程流程图。

[0021] 图8是适合于在一实施例中使用的移动装置的组件框图。

具体实施方式

[0022] 将参看随附图式详细描述各种实施例。只要可能，便将在图式中使用相同参考标号来指代相同或相似部分。对特定实例和实施方案进行的参考是用于说明性目的，且不希望限制本发明或权利要求书的范围。

[0023] 概括来说，各种实施例包含使用基于行为且机器学习的技术来检测且响应于虚假用户交互(UI)事件的方法以及经配置以实施所述方法的计算装置。在实施例中，计算装置可经配置以实施与由高层级操作系统产生或接收的UI信息结合而分析由一或多个硬件驱动器或用户输入装置产生的原始数据的方法，且使用此分析的结果来确定UI事件是否与计算装置的用户相关和/或将所检测UI事件分类为真实UI事件或虚假UI事件。所述计算装置还可包含综合的基于行为的安全系统，其经配置以基于UI事件是否为真实或虚假UI事件而识别且响应于非良性装置行为(例如，由恶意或使性能降级的软件应用程序等造成的行为)。

[0024] 大体上，每一软件应用程序在计算装置上执行多个任务或活动。一些应用程序任务/活动直接或固有地涉及或需要与装置的某一形式的用户交互。举例来说，相机的使用、激活麦克风以记录音频以及发送优质短消息服务(SMS)消息是涉及与装置的某一形式的用户交互的所有任务/活动，例如用户致动相机的快门释放按钮，按压记录按钮以激活麦克风，键入文字且触摸发送按钮以发送SMS消息等等。

[0025] 与装置的大多数用户交互将致使计算装置产生一或多个UI事件(例如，View::onTouchEvent、onKeyDown、onKeyUp、onTrackBallEvent等等)。举例来说，触摸计算装置的电子触摸屏显示器可致使装置驱动器产生“触摸事件”，其识别触摸的区域(例如，经由矩形坐标X和Y等等)。操作系统可从装置驱动器接收UI事件(例如，“触摸事件”)，且作为响应而执行UI事件相关的软件应用程序的程序。

[0026] 因此，一些任务/活动直接或固有地涉及或需要某一形式的用户交互，且大多数用户交互产生某一形式的UI事件。因此，不具有对应UI事件的应用程序的某些任务/活动的执行可能是所述应用程序为非良性或另外应得到更靠近的审查、监视或分析的强指示符。因此，在一些实施例中，计算装置的基于行为的安全系统可经配置以对直接或固有地涉及或需要用户交互但并不与UI事件相关联的活动分类为可疑或非良性。举例来说，在实施例中，基于行为的安全系统可经配置以监视软件应用程序的活动，确定所监视活动(例如，相机的使用等)是否直接或固有地涉及或需要某一形式的用户交互，响应于确定所监视活动直接

或固有地涉及或需要用户交互而确定是否存在对应于所监视活动的UI事件(例如，onTouchEvent等)，且响应于确定所监视直接或固有地涉及或需要用户交互且不存在对应于所监视活动的UI事件而将所述应用程序分类为非良性(或需要更靠近的审查、较详细的分析等)。

[0027] 基于行为的安全系统大体上有效于识别非良性行为且防止装置随时间的性能和电力利用水平的降级。举例来说，通过使用UI事件信息作为活动或软件应用程序是否为非良性的指示符，基于行为的安全系统允许计算装置识别且响应于非良性装置行为(例如，恶意软件应用程序等)而不会消耗过量的其处理、存储器或电池资源。因此，基于行为的安全系统较适合于包含在移动装置和资源受限制的计算装置中且在移动装置和资源受限制的计算装置中使用，所述资源受限制的计算装置例如智能电话，其具有有限的资源、通过电池电力运行且性能和安全是重要的。

[0028] 虽然上述系统是大体上有效的，但恶意软件应用程序可能通过产生且发送虚假UI事件信息到装置的操作系统而避开或躲避安全系统的检测。举例来说，恶意软件应用程序可激活计算装置的相机以捕获图像而不需要用户的知道或同意，并且然后将虚假onTouchEvent发送到装置的操作系统以致使安全系统不正确地确定所检测活动(相机的激活)与对应UI事件相关联。这可致使安全系统将恶意应用程序不正确地分类为良性。

[0029] 通过使用基于行为且机器学习的技术与由高层级操作系统接收的UI事件信息结合来分析由一或多个硬件/装置驱动器产生的原始数据，各种实施例允许计算装置确定UI事件是否为虚假UI事件，且当分析装置行为时使用此信息以便防止恶意软件应用程序使用虚假UI事件信息来避开或躲避检测。

[0030] 各种实施例通过允许装置更准确且高效地识别、防止、校正和/或另外响应于非良性软件应用程序而改进计算装置的功能。各种实施例还通过允许计算装置(或其基于行为的安全系统)使用UI事件信息来智能地聚焦其监视和/或分析操作而改进计算装置的功能，进而减少其对装置的响应性、性能和电力消耗特性的影响。

[0031] 计算装置的功能、功能性和/或机能的额外的改进从下文所提供的实施例的详细描述中是显而易见的。

[0032] 术语“性能降级”在本申请案中用于指代计算装置的广泛多种不合意的操作和特性，例如较长处理时间、较慢实时响应性、较低电池寿命、私人数据的损失、恶意经济活动(例如，发送未经授权的优质SMS消息)、拒绝服务(DoS)、不良写入或设计的软件应用程序、恶意的软件、恶意软件、病毒、分段存储器、与强占移动装置或利用电话用于间谍或僵尸网络活动相关的操作等等。并且，出于这些原因中的任一者而使性能降级的行为、活动和条件在本文中被称作“不是良性”或“非良性”。

[0033] 术语“移动计算装置”和“移动装置”在本文中互换地使用以指代以下各项中的任何一者或全部：蜂窝式电话、智能电话、个人或移动多媒体播放器、个人数据助理(PDA)、膝上型计算机、平板计算机、智能本、超级本、掌上型计算机、无线电子邮件接收器、具多媒体互联网功能的蜂窝式电话、无线游戏控制器，以及包括存储器和可编程处理器的类似的个人电子装置，对于所述电子装置性能是重要的，并且所述电子装置在电池电力下运行使得节约电力的方法是有益的。虽然各种实施例对于移动计算装置(例如，具有有限的资源且通过电池运行的智能电话)是尤其有用的，但是实施例通常在包括处理器且执行应用程序的

任何电子装置中是有用的。

[0034] 一般而言，移动装置的性能和功率效率随时间推移降低。近年来，杀毒软件公司(例如，McAfee、Symantec等)已经开始营销旨在减缓这种降低的手机杀毒软件、防火墙和加密产品。然而，这些解决方案中的许多依赖于在移动装置上周期性地执行计算密集型扫描引擎，这可能消耗许多的移动装置的处理和电池资源、在延长的时间周期减缓或放弃移动装置和/或另外降低用户体验。另外，这些解决方案是通常限制在检测已知的病毒和恶意代码，且并不解决通常结合以导致移动装置的随时间推移的降低的多个复杂的因素和/或相互作用(例如，当性能下降并不是由病毒或恶意代码引起的时)。出于这些和其它原因，现有杀毒软件、防火墙和加密产品并不提供可以胜任以下问题的解决方案：识别可以造成移动装置随时间推移降级的多个因素、防止移动装置降级或者有效恢复老化的移动装置到其初始状态。

[0035] 另外，现代移动装置是高度可配置的并且是复杂的系统。因而，对于确定特定装置行为是否是良性或非良性(例如，恶意或性能降级)的最重要特征可能在每个移动装置中不同。另外，存在可以造成随时间推移的移动计算装置的性能和电力利用水平下降的各种各样的因素，其包括不充分地编写或设计的软件应用程序、恶意代码、病毒、分段存储器、后台进程等。由于这些因素的数量多、种类广和其复杂性，评估在现代移动计算装置的复杂而资源受限制的系统的性能和/或电力利用水平中造成下降的全部因素通常是不可行的。因而，对于用户、操作系统和/或应用程序(例如，杀毒软件等)而言准确地且有效地识别问题的来源是困难的。因此，当前移动装置用户几乎没有防止随时间推移在移动装置的性能和电力利用水平中的降级的补救措施，或者恢复老化的移动装置到其初始性能和电力利用水平的补救措施。

[0036] 为了克服现有解决方案的限制，各种实施例包含配备有行为监视和分析系统的计算装置，所述系统经配置以快速且高效地识别非良性软件应用程序(例如，恶意的、不良写入的、不与装置兼容的应用程序等)，且防止这些应用程序使计算装置的性能、电力利用水平、网络使用水平、安全性和/或隐私随时间而降级。所述行为监视和分析系统可经配置以识别、防止且校正所识别的问题而对计算装置的响应性、性能或电力消耗特性没有显著、不利或用户可察觉的影响。在实施例中，所述行为监视和分析系统可为基于行为的安全系统。

[0037] 基于行为的监视和分析系统可包含观测器过程、后台程序、模块或子系统(本文中统称为“模块”)行为提取器模块和分析器模块。观测器模块可经配置以在计算装置系统的各种层级仪表化或协调各种应用程序编程接口(API)、寄存器、计数器或其它装置组件(本文统称为“仪表化组件”)，从仪表化组件收集行为信息，且将收集的行为信息传送(例如，经由存储器写入操作、功能调用等)到行为提取器模块。行为提取器模块可以使用所收集的行为信息以产生各自表示或表征与装置的一或多个特定的线程、过程、软件应用程序、模块或组件相关联的许多或全部观测到的事件、条件、任务、活动和/或行为(本文中统称为“行为”)的行为向量。行为提取器模块可将所产生行为向量传送(例如，经由存储器写入操作、功能调用等)到分析器模块，所述分析器模块可将行为向量应用于分类器模型以产生分析结果，且使用分析结果以确定软件应用程序或装置行为是否为良性或非良性(例如，恶意、不良写入、性能降低等)。装置处理器可随后执行各种操作以校正、治愈、解决、隔离或者另外修复所识别的问题(例如，确定为非良性的行为)。

[0038] 每个行为向量可以为包含或囊封一或多个“行为特征”的信息结构。行为特征可以为表示在计算装置中观测到的事件、条件、活动、操作、关系、交互或行为的全部或一部分的数字或符号。每个行为特征可以与识别一系列可能值的数据类型以及可以在那些值、值的含义和其它类似信息上执行的操作相关联。数据类型可以由计算装置使用以确定应当如何测量、分析、加权或使用对应的行为特征(或特征值)。

[0039] 分类器模型可以为包括数据、条目、决策节点、决策标准和/或信息结构的行为模型,所述结构信息可以由装置处理器使用以快速地且有效地测试或评估特定的特征、因素、数据点、条目、API、状态、状况、行为、软件应用程序、过程、操作、组件等(本文中统称为“特征”)或装置行为的其它实施例。分类器模型还可以包括可以由装置处理器使用以确定软件应用程序之间关系的本质和/或在移动装置中所监视的行为的信息。

[0040] 每个分类器模型可以分类为完整分类器模型或精益分类器模型。完整分类器模型可以为稳健数据模型,所述数据模型是作为大量培训数据集的函数产生的,其可以包括数千特征和数十亿的条目。精益分类器模型可以为更为集中的数据模型,所述数据模型由简化数据集产生,所述简化数据集包括或优先考虑与确定特定移动装置行为是否是非良性的最相关的特征/条目上的测试。本地分类器模型可以为在计算装置中产生的精益分类器模型。用户特定分类器模型可为包含高度聚焦数据模型的本地分类器模型,所述数据模型包含决策节点或将决策节点列入优先,所述节点测试或评估最相关的装置特征/条目以用于确定装置行为是否与特定用户对计算装置的普通使用一致。

[0041] 每个人大体上以唯一或相异方式与他/她的计算装置交互。举例来说,移动装置用户常常具有相异的工作或通信方式,使用特定软件应用程序或特定类型的软件应用程序,使用其移动装置执行特定活动或实现特定任务,以特定次序执行活动,在特定时间执行特定活动,以特定方式与特定软件应用程序交互等等。用户与她的/她的装置交互的相异方式可随时间而学习,且用以确定软件应用程序是否为非良性的。举例来说,在实施例中,计算装置可经配置以学习用户随时间与他的/她的装置交互的相异方式,使用此信息以确定活动、任务或行为是否应当与对应UI事件相关联,产生考虑对应UI事件的存在的行为向量和/或分类器模型,将行为向量应用于分类器模型以产生分析结果,且使用分析结果以确定与所述活动、任务或行为相关联的软件应用程序是否为非良性的(例如,恶意等)。

[0042] 现代计算装置具有对由其用户产生或涉及其用户的信息的前所未有的存取水平。举例来说,移动计算装置常常配备有收集或产生关于用户的详细个人信息的传感器(例如,加速度计、陀螺仪、地理空间定位传感器、相机、心率监视器、血糖仪等)。另外,移动计算装置现在包含允许执行复杂的软件应用程序的强力处理器,所述软件应用程序包含用于导览网页、购买商品、监视用户的健康、控制家用电器、玩游戏、观看/记录视频、导航新城市、跟踪锻炼、进行金融交易等等的应用程序。这些软件应用程序常常收集或产生关于用户的详细个人信息。由这些软件应用程序和传感器收集、产生或使用的信息可由实施例计算装置使用以产生表征用户的活动、偏好、年龄、职业、习惯、情绪、感情状态、个性等的用户个人信息。实施例计算装置可经配置以收集和使用这些用户个人信息以确定装置随时间的正常操作模式,包含活动、任务或行为是否应当与对应UI事件相关联。用户个人信息也可以用以产生适合用于确定软件应用程序是否为非良性的行为向量和/或分类器模型(例如,用户特定的分类器模型等)。

