(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 104662517 B
(45)授权公告日 2019.02.15

(21)申请号 201480002261.5

(22)申请日 2014.06.26

(65)同一申请的已公布的文献号
申请公布号 CN 104662517 A

(43)申请公布日 2015.05.27

(30)优先权数据
13/931426 2013.06.28 US

(85)PCT国际申请进入国家阶段日
2015.02.28

(86)PCT国际申请的申请数据
PCT/US2014/044302 2014.06.26

(87)PCT国际申请的公布数据
WO2014/210289 EN 2014.12.31

(73)专利权人 赛门铁克公司
地址 美国加利福尼亚州

(72)发明人 S·里韦拉 P·艾希莉

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 周亚荣 安翔

(51)Int.Cl.
G06F 11/00(2006.01)

(56)对比文件
CN 101562609 A,2009.10.21,
US 2006253584 A1,2006.11.09,
US 8001606 B1,2011.08.16,
US 2012124664 A1,2012.05.17,
US 2010077445 A1,2010.03.25,
JP 2010079901 A,2010.04.08,
JP 2013045279 A,2013.03.04,
EP 2169580 A2,2010.03.31,

审查员 王倩

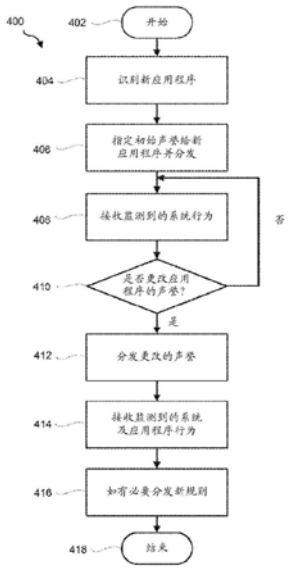
权利要求书3页 说明书11页 附图5页

(54)发明名称

安全漏洞检测技术

(57)摘要

本发明公开了安全漏洞检测技术。在一个具体实施例中,所述技术可实现为用于检测安全漏洞的方法,所述方法包括:指定声誉给应用程序;分发所述声誉给客户端;从所述客户端接收与执行所述应用程序的所述客户端有关的监测到的系统行为;根据所述监测到的系统行为确定是否更改所述应用程序的所述声誉;分发更改的声誉给所述客户端;从所述客户端接收进一步监测到的系统行为;以及根据从所述客户端接收的所述监测到的系统行为确定是否生成针对所述应用程序的规则。



CN 104662517 B

1.一种检测安全漏洞的方法,所述方法包括:

在后台系统处确定应用程序的初始声誉,其中,所述应用程序是先前在多个客户端上卸载的新的应用程序并且所述初始声誉是基于对以下的分析:所述应用程序的作者和在所述应用程序的安装期间所述多个客户端的行为;

从所述后台系统经由网络将所述初始声誉分发给所述多个客户端;

在所述后台系统处从所述多个客户端中的一个客户端接收与执行所述应用程序的所述多个客户端中的所述一个客户端有关的监测到的系统行为,其中,所述多个客户端中的所述一个客户端基于针对所述应用程序的安全强制执行来执行所述应用程序,针对所述应用程序的安全强制执行是根据所述应用程序的所述初始声誉和所述应用程序的行为确定的;

在所述后台系统处基于所述监测到的系统行为确定是否更改所述应用程序的所述初始声誉;

分发所更改的声誉给所述多个客户端;

从所述多个客户端中的所述一个客户端接收进一步监测到的系统行为;以及

基于从所述多个客户端中的所述一个客户端接收的所述进一步监测到的系统行为确定要执行的动作。

2.根据权利要求1所述的方法,其中,确定所述应用程序的所述初始声誉包括指定所述初始声誉,并且其中,所述初始声誉指示所述应用程序是否是可信、中性、可疑、和恶意程序中的一种。

3.根据权利要求1所述的方法,其中,所述分析包括确定所述应用程序是否是来自已知实体,并且其中在所述应用程序的安装期间所述多个客户端的所述行为是使用探试法来分析的。

4.根据权利要求3所述的方法,其中,确定所述应用程序的所述初始声誉包括指定所述初始声誉,所述初始声誉是基于所述已知实体来指定的。

5.根据权利要求1所述的方法,其中,所述应用程序是基于由所述多个客户端接收到的声誉而在所述多个客户端上执行的。

6.根据权利要求1所述的方法,其中,在所述监测到的系统行为指示所述应用程序正表现出可疑行为时所述应用程序的所述初始声誉被更改。

7.根据权利要求5所述的方法,其中,所述应用程序的所述初始声誉是基于从执行所述应用程序的所述多个客户端接收的监测到的系统行为而更改的。

8.根据权利要求1所述的方法,其中,所述监测到的系统行为包括与客户端系统的行为以及在所述多个客户端中的所述一个客户端上执行的所述应用程序有关的详细信息。

9.根据权利要求1所述的方法,其中,所述要执行的动作包括针对所述应用程序生成规则,并且其中,针对所述应用程序的所述规则指示所述应用程序将是以下一种:隔离的、防止访问特定客户端资源的、在虚拟客户端上执行的、以及允许完全访问客户端资源的。

10.根据权利要求9所述的方法,还包括:

将针对所述应用程序生成的所述规则传送到所述客户端。

11.至少一种存储计算机程序指令的非瞬时性处理器可读存储介质,所述非瞬时性处理器可读存储介质被配置为能够由至少一个处理器读取以指示所述至少一个处理器执行

用于执行根据权利要求1所述的方法的计算机进程。

12.一种检测安全漏洞的方法,所述方法包括:

从后台系统接收应用程序的初始声誉,其中,所述应用程序是先前在多个客户端上卸载的新的应用程序并且所述初始声誉是基于对以下的分析:所述应用程序的作者和在所述应用程序的安装期间所述多个客户端的行为;

基于所述应用程序的所述初始声誉和所述应用程序的行为,确定所述应用程序的安全强制执行;

基于所述初始声誉和所确定的安全强制执行而执行所述应用程序;

在执行所述应用程序时监测系统行为;

将监测到的系统行为报告给所述后台系统;

确定是否已从所述后台系统接收到所述应用程序的更改的声誉;

基于所述更改的声誉监测所述系统行为;以及

将监测到的系统行为传送给所述后台系统。

13.根据权利要求12所述的方法,其中,所述初始声誉是指定的声誉。

14.根据权利要求12所述的方法,其中,监测所述系统行为包括以下至少一个:监测未经授权的系统资源访问、对系统操作系统的未经授权写入、安全应用程序的终止、以及未经授权的网络活动。

15.根据权利要求12所述的方法,其中,所述系统行为是基于探试法而针对已知的可疑和恶意行为来监测的。

16.根据权利要求12所述的方法,其中,当所述初始声誉指示所述应用程序可信时以第一频率监测所述系统行为,并且当所述更改的声誉指示所述应用程序不可信时以高于所述第一频率的第二频率监测所述系统行为。

17.根据权利要求12所述的方法,其中,检测到可疑的系统行为时,根据指定的声誉为可信的而继续执行所述应用程序。

18.根据权利要求12所述的方法,还包括:

确定是否已经从所述后台系统接收了针对所述应用程序的新规则;以及

基于所接收的规则执行所述应用程序。

19.至少一种存储计算机程序指令的非瞬时性处理器可读存储介质,所述非瞬时性处理器可读存储介质被配置为能够由至少一个处理器读取以指示所述至少一个处理器执行用于执行根据权利要求12所述的方法的计算机进程。

20.一种检测安全漏洞的系统,包括:

通信地耦接到网络的一个或多个处理器;其中所述一个或多个处理器被配置为:

在后台系统处确定应用程序的初始声誉,其中,所述应用程序是先前在多个客户端上卸载的新的应用程序并且所述初始声誉是基于对以下的分析:所述应用程序的作者和在所述应用程序的安装期间所述多个客户端的行为;

从所述后台系统经由网络将所述初始声誉分发给所述多个客户端;

在所述后台系统处从所述多个客户端中的一个客户端接收与执行所述应用程序的所述多个客户端中的所述一个客户端有关的监测到的系统行为,其中,所述多个客户端中的所述一个客户端基于针对所述应用程序的安全强制执行来执行所述应用程序,针对所述应

用程序的安全强制执行是根据所述应用程序的所述初始声誉和所述应用程序的行为的；

在所述后台系统处基于所述监测到的系统行为确定是否更改所述应用程序的所述初始声誉以产生更改的声誉；

分发所述更改的声誉给所述多个客户端；

从所述多个客户端中的所述一个客户端接收进一步监测到的系统行为；以及

基于从所述多个客户端中的所述一个客户端接收的所述监测到的系统行为确定要执行的动作。

安全漏洞检测技术

技术领域

[0001] 本发明整体涉及计算机病毒和恶意软件，更具体地讲，涉及安全漏洞检测技术。

背景技术

[0002] 此前，计算机病毒和恶意软件常利用先前未知的安全漏洞，也即零日漏洞利用(zero day exploits)。这些计算机病毒和恶意软件可引起多个问题，包括：触及敏感或私人数据、降低系统性能以及分流系统资源。因此，检测此类安全漏洞已经变得非常重要。然而，传统的安全漏洞检测方法需要对系统行为进行追溯分析，以识别计算机病毒或恶意软件所利用的安全漏洞。

[0003] 鉴于上述，可以理解，可能存在与传统安全漏洞检测相关的显著问题和缺陷。

发明内容

[0004] 本发明公开了安全漏洞检测技术。在一个具体实施例中，所述技术可实现为检测安全漏洞的方法，所述方法包括指定声誉(reputation)给应用程序；分发所述声誉给客户端(client)；从所述客户端接收与执行所述应用程序的所述客户端有关的监测到的系统行为；根据所述监测到的系统行为确定是否更改所述应用程序的所述声誉；分发更改的声誉给所述客户端；从所述客户端接收进一步监测到的系统行为；以及根据从所述客户端接收的所述监测到的系统行为确定是否生成针对所述应用程序的规则。

[0005] 根据该具体实施例的其他方面，所述声誉指示应用程序是否是可信的、中性的、可疑的和恶意的应用程序中的一种。

[0006] 根据该具体实施例的其他方面，所述应用程序是来自已知实体的新应用程序。

[0007] 根据该具体实施例的其他方面，根据所述已知实体指定所述应用程序的所述声誉。

[0008] 根据该具体实施例的其他方面，根据所述接收的声誉在所述客户端执行所述应用程序。

[0009] 根据该具体实施例的其他方面，在所述监测到的系统行为指示所述应用程序正表现出可疑行为时更改所述应用程序的所述声誉。

[0010] 根据该具体实施例的其他方面，根据从执行所述应用程序的多个客户端接收的监测到的系统行为来更改所述应用程序的所述声誉。

[0011] 根据该具体实施例的其他方面，所述监测到的系统行为包括与客户端系统的行为以及在所述客户端上执行的所述应用程序的行为有关的详细信息。

[0012] 根据该具体实施例的其他方面，针对所述应用程序的所述规则指示所述应用程序将是隔离的、防止访问某些客户端资源的、在虚拟客户端上执行的以及允许完全访问客户端资源的应用程序中的一种。

[0013] 根据该具体实施例的其他方面，所述方法包括将针对所述应用程序生成的所述规则传送到所述客户端。

[0014] 在另一个具体实施例中，所述技术可实现为至少一种存储计算机程序指令的非瞬时性处理器可读存储介质，所述非瞬时性处理器可读存储介质被配置为可由至少一个处理器读取以指示所述至少一个处理器执行用于执行一种方法的计算机进程，所述方法包括：指定声誉给应用程序；分发所述声誉给客户端；从所述客户端接收与执行所述应用程序的所述客户端有关的监测到的系统行为；根据所述监测到的系统行为确定是否更改所述应用程序的所述声誉；分发更改的声誉给所述客户端；从所述客户端接收进一步监测到的系统行为；以及根据从所述客户端接收的所述监测到的系统行为确定是否生成针对所述应用程序的规则。

[0015] 在另一个具体实施例中，所述技术可实现为一种检测安全漏洞的方法，所述方法包括指定声誉给应用程序；根据所述指定的声誉执行所述应用程序；在执行所述应用程序时监测系统行为；将监测到的系统行为报告给后台系统；确定是否已从所述后台系统接收到所述应用程序的更改的声誉；根据所述更改的声誉监测所述系统行为；将监测到的系统行为传送给所述后台系统；以及确定是否已从所述后台系统接收到针对所述应用程序的新规则。

[0016] 根据该具体实施例的其他方面，根据在所述应用程序安装期间所述应用程序的行为指定所述声誉给所述应用程序。

[0017] 根据该具体实施例的另外的方面，监测所述系统行为包括监测未经授权的系统资源访问、对系统操作系统的未经授权写入、安全应用程序的终止以及未经授权的网络活动中的至少一者。

[0018] 根据该具体实施例的另外的方面，根据探试法针对已知的可疑和恶意行为监测所述系统行为。

[0019] 根据该具体实施例的另外的方面，当所述指定的声誉指示所述应用程序可信时以第一频率监测所述系统行为，并在所述更改的声誉指示所述应用程序不可信时以高于所述第一频率的第二频率监测所述系统行为。

[0020] 根据该具体实施例的另外的方面，当检测到可疑的系统行为时，根据所述指定的为可信的声誉继续执行所述应用程序。

[0021] 根据该具体实施例的其他方面，所述方法包括根据所述接收到的规则执行所述应用程序。

[0022] 在另一个具体实施例中，所述技术可实现为至少一种存储计算机程序指令的非瞬时性处理器可读存储介质，所述非瞬时性处理器可读存储介质被配置为可由至少一个处理器读取以指示所述至少一个处理器执行用于执行一种方法的计算机进程，所述方法包括：指定声誉给应用程序；根据所述指定的声誉执行所述应用程序；在执行所述应用程序时监测系统行为；将监测到的系统行为报告给后台系统；确定是否已从所述后台系统接收到所述应用程序的更改的声誉；根据所述更改的声誉监测所述系统行为；将监测到的系统行为传送给所述后台系统；以及确定是否已从所述后台系统接收到针对所述应用程序的新规则。

[0023] 在另一个具体实施例中，所述技术可实现为一种检测安全漏洞的系统，所述系统包括：通信地耦接到网络的一个或多个处理器；其中所述一个或多个处理器被配置为：指定声誉给应用程序；分发所述声誉给客户端；从所述客户端接收与执行所述应用程序的所述

客户端有关的监测到的系统行为;根据所述监测到的系统行为确定是否更改所述应用程序的所述声誉;分发更改的声誉给所述客户端;从所述客户端接收进一步监测到的系统行为;以及根据从所述客户端接收的所述监测到的系统行为确定是否生成针对所述应用程序的规则。

