(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 102656587 B
(45)授权公告日 2016.06.08

(21)申请号 201080032172.7
(22)申请日 2010.08.10
(30)优先权数据
12/540907 2009.08.13 US
(85)PCT国际申请进入国家阶段日
2012.01.17
(86)PCT国际申请的申请数据
PCT/US2010/045022 2010.08.10
(87)PCT国际申请的公布数据
WO2011/019720 EN 2011.02.17
(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 Z·拉姆扎恩 W·伯格拉德
A·扎维拉 V·安特努维
C·S·纳彻伯格
(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 21/55(2013.01)
G06F 21/56(2013.01)
H04L 12/58(2006.01)
H04L 29/06(2006.01)

(56)对比文件
WO 2005/043351 A2,2005.05.12,
US 2006/0253581 A1,2006.11.09,
CN 101335721 A,2008.12.31,
CN 101459718 A,2009.06.17,
CN 101399683 A,2009.04.01,
Vipual Ved Parkash 等.A Reputation-Based Approach for Efficient Filtration of Spam.《http://www.cloudmark.com/releases/docs/wp_reputation_filtration_10640406.pdf》.2007, 第1-12页.

审查员 潘秋羽

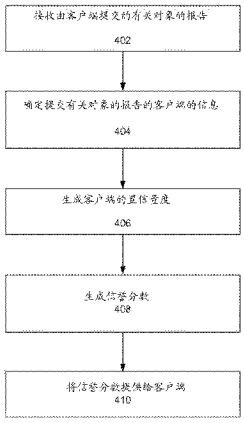
权利要求书2页 说明书9页 附图4页

(54)发明名称

在信誉系统中使用客户端装置的置信量度

(57)摘要

通过一个信誉系统使用来自多个客户端的、标识多个对象的报告来确定这些对象的信誉。使用从这些报告中确定的信息来生成对于这些客户端的置信量度。置信量度表明了对于这些报告的真实性的置信度的量值。使用来自这些客户端的报告以及对于这些客户端的置信量度来计算多个对象的信誉分数。与这些对象的标识符相关联地存储置信量度以及信誉分数。响应于一个请求,将一个对象的信誉分数提供给一个客户端。



CN 102656587 B

1.一种使用计算机来确定在信誉系统中的对象的信誉的方法，该方法包括：

从在该信誉系统中的多个客户端接收多个报告，这些报告标识了在这些客户端处所检测到的一个对象；

基于从这些客户端接收的这些报告来确定该对象在该信誉系统中的这些客户端上的一个流行程度；

由从这些客户端接收的这些报告中确定有关这些客户端的信息；

响应于有关这些客户端所确定的信息来生成对于这些客户端的置信量度，这些置信量度表明对于从这些客户端接收的报告的真实性的置信度的量值，其中对于这些客户端的更高的置信量度指示从这些客户端接收到的报告中的信息更有可能是真实的；

至少部分地响应于从这些客户端接收的这些报告、该对象的流行程度、以及对于这些客户端的置信量度来计算该对象的一个信誉分数，其中具有一个较高流行程度的对象收到一个较高的信誉分数，所述较高的信誉分数指示该对象不太可能包含恶意软件；并且

对该对象的信誉分数进行存储。

2.如权利要求1所述的方法，其中来自一个客户端的一个报告包括对该对象的信誉分数的一个请求，并且该方法进一步包括：

将该对象的信誉分数提供给该客户端。

3.如权利要求1所述的方法，其中所确定的有关这些客户端的信息包括在该信誉系统中的一个客户端的年龄，该客户端的年龄是响应于该客户端在该信誉系统中一直处于活跃状态所经历的时间而被确定的，对于该客户端的一个置信量度至少部分地是基于该客户端的年龄，并且一个较年长的客户端收到一个较高置信量度。

4.如权利要求1所述的方法，其中所确定的有关这些客户端的信息包括由一个客户端提交的多个报告的期望的频率提交模式，并且其中对于该客户端的一个置信量度至少部分地是基于由该客户端提交的多个报告的频率是否偏离所述的期望的频率提交模式。

5.如权利要求3所述的方法，其中所确定的有关这些客户端的信息包括该信誉系统中的一个客户端的年龄，该客户端的年龄是响应于确定该客户端已经提交了多少对于具有高流行程度的对象的报告而被确定的，已提交了较多的具有高流行程度的对象的报告的一个客户端被当作年长于已提交了较少的具有高流行程度的对象的报告的多个客户端来对待，并且一个更年长的客户端接收到更高的置信量度。