[0043] 某些任务/活动直接或固有地涉及或需要操作系统或软件应用程序(或进程、线程等)处于支持那些任务/活动或与其兼容的执行状态。举例来说,相机的使用、发送短消息服务(SMS)消息以及收集加速度计数据是通常需要与装置的某一形式的用户交互的所有任务/活动。因此,这些活动大体上必须在“前台”执行状态中或在支持与计算装置的用户交互的另一执行状态中执行。当这些或其它相似任务/活动在不支持与装置的高度用户交互的执行状态中(例如在后台执行状态中)执行时,此操作条件可为与所述活动相关联的装置行为是非良性或另外应得到额外或更靠近的审查、监视或分析的指示符。因此,在实施例中,计算装置可经配置以使用特定执行状态,其中执行活动或任务以确定活动、任务或行为是否应当与对应UI事件相关联,产生考虑执行状态和/或对应UI事件的存在的行为向量和/或分类器模型,将行为向量应用于分类器模型以产生分析结果,且使用分析结果以确定软件应用程序是否为非良性的。

[0044] 在实施例中,行为监视和分析系统可使用UI事件的存在作为当产生用以确定软件应用程序是否为非良性的分析结果时测试/评估(例如,经由将行为向量应用于分类器模型等)的因数。

[0045] 在上述实例中,计算装置使用经由与装置的用户交互产生的信息,例如对应UI事件的存在,以确定软件应用程序是否为非良性的。此信息通常包含(例如,当用户触摸装置的触摸屏等时)由装置的传感器或硬件产生的数据,其发送到操作系统以用于转发到行为监视和分析系统(例如,经由操作系统将信息存储在日志中等)。由于行为监视和分析系统使用此信息以确定软件应用程序是否为非良性的,所以恶意软件应用程序可能通过产生且发送虚假UI事件信息到操作系统,以便致使操作系统向行为监视和分析系统不正确地报告UI事件的存在,来尝试躲避或避开系统的检测。

[0046] 为了防止产生虚假用户交互信息(例如,虚假UI事件)的软件应用程序躲避或避开行为监视和分析系统(例如,基于行为的安全系统)的检测,在实施例中,计算装置可配备有虚假UI事件检测模块,其经配置以接收来自传感器和硬件驱动器的原始数据以及来自操作系统的UI事件信息,比较所接收原始数据与所接收UI事件信息以确定UI事件是真实UI事件还是虚假UI事件,且将虚假UI事件事件报告给行为监视和分析系统。

[0047] 在实施例中,行为监视和分析系统可经配置以将与虚假UI事件相关联的软件应用程序分类为非良性的。

[0048] 在实施例中,行为监视和分析系统可经配置以将与虚假UI事件相关联的软件应用程序分类为可疑的,且增加其审查或分析等级(例如,通过使用更稳健的分类器模型、监视软件应用程序的更多活动、产生更大行为向量等)。

[0049] 在实施例中,行为监视和分析系统可经配置以例如通过使用不测试与对应UI事件的存在或现存相关的条件的分类器模型而忽略经确定为虚假UI事件的UI事件。这允许系统聚焦于其监视和/或分析操作是对确定活动或行为是否为非良性来说最重要的特征或因数。

[0050] 在实施例中,计算装置的装置处理器可经配置以比较从不同装置驱动器或硬件组件接收的信息且使其相关以确定所检测UI事件是否为虚假UI事件。举例来说,用户触摸计算装置的触摸屏显示器可致使显示器产生呈识别显示器被触摸的时间的时戳以及识别所触摸显示区域的坐标信息的形式的原始数据。另外,由于计算装置当其显示器被触摸时通

常移动(由于用户的触摸的力),因此其陀螺仪和加速度计可产生指示所述装置在所述触摸事件的同时稍微移动的原始数据。因此,装置处理器可确定在触摸事件产生时装置的移动是否与用户交互一致。

[0051] 各种实施例(包含参考图2到7描述的实施例)可在许多不同移动装置中实施,包含单处理器和多处理器系统以及芯片上系统(SOC)。图1是说明可以用于实施各种实施例的计算装置中的实例芯片上系统(SOC)100架构的架构图。SOC 100可包含若干异构处理器,例如数字信号处理器(DSP)102、调制解调器处理器104、图形处理器106以及应用程序处理器108。SOC 100还可包含连接到异构处理器102、104、106、108中的一或多者的一或多个协处理器110(例如,向量协处理器)。每一处理器102、104、106、108、110可包含一或多个核心,且每一处理器/核心可独立于其它处理器/核心而执行操作。举例来说,SOC 100可包含执行第一类型的操作系统(例如,FreeBSD、LINUX、OS X等)的处理器和执行第二类型的操作系统(例如,微软视窗10)的处理器。

[0052] SOC 100还可包含模拟电路和定制电路114,以用于管理传感器数据、模/数转换、无线数据发射,且用于执行其它专用操作,例如处理用于游戏和电影的经编码音频信号。SOC 100可进一步包含系统组件/资源116,例如,电压调节器、振荡器、锁相环、外围桥接器、数据控制器、存储器控制器、系统控制器、存取端口、计时器和用于支持在计算装置上运行的处理器和客户端的其它类似组件。

[0053] 系统组件/资源116和定制电路114可包含用以与例如相机、电子显示器、无线通信装置、外部存储器芯片等外围装置介接的电路。处理器102、104、106、108可经由互连/总线模块124互连到一或多个存储器元件112、系统组件/资源116和定制电路114,所述互连/总线模块可包含可配置逻辑门的阵列和/或实施总线架构(例如,CoreConnect、AMBA等)。通信可由例如高性能芯片上网络(NoC)等高级互连件提供。

[0054] SOC 100可进一步包含用于与SOC外部的资源通信的输入/输出模块(未示出),所述资源例如时钟118和电压调节器120。SOC外部的资源(例如,时钟118、电压调节器120)可由内部SOC处理器/核心(例如,DSP 102、调制解调器处理器104、图形处理器106、应用程序处理器108等)中的两个或更多个共享。

[0055] SOC 100还可包含适用于从传感器收集传感器数据的硬件和/或软件组件,包含扬声器、用户接口元件(例如,输入按钮、触摸屏显示器等)、麦克风阵列、用于监视物理状态(例如,位置、方向、运动、取向、振动、压力等)的传感器、相机、罗盘、GPS接收器、通信电路系统(例如,Bluetooth®、WLAN、WiFi等)和现代电子装置的其它众所周知的组件(例如,加速度计等)。

[0056] 除了上文所论述的SOC 100之外,各种实施例还可以在多种多样的计算系统中实施,所述计算系统可包含单个处理器、多个处理器、多核心处理器或其任何组合。

[0057] 图2说明根据各种实施例的在经配置以识别虚假UI事件的实施例计算装置200中的实例逻辑组件和信息流。在图2中说明的实例中,计算装置200包含各种传感器和硬件组件202、装置驱动器模块204、操作系统206、虚假UI事件检测模块212、基于行为的安全模块214以及动作日志220。所述计算装置还包含软件应用程序208和恶意软件应用程序210,其两者可经由计算装置200的处理器或处理核心中的一或多者而在所述计算装置上操作或执行。

[0058] 软件应用程序208、210可使用应用程序接口(API)来调用操作系统206的服务。操作系统206可经由装置驱动器模块204与传感器/硬件组件202通信，所述装置驱动器模块可充当或提供传感器/硬件组件202与操作系统206之间的软件接口。装置驱动器模块204可经配置以经由由传感器/硬件组件202实施的操作代码(操作码)和原生命令而控制或与传感器/硬件组件202通信。装置驱动器模块204可经配置以使用从传感器/硬件组件202接收的原始数据以产生适合于由操作系统206解译和使用的信息。

[0059] 传感器/硬件组件202可经配置以响应于检测到用户交互事件而产生原始数据且将原始数据发送到装置驱动器模块204，且装置驱动器模块204可经配置以使用从传感器/硬件组件202接收的原始数据以产生适合于由操作系统206解译和使用的UI事件信息。举例来说，传感器/硬件组件202可包含电子触摸屏显示器(例如，电容式感测触摸屏面板等)，其经配置以在每次用户触摸触摸屏时以X和Y位置坐标的形式将原始数据发送到装置驱动器模块204。装置驱动器模块204可经配置以将此原始数据(即，位置坐标X和Y)转换为适合于由操作系统206解译和使用的UI事件信息(例如，screenTouch(X,Y))。操作系统206可接收且使用所述UI事件信息以确定应当调用软件应用程序208的onTouch(X,Y)功能，且致使软件应用程序208执行onTouch(X,Y)功能的操作。这些操作可包含打开相机快门、捕获图像、处理所捕获图像等。

[0060] 操作系统206和软件应用程序208两者可在动作日志220中记录其相应操作、活动和/或任务。举例来说，操作系统可在动作日志220中记录UI事件(例如，screenTouch(X,Y))的检测，且软件应用程序208可在动作日志220中记录操作(例如，打开相机快门、捕获图像、将信息写入到存储器等)或其相关联API调用。

[0061] 基于行为的安全模块214可经配置以监视软件应用程序208的操作、活动，从动作日志220收集行为信息，使用所收集行为信息以产生行为向量结构，将所产生行为向量结构应用于分类器模型以产生分析结果，且使用分析结果以确定软件应用程序208是否为非良性的。作为这些操作的部分，基于行为的安全模块214可确定软件应用程序208的行为或活动直接或固有地涉及或需要与装置的某一形式的用户交互，响应于确定所述行为/活动直接或固有地涉及或需要用户交互而确定动作日志220是否包含对应于所述行为/活动的UI事件，且当确定软件应用程序208是否为非良性时使用评估对应UI事件的存在或现存的行为向量和/或分类器模型。

[0062] 在图2中说明的实例中，恶意软件应用程序210通过产生且发送虚假UI事件到操作系统而尝试躲避或避开基于行为的安全模块214的检测。举例来说，恶意软件应用程序210可激活相机以捕获图像而没有用户的知道同意，且致使操作系统不正确地记录对应相机的激活的UI事件的存在。这可致使基于行为的安全模块214不正确地确定存在对应于受监视活动的UI事件。

[0063] 虚假UI事件检测模块212可经配置以防止恶意软件应用程序210躲避或避开基于行为的安全模块214的检测。装置驱动器模块204可包含驱动器仪表化模块216，其经配置以将原始数据发送到虚假UI事件检测模块212，且操作系统206可包含操作系统仪表化模块218，其经配置以将UI事件信息发送到虚假UI事件检测模块212。虚假UI事件检测模块212可经配置以接收来自驱动器仪表化模块216的原始数据以及来自操作系统仪表化模块218的UI事件信息，比较所接收原始数据与所接收UI事件信息以确定所述UI事件是真实UI事件还

是虚假UI事件，且向基于行为的安全模块214报告虚假UI事件事件。

[0064] 响应于接收到虚假UI事件的报告，基于行为的安全模块214可将与虚假UI事件相关联的软件应用程序分类为非良性的，将与虚假UI事件相关联的软件应用程序分类为可疑的，更新分类器模型以排除测试与UI事件的存在/现存相关的条件的决策节点，或选择/使用并不测试与UI事件的存在/现存相关的条件的行为向量和分类器模型。

[0065] 图3说明在一个实施例移动计算装置中的实例逻辑组件和信息流，所述移动计算装置包含经配置以使用行为分析技术来识别和响应于非良性装置行为的基于行为的安全模块214。在图3中说明的实例中，所述计算装置是包含装置处理器(即，移动装置处理器)的移动装置300，所述处理器被配置成具有可执行指令模块，所述模块包含行为观测器模块302、行为提取器模块304、行为分析器模块306以及致动器模块308。模块302到308中的每一者可为以软件、硬件或其组合实施的线程、进程、后台程序、模块、子系统或组件。在各种实施例中，模块302到308可在操作系统的部分内(例如，内核内、内核空间中、用户空间中等)、单独程序或应用程序内、专用硬件缓冲器或处理器中或其任何组合内实施。在一实施例中，模块302到308中的一或多个可以被实施为在移动装置300的一或多个处理器上执行的软件指令。

[0066] 行为观测器模块302可经配置以在装置的各种层级/模块处仪表化应用程序编程接口(API)、计数器、硬件监视器等，且监视在一时间周期内在各种层级/模块处的活动、条件、操作和事件(例如，系统事件、状态改变等)。行为观测器模块302可以收集关于所监视的活动、条件、操作或事件的行为信息，并且将所收集的信息存储在存储器中(例如，在日志文件中等)。

[0067] 在一些实施例中，行为观测器模块302可经配置以从在计算装置中操作的软件应用程序、计算装置的传感器和/或从用户与计算装置或其软件应用程序的交互收集基于用户的信息(例如，用户个人信息等)。基于用户的信息可包含适合于识别或表征装置用户的活动、装置使用模式、习惯、情绪、职业和/或感情状态的任何信息。举例来说，基于用户的信息可包含识别用户与装置的交互、在装置上执行的定制的数目和类型、由用户下载或使用的软件应用程序的类型、用户触摸或与屏幕交互的速率、装置的图形处理单元(GPU)使用水平、用户使用装置与他人通信的频率、用户的优选通信方法(例如，文字对话音)、用户通信有多快、装置存储器大小等的信息。装置处理器可使用所收集基于用户的信息来学习用户通常如何与计算装置交互，确定装置的正常操作模式和/或确定活动、任务或行为是否应当与UI事件相关联。举例来说，装置过程可使用基于用户的信息以确定装置的正常操作模式是否指示特定活动与特定UI事件相关联和/或不具有其相应UI事件的特定活动的执行不与装置的正常操作模式一致。

[0068] 行为观测器模块302可经配置以通过监视多种软件应用程序(或软件应用程序类型)中的任一者来收集用户个人信息，所述软件应用程序包含：日历应用程序、提醒应用程序、通信应用程序、金融应用程序、用于实现特定任务(例如，文字处理、准备税制改革、演示应用程序、会计应用程序等)的应用程序、基于位置的应用程序(例如，测绘和地理位置应用程序等)、社交媒体应用程序、网络浏览器(例如，获得关于过去搜索、浏览历史、访问网站类型、访问网站内容等的信息)、娱乐应用程序(例如，音频或多媒体播放器应用程序)、用于接入用户帐户的应用程序(例如，银行应用程序等)、个人训练和开发应用程序等等。