附图说明

[0024] 为了有利于更全面地理解本发明,现在参考附图,其中类似的标号表示类似的元件。这些附图不应被理解为限制本发明,而是旨在仅为示例性的。

[0025] 图1示出了根据本发明实施例的网络体系结构的框图。

[0026] 图2示出了根据本发明实施例的计算机系统的框图。

[0027] 图3示出了根据本发明实施例的安全漏洞检测模块。

[0028] 图4示出了根据本发明实施例的一种检测安全漏洞的方法。

[0029] 图5示出了根据本发明实施例的一种检测安全漏洞的方法。

具体实施方式

[0030] 图1示出了根据本发明实施例的用于检测安全漏洞的网络体系结构的框图。

[0031] 图1为网络体系结构100的简化视图,该网络体系结构可以包括未示出的另外的元件。网络体系结构100可以包含客户端系统110、120和130,以及服务器140A和140B(可使用图2所示的计算机系统200来实施它们中的一者或多者)。客户端系统110、120和130可以通信地耦接到网络150。服务器140A可以通信地耦接到存储设备160A(1)-(N),而服务器140B可以通信地耦接到存储设备160B(1)-(N)。客户端系统110、120和130可以包含安全漏洞检测模块(如安全漏洞检测模块300)。另外,服务器140A和140B可以包含安全漏洞检测模块(如安全漏洞检测模块300)。服务器140A和140B可以通信地耦接到SAN(存储区域网络)光纤网170。SAN光纤网170可以经由网络150支持通过服务器140A和140B以及通过客户端系统110、120和130来访问存储设备180(1)-(N)。

[0032] 参考图2的计算机系统200,可使用调制解调器247、网络接口248或一些其他方法来提供从客户端系统110、120和130中的一者或多者到网络150的连接。客户端系统110、120和130可使用(例如)web浏览器或其他客户端软件(未示出)来访问服务器140A或140B上的信息。此类客户端可允许客户端系统110、120和130访问由服务器140A或140B或存储设备160A(1)-(N)、160B(1)-(N)和/或180(1)-(N)中的一者托管的数据。在一些实施例中,客户端系统110、120和130可具有在其上实施的安全代理,以保护客户端系统不受计算机病毒和/或恶意软件的攻击,并与在服务器140A上实施的后台安全系统通信。

[0033] 网络150和190可以为局域网(LAN)、广域网(WAN)、互联网、蜂窝网络、卫星网络或允许在客户端110、120、130、服务器140、以及通信地耦接到网络150和190的其他设备之间通信的其他网络。网络150和190还可以包括一个或任意数量的示例类型的上述网络,所述网络作为独立的网络运行或与相互间协同运行。网络150和190可以利用其通信地耦接到的一个或多个客户端或服务器的一个或多个协议。网络150和190可以转换到或从其他协议转换到网络设备的一个或多个协议。虽然网络150和190各自被描述为一个网络,但应当理解,根据一个或多个实施例,网络150和190可各自包括多个互连的网络。

[0034] 存储设备160A(1)-(N)、160B(1)-(N)和/或180(1)-(N)可以是网络可访问存储器，并且相对于服务器140A或140B可以是本地的、远程的或它们的组合。存储设备160A(1)-(N)、160B(1)-(N)和/或180(1)-(N)可以利用廉价磁盘冗余阵列(“RAID”)、磁带、磁盘、存储区域网络(“SAN”)、互联网小型计算机系统接口(“iSCSI”)SAN、光纤通道SAN、通用互联网文件系统(“CIFS”)、网络附加存储器(“NAS”)、网络文件系统(“NFS”)、基于光的存储器或其他计算机可访问存储器。存储设备160A(1)-(N)、160B(1)-(N)和/或180(1)-(N)可用于备份或存档目的。例如，存储设备160B(1)-(N)和/或180(1)-(N)可用于存储从存储设备160A(1)-(N)复制的数据。

[0035] 根据一些实施例，客户端110、120和130可以为智能电话、PDA、台式计算机、膝上型计算机、服务器、其他计算机或计算设备，或通过无线或有线连接而连接到网络150的其他设备。客户端110、120和130可以从用户输入、数据库、文件、网络服务和/或应用程序编程接口接收数据。

[0036] 服务器140A和140B可以是应用程序服务器、存档平台、备份服务器、网络存储设备、媒体服务器、电子邮件服务器、文档管理平台、企业搜索服务器、防恶意软件/病毒的安全服务器，或通信地耦接到网络150的其他设备。服务器140A和140B可利用存储设备160A(1)-(N)、160B(1)-(N)和/或180(1)-(N)中的一者来存储应用程序数据、备份数据或其他数据。服务器140A和140B可以为主机，如应用程序服务器，该主机可以处理在客户端110、120和130与备份平台、备份进程和/或存储器之间传输的数据。

[0037] 根据一些实施例，服务器140A和140B可以为用于备份和/或存档数据的平台。可根据备份策略和/或所应用的存档文件、与数据源相关联的属性、可用于备份的空间、在数据源处的可用空间，或其他因素来备份或存档数据的一个或多个部分。另外，已备份或存档的数据的所述一个或多个部分可根据故障转移策略(failover policy)在发生特定事件时进行恢复。根据其他实施例，服务器140A和140B可根据从包括客户端110、120和130在内的任何源收集的信息识别安全漏洞。因此，服务器140A和140B可分发信息给客户端110、120和130，从而在客户端110、120和130防止恶意软件和病毒利用安全漏洞。

[0038] 根据一些实施例，客户端110、120和130可包含检测安全漏洞的软件的一个或多个部分，例如安全漏洞检测模块300。另外，服务器140A可包含检测安全漏洞的软件的一个或多个部分，例如安全漏洞检测模块300。如图所示，安全漏洞检测模块300的一个或多个部分可驻存在网络中心位置处。根据一些实施例，网络190可以为外部网络(例如，互联网)，并且服务器140A可以为在一个或多个内部组件和客户端与外部网络之间的网关或防火墙。根据一些实施例，安全漏洞检测模块300可作为云计算环境的一部分加以实施。

[0039] 图2示出了根据本发明实施例的计算机系统200的框图。计算机系统200适用于实施根据本发明的技术。计算机系统200可包括总线212，该总线可以将计算机系统200的主要子系统互连，所述主要子系统诸如中央处理器214、系统存储器217(例如，RAM(随机存取存储器)、ROM(只读存储器)、闪存RAM等)、输入/输出(I/O)控制器218、外部音频设备(如经由音频输出接口222的扬声器系统220)、外部设备(诸如经由显示适配器226的显示屏224)、串行端口228和230、键盘232(经由键盘控制器233连接)、存储接口234、用于接收软盘238的软盘驱动器237、用于与光纤通道网络290连接的主机总线适配器(HBA)接口卡235A、用于连接到SCSI总线239的主机总线适配器(HBA)接口卡235B，以及用于接收光盘242的光盘驱动器

240。此外，还可以包括鼠标246(或经由串行端口228连接到总线212的其他点击设备)、调制解调器247(经由串行端口230连接到总线212)、网络接口248(直接连接到总线212)、电源管理器250，以及电池252。

[0040] 总线212允许在中央处理器214和系统存储器217之间进行数据通信，如前文提及，系统存储器217可以包括只读存储器(ROM)或闪存存储器(均未示出)以及随机存取存储器(未示出)。RAM可以是可将操作系统和应用程序加载到其中的主存储器。除了其他代码，ROM或闪存存储器可以包含控制基本硬件操作(诸如与外围组件的交互)的基本输入输出系统(BIOS)。与计算机系统200驻存在一起的应用程序可以存储在计算机可读介质上并经由计算机可读介质进行访问，计算机可读介质诸如硬盘驱动器(例如，固定磁盘244)、光盘驱动器(例如，光盘驱动器240)、软盘单元237、可移动磁盘驱动器(例如，通用串行总线驱动器)或其他存储介质。根据一些实施例，安全漏洞检测模块300可驻存在系统存储器217中。