6.如权利要求1所述的方法，其中计算该对象的信誉分数包括：

使用一个置信量度阈值来标识具有低置信量度的多个客户端；

确定曾提交标识该对象的多个报告的具有低置信量度的多个客户端与曾提交标识该对象的报告的所有客户端的一个比率；并且

至少部分地响应于所确定的比率，计算该对象的信誉分数。

7.如权利要求1所述的方法，其中计算该对象的信誉分数包括：

使用一个置信量度阈值来标识具有高置信量度的多个客户端；

确定曾提交标识该对象的多个报告、具有高置信量度的多个客户端与曾提交标识该对象的多个报告的所有客户端的一个比率；并且

至少部分地响应于所确定的比率来计算该对象的信誉分数。

8.如权利要求1所述的方法，其中生成对于这些客户端的信誉量度包括：

确定对于一个客户端的多个置信因素；

将不同的权重关联到不同的置信因素；

响应于与这些置信因素相关联的这些权重而生成对于该客户端的置信量度。

9.如权利要求1所述的方法，其中生成对于这些客户端的信誉量度包括：

确定一个客户端是否提交了残缺的报告；以及

响应于确定该客户端提交了残缺的报告，降低该客户端的置信量度。

10.一种用于确定在信誉系统中的对象的信誉的计算机系统，该计算机系统包括：

用于从该信誉系统中的多个客户端接收多个报告的装置，这些报告标识了在这些客户端处所检测到的一个对象；

用于基于从这些客户端接收的报告来确定该对象在该信誉系统中的这些客户端上的一个流行程度的装置；

用于由从这些客户端接收的这些报告中确定有关这些客户端的信息的装置；

用于响应于所确定的有关这些客户端的信息来生成对于这些客户端的置信量度的装置，这些置信量度表明对于从这些客户端接收的报告的真实性的置信度的量值，其中对于这些客户端的更高的置信量度指示从这些客户端接收到的报告中的信息更有可能是真实的；以及

用于至少部分地响应于从这些客户端接收的这些报告、该对象的流行程度、以及对于这些客户端的置信量度来计算该对象的一个信誉分数的装置，其中具有一个较高流行程度的对象收到一个较高的信誉分数，所述较高的信誉分数指示该对象不太可能包含恶意软件。

11.如权利要求10所述的计算机系统，其中来自一个客户端的一个报告包括对于该对象的信誉分数的一个请求，并且该计算机系统进一步包括：

用于将该对象的信誉分数提供给该客户端的装置。

12.如权利要求10所述的计算机系统，其中所确定的有关这些客户端的信息包括该信誉系统中的一个客户端的年龄，该客户端的年龄是响应于确定对于该客户端已经提交了多少对于具有高流行程度的多个对象的报告而被确定的，已提交了较多具有高流行程度的对象的报告的一个客户端被当作年长于已提交了较少的具有高流行程度的对象的报告的多个客户端来对待，并且一个更年长的客户端接收到更高的置信量度。

13.如权利要求10所述的计算机系统，其中用于计算该对象的信誉分数的装置包括：

用于使用一个置信量度阈值来标识具有低置信量度的多个客户端的装置；

用于确定曾提交标识该对象的多个报告的具有低置信量度的多个客户端与曾提交标识该对象的报告的所有客户端的一个比率的装置；以及

用于至少部分地响应于所确定的比率来计算该对象的信誉分数的装置。

14.如权利要求10所述的计算机系统，其中该用于计算该对象的信誉分数的装置包括：

用于使用一个置信量度阈值来标识具有高置信量度的多个客户端的装置；

用于确定曾提交标识该对象的多个报告的具有高置信量度的多个客户端与曾提交标识该对象的报告的所有客户端的一个比率的装置；以及

用于至少部分地响应于所确定的比率来计算该对象的信誉分数的装置。

在信誉系统中使用客户端装置的置信量度

技术领域

[0001] 本发明总体上涉及计算机安全性，并且具体涉及对操纵信誉系统的企图进行检测用于检测恶意对象。

背景技术

[0002] 多种多样的恶意软件能够攻击现代计算机。恶意软件威胁包括计算机病毒、蠕虫、特洛伊木马程序、间谍软件、促销软件、犯罪软件、以及钓鱼网站。恶意实体有时会攻击存储敏感或机密数据的服务器，这些数据可以用于恶意实体的自身利益。类似地，当用户下载新程序或程序更新时以及在很多其他情形下，必须一直保护包括家用计算机的其他计算机免受恶意软件的攻击，当用户经由电子邮件与其他人通信时可以传送这些恶意软件。有很多不同的选择及方法可用于恶意实体对计算机进行攻击。