[0069] 行为观测器模块302还可通过从心率监视器、血压监视器、温度计、计步器、血糖仪、湿度传感器、体内酒量测定器、皮肤电响应传感器或装置中的其它传感器获得数据而收集用户个人信息。举例来说，行为观测器模块302可通过以下方式来收集用户个人信息：监视装置的地理空间定位和导航系统以确定用户的当前位置(例如，在办公室、在家、在餐馆、健身房、旅行等)、用户的当前移动(例如，当前在旅行、在锻炼、静止等)、移动历史(例如，广泛地旅行、从不离开城镇等)、用户是否遵循他的/她的所建立例程(例如，准时上班、仍在工作)或脱离他的/她的例程(例如，比通常更晚到达、比通常更早离开)。

[0070] 在一些实施例中，移动装置300的装置处理器可经配置以使用用户个人信息和/或表征用户与装置的交互的信息以产生行为向量和/或分类器模型。举例来说，装置处理器可经配置以使用用户交互信息来动态确定受监视的装置特征、包含在行为向量中的行为信息、包含在分类器模型中(且因此由其评估)的特定装置特征等等。作为另一实例，装置处理器可经配置以产生分类器模型，所述分类器模型评估聚焦于在某些类型的软件应用程序(例如，游戏等)的使用或执行期间识别UI事件的存在的条件/特征。

[0071] 在一些实施例中，装置处理器可经配置以确定用户交互信息是否与分析所收集行为信息的全部或部分相关，产生包含相对于用户交互(如果相关)评估装置特征的决策节点的分类器模型，产生使用户交互相关的所收集行为信息相关的行为向量，且将所产生行为向量应用于所产生分类器模型以确定装置行为是否为非良性的。

[0072] 行为观测器模块302还可经配置以通过收集关于以下各项的信息而监视移动装置300的活动：应用程序框架或运行时间库中的库应用程序编程接口(API)调用、系统调用API、文件系统和联网子系统操作、装置(包含传感器装置)状态改变，以及其它相似事件。另外，行为观测器模块302可以监视文件系统活动，文件系统活动可包含搜索文件名称、文件存取的类别(个人信息或普通数据文件)、创建或删除文件(例如，类型exe、zip等)、文件读取/写入/搜寻操作、改变文件许可等。

[0073] 行为观测器模块302还可通过监视数据网络活动而监视移动装置300的活动，其可包含连接类型、协议、端口号、装置连接到的服务器/客户端、连接的数目、通信的量或频率等。行为观测器模块302可监视电话网络活动，其可包含监视发出、接收或拦截的呼叫或消息(例如，SMS等)的类型和数目(例如，进行的优质呼叫的数目)。

[0074] 行为观测器模块302还可通过监视系统资源使用而监视移动装置300的活动，其可包含监视复刻的数目、存储器存取操作、打开的文件的数目等。行为观测器模块302可监视移动装置300的状态，其可包含监视各种因数，例如显示器是接通还是断开、装置是锁定还是解锁、剩余的电池量、相机的状态等等。行为观测器模块302还可通过例如监视关键服务(浏览器、联系人提供器等)的意图、进程间通信的程度、弹出式窗口等而监视进程间通信(IPC)。

[0075] 行为观测器模块302也可以通过监视一或多个硬件组件的驱动器统计数据和/或状态来监视移动装置300的活动，这些硬件组件可包含相机、传感器、电子显示器、WiFi通信组件、数据控制器、存储器控制器、系统控制器、存取端口、计时器、外围装置、无线通信组件、外部存储器芯片、电压调节器、振荡器、锁相环、外围桥接器以及用于支持在移动装置300上运行的处理器和客户端的其它类似组件。

[0076] 行为观测器模块302还可通过监视表示移动装置300和/或计算装置子系统的状态

的一或多个硬件计数器而监视移动装置300的活动。硬件计数器可包含经配置以存储发生在移动装置300中的硬件相关活动或事件的计数值或状态的处理器/核心的专用寄存器。

[0077] 行为观测器模块302还可通过监视软件应用程序的动作或操作、从应用程序下载服务器(例如，Apple®应用商店服务器)下载的软件、由软件应用程序使用的计算装置信息、呼叫信息、文本消息接发信息(例如，发送SMS、阻断SMS、读取SMS等)、媒体消息接发信息(例如，接收MMS)、用户帐户信息、位置信息、相机信息、加速度计信息、浏览器信息、基于浏览器通信的内容、基于话音通信的内容、短程无线电通信(例如，蓝牙、WiFi等)、基于文本通信的内容、所记录的音频文件的内容、电话簿或联系人信息、联系人列表等来监视移动装置300的活动。

[0078] 行为观测器模块302还可通过监视移动装置300的发射或通信来监视移动装置300的活动，所述通信包括包含以下各项的通信：话音邮件(VoiceMailComm)、装置识别符(DeviceIDComm)、用户帐户信息(UserAccountComm)、日历信息(CalendarComm)、位置信息(LocationComm)、所记录的音频信息(RecordAudioComm)、加速度计信息(AccelerometerComm)等。

[0079] 行为观测器模块302还可通过监视指南针信息、计算装置设定、电池寿命、陀螺仪信息、压力传感器、磁体传感器、屏幕活动等的使用以及对其的更新/改变而监视移动装置300的活动。行为观测器模块302可监视传送到软件应用程序和从软件应用程序传送的通知(AppNotifications)、应用程序更新等。行为观测器模块302可监视关于第一软件应用程序请求第二软件应用程序的下载和/或安装的条件或事件。行为观测器模块302可以监视关于用户检验的条件或事件，例如密码的输入等。

[0080] 行为观测器模块302还可通过监视在移动装置300的多个层级处的条件或事件来监视移动装置300的活动，这些层级包括应用程序层级、无线电层级和传感器层级。应用程序层级观测可包含经由面部辨识软件来观测用户、观测社交流、观测用户输入的笔记、观测关于PassBook®、Google®Wallet、Paypal®和其它类似应用程序或服务的使用的事件。应用程序层级观测还可包含观测涉及虚拟专用网络(VPN)的使用的事件和关于同步、语音搜索、语音控制(例如，通过说出一个词语来锁定/解锁电话)、语言翻译程序、为了计算的数据的卸载、视频串流、不含用户活动的相机使用、不含用户活动的麦克风使用等的事件。

[0081] 无线电层级观测可包含确定以下各项中的任一者或更多的存在、现存或量：在建立无线电通信链路或发射信息之前与移动装置300的用户交互、双/多订户识别模块(SIM)卡、因特网无线电、移动电话网络共享、卸载用于计算的数据、装置状态通信、作为游戏控制器或家庭控制器的使用、交通工具通信、计算装置同步等。无线电层级观测还可包含监视无线电(WiFi、WiMax、蓝牙等)的使用以用于定位、对等式(p2p)通信、同步、交通工具到交通工具通信，和/或机器到机器(m2m)。无线电层级观测可以进一步包括监视网络业务使用、统计数据或简档。

[0082] 传感器层级观测可包含监视磁体传感器或其它传感器以确定移动装置300的使用和/或外部环境。举例来说，计算装置处理器可经配置以确定装置是否在皮套中(例如，经由皮套内的经配置以感测磁体的磁体传感器)或在用户的口袋中(例如，经由相机或光传感器检测到的光量)。检测移动装置300在皮套中可以与辨识可疑行为相关，举例来说，因为与用户的主动使用相关的活动和功能(例如，拍摄照片或视频、发送消息、进行话音呼叫、记录声

音等)在移动装置300装在皮套中的同时发生可以是在装置上执行违法过程(例如,跟踪或监视用户)的征兆。

[0083] 与使用或外部环境相关的传感器层级观测的其它实例可包含:检测近场通信(NFC)信令、从信用卡扫描仪、条形码扫描仪或移动标签读取器收集信息、检测通用串行总线(USB)电力充电源的存在、检测已经耦合到移动装置300的键盘或辅助装置、检测移动装置300已经耦合到另一计算装置(例如,经由USB等)、确定LED、闪光灯、手电筒或光源是否已经是经修改或停用的(例如,恶意停用紧急信令应用程序等)、检测扬声器或麦克风已经接通或供电、检测充电或电源事件、检测移动装置300被用作游戏控制器等。传感器层级观测还可包含:从医学或医疗传感器中收集信息或者通过扫描用户的身体收集信息、从插入到USB/音频插孔中的外部传感器收集信息、从触感或触觉传感器收集信息(例如,经由振动器接口等)、收集关于移动装置300的热状态的信息等。

[0084] 为了将所监视因数的数目减少到可管理的水平,在一个实施例中,行为观测器模块302可经配置以通过监视/观测行为或因数的初始集合来执行粗略观测,所述行为或因数的初始集合是可以造成计算装置的降级的全部因数的较小子集。在一个实施例中,行为观测器模块302可以从云服务或网络中的服务器和/或组件中接收行为和/或因数的初始集合。在一个实施例中,可以在机器学习分类器模型中指定行为/因数的初始集合。

[0085] 行为观测器模块302可将所收集行为信息传送(例如,经由存储器写入操作、功能调用等)到行为提取器模块304。行为提取器模块304可经配置以接收或检索所收集行为信息,且使用此信息以产生一或多个行为向量。每一行为向量可在值或向量数据结构中简明地描述装置、软件应用程序或进程的行为。向量数据结构可包含数字的系列,其中的每一系列表示移动装置的特征或行为,例如移动装置的相机是否在使用中(例如,为零或一)、已从移动装置发射或产生多少网络业务(例如,20KB/秒等)、已经传送多少因特网消息(例如,SMS消息的数目等),和/或由行为观测器模块302收集的任何其它行为信息。在实施例中,行为提取器模块304可经配置以产生行为向量以使得它们充当识别符,所述识别符使得移动装置系统(例如,行为分析器模块306)能够快速地辨识、识别或分析装置的行为。

[0086] 在实施例中,行为提取器模块304可经配置以产生行为向量以包含可输入到机器学习分类器中的特征/决策节点的信息以产生对关于所监视的一或多个活动的询问的回答。

[0087] 在实施例中,行为提取器模块304可经配置以产生行为向量以包含执行信息。执行信息可以包含于行为向量中作为行为的一部分(例如,通过后台过程相机在三秒中使用五次、通过前台过程相机在三秒中使用三次等)或者作为独立特征的一部分。在一个实施例中,执行状态信息可以包含于行为向量中作为阴影特征值子向量或数据结构。在一实施例中,行为向量可存储与同执行状态相关的特征、活动、任务相关联的阴影特征值子向量/数据结构。

[0088] 行为提取器模块304可将所产生行为向量传送(例如,经由存储器写入操作、功能调用等)到行为分析器模块306。行为分析器模块306可经配置以将行为向量应用于分类器模块以确定装置行为是否为随时间而贡献于(或可能贡献于)装置的降级和/或可能另外对装置造成问题的非良性行为。

[0089] 每一分类器模型可以是包含数据和/或信息结构(例如,特征向量、行为向量、组件

列表等)的行为模型,所述数据和/或信息结构可以由计算装置处理器使用以评估计算装置的行为的特定特征或实施例。每个分类器模型还可以包括用于监视计算装置中的多个特征、因数、数据点、条目、API、状态、条件、行为、应用程序、过程、操作、组件等(本文中统称为“特征”)的决策标准。分类器模型可以预先安装在计算装置上、从网络服务器中下载或接收、产生于计算装置中,或其任何组合。分类器模型可以通过使用众包解决方案、行为模拟技术、机器学习算法等产生。

[0090] 每个分类器模型可以分类为完整分类器模型或精益分类器模型。完整分类器模型可以为稳健数据模型,所述数据模型是作为大量培训数据集的函数产生的,其可包含数千特征和数十亿的条目。精益分类器模型可以是从简化数据集中产生的更集中的数据模型,其仅包含/测试与用于确定特定活动是否是进行中的关键活动和/或特定计算装置行为是否并不是良性的最相关的特征/条目。作为实例,装置处理器可以是可经配置以从网络服务器中接收完整分类器模型、在移动装置中基于完整分类器产生精益分类器模型,并且使用本地产生的精益分类器模型来将装置的行为分类为良性或非良性的(即,恶意、性能降级等)。

[0091] 本地产生的精益分类器模型是产生于计算装置中的精益分类器模型。即,由于移动装置是高度可配置且复杂的系统,因此对于确定特定装置行为是否为非良性的(例如,恶意或性能降级)来说最重要的特征可能在每一装置中不同。另外,可能需要在每个装置中监视和/或分析特征的不同组合以便所述装置快速地且有效地确定特定行为是否为非良性的。然而,需要监视和分析的特征的精确组合和每个特征或特征组合的相对优先级或重要性通常仅可以使用从其中行为待监视或分析的特定的装置中获得的信息来确定。出于这些和其它原因,各种实施例可以在其中使用模型的移动装置中产生分类器模型。这些本地分类器模型使得装置处理器能够准确地识别在确定特定的装置上的行为是否是非良性的(例如,贡献于装置性能降级)中最重要的特定特征。本地分类器模型还允许装置处理器根据特征的相对重要性将所测试或评估的特征区分优先级以对所述特定装置中的行为进行分类。

[0092] 装置特定的分类器模型是包括集中数据模型的分类器模型,所述集中数据模型仅包含/测试经确定为与对特定计算装置中的活动或行为进行分类最相关的计算装置特定的特征/条目。

[0093] 应用程序特定的分类器模型是包含集中数据模型的分类器模型,所述集中数据模型仅包含/测试与用于评估特定软件应用程序最相关的特征/条目。

[0094] 用户特定的分类器模型可为包含集中数据模型的本地分类器模型,所述集中数据模型包含或将对与以下各项最相关的特征/条目的测试区分优先级:识别装置的用户、确定用户的个人信息、确定装置行为是否与经识别用户的个人信息一致、确定装置行为是否与其经识别用户中的一者对所述装置的普通使用一致,或确定用户的活动是否指示非良性装置行为。