[0041] 存储接口234与计算机系统200的其他存储接口一样可以连接到标准计算机可读介质(诸如固定磁盘驱动器244)以用于存储和/或检索信息。固定磁盘驱动器244可以是计算机系统200的一部分，或者可以是独立的，并且可以通过其他接口系统进行访问。调制解调器247可以经由电话链路提供到远程服务器的直接连接，或经由互联网服务提供方(ISP)提供到互联网的直接连接。网络接口248可以经由直接网络链路提供到远程服务器的直接连接，或经由POP(入网点)提供到互联网的直接连接。网络接口248可以使用无线技术提供此类连接，包括数字蜂窝电话连接、蜂窝数字分组数据(CDPD)连接、数字卫星数据连接等。

[0042] 很多其他设备或子系统(未示出)可以通过相似的方式进行连接(例如文档扫描仪、数码相机等)。相反，不需要提供图2中显示的所有设备亦可实施本发明。可以使用与图2中所示方式不同的方式来互连设备和子系统。用于实施本发明的代码可以存储在计算机可读存储介质中，所述计算机可读存储介质诸如系统存储器217、固定磁盘244、光盘242或软盘238中的一者或多者。用于实施本发明的代码还可以通过一个或多个接口来接收并存储在存储器中。计算机系统200上提供的操作系统可以是MS-DOS®、MS-WINDOWS®、OS/2®、OS X®、UNIX®、Linux®或其他操作系统。

[0043] 电源管理器250可以监测电池252的电量水平。电源管理器250可以提供一个或多个API(应用程序编程接口)以允许确定电量水平、在关闭计算机系统200之前保留的时窗、电源消耗率、计算机系统正使用市电(例如，交流电源)还是电池电源的指示器、以及其他电源相关的信息。根据一些实施例，可以远程访问电源管理器250的API(例如，可以通过网络连接访问远程备份管理模块)。根据一些实施例，电池252可以是位于计算机系统200近旁的或远离计算机系统200的不间断电源(UPS)。在此类实施例中，电源管理器250可以提供与UPS的电量水平有关的信息。

[0044] 图3示出了根据本发明实施例的安全漏洞检测模块300。如图所示，安全漏洞检测模块300可包含一个或多个组件，包括声誉模块310、系统及应用程序监测模块320、系统及应用程序行为报告模块330、系统及应用程序行为接收模块340、规则生成模块350、应用程序控制模块360和用户接口370。

[0045] 声誉模块310可管理将在一个或多个客户端(例如，客户端110、120和130)上执行

的一个或多个应用程序和进程的声誉。在一些实施例中，声誉模块310可根据多个因素指定声誉给正在网络内的每个客户端上执行的每个应用程序或进程。例如，声誉模块310可根据应用程序开发者、应用程序前一版本的声誉、安装时或安装后应用程序的特征或行为、白名单或任何其他因素来指定声誉给应用程序。另外，如果应用程序开始表现出可疑或恶意行为，声誉模块310可修改应用程序的声誉。该行为可通过使用探试法(heuristics)并根据至少一个客户端报告的系统及应用程序行为来加以确定。

[0046] 系统及应用程序监测模块320可监测系统及正由客户端执行的每个应用程序或进程的行为。在一些实施例中，系统及应用程序监测模块320可作为客户端处的安全代理的一部分进行实施。系统及应用程序监测模块320可监测客户端的各种行为。例如，系统及应用程序监测模块320可监测客户端的未经授权的系统目录访问或修改、对操作系统的未经授权写入、安全应用程序(诸如防病毒应用程序)的终止以及恶意的网络活动。在一些情况下，系统及应用程序监测模块320可利用探试法监测客户端的行为，以识别将要报告的特定风险或可疑行为。

[0047] 系统及应用程序行为报告模块330可报告由系统及应用程序监测模块320监测到的系统及应用程序行为的结果。在一些实施例中，系统及应用程序行为报告模块330可从客户端(例如，客户端110、120或130)报告行为到后台系统(例如，服务器140A)。系统及应用程序行为报告模块330可定期(可视客户端的活动而变化)、连续或在客户端发生特定行为或活动时报告监测到的系统及应用程序行为的结果。

[0048] 系统及应用程序行为接收模块340可接收系统及应用程序行为报告模块330传送的系统及应用程序行为的结果。在一些实施例中，系统及应用程序行为接收模块340可设置在后台系统(例如，服务器140A)处并被配置为从一个或多个客户端(例如，客户端110、120和130)接收系统及应用程序行为信息。

[0049] 规则生成模块350可根据系统及应用程序行为接收模块340接收的系统及应用程序行为生成针对特定应用程序的规则。在一些情况下，当确定应用程序正表现出可疑行为时，规则生成模块350可生成规则以限制该应用程序。例如，规则可指示由于已知病毒或恶意软件感染而将完全阻止该应用程序，由于疑似感染病毒或恶意软件而只在虚拟客户端执行该应用程序，或由于已知不存在任何病毒或恶意软件而被允许访问所有系统资源。

[0050] 应用程序控制模块360可根据规则生成模块350生成的规则控制应用程序。应用程序控制模块360可根据来自声誉模块310的声誉、来自规则生成模块350的规则以及系统及应用程序监测模块320检测到的系统及应用程序行为来确定应用程序的权限(permission)。在一些实施例中，应用程序控制模块360可根据生成的规则限制应用程序对某些系统资源的访问。在其他实施例中，应用程序控制模块360可在应用程序具有可信声誉时允许应用程序完全访问系统资源。在另一个实施例中，应用程序控制模块360可根据可信声誉允许应用程序有限制地访问某些系统资源，即使该应用程序正表现出可疑行为。

[0051] 用户界面370可向用户或管理员提供界面，以控制下述进程的任何方面。例如，用户界面370可显示系统及应用程序监测模块320监测到的系统及应用程序行为的相关信息。

[0052] 图4示出了根据本发明实施例的一种检测安全漏洞的方法400。方法400可独立地在例如包括客户端110、120、130和服务器140A在内的多个设备执行。然而，下述方法400的任何部分可在客户端110、120、130和服务器140A中的任一者上执行。在方框402处，方法400

可以开始。

[0053] 在方框404处，可识别新应用程序。在一些实施例中，新应用程序可通过声誉模块310加以识别。新识别的应用程序可以是开发者最近发布的新软件程序或应用程序。另外，新识别的应用程序可以是先前已知应用程序的更新版本。在一些实施例中，新应用程序可由开发者报告给后台系统，该后台系统可对已知应用程序的列表进行维护。另外，已安装新应用程序的客户端(例如，客户端110、120和130)可向后台系统(例如，服务器140A)报告新应用程序的存在。还可在后台系统处根据从多个安装同一应用程序的客户端接收的信息来进行新应用程序的识别。新应用程序被识别后，整个过程可进入方框406。

[0054] 在方框406，初始声誉可指定给新识别的应用程序。在一些实施例中，初始声誉可由声誉模块310指定。声誉可指示新应用程序的可信度。例如，根据发布新应用程序的开发者，新应用程序可被指定为具有高可信度的良好声誉(例如，“安全”)。另外，根据在多个客户端上安装应用程序且安装时未检测到相关的恶意软件感染，新应用程序可被指定为良好声誉(例如，“安全”)。在一些实施例中，根据安装新应用程序时新应用程序的行为由客户端指定初始声誉给新应用程序。在其他实施例中，基于有关软件的信息和/或从至少一个已安装应用程序的客户端报告的信息，后台系统可指定初始声誉给新应用程序。然而，可基于任意数目的因素，将声誉指定给新应用程序。另外，当指定给新应用程序的初始声誉是良好声誉时，信息可存储在可信应用程序的白名单中。初始声誉已指定给新识别的应用程序后，整个过程可进入方框408。