[0003] 用于检测恶意软件的常规技术(如签名字符串扫描)变得不太有效。现代的恶意软件往往针对并被传送到相对少数的计算机上。例如，特洛伊木马程序可以被设计为针对特定公司的特定部门中的计算机。安全分析师可能永远不会遇到这样的恶意软件，并且因此安全软件可能永远不会配置用于检测这种恶意软件的签名。大量分布的恶意软件进而可以包含使恶意软件的每个实例唯一化的多态性。其结果是，难以开发出能可靠地检测出恶意软件的所有实例的签名字符串。

[0004] 用于检测恶意软件的较新技术涉及信誉系统的使用。信誉系统可以确定在计算机上遇到的一个文件或其他对象的信誉，以评估该对象是恶意软件的可能性。制定一个对象的信誉的一种方法是从在其上发现该对象的多个联网计算机中收集多个报告并且以这些报告中的信息为信誉的基础。

[0005] 然而，因为这样一种信誉系统依赖于来自于实质上是未知方的报告，所以它容易被恶意行为者破坏。例如，散布恶意软件的实体可以通过提交表明该恶意软件是合法的虚假报告来企图对“欺骗”该信誉系统。因此，对于能够经受破坏其操作的这种企图的信誉系统存在着一种需要。

发明内容

[0006] 一种用于在信誉系统中确定一个对象的信誉的方法、计算机可读存储媒质、以及计算机系统满足了以上及其他的需要。该方法的一个实施方案包括从多个客户端中接收多个报告，这些报告标识了在这些客户端处所检测的一个对象。该方法进一步包括从这些报告中确定有关这些客户端的信息。另外，该方法包括响应于所确定的有关这些客户端的信息生成这些客户端的置信量度，这些置信量度表明在从这些客户端接收的报告的真实性的置信度的量值。该方法还包括至少部分地是基于来自这些客户端的报告以及这些客户端的置信量度来计算该对象的一个信誉分数并且对该对象的信誉分数进行存储。

[0007] 该计算机可读媒质的实施方案存储了多个计算机程序指令用于在信誉系统中确定一个对象的信誉，这些指令包括多个指令用于从该信誉系统中的多个客户端接收多个报

告，这些报告标识了在这些客户端处所检测到的一个对象，并且用于从这些报告中确定有关这些客户端的信息。这些指令进一步包括多个指令用于响应于所确定的有关这些客户端的信息生成这些客户端的置信量度，这些置信量度表明在从这些客户端接收的报告的真实性的置信度的量值。这些指令额外地还包括多个指令用于至少部分地响应于来自这些客户端的报告以及这些客户端的置信量度来计算该对象的一个信誉分数并且对该对象的信誉分数进行存储。

[0008] 该计算机系统的实施方案包括一种存储了多个可执行的计算机程序指令的计算机可读存储媒质，这些指令包括多个指令用于从该信誉系统中的多个客户端接收多个报告，这些报告标识了在这些客户端处所检测到的一个对象，并且用于从这些报告中确定有关这些客户端的信息。这些指令进一步包括多个指令用于响应于所确定的有关这些客户端的信息生成这些客户端的置信量度，这些置信量度表明在从这些客户端接收的报告的真实性的置信度的量值。这些指令额外地还包括多个指令用于至少部分地响应于来自这些客户端的报告以及这些客户端的置信量度来计算该对象的一个信誉分数并且对该对象的信誉分数进行存储。该计算机系统进一步包括一个用于执行这些计算机程序指令的处理器。

[0009] 在本披露中以及在以下的详细说明中说明的这些特征及优点并不是包揽无遗的，并且具体地讲，通过参看本发明的附图、说明书、以及权利要求书，很多额外的特征和优点对相关领域的普通技术人员将变得清楚。另外，应该注意到本说明书中所使用的语言的选择主要是为了易读性和指导性的目的，并且也许不是被选用为描绘或限制本发明的主题，对于确定这种发明主题必须求助于权利要求书。

附图说明

[0010] 图1是根据本发明的一个实施方案的一种计算环境的高级框图。

[0011] 图2是根据一个实施方案的用作安全服务器和/或客户端的一台计算机的高级框图。

[0012] 图3是一个高级框图，展示了根据一个实施方案的信誉模块中的多个模块。

[0013] 图4是一个流程图，展示了根据一个实施方案的信誉模块使用来自从多个客户端接收的多个报告的信息来确定有关多个对象的信誉分数的操作。

[0014] 这些附图描绘了本发明的不同的实施方案，仅用于说明的目的。本领域的普通技术人员将从以下讨论中容易地认识到，可以使用本文所示例的这些结构以及方法的替代性实施方案而不背离本文所描述的本发明的原理。