[0095] 通过在移动装置中本地动态地产生用户特定、装置特定和/或应用程序特定的分类器模型,各种实施例允许装置处理器将其监视和分析操作集中于对确定所述特定移动装置和/或在所述装置中操作的特定软件应用程序的操作是否与所述特定装置的已知用户的个性、习惯或普通使用模式一致而言最重要的少数特征。

[0096] 在实施例中,行为分析器模块306可经配置以当其行为分析操作的结果并不提供

足够信息以将装置行为分类为良性或非良性时将行为分类为“可疑”。行为分析器模块306可经配置以响应于确定装置行为是可疑的而通知行为观测器模块302。作为响应，行为观测器模块302可调整其观测的粒度(即，监视到计算装置特征的细节水平)和/或改变基于从行为分析器模块306接收的信息(例如，实时分析操作的结果)监视的因数或行为，产生或收集新的或额外的行为信息，并且发送新的/额外的信息到行为分析器模块306以用于进一步的分析/分类。行为观测器模块302与行为分析器模块306之间的此类反馈通信使得移动装置300能够以递归方式增大观测的粒度(即，进行更加精细或更加详细的观测)或改变所观测到的特征/行为直到共同行为被分类为良性或非良性的、识别出可疑或性能降级行为的来源、直到达到处理或电池消耗阈值为止，或直到装置处理器确定可疑或性能降级装置行为的来源无法通过观测粒度的进一步的改变、调整或增加而识别为止。此类反馈通信还使得移动装置300能够调整或修改行为向量和分类器模型而不会消耗过量的计算装置的处理、存储器或能量资源。

[0097] 在实施例中，行为分析器模块306可经配置以接收且分析由各种移动装置子系统和/或在各种时间周期中收集的信息以学习移动装置在多种情境和条件下的正常操作行为，且产生在各种情境/条件下的正常移动装置行为的模型(例如，呈分类器模型等的形式)。在实施例中，行为分析器模块306可经配置以对照所产生行为模型使所收集行为信息或行为向量相关，且基于所述相关而执行行为分析操作以确定所接收观测是否与学习的正常操作行为冲突(或不匹配)。

[0098] 作为高级实例，移动装置300可能检测(经由所收集行为信息)到相机已经使用、移动装置300正在尝试将图片上载到服务器，以及当装置在皮套中且附接到用户的皮带时在移动装置上的应用程序拍摄照片。移动装置300可确定此检测到的行为(例如，在皮套中时相机的使用)是否为对于用户可接受或常见的行为。这可通过将所检测行为(例如，所产生行为向量)与移动装置300或用户的过去行为进行比较而实现。由于在皮套中时拍摄照片且将照片上载到服务器是不寻常的行为(如从在皮套中的情境中观测到的正常行为可确定)，因此在此情形下，计算装置可将此辨识为与用户对计算装置的普通使用模式不一致，且起始适当的响应(例如，关断相机、发出警报声等)。

[0099] 在各种实施例中，移动装置300可经配置以结合网络服务器工作以智能地且有效地识别与确定活动或行为是否是非良性的最相关的特征、因数和数据点。举例来说，装置处理器可经配置以从网络服务器接收完整分类器模型，并且使用接收到的完整分类器模型来产生特定针对于装置的用户和/或装置或其软件应用程序的特征和功能性的精益分类器模型(即，数据/行为模型)。装置处理器可使用完整分类器模型来产生不同复杂度水平(或“精益度”)的一系列精益分类器模型。可以常规地应用最精益系列的精益分类器模型(即，基于最少数目的测试条件的精益分类器模型)直到遇到分类器模型无法将其分类为良性或非良性(并且因此被模型分类为可疑)的行为，此时可以应用更加稳健(即，不太精益)的精益分类器模型以尝试对所述行为进行分类。可以应用在所述系列的所产生精益分类器模型内的甚至更加稳健的精益分类器模型的应用直到实现行为的确定性分类。以此方式，装置处理器可以通过将最完整但是资源密集型精益分类器模型的使用限制于其中需要稳健分类器模型以确定性地对行为进行分类的那些情况而在效率与准确性之间形成均衡。

[0100] 在各种实施例中，装置处理器可经配置以通过将包含于完整分类器模型中的有限

状态机表示或表达转换为增强的决策柱而产生精益分类器模型。装置处理器可基于用户个人信息或用户特定的装置特征而删除或挑选增强的决策柱的完整集合以产生包括包含于完整分类器模型中的增强的决策柱的子集的精益分类器模型。装置处理器可随后使用精益分类器模型以智能地监视、分析装置行为和/或对装置行为进行分类。

[0101] 增强的决策柱是具有恰好一个节点(并且因此一个测试问题或测试条件)和权重值的一个层级决策树,并且因此较适合于在数据/行为的二进制分类中使用。也就是说,将行为向量应用于增强的决策柱引起二进制回答(例如,是或否)。举例来说,如果通过增强的决策柱测试的问题/条件是“短消息服务(SMS)发射的频率小于每分钟x”,那么将“3”的值应用于增强的决策柱将引起“是”的回答(对于“小于3”的SMS发射)或“否”的回答(对于“3或大于3的”SMS发射)。增强的决策柱是高效的因为它们是非常简单且原始的(并且因此并不需要相当大的处理资源)。增强的决策柱也是非常可并行化的,并且因此许多柱可以并行/同时应用或测试(例如,通过计算装置中的多个核心或处理器)。

[0102] 图4A说明根据一实施例的检测且响应于虚假UI事件的方法400。方法400可由移动或资源受限的计算装置的装置处理器执行。在框402中,装置处理器可从计算装置的一或多个装置驱动器接收原始数据。在框404中,装置处理器可从计算装置的高层级操作系统(HLOS)接收用户交互(UI)信息。在框406中,装置处理器可将从装置驱动器接收的原始数据与从HLOS接收的用户交互事件信息进行比较以产生第一分析结果。

[0103] 在确定框408中,装置处理器可使用所产生第一分析结果以确定用户交互(UI)事件是否与用户交互相关。此确定可评估从一或多个装置驱动器接收的原始数据是否匹配或另外相关于报告给HLOS/由HLOS报告的UI事件。如果装置驱动器原始数据不相关(或匹配)于来自HLOS的UI信息,那么这可指示所接收UI事件是虚假的,且计算装置可将所检测UI事件分类为虚假UI事件。

[0104] 响应于确定UI事件与用户交互相关,且因此UI事件不是虚假UI事件(即,确定框408=“是”),装置处理器可在框410中将行为向量应用于分类器模型以产生第二分析结果。在框412中,装置处理器可使用第二分析结果以确定装置行为是否为非良性的。作为框410和412的操作的部分,装置处理器可执行上文参考图3论述的操作中的任一者或全部。

[0105] 响应于确定UI事件不与用户交互相关,且因此UI事件是虚假UI事件(即,确定框408=“否”),装置处理器可在框414中向计算装置的基于行为的安全系统报告虚假UI事件。在框414中,装置处理器可(例如,经由基于行为的安全系统)将所述装置行为分类为非良性的。因此,在实施例中,基于行为的安全系统可经配置以将经确定为与虚假UI事件相关联的所有软件应用程序分类为非良性的。

[0106] 图4B说明根据另一实施例的检测且响应于虚假UI事件的另一方法420。方法420可由移动或资源受限的计算装置的装置处理器执行,所述计算装置以处理器可执行指令配置以执行所述方法的操作。在框422中,装置处理器可将从一或多个装置驱动器接收的原始数据与从HLOS接收的UI信息进行比较。在确定框424中,装置处理器可使用所述比较结果以确定UI事件是否与用户交互相关且因此是或不是虚假UI事件。响应于确定UI事件与用户交互相关,且因此UI事件不是虚假UI事件(即,确定框424=“是”),装置处理器可在框426中通过将行为向量应用于分类器模型而产生分析结果,所述分类器模型包含测试与用户交互相关的条件的决策节点。在框428中,装置处理器可使用所述分析结果以确定装置行为(例如,软

件应用程序的活动等)是否为非良性的。

[0107] 响应于确定UI事件不与用户交互相关,且因此UI事件是虚假UI事件(即,确定框424=“否”),装置处理器可在框430中向基于行为的安全系统报告虚假UI事件。在框432中,装置处理器可通过在框426中将行为向量应用于分类器模型而产生分析结果,所述分类器模型不包含测试与用户交互相关的条件的任何决策节点。在框428中,使用分析结果以确定装置行为(例如,软件应用程序的活动等)是否为非良性的。

[0108] 各种实施例也可以用来辨识或至少识别泄密的用户输入传感器装置驱动器的可能性。这些能力可有用于辨识恶意软件何时已包括或将面部UI事件插入到用于用户输入装置或传感器的装置驱动器中。举例来说,如果用于触摸屏的装置驱动器已泄密,那么从装置驱动器接收(例如,在框402中)的原始数据可能自身为虚假的,在此情况下比较来自HLOS的UI信息可能不足以检测此水平的攻击。

[0109] 为了解决此可能,图4C说明根据另一实施例的用于检测且响应于泄密的用户输入传感器装置驱动器的另一方法450。方法450可由移动或资源受限的计算装置的装置处理器执行,且可除上述方法400和420之外或作为其中任一者的替代而执行。在框452中,装置处理器可比较从一或多个用户输入传感器接收的原始数据与从输入传感器装置驱动器接收的数据。举例来说,装置处理器可接收由触摸屏提供的原始输出数据且比较所述数据与从触摸屏装置驱动器接收的数据。

[0110] 在确定框454中,装置处理器可使用所述比较结果以确定用户输入传感器数据是否与对应装置驱动器数据相关。此确定可考虑传感器数据和装置驱动器数据的不同格式。举例来说,装置处理器可以类似于装置驱动器的方式应用变换或分析原始传感器数据以便基于原始传感器数据确定应当接收的装置驱动器输出数据,且然后比较所接收装置驱动器数据与预期数据以确定是否存在匹配。举例来说,在确定框454中,装置处理器可进入由触摸屏提供的输出数据流,处理触摸屏幕数据流以确定来自触摸屏装置驱动器的适当输出,且然后比较所确定的适当输出与由触摸屏装置驱动器产生的原始数据。

[0111] 响应于确定原始UI传感器数据与从用于所述传感器的装置驱动器接收的原始数据相关(即,确定框454=“是”),装置处理器可通过如上文所描述在框426中将行为向量应用于分类器模型而产生分析结果,所述分类器模型包含测试与用户交互相关的条件的决策节点。

[0112] 响应于确定原始UI传感器数据与从用于所述传感器的装置驱动器接收的原始数据相关(即,确定框424=“否”),装置处理器可在框456中向基于行为的安全系统报告装置驱动器潜在地被破坏。在一些实施例中,缺乏原始传感器数据到装置驱动器数据的相关可足以确定恶意软件或类似地不可接受的条件存在,在此情况下向基于行为的安全系统的报告可足以将装置行为(例如,软件应用程序的活动)分类为非良性。然而,在一些实施例中,原始传感器数据与装置驱动器数据的比较可能不足以确定性地确定装置驱动器泄密,因为数据失配可能是由于传感器的问题、传感器与装置驱动器之间的连接中的噪声、装置驱动器是与在确定框454中由装置处理器模拟的版本不同的版本等等。因此,在此类实施例中,向安全系统的报告可能仅为存在装置驱动器已泄密的可能,并且基于行为的安全系统的进一步分析可为必要的(例如,框432和428中)以便将装置行为分类为良性或非良性。

[0113] 在框432中,装置处理器可如上文所描述通过将行为向量应用于分类器模型而产

生分析结果，所述分类器模型不包含测试与用户交互相关的条件的任何决策节点。此分析可避免受到在装置驱动器层级起始的虚假UI事件的欺骗，以及避免可能由UI传感器和传感器的装置驱动器中的任一者中或之间的故障引起的错误肯定。

[0114] 在框428中，装置处理器可如上文所描述使用来自框426或432的分析结果以确定装置行为(例如，软件应用程序的活动等)是否为非良性的。

[0115] 图5说明使用一系列精益分类器模型对计算装置中的装置行为进行分类的实施例方法500。方法500可由移动或资源受限的计算装置的装置处理器执行，所述计算装置以处理器可执行指令配置以执行所述方法的操作。

[0116] 在框502中，装置处理器可执行观测以从在移动装置系统的各种层级处仪表化的各种组件收集行为信息。在实施例中，这可经由上文参考图3所论述的行为观测器模块302而实现。在框504中，装置处理器可产生表征所收集行为信息和/或移动装置行为的行为向量。另外，在框504中，装置处理器可以使用从网络服务器接收的完整分类器模型以产生不同复杂度水平(或“精益度”)的精益分类器模型或一系列精益分类器模型。为了实现这一点，装置处理器可以剔除包含于完整分类器模型中的一系列增强的决策柱以产生包含减少的数目的增强的决策柱和/或评估有限数目的测试条件的精益分类器模型。在实施例中，精益分类器模型中的一或多者可为用户特定的分类器模型。

[0117] 在框506中，装置处理器可以选择在所述系列的精益分类器模型中的最精益的分类器(即，基于最少数目的不同的移动装置状态、特征、行为或条件的模型)，但所述最精益的分类器尚未由移动装置评估或应用。在一实施例中，这可以通过装置处理器选择分类器模型的有序列表中的第一分类器模型而实现。在框508中，装置处理器可以将所收集的行为信息或行为向量应用于所选择的精益分类器模型中的每个增强的决策柱。因为增强的决策柱是二进制决策并且精益分类器模型是通过基于同一测试条件选择许多二进制决策产生的，所以将行为向量应用于精益分类器模型中的增强的决策柱的过程可以在并行操作中执行。替代地，行为向量可经截断或过滤以仅包含有限数目的包含于精益分类器模型中的测试条件参数，从而进一步减少应用所述模型时的计算努力。