[0055] 在方框408，可从至少一个客户端接收监测到的系统行为。在一些实施例中，监测到的系统行为可由系统及应用程序行为接收模块340接收。在一些情况下，可在后台系统(例如，服务器140A)从多个客户端(例如，客户端110、120和130)接收监测到的系统行为。监测到的系统行为可指示客户端是否正表现出可疑行为，并且包括有关可疑行为的详情。或者，监测到的系统行为可指示客户端未发生可疑行为。接收的系统行为可具体列明哪些应用程序正在客户端上执行或运行以及与特定应用程序相关的任何行为。另外，接收的系统行为信息可指示是否正观察到新的可能恶意的行为，即使客户端并未安装新应用程序。监测到的系统行为可包括整个客户端的行为信息、先前已有的应用程序或进程、新应用程序以及用于确定应用程序或进程是否正表现出可疑行为或是否应当被隔离的信息的组合。监测到的系统行为可定期、连续或在任何其他时间接收。接收到监测到的系统行为后，过程然后可进入方框410。

[0056] 在方框410，可确定是否更改新应用程序的初始声誉。在一些实施例中，可由声誉模块310确定是否更改新应用程序的初始声誉。根据从一个或多个客户端接收的监测到的系统行为，新应用程序的初始声誉可从良好或安全声誉更改为可信度较低的声誉。例如，当一个客户端报告应用程序正表现出可疑行为时，初始声誉可从良好更改为可疑。在一些实施例中，可根据探试法确定是否更改应用程序的声誉。

[0057] 另外，当多个客户端报告特定应用程序正表现出可疑行为时，初始声誉可由良好更改为可疑。在一些实施例中，当预设数目的客户端或阈值数目的客户端报告应用程序正表现出可疑行为时可更改声誉。另外，当确定应用程序正从一个或多个客户端表现出特定恶意软件或病毒特征时，新应用程序的声誉可从良好或安全更改为不良。然而，如果客户端未报告可疑特征或行为，可维持良好或安全声誉。根据从至少一个客户端接收的监测到的

系统行为，应用程序的声誉可从不良提升为可疑，或从可疑提升为安全。例如，可确定疑似对可疑行为负责的第一应用程序并非表现出可疑行为的实际应用程序。因此，应用程序的声誉可从可疑更改为中性或良好。

[0058] 在方框410，还可根据从至少一个客户端报告的系统行为确定更改任何其他已知应用程序或进程的声誉。如果确定不需要更改新应用程序或任何其他应用程序的声誉，则过程可后退到方框408，在此可再次接收另外的系统行为。如果确定确实需要更改新应用程序或任何其他应用程序的声誉，则过程可后退到方框412。

[0059] 在方框412，所识别的应用程序的更改声誉可分发给网络内的每个客户端。在一些实施例中，所识别的应用程序的更改声誉可由声誉模块310分发。在一些情况下，更改声誉可从后台系统(例如，服务器140A)分发到网络内的每个客户端(例如，客户端110、120和130)。分发更改声誉后，过程可进入方框414。

[0060] 在方框414，可从至少一个客户端接收监测到的系统及应用程序行为。在一些实施例中，监测到的系统及应用程序行为可由系统及应用程序行为接收模块340接收。在一些情况下，监测到的系统及应用程序行为可包括与一个应用程序或进程、多个应用程序或进程及系统行为有关的信息。另外，监测到的系统及应用程序行为可包括与具有可疑或不可信声誉的应用程序或进程有关的详细信息。可从一个或多个执行各种可信和/或可疑应用程序的客户端接收监测到的系统及应用程序行为。在一些实施例中，根据在方框412处分发给客户端的应用程序的声誉的更改，监测到的系统及应用程序行为可包括与特定应用程序的行为有关的更多细节。可定期、连续或在任何其他时间从所述多个客户端同时或依次接收监测到的系统及应用程序行为。接收到监测到的系统及应用程序行为后，过程可进入方框416。

[0061] 在方框416，可根据接收的系统及应用程序行为确定是否生成并分发新规则给至少一个客户端。在一些实施例中，规则生成模块350可确定是否应生成并分发新规则给客户端。在一些情况下，当接收的监测到的系统及应用程序行为指示特定应用程序或进程表现出可疑和/或恶意行为时，可生成新规则。可根据对从一个或多个客户端接收的监测到的系统及应用程序行为进行的分析，确定是否生成新规则。在一些实施例中，当监测到的应用程序行为指示特定应用程序对来自一个客户端的可疑和/或恶意行为负责时，可生成针对该特定应用程序的新规则。

[0062] 另外，当监测到的应用程序行为指示在多个客户端上表现出可疑的特定行为并且每个客户端都在执行或进行特定应用程序时，可生成针对该特定应用程序的新规则。因此，可得出推论，该特定应用程序对可疑或恶意行为负责，并且可针对该特定应用程序生成新规则。新规则可指示客户端执行多个已知安全措施中的任何一个。例如，新规则可指示将阻止加载或执行该应用程序，该应用程序将在安全沙箱中执行，或该应用程序将移至虚拟客户端执行。

[0063] 新规则可分发给网络内的每个客户端。在一些情况下，新规则可分发给执行与新规则相关联的特定应用程序的客户端，而不将新规则传送给不执行该特定应用程序的客户端。生成新规则后可立即分发新规则给客户端或作为定期更新的一部分分发给客户端。分发新规则后，整个过程然后可进入方框418。然后，整个方法400可定期或连续重复。在一些情况下，整个过程的各个要素可同时或依次进行。例如，可从多个客户端接收监测到的系统

行为，同时另一个应用程序的更改声誉正分发给所述客户端。

[0064] 图5示出了根据本发明实施例的一种检测安全漏洞的方法500。方法500可在例如包括客户端110、120、130和服务器140A在内的多个设备上执行。然而，下述方法500的任何部分可在客户端110、120、130和服务器140A中的任一者上执行。在方框502处，方法500可开始。

[0065] 在方框504，可根据初始声誉执行或进行应用程序。在一些实施例中，可在客户端独立地执行应用程序，或与多个另外的应用程序或进程同时执行。初始声誉可指示应用程序是否可信且安全、可能可疑、可疑、恶意或属于任何其他类别。在一些情况下，执行应用程序的客户端可根据安装应用程序期间和/或之后应用程序的行为确定初始声誉。在其他情况下，客户端可从后台系统接收初始声誉。根据该声誉，客户端可在声誉良好或安全时通过允许该应用程序访问所有可用资源来执行该应用程序。另外，客户端可在声誉不良或不安全时通过限制访问资源来执行应用程序。根据初始声誉执行应用程序后，整个过程可进入方框506。

[0066] 在方框506，可监测客户端系统的行为。在一些实施例中，系统及应用程序监测模块320可监测客户端(例如，客户端110)的行为。客户端行为的监测有多种方式。例如，可监测系统的未经授权的系统目录访问或修改、对操作系统的未经授权写入、安全应用程序(防病毒应用程序)的终止以及恶意的网络活动。在一些情况下，可利用探试法监测客户端的行为，以识别危险或可疑行为。