具体实施方式

[0015] 图1是根据一个实施方案的一种计算环境100的高级框图。图1展示了连接到一个网络114上的一个安全服务器102。网络114还连接到多个客户端112上。图1以及其他图示使用类似的参考号来指代相似的要素。参考号后的字母如“112A”表示该文字专指具有这个具体参考号的要素。该文本中没有后续字母的参考号如“112”是指图示中包含该参考号的任何或全部要素(例如，文本中的“112”是指图示中的参考号“112A”、“112B”、和/或“112C”)。为了使说明简化并清晰，在图1中仅示出了三个客户端112。计算环境100的实施方案可以具有成千上万个客户端112以及多个服务器102。在一些实施方案中，这些客户端112仅在某一

时间段连接到网络114上或根本不连接。

[0016] 客户端112是能够托管恶意软件的一个电子装置。在一个实施方案中，客户端112是执行例如可兼容Microsoft Windows的操作系统(OS)、Apple OS X、和/或Linux发行版的一个常规的计算机系统。在另一个的实施方案中，客户端112是具有计算机功能的另一种装置，如个人数字助理(PDA)、移动电话、视频游戏系统，等等。客户端112典型地存储了能够托管恶意软件的数目众多的计算机文件和/或软件应用程序(统称为“对象”)。

[0017] 恶意软件一般被定义为在客户端112上暗中执行的或具有一些不正当功能的软件。恶意软件可以采取很多形式，如附加到合法文件上的寄生病毒、利用计算机的安全弱点以便感染计算机并传播到其他计算机的蠕虫、看似合法但实际上包含隐藏的恶意代码的特洛伊木马程序、以及监控计算机上的按键和/或其他动作以便捕获敏感信息或显示广告的间谍软件。

[0018] 客户端112执行一个安全模块110用于检测恶意软件的出现。安全模块110可以例如被结合到计算机的OS中或是一个独立的全面安全包的一部分。在一个实施方案中，安全模块110由操作安全服务器102的实体来提供。安全模块110可经由网络114与安全服务器102通信，以便下载用来检测恶意软件的信息。安全模块110还可经由网络114与安全服务器102通信，以便提交有关在客户端112处检测到的多个对象的信息。

[0019] 在一个实施方案中，安全模块110将在该客户端处检测到的多个对象的标识符提交给安全服务器102并且接收由其返回的这些对象的信誉分数。信誉分数代表对象的可信任度的一种评估。具有高信誉分数的对象具有良好的信誉并且不太可能包含恶意软件。相反，具有低信誉分数的对象具有不良信誉并且可能包含恶意软件。安全模块110使用该信誉分数连同如行为的其他因素来评估在客户端112处的一个对象是否是恶意软件。安全模块110可以将该评估的结果上报给安全服务器102。

[0020] 安全服务器102是由安全软件供应商或其他实体提供的。安全服务器102可以包括一个或多个标准计算机系统，这个或这些标准计算机系统被配置为经由网络114与客户端112通信。安全服务器102经由网络114接收包含多个对象的标识符以及来自这些客户端112的其他信息的报告。作为响应，安全服务器102经由网络114将这些对象的信誉分数发送给这些客户端112。

[0021] 在一个实施方案中，安全服务器102包括一个数据存储器104以及一个信誉模块106。信誉模块106基于多个因素(如这些客户端112遇见这些对象的频率)来确定这些对象的信誉分数。这些信誉分数由信誉模块106存储在数据存储器104中。信誉模块106响应于经由网络114的来自客户端112的查询或提交来访问数据存储器104。

[0022] 信誉模块106的一个实施方案还确定这些客户端112的置信量度。一个客户端112的置信量度表明在从该客户端接收的信息的真实性的置信度的量值，其中高置信量度表明该信息可能是真实的。例如，来自一个特定客户端112的大量报告可能表明该客户端正被一个恶意实体所控制，该恶意实体正企图通过提交虚假报告来影响对象的信誉。信誉模块106可以对这种影响对象的信誉的企图进行检测并降低相应客户端112的置信量度。当确定多个对象的信誉时，信誉模块106可以降低来自具有低置信量度的客户端112的报告的权重，并提高来自具有高置信量度的客户端的报告的权重。因此，信誉模块106可以抵抗来自恶意实体的操纵或以其他方式“欺骗”安全服务器102的企图。