[0118] 在框510中，装置处理器可以计算或确定将所收集的行为信息应用于精益分类器模型中的每个增强的决策柱的结果的加权平均。在框512中，装置处理器可将所计算加权平均与阈值进行比较。在确定框514中，装置处理器可以确定此比较的结果和/或通过应用所选择的精益分类器模型产生的结果是否为可疑的。举例来说，装置处理器可以确定这些结果是否可用于以较高程度的置信度将行为分类为恶意或良性的，并且如果不是则将行为作为可疑的对待。

[0119] 如果装置处理器确定所述结果是可疑的(例如，确定框514＝“是”)，那么装置处理器可重复框506到512中的操作以选择和应用较强(即，较不精益)分类器模型，其评估更多装置状态、特征、行为或条件直到以高度的置信度将行为分类为恶意或良性的。如果装置处理器确定结果不是可疑的(例如，确定框514＝“否”)，例如通过确定行为可以高度的置信度被分类为恶意或良性的，那么在框516中，装置处理器可以使用产生于框512中的比较的结果以将移动装置的行为分类为良性或潜在恶意的。

[0120] 在替代实施例方法中，上文所述的操作可以依序通过以下各项而实现：选择并非已经在精益分类器模型中的增强的决策柱；识别取决于与所选择的决策柱相同的移动装置

状态、特征、行为或条件(且因此可以基于一个确定结果应用)的全部其它增强的决策柱;在精益分类器模型中包含所选择的和取决于相同移动装置状态、特征、行为或条件的全部所识别的其它增强的决策柱;并且以等于测试条件的所确定数目的次数重复所述过程。因为取决于与所选择的增强的决策柱相同的测试条件的全部增强的决策柱每次被添加到精益分类器模型,所以限制执行这一过程的次数将限制包含于精益分类器模型中的测试条件的数目。

[0121] 图6说明根据各种实施例的适合于产生适合使用的决策树/分类器的实例方法600。方法600可由移动或资源受限的计算装置的装置处理器执行,所述计算装置以处理器可执行指令配置以执行所述方法的操作。在框602中,装置处理器可以产生和/或执行决策树/分类器、从决策树/分类器的执行中收集训练样本,并且基于训练样本产生新的分类器模型(h1(x))。训练样本可包含从移动装置行为、软件应用程序或移动装置中的过程的先前观测或分析中收集的信息。训练样本和/或新的分类器模型(h1(x))可基于包含在先前分类器中的问题或测试条件的类型和/或基于从先前数据/行为模型或分类器的执行/应用中收集的准确性或性能特性而产生。

[0122] 在框604中,装置处理器可以增强(或增加)通过所产生的决策树/分类器(h1(x))错分类的条目的权重以产生第二新树/分类器(h2(x))。在一实施例中,训练样本和/或新分类器模型(h2(x))可以基于分类器的先前执行或使用(h1(x))的错误率而产生。在一实施例中,训练样本和/或新分类器模型(h2(x))可以基于确定为对分类器的先前执行或使用中的错误率或数据点的错分类有贡献的属性而产生。

[0123] 在一实施例中,错分类条目可以基于它们的相对准确性或有效性而加权。在操作606中,处理器可以增强(或增加)通过所产生的第二树/分类器(h2(x))错分类的条目的权重以产生第三新树/分类器(h3(x))。在操作608中,可重复604到606的操作以产生“t”数目的新树/分类器($h_t(x)$)。

[0124] 通过增强或增加通过第一决策树/分类器(h1(x))错分类的条目的权重,第二树/分类器(h2(x))可以更准确地对通过第一决策树/分类器(h1(x))错分类的实体进行分类,但是也可能对通过第一决策树/分类器(h1(x))正确地分类的实体中的一些进行错分类。类似地,第三树/分类器(h3(x))可准确地对由第二决策树/分类器(h2(x))错分类的实体进行分类并且对通过第二决策树/分类器(h2(x))正确地分类的实体中的一些进行错分类。也就是说,产生所述系列的树/分类器$h1(x)-h_t(x)$不会导致整体收敛的系统,而是导致可以并行地执行的多个决策树/分类器。

[0125] 图7说明了根据一实施例用于执行动态和自适应观测的实例方法700。方法700可由移动或资源受限的计算装置的装置处理器执行,所述计算装置以处理器可执行指令配置以执行所述方法的操作。在框702中,装置处理器可通过监视/观测可能贡献于移动装置的降级的大量因数、行为和活动的子集而执行粗略观测。在框703中,装置处理器可产生表征所述粗略观测和/或基于粗略观测的移动装置行为的行为向量。在框704中,装置处理器可识别与粗略观测相关联的可能潜在地贡献于移动装置的降级的子系统、过程和/或应用程序。举例来说,这可以通过比较从多个来源接收的信息与从移动装置的传感器接收的情境信息而实现。在框706中,装置处理器可基于粗略观测而执行行为分析操作。

[0126] 在确定框708中,装置处理器可以确定可疑行为或潜在问题是否可以基于行为分

析的结果得到识别和校正。当装置处理器确定可疑行为或潜在问题可以基于行为分析的结果得到识别和校正时(即,确定框708＝“是”),在框718中,处理器可以起始过程以校正行为并且返回到框702以执行额外的粗略观测。

[0127] 当装置处理器确定可疑行为或潜在问题无法基于行为分析的结果得到识别和/或校正时(即,确定框708＝“否”),在确定框709中装置处理器可以确定是否存在问题的可能性。在一实施例中,装置处理器可以确定存在问题的可能性,方法是计算移动装置遇到潜在问题和/或参与可疑行为的概率,并且确定计算出的概率是否大于预定阈值。当装置处理器确定所计算概率不大于预定阈值和/或不存在可疑行为或潜在问题存在和/或可检测的可能性时(即,确定框709＝“否”),处理器可返回到框702以执行额外粗略观测。

[0128] 当装置处理器确定存在可疑行为或潜在问题存在和/或可检测的可能性时(即,确定框709＝“是”),在框710中,装置处理器可在所识别的子系统、过程或应用程序上执行更深入的记录/观测或最终记录。在框712中,装置处理器可在所识别的子系统、过程或应用程序上执行更深入且更详细的观测。在框714中,装置处理器可以基于更深入且更详细的观测执行进一步和/或更深入的行为分析。在确定框708中,装置处理器可以再次确定可疑行为或潜在问题是否可以基于更深入的行为分析的结果得到识别和校正。当装置处理器确定可疑行为或潜在问题无法基于更深入的行为分析的结果得到识别和校正时(即,确定框708＝“否”),处理器可以重复在框710到714中的操作直到细节水平足够精细以识别问题或直到确定所述问题无法通过额外的细节得到识别或不存在问题为止。

[0129] 当装置处理器确定可疑行为或潜在问题可以基于更深入行为分析的结果得到识别和校正时(即,确定框708＝“是”),在框718中,装置处理器可以执行操作以校正问题/行为,并且处理器可以返回到框702以执行额外的操作。

[0130] 在一实施例中,作为方法700的框702到718的一部分,装置处理器可执行系统的行为的实时行为分析以从有限的且粗略的观测中识别可疑行为、动态地确定行为以更详细地观测,并且动态地确定观测所需要的精确细节水平。这使得装置处理器能够有效地识别问题并且防止问题的发生,而无需使用装置上的大量的处理器、存储器或电池资源。

[0131] 各种实施例通过使用行为分析和/或机器学习技术(与基于许可、策略或规则的方法相反)以监视和分析软件应用程序的选择群组的共同行为来改进现有解决方案。行为分析或机器学习技术的使用是重要的,这是因为现代计算装置是高度可配置的且复杂的系统,并且对于确定软件应用程序是否是串通的最重要的因素在每个装置中可能是不同的。另外,装置特征/因数的不同组合可能需要在每个装置中的分析以便所述装置确定软件应用程序是否是串通的。但需要监视和分析的特征/因数的精确组合常常仅可使用从其中执行一或多个活动的特定计算装置获得的信息且在所述活动/多个活动在进行中时确定。出于这些和其它原因,现有解决方案无法胜任在行为进行中的同时实时监视、检测和表征计算装置中的多个软件应用程序的共同行为或它们之间的关系,且不消耗大量的计算装置的处理、存储器或电力资源。

[0132] 包含上文参考图2到7所论述的实施例的各种实施例可在以处理器可执行指令配置的多种计算装置上实施,所述计算装置的实例在图8中以智能电话的形式说明。智能电话800可包含处理器802,其耦合到内部存储器804、显示器812和扬声器814。另外,智能电话800可包含用于发送和接收电磁辐射的天线,其可连接到耦合到处理器802的无线数据链路

和/或蜂窝式电话收发器808。智能电话800通常还包含用于接收用户输入的菜单选择按钮或摇臂开关820。

[0133] 典型智能电话800还包含声音编码/解码(编解码器)电路806,所述电路将从麦克风接收的声音数字化为适合于无线发射的数据包,且解码所接收的声音数据包以产生提供到扬声器以产生声音的模拟信号。而且,处理器802、无线收发器808及编解码器806中的一或多者可包含数字信号处理器(DSP)电路(未单独地展示)。

[0134] 处理器802可为可由处理器可执行指令(应用程序)配置以执行多种功能和操作(包含如下所述的各种实施例的操作)的任何可编程微处理器、微型计算机或多处理器芯片。在一些移动装置中,可以提供多个处理器802,例如一个处理器专用于无线通信功能,并且一个处理器专用于运行其它应用程序。通常,软件应用程序可在它们被存取且加载到处理器802中之前存储在内部存储器804中。处理器802可包含足以存储应用程序软件指令的内部存储器。在各种实施例中,处理器802可为装置处理器、处理核心或SOC(例如在图1中说明的实例SOC 100)。在实施例中,智能电话800可包含SOC,且处理器802可为包含在所述SOC中的处理器中的一者(例如在图1中说明的处理器102、104、106、108、110中的一者)。

[0135] 各种实施例可进一步包含计算装置,其包含用于将从用户输入装置接收的原始数据与用户交互事件信息进行比较以产生分析结果的装置,以及用于使用所产生分析结果以确定用户交互(UI)事件是否与计算装置的用户相关的装置。在一些实施例中,所述用于将从用户输入装置接收的原始数据与用户交互事件信息进行比较以产生分析结果的装置可包含用于将从装置驱动器接收的原始数据与从高层级操作系统接收的交互信息进行比较的装置。在一些实施例中,所述计算装置可进一步包含用于响应于确定所述UI事件不与计算装置的用户相关而将软件应用程序的活动分类为非良性的装置。在一些实施例中,所述计算装置可进一步包含:用于产生表征软件应用程序的活动的行为向量的装置;用于响应于确定UI事件不与计算装置的用户相关而将所产生行为向量应用于包含决策节点的分类器模型的装置,所述决策节点评估是否存在对应于所述活动的UI事件;以及用于使用将所产生行为向量应用于所述分类器模型的结果以确定软件应用程序的活动是否为非良性的装置。在一些实施例中,所述计算装置可进一步包含:用于产生表征软件应用程序的活动的行为向量的装置;用于响应于确定UI事件不与计算装置的用户相关而选择不包含决策节点的分类器模型的装置,所述决策节点测试是否存在对应于所述活动的UI事件;用于将所产生行为向量应用于选定分类器模型以产生额外分析结果的装置;以及用于使用所产生额外分析结果以确定软件应用程序的活动是否为非良性的装置。在一些实施例中,所述计算装置可进一步包含:用于响应于确定UI事件不与计算装置的用户相关而选择一系列稳健分类器模型的装置;以及用于将多个行为向量应用于选定系列的稳健分类器模型以确定软件应用程序的活动是否为非良性的装置。

[0136] 如本申请中所使用,术语“组件”、“模块”等等意图包括计算机相关实体,例如但不限于,硬件、固件、硬件与软件的组合、软件或执行中的软件,其经配置以执行特定操作或功能。举例来说,组件可为但不限于在处理器上运行的过程、处理器、对象、可执行程序、执行线程、程序和/或计算机。借助于说明,在计算装置上运行的应用程序以及所述计算装置可被称为组件。一或多个组件可以驻留在过程和/或执行线程内,并且组件可以局部化于一个处理器或核心上和/或分布在两个或大于两个处理器或核心之间。另外,这些组件可以从具

有存储在其上的各种指令和/或数据结构的各种非暂时性计算机可读媒体中执行。组件可以借助于本地和/或远程过程、功能或过程调用、电子信号、数据包、存储器读取/写入和其它已知的网络、计算机、处理器和/或过程相关通信方法进行通信。

[0137] 用于在可编程处理器上执行以用于执行各种实施例的操作的计算机程序代码或“程序代码”可以例如C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、结构化查询语言(例如,Transact-SQL)、Perl或各种其它编程语言等高级编程语言编写。存储在计算机可读存储媒体上的程序代码或程序如在本申请中所使用可以指机器语言代码(例如,目标代码),所述机器语言代码的格式可由处理器理解。

[0138] 许多移动计算装置操作系统内核被组织到用户空间(其中运行非特许代码)和内核空间(其中运行特许代码)中。这一分离在Android®和其它通用公共许可证(GPL)环境中是尤其重要的,在所述环境中作为内核空间的一部分的代码必须是GPL授权的,而在用户空间中运行的代码可以不是GPL授权的。应理解除非另外明确地陈述,否则此处所讨论的各种软件组件/模块可以在内核空间或用户空间中实施。

[0139] 前述方法描述和过程流程图仅仅作为说明性实例提供,并且其并不意图要求或暗示各种实施例的操作必须以所呈现的顺序进行。如所属领域的技术人员将了解,可以任何次序执行前述实施例中的操作的次序。例如“此后”、“接着”、“接下来”等词无意限制操作的次序;这些词仅用以引导读者浏览对方法的描述。另外,举例来说,使用冠词“一”、“一个”或“所述”对单数形式的权利要求要素的任何参考不应被解释为将所述要素限制为单数。