[0067] 系统行为的监测可与由方框504执行应用程序同时进行。另外，可定期或连续地以预定时间周期进行监测。在一些实施例中，可根据客户端执行的应用程序或进程的声誉来监测系统行为。例如，当每个应用程序具有可信或安全的声誉时，系统行为的监测频率可较低；反之，如果应用程序具有可疑或不可信的声誉时，系统的监测频率较高。客户端还可根据相关联的可信声誉以较低频率监测某些应用程序，而根据相关联的可疑声誉以较高频率监测其他应用程序。即使检测到可疑行为，客户端也可根据其声誉继续执行应用程序。在这种情况下，应用程序的声誉可优先于可疑行为，直至接收到更新的声誉。然而，如果检测到特定的已知恶意行为，客户端可终止应用程序。监测到系统行为后，整个方法可进入方框508。

[0068] 在方框508，监测到的系统行为可被报告给后台系统(例如，服务器140A)。在一些实施例中，系统及应用程序行为报告模块330可将客户端(例如，客户端110)的监测到的系统行为报告到后台系统(例如，服务器140A)。监测到的系统及应用程序行为报告到后台系统后，过程可进入方框510。

[0069] 在方框510，可确定是否已接收到新的应用程序声誉。在一些实施例中，可通过应用程序控制模块360接收新的应用程序声誉。响应于后台系统检测到与应用程序相关联的可疑行为，可从后台系统(例如，服务器140A)接收新的应用程序声誉。例如，在确定特定应用程序正表现出上述可疑行为时，后台系统可自动分发该特定应用程序的新声誉给网络内的所有客户端。如果未接收到新的应用程序声誉，则过程可退回到方框504，以便客户端可继续执行应用程序、监测系统行为并向后台系统报告系统行为。然而，如果接收到新的应用程序声誉，方法可进入方框512。

[0070] 在方框512，可根据新接收的应用程序声誉监测系统及应用程序。在一些实施例

中，可根据新接收的声誉由系统及应用程序监测模块320监测系统及应用程序。在一些情况下，新声誉可指示特定应用程序或进程的声誉已从可信水平降低至可疑水平或从可疑水平降低至恶意水平。如果新声誉指示应用程序是恶意的，则该应用程序可能被完全阻止或仅限于在安全沙箱或虚拟客户端运行。另外，当应用程序被识别为恶意时，可更详细地监测所有的系统及应用程序行为。

[0071] 如果新声誉指示特定应用程序是可疑的，则可调整该应用程序及整个系统的行为。例如，如果应用程序在先前被指示为可信，则行为可能已被不频繁地监测。然而，既然应用程序的声誉已降至可疑，系统及该特定应用程序的行为就可以增加的频率加以监测。或者，如果新声誉指示特定应用程序不再可疑，则监测该系统及应用程序行为的频率可降低。可以预定时间周期监测系统及应用程序行为，之后过程进入方框514。然而，如果检测到系统或应用程序的特定行为，过程可立即进入将要报告的方框514。因此，系统及应用程序的行为已被监测后，过程进入方框514。

[0072] 在方框514，可根据新声誉将监测到的系统及应用程序行为报告给后台系统(例如，服务器140A)。在一些实施例中，系统及应用程序行为报告模块330可将客户端(例如，客户端110)的新监测到的系统及应用程序行为报告到后台系统(例如，服务器140A)。监测到的系统及应用程序行为报告到后台系统后，过程可进入方框516。

[0073] 在方框516，如果接收到新规则，则根据新规则控制正在执行的应用程序。在一些实施例中，可根据接收的规则由应用程序控制模块360控制应用程序。在一些情况下，后台系统可根据如上所述报告给后台系统的客户端行为分发新规则给客户端。具体地讲，后台系统可发布新规则，即，将禁止执行特定应用程序，将在安全沙箱中执行应用程序、在虚拟客户端执行应用程序，或将限制应用程序对特定系统资源的访问。因此，如果后台系统分发了针对特定应用程序的新规则，则客户端(例如，客户端110)可根据该规则执行应用程序。然而，如果未从后端接收到新规则，则客户端可继续执行应用程序，并且整个过程进入方框518。在方框518，整个过程可连续或定期重复。

[0074] 然后，整个方法500可定期或连续重复。在一些情况下，整个过程的各个要素可同时或依次进行。例如，可根据初始声誉执行应用程序，同时还向后台系统报告系统行为。

[0075] 此时，应当注意，根据如上所述的本发明检测安全漏洞可在一定程度上涉及输入数据的处理以及输出数据的生成。输入数据处理和输出数据生成可在硬件或软件中实施。例如，可以在检测安全漏洞中或用于实施与根据如上所述的本发明检测安全漏洞相关联的功能的类似或相关电路中采用特定电子组件。或者，根据指令进行操作的一个或多个处理器可以实施与根据如上所述的本发明检测安全漏洞相关联的功能。如果是这种情况，则其在本发明的范围之内，因为此类指令可存储在一个或多个非瞬时性处理器可读存储介质(例如，磁盘或其他存储介质)上，或经由一个或多个载波中体现的一个或多个信号而传输到一个或多个处理器。

[0076] 本发明并不限于本文所述的特定实施例的范围。实际上，通过前述描述和附图，除了本文所述的内容之外，本发明的其他各种实施例和修改形式对于本领域的普通技术人员而言将是显而易见的。因此，此类其他实施例和修改形式旨在落入本发明的范围内。此外，虽然本文针对至少一个特定用途在至少一个特定环境中以至少一种特定具体实施的情形来对本发明进行了描述，但本领域的那些普通技术人员将认识到，本发明的适用性并不局