[0140] 结合本文中所公开的实施例描述的各种说明性逻辑块、模块、电路和算法操作可实施为电子硬件、计算机软件,或两者的组合。为了清楚地说明硬件与软件的此可互换性,上文已大体上就其功能性来说描述了各种说明性组件、块、模块、电路和步骤。此类功能性是实施为硬件还是软件取决于具体应用及强加于整个系统的设计约束。熟练的技术人员可以针对每一特定应用以不同方式来实施所描述的功能性,但此类实施决策不应被解释为会导致脱离本发明的范围。

[0141] 用于实施结合本文中所揭示的实施例而描述的各种说明性逻辑、逻辑块、模块和电路的硬件可用以下各项来实施或执行: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)或经设计以执行本文中所描述的功能的其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件,或其任何组合。通用处理器可为多处理器,但在替代方案中,处理器可为任何常规的处理器、控制器、微控制器或状态机。处理器也可以被实施为计算装置的组合,例如,DSP和多处理器的组合、多个多处理器、一或多个多处理器结合DSP核心,或任何其它此类配置。替代地,可由特定地针对给定功能的电路来执行一些步骤或方法。

[0142] 在一或多个示范性实施例中,所述功能可以在硬件、软件、固件或其任何组合中实施。如果在软件中实施,那么所述功能可以作为一或多个处理器可执行指令或代码存储在非暂时性计算机可读储存媒体或非暂时性处理器可读存储媒体上。本文所揭示的方法或算法的操作可实施于处理器可执行软件模块中,所述软件模块可呈存储在非暂时性计算机可读存储媒体或处理器可读存储媒体上的所存储处理器可执行软件指令的形式。非暂时性计算机可读或处理器可读媒体可为可由计算机或处理器存取的任何存储媒体。借助实例但非限制,此类非暂时性计算机可读或处理器可读媒体可包含RAM、ROM、EEPROM、快闪存储器、

CD-ROM或其它光盘存储器、磁盘存储器或其它磁性存储装置，或可用于以指令或数据结构的形式存储所要的程序代码且可由计算机存取的任何其它媒体。如本文中所使用的磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘用激光以光学方式再现数据。以上各者的组合还包含在非暂时性计算机可读和处理器可读媒体的范围内。另外，方法或算法的操作可作为代码和/或指令中的一者或任何组合或集合而驻留在可并入到计算机程序产品中的非暂时性处理器可读媒体和/或计算机可读媒体上。

[0143] 提供对所揭示的实施例的先前描述以使所属领域的技术人员能够制作或使用本发明。所属领域的技术人员将容易了解对这些实施例的各种修改，且可在不脱离本发明的精神或范围的情况下将本文定义的一般原理应用于其它实施例。因此，本发明并不希望限于本文中所示的实施例，而应被赋予与随附权利要求书和本文中所揭示的原理和新颖特征相一致的最广泛范围。

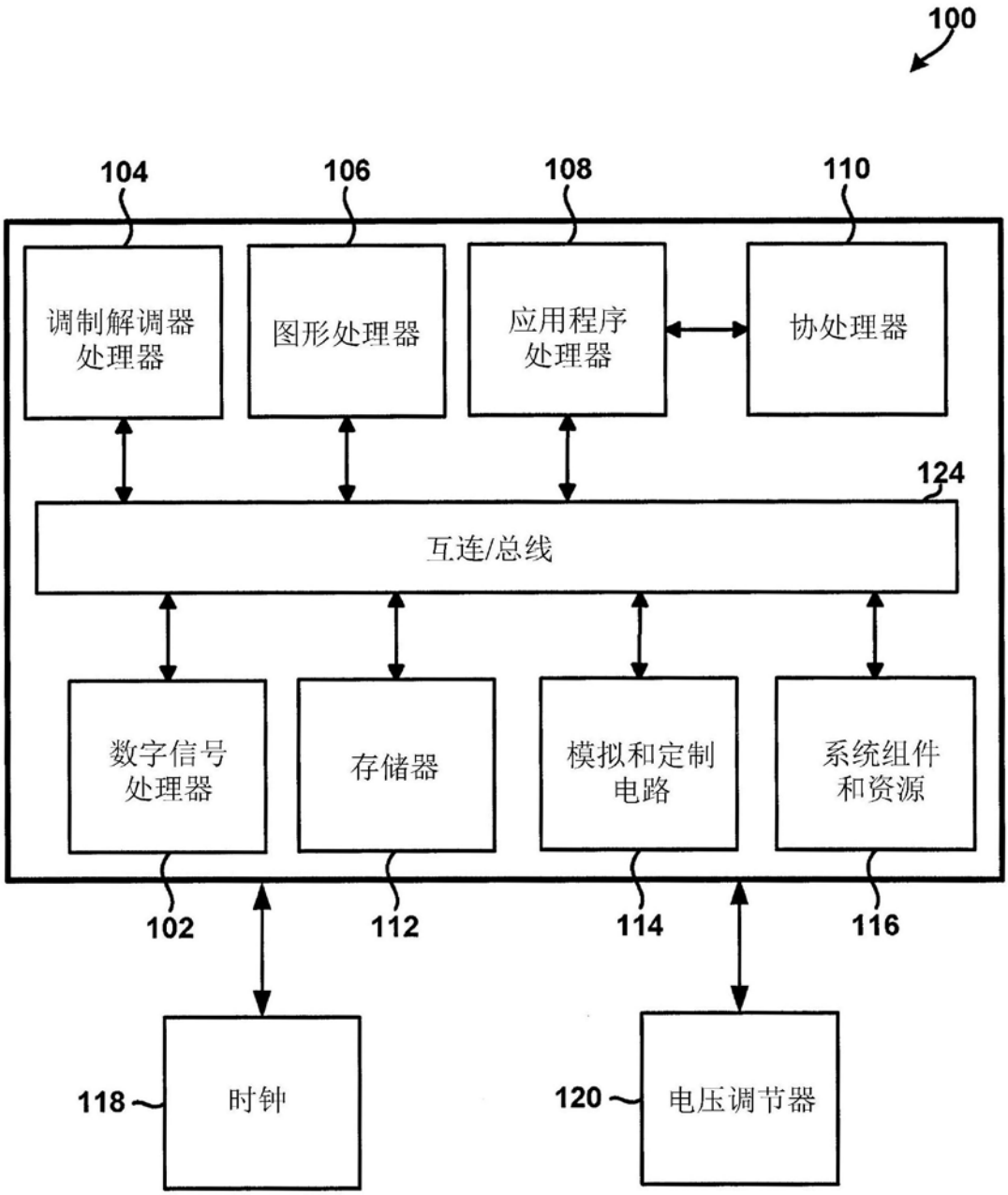

100
104
106
108
110
调制解调器处理器
图形处理器
应用程序处理器
协处理器
124
互连/总线
数字信号处理器
存储器
模拟和定制电路
系统组件和资源
102
112
114
116
118
时钟
120
电压调节器

图1

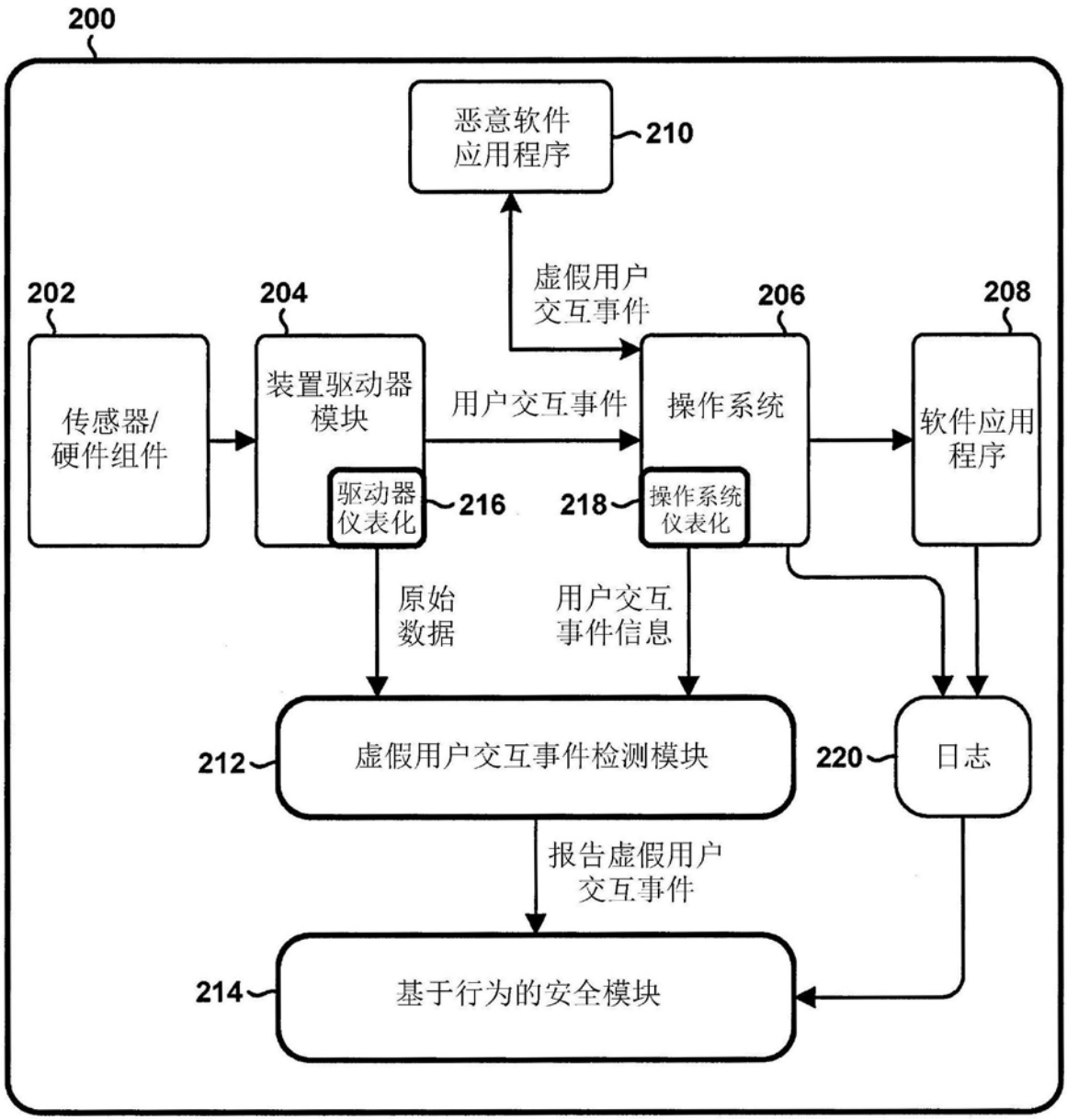

200
恶意软件
应用程序
210
虚假用户
交互事件
202
204
206
208
传感器/
硬件组件
装置驱动器
模块
用户交互事件
操作系统
软件应用
程序
驱动器
仪表化
216
218
操作系统
仪表化
原始
数据
用户交互
事件信息
212
虚假用户交互事件检测模块
220
日志
报告虚假用户
交互事件
214
基于行为的安全模块