限于此，并且本发明可针对任意数量的用途在任意数量的环境中有利地实施。因此，应根据如本文所述的本发明的全部范围和精神来理解下文所阐述的权利要求。

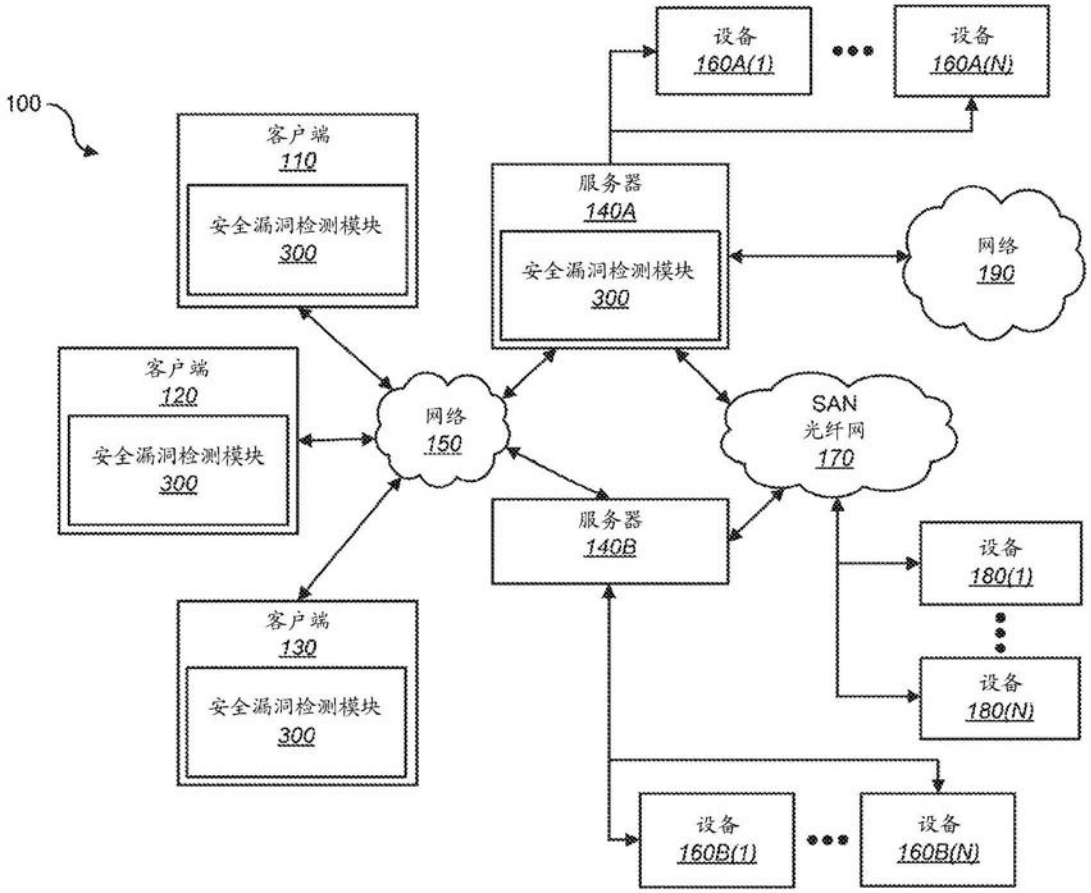

100
客户端
110
安全漏洞检测模块
300
客户端
120
安全漏洞检测模块
300
客户端
130
安全漏洞检测模块
300
网络
150
服务器
140A
安全漏洞检测模块
300
服务器
140B
SAN
光纤网
170
网络
190
设备
160A(1)
设备
160A(N)
设备
180(1)
设备
180(N)
设备
160B(1)
设备
160B(N)

图1

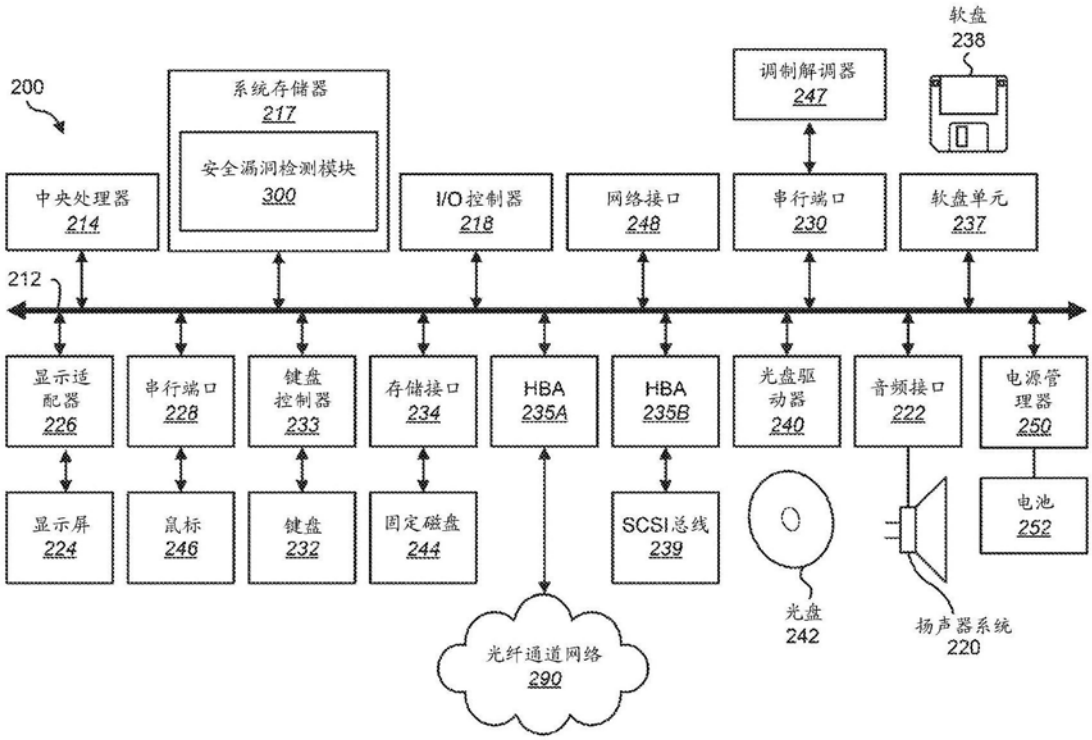

200
系统存储器
217
安全漏洞检测模块
300
中央处理器
214
I/O控制器
218
网络接口
248
调制解调器
247
串行端口
230
软盘
238
软盘单元
237
212
显示适配器
226
串行端口
228
键盘控制器
233
存储接口
234
HBA
235A
HBA
235B
光盘驱动器
240
音频接口
222
电源管理器
250
显示屏
224
鼠标
246
键盘
232
固定磁盘
244
SCSI总线
239
电池
252
光盘
242
扬声器系统
220
光纤通道网络
290

图2

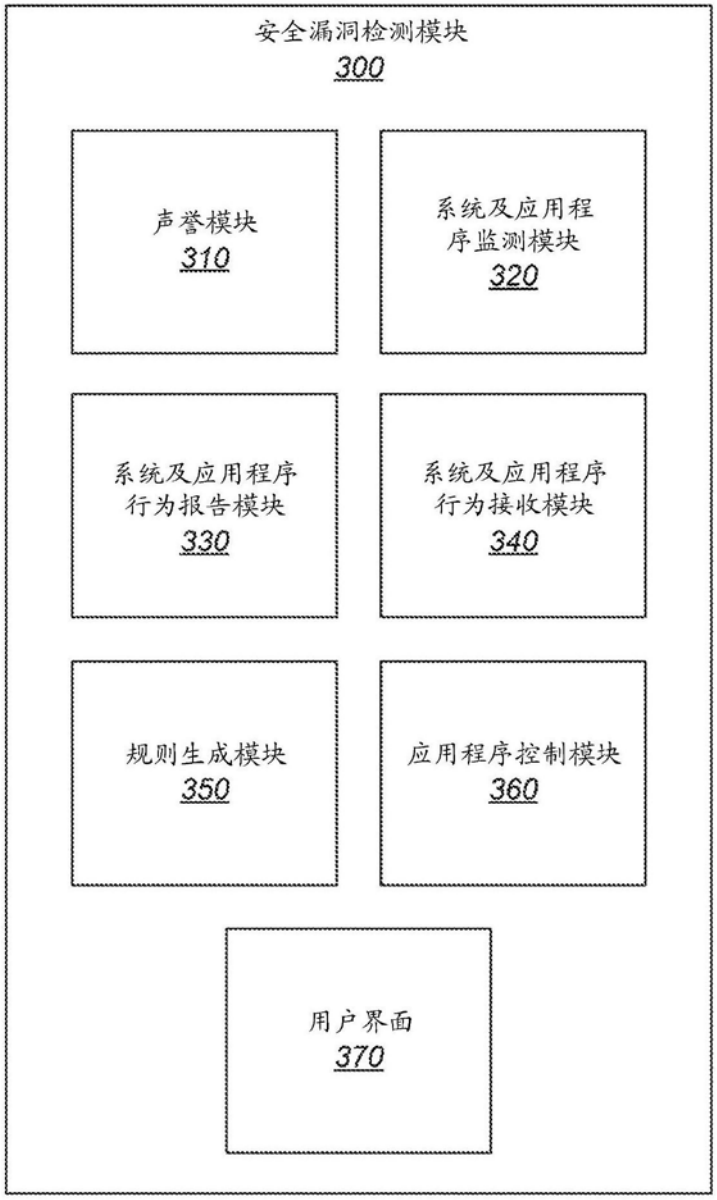

安全漏洞检测模块
300
声誉模块
310
系统及应用程序监测模块
320
系统及应用程序行为报告模块
330
系统及应用程序行为接收模块
340
规则生成模块
350
应用程序控制模块
360
用户界面
370