图2

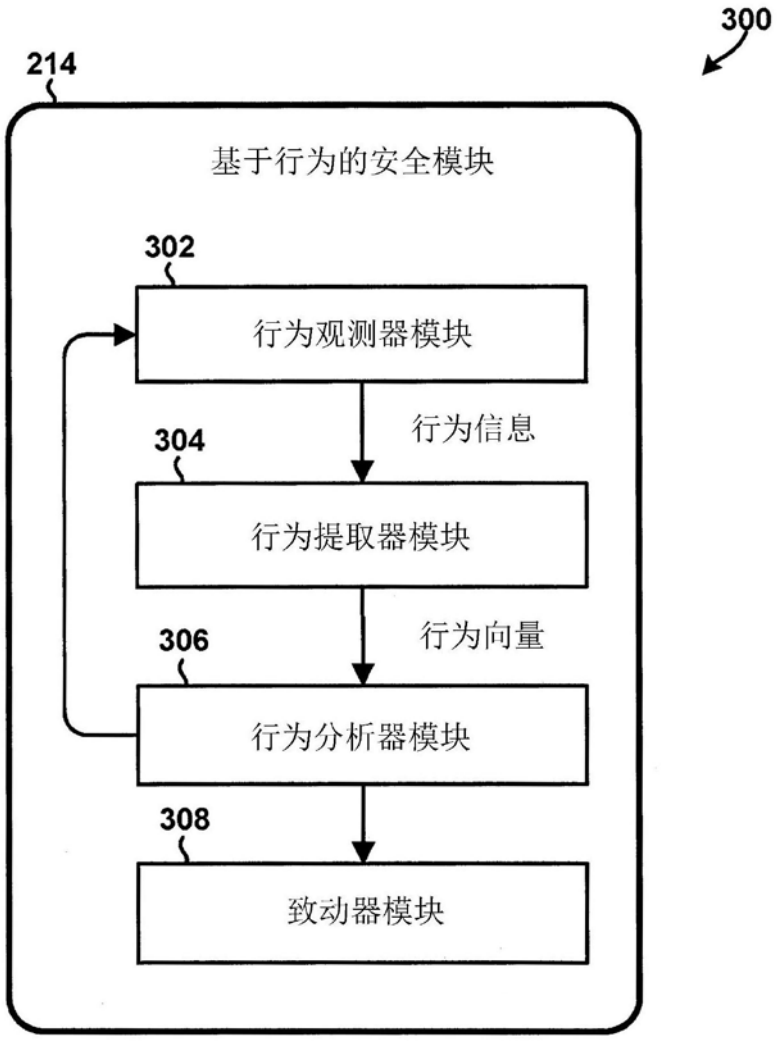

300
214
基于行为的安全模块
302
行为观测器模块
行为信息
304
行为提取器模块
行为向量
306
行为分析器模块
308
致动器模块

图3

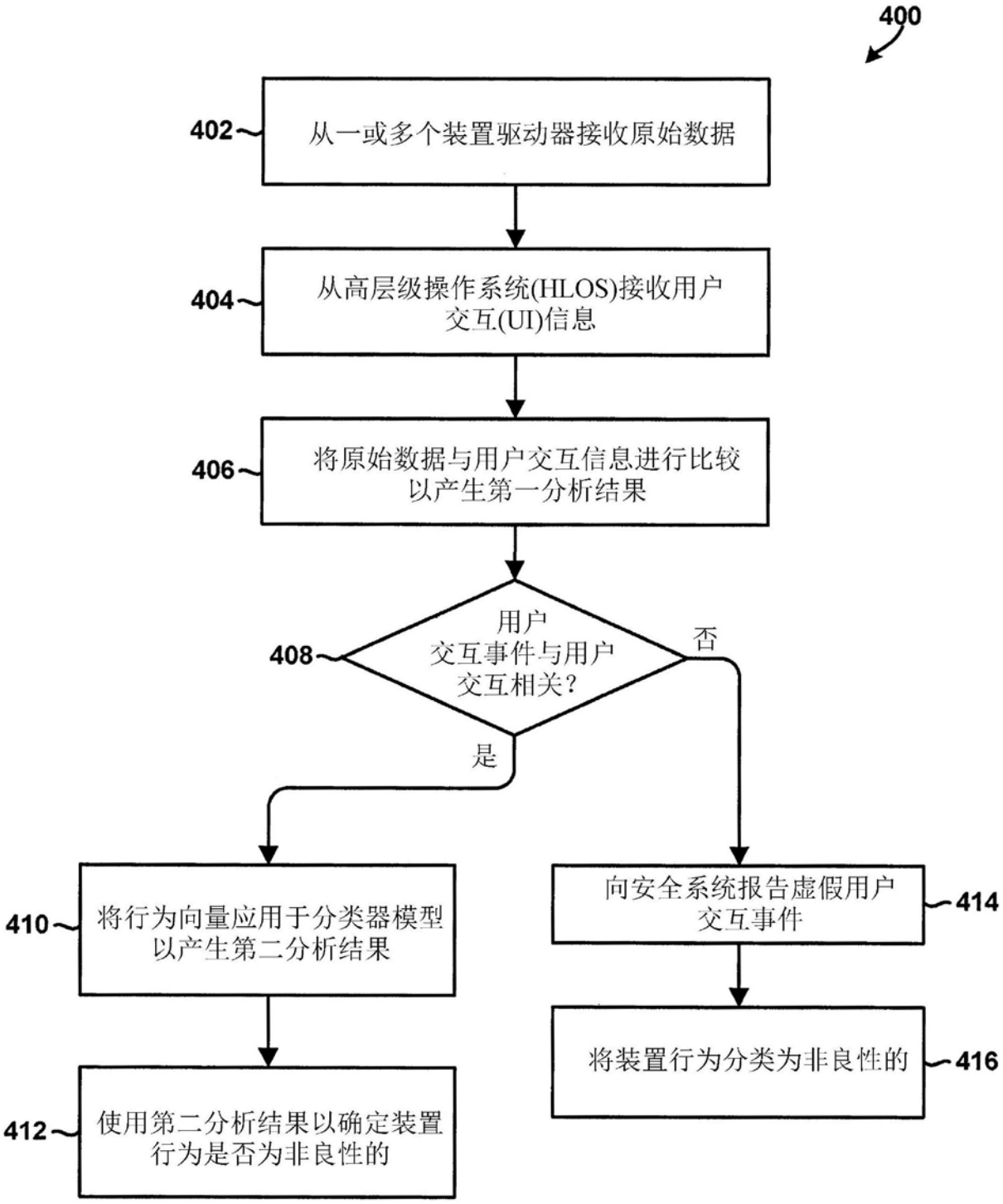

400
402
从一或多个装置驱动器接收原始数据
404
从高层级操作系统(HLOS)接收用户交互(UI)信息
406
将原始数据与用户交互信息进行比较以产生第一分析结果
408
用户交互事件与用户交互相关?
否
是
410
将行为向量应用于分类器模型以产生第二分析结果
412
使用第二分析结果以确定装置行为是否为非良性的
414
向安全系统报告虚假用户交互事件
416
将装置行为分类为非良性的

图4A

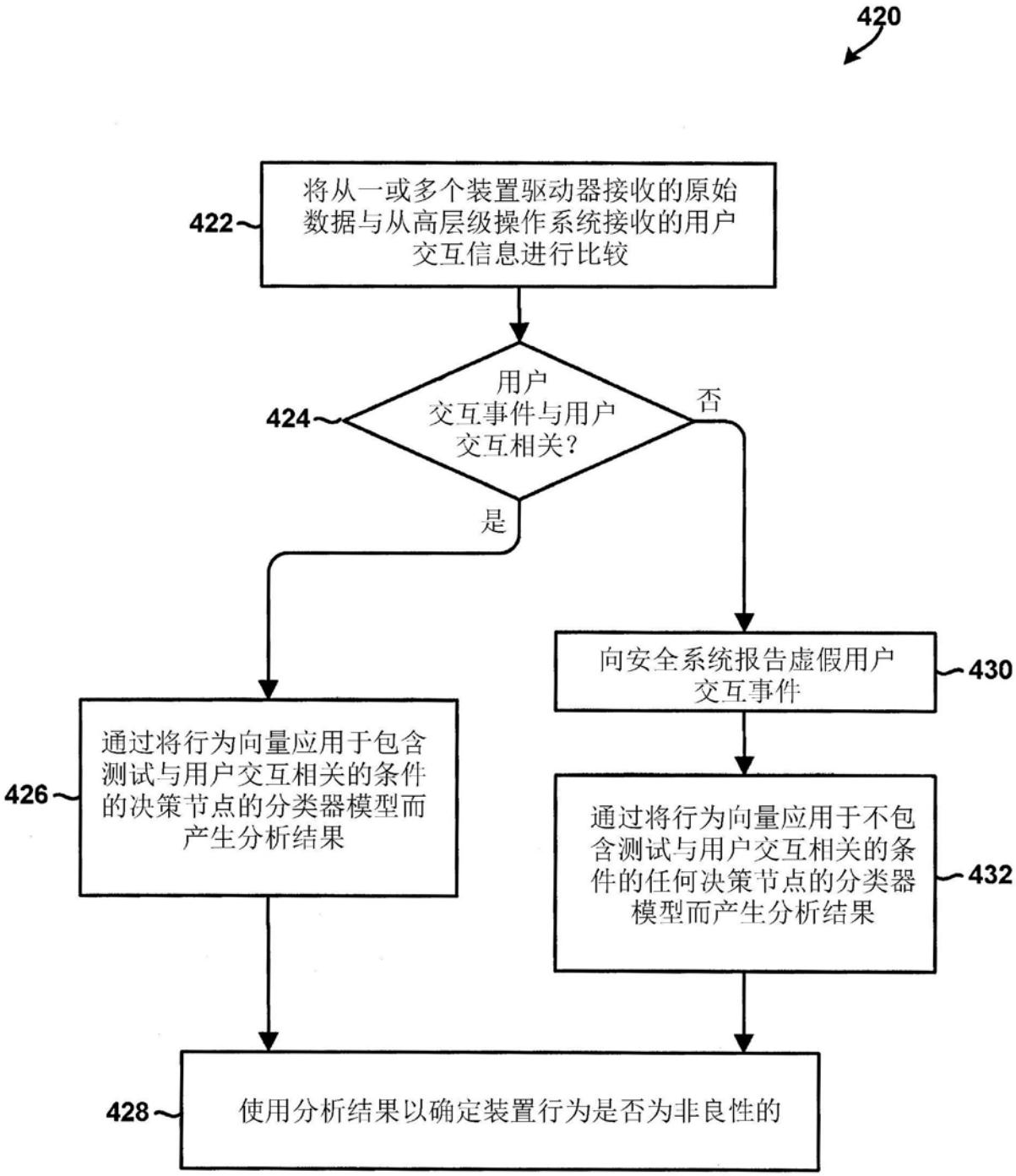

420
422
将从一或多个装置驱动器接收的原始数据与从高层级操作系统接收的用户交互信息进行比较
424
用户交互事件与用户交互相关?
否
是
426
通过将行为向量应用于包含测试与用户交互相关的条件的决策节点的分类器模型而产生分析结果
430
向安全系统报告虚假用户交互事件
432
通过将行为向量应用于不包含测试与用户交互相关的条件的任何决策节点的分类器模型而产生分析结果
428
使用分析结果以确定装置行为是否为非良性的

图4B

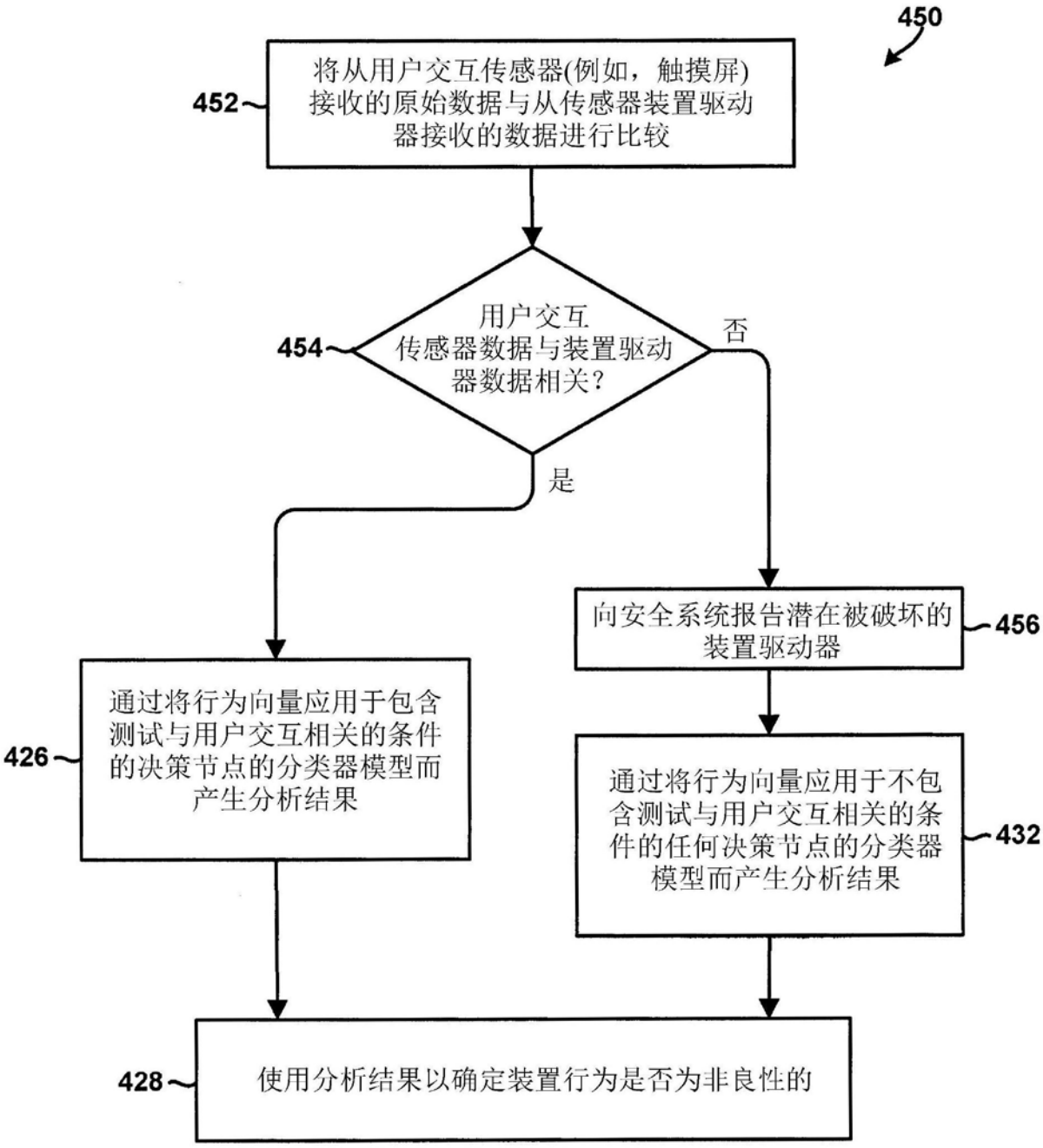

450
452
将从用户交互传感器(例如，触摸屏)接收的原始数据与从传感器装置驱动器接收的数据进行比较
454
用户交互传感器数据与装置驱动器数据相关?
否
是
向安全系统报告潜在被破坏的装置驱动器
456
通过将行为向量应用于包含测试与用户交互相关的条件的决策节点的分类器模型而产生分析结果
426
通过将行为向量应用于不包含测试与用户交互相关的条件的任何决策节点的分类器模型而产生分析结果
432
428
使用分析结果以确定装置行为是否为非良性的

图4C

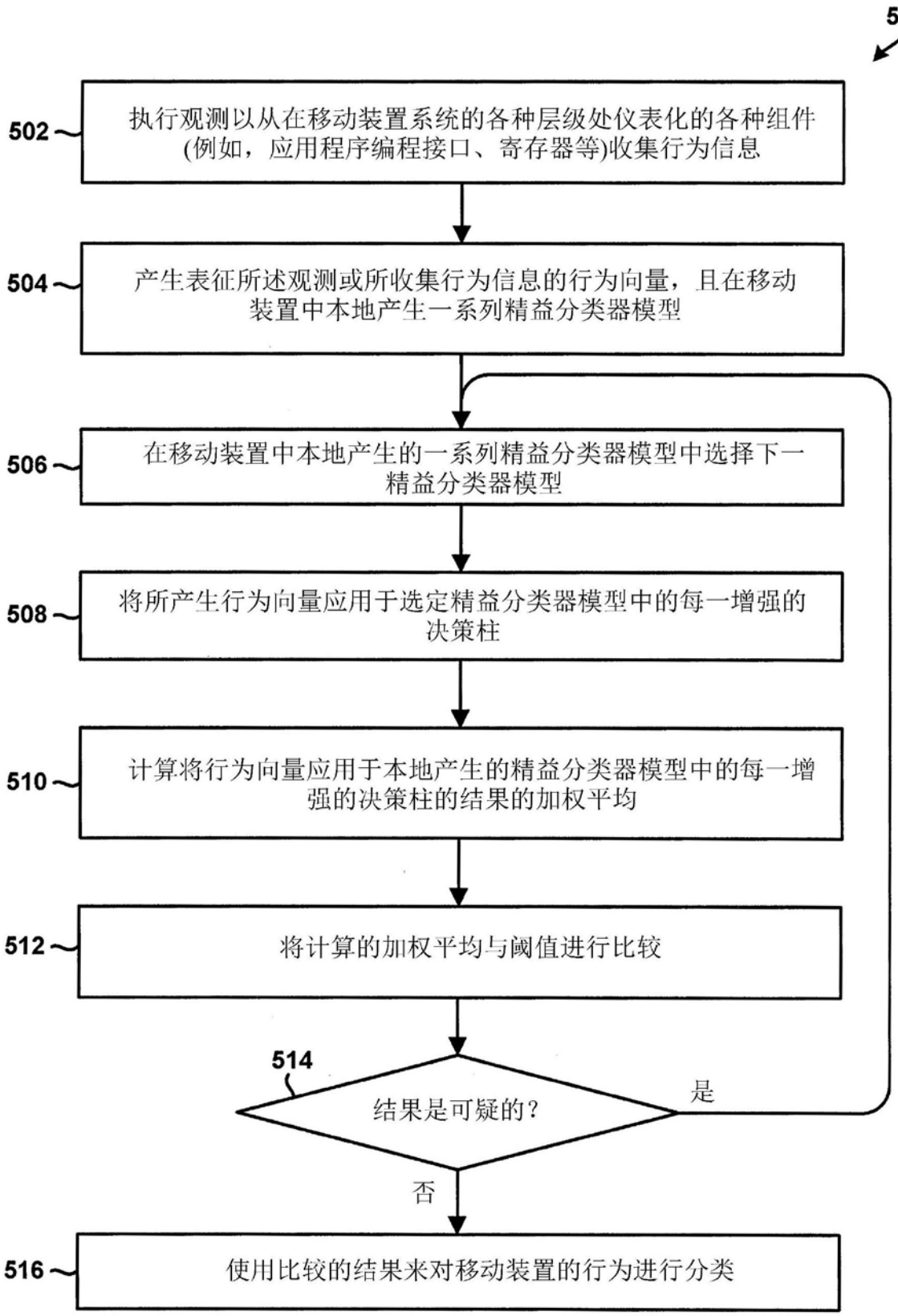

500
502
执行观测以从在移动装置系统的各种层级处仪表化的各种组件(例如，应用程序编程接口、寄存器等)收集行为信息
504
产生表征所述观测或所收集行为信息的行为向量，且在移动装置中本地产生一系列精益分类器模型
506
在移动装置中本地产生的一系列精益分类器模型中选择下一精益分类器模型
508
将所产生行为向量应用于选定精益分类器模型中的每一增强的决策柱
510
计算将行为向量应用于本地产生的精益分类器模型中的每一增强的决策柱的结果的加权平均
512
将计算的加权平均与阈值进行比较
514
结果是可疑的？
是
否
516
使用比较的结果来对移动装置的行为进行分类

图5

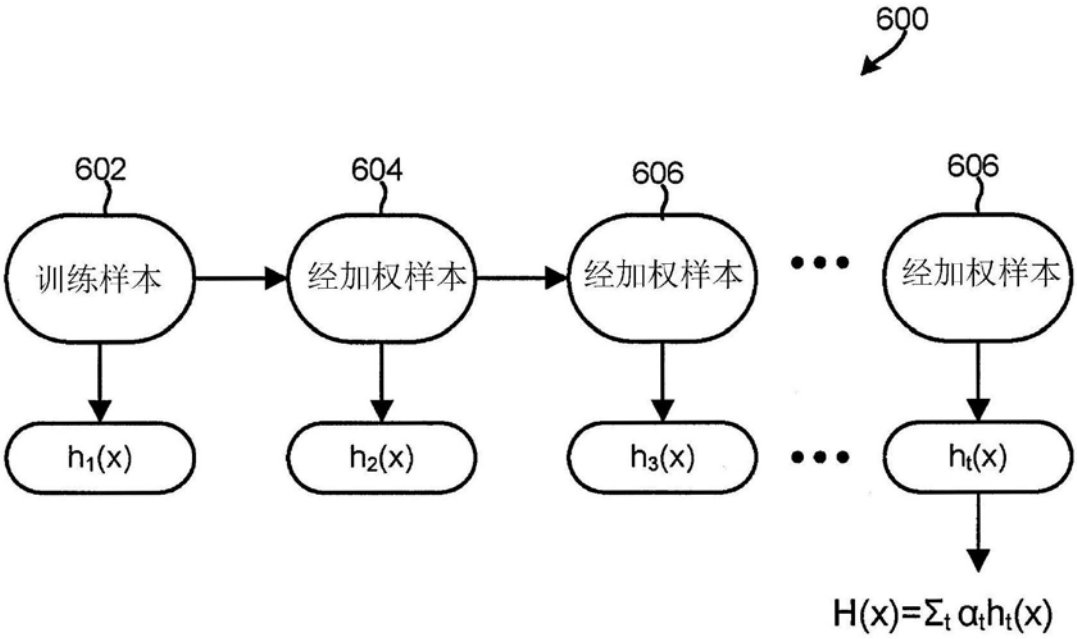

600
602
604
606
606
训练样本
经加权样本
经加权样本
经加权样本
h1(x)
h2(x)
h3(x)
ht(x)
H(x)=Σt αtht(x)

图6

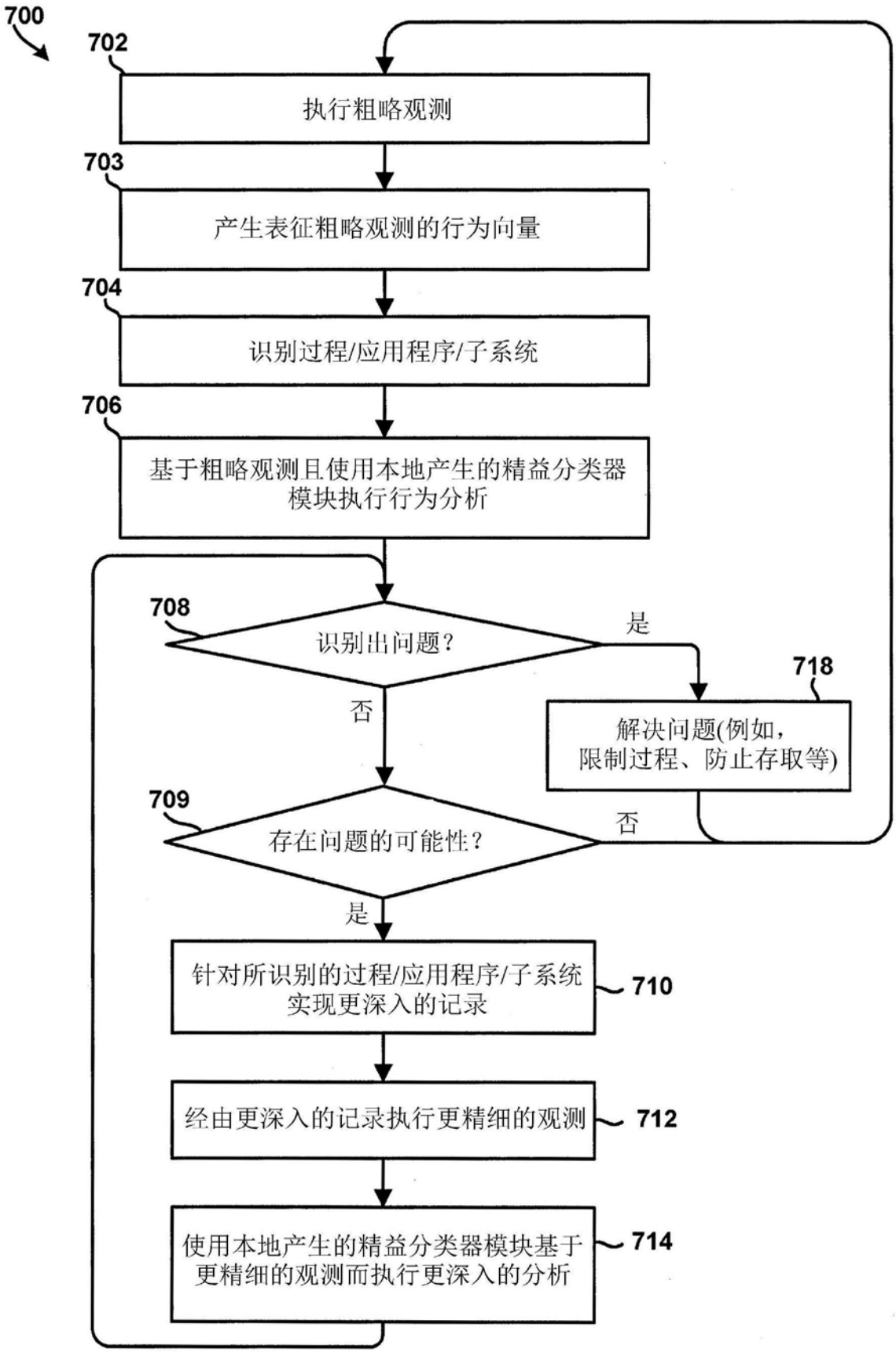

700
702
执行粗略观测
703
产生表征粗略观测的行为向量
704
识别过程/应用程序/子系统
706
基于粗略观测且使用本地产生的精益分类器模块执行行为分析
708
识别出问题?
是
718
解决问题(例如，限制过程、防止存取等)
否
709
存在问题的可能性?
否
是
针对所识别的过程/应用程序/子系统实现更深入的记录
710
经由更深入的记录执行更精细的观测
712
使用本地产生的精益分类器模块基于更精细的观测而执行更深入的分析
714

图7

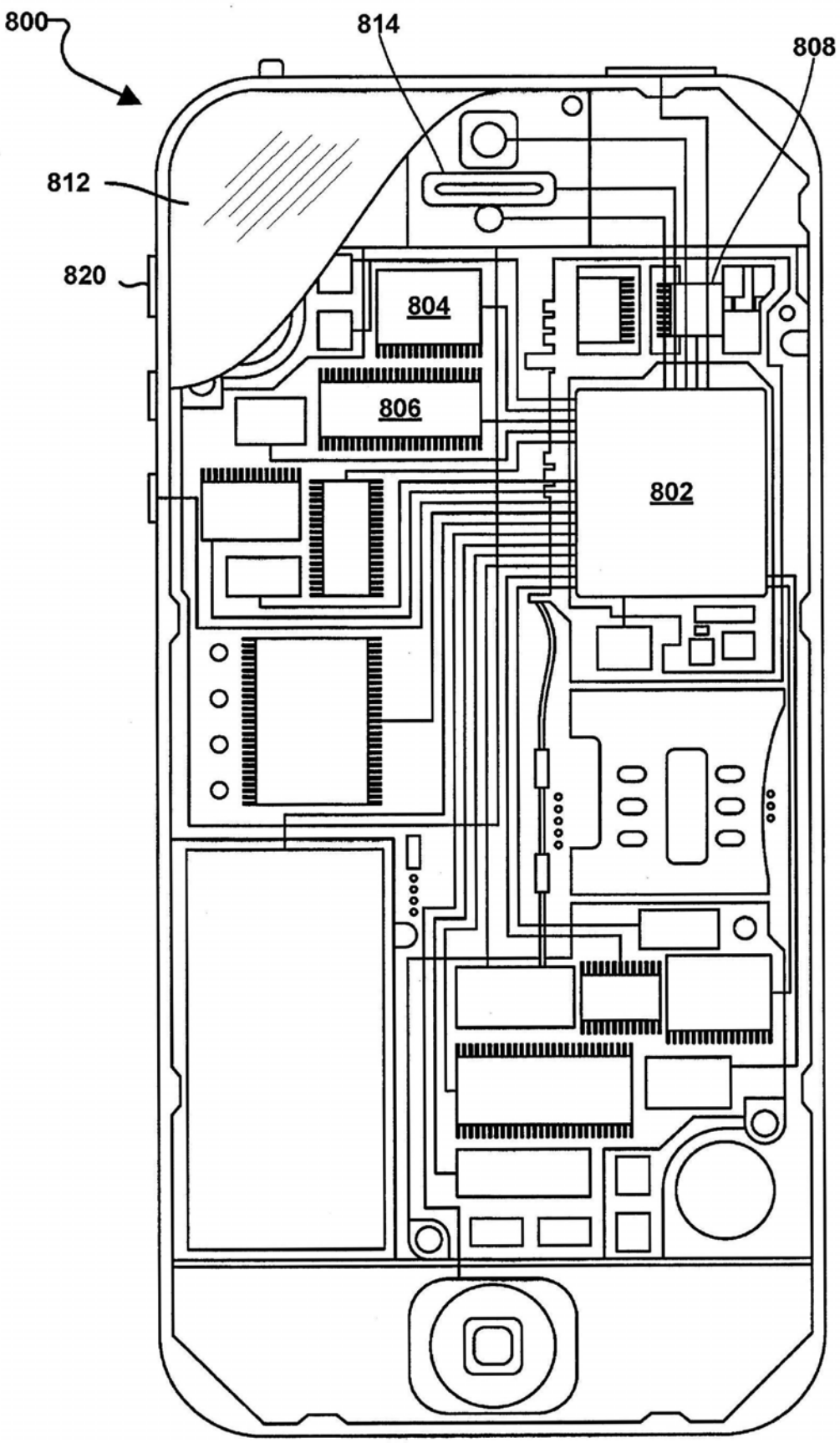


图8