图3

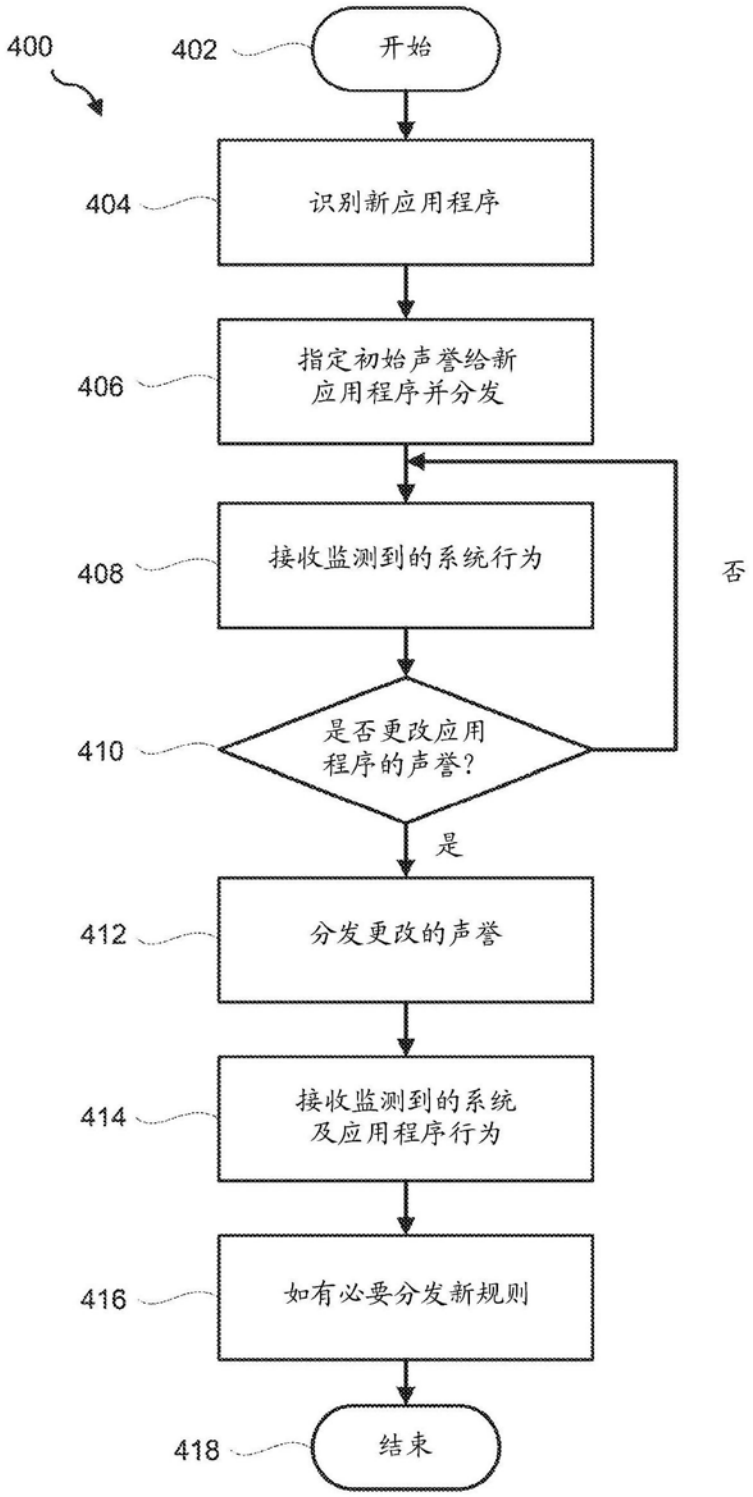

400
402
开始
404
识别新应用程序
406
指定初始声誉给新应用程序并分发
408
接收监测到的系统行为
否
410
是否更改应用程序的声誉?
是
412
分发更改的声誉
414
接收监测到的系统及应用程序行为
416
如有必要分发新规则
418
结束

图4

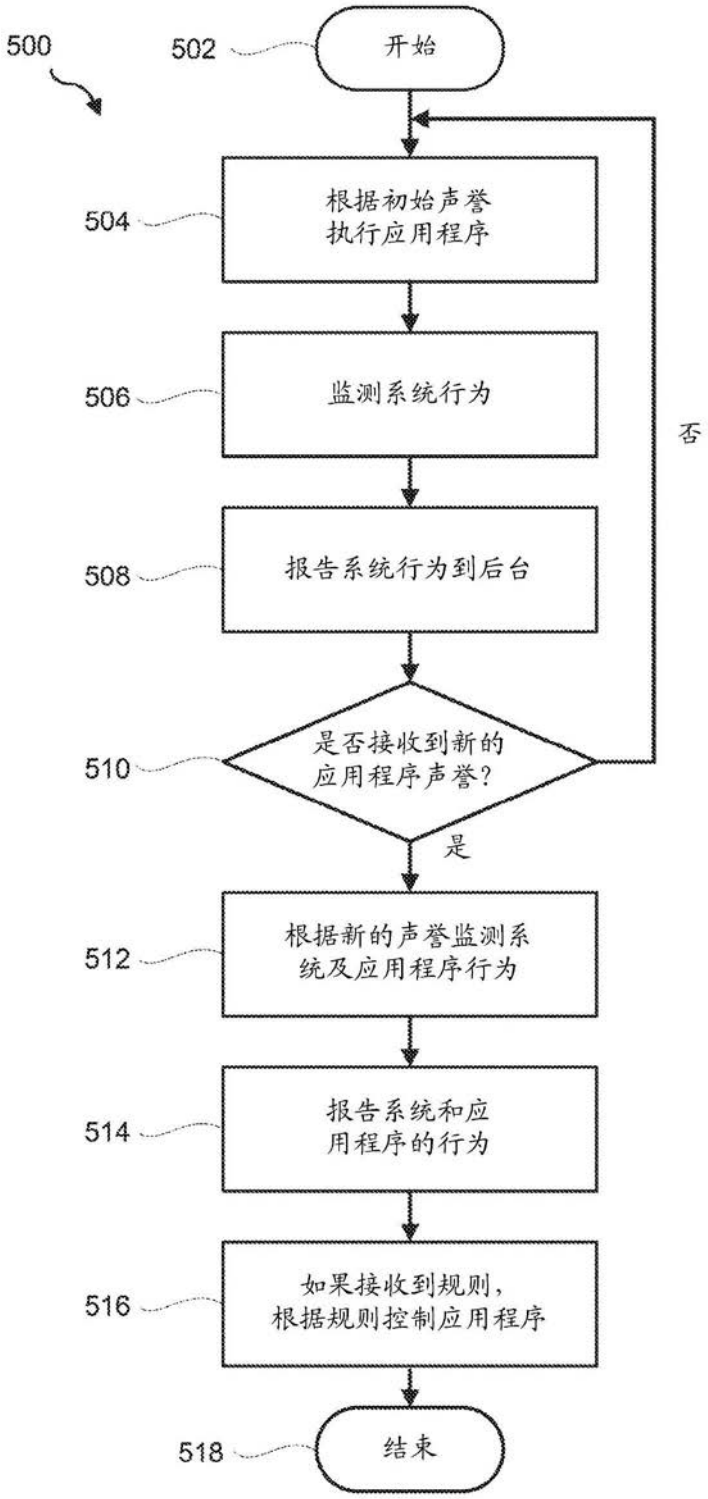

500
502
开始
504
根据初始声誉
执行应用程序
506
监测系统行为
508
报告系统行为到后台
510
是否接收到新的
应用程序声誉?
否
是
512
根据新的声誉监测系
统及应用程序行为
514
报告系统和应
用程序的行为
516
如果接收到规则,
根据规则控制应用程序
518
结束

图5