[0023] 网络114使能安全服务器102与客户端112之间的通信。在一个实施方案中，网络114使用多种标准通信技术和/或协议并且包括互联网。因此，网络114可以包括采用例如以太网、802.11、全球微波互联接入(WiMAX)、3G、数字用户线路(DSL)、异步传输模式(ATM)、InfiniBand、PCI Express高级转换等技术的多条链路。类似地，网络114上所用的网络协议可以包括多协议标签交换(MPLS)、传输控制协议/互联网协议(TCP/IP)、用户数据报协议(UDP)、超文本传输协议(HTTP)、简单邮件传输协议(SMTP)、文件传输协议(FTP)，等等。可以使用包括超文本标记语言(HTML)、可扩展标记语言(XML)等的技术和/或格式表示网络114上交换的数据。另外，所有的或部分的链路可以用常规的加密技术进行加密，例如安全套接字层(SSL)、传输层安全(TLS)、虚拟专用网络(VPN)、互联网协议安全(IPsec)，等等。在另一个实施方案中，这些实体可以使用定制的和/或专门的数据通信技术来替代以上说明的那些或添加到以上说明的那些。

[0024] 图2是根据一个实施方案的用作安全服务器102和/或客户端112的一台计算机200的高级框图。所展示的是连接到一个芯片组204上的至少一个处理器202。同样连接到芯片组204上的是一个存储器206、一个存储装置208、一个键盘210、一个图形适配器212、一个定点装置214、以及一个网络适配器216。一个显示器218连接到图形适配器212上。在一个实施方案中，由一个存储器控制器集线器220与一个I/O控制器集线器222来提供芯片组204的功能。在另一个实施方案中，存储器206被直接连接到处理器202上而不是芯片组204上。

[0025] 存储装置208是任何计算机可读存储媒质，如硬盘驱动器、光盘只读存储器(CD-ROM)、DVD、或者固态存储装置。存储器206保持由处理器202使用的多个指令与数据。定点装置214可以是鼠标、轨迹球、或其他类型的定点装置，并且与键盘210一起使用以便将数据输入计算机系统200中。图形适配器212在显示器218上显示图像和其他信息。网络适配器216将计算机系统200连接到一个局域网或广域网上。

[0026] 如在本领域中所皆知的，计算机200可以具有不同于图2所示的部件和/或其他部件。另外，计算机200可以缺少某些展示出的部件。在一个实施方案中，用作安全服务器102的计算机200缺少了键盘210、定点装置214、图形适配器212、和/或显示器218。而且，存储装置208可以位于计算机200中和/或使其与之远离(如实施在一个存储区域网络(SAN)内)。

[0027] 如本领域中所皆知的，计算机200被适配为执行多个计算机程序模块用于提供在此所述的功能。如在此所使用的，术语“模块”是指被利用来提供特定功能的计算机程序逻辑。这样，模块可以在硬件、固件、和/或软件中实施。在一个实施方案中，将多个程序模块存储在存储装置208上、载入到存储器206中、并且由处理器202来执行。

[0028] 在此所述的实体的实施方案可以包括其他的和/或与在此所述不同的模块。另外，归因于这些模块的功能可以在其他的实施方案中由其他的或不同的模块来执行。而且，为了明晰与方便的目的，本说明书偶尔省略了术语“模块”。

[0029] 图3是一个高级框图，展示了根据一个实施方案的信誉模块106的细节图。在一些实施方案中，信誉模块106被结合到安全服务器102中作为一个独立的应用程序或作为另一个产品的一部分。如图3所示，信誉模块106包括多个模块。本领域中的普通技术人员将会认识到信誉模块106的其他实施方案可以具有不同于在此所述的模块和/或其他模块，并且这些功能能够以不同的方式分布在这些模块中。

[0030] 通信模块302经由网络114与客户端112的安全模块110交换信息。通信模块302接

收有关由安全模块110在客户端112处检测到的多个对象(如文件)的信息。例如,通信模块302可以从安全模块110接收一个报告,该报告包含在一个客户端112处检测到的一个对象的标识符连同对该对象的信誉分数的一个请求。该对象的标识符可以是例如该对象的一个散列。通信模块302与信誉模块106的其他模块进行交互以便确定所标识对象的信誉分数并且将该分数提供给请求安全模块110。

[0031] 在一个实施方案中,这些报告还包括通信模块302可以用来标识提交报告的客户端112的信息。在一个实施方案中,一个报告包括客户端112的一个唯一性标识符。该唯一性标识符可以是伴随该报告和/或用于签署或验证该报告的一个加密密钥或令牌。通信模块302还可以对能用来标识客户端112的其他信息(如从其接收的这些报告的IP地址)进行检测。取决于该实施方案,通信模块302可以访问数据存储器104中将该唯一性标识与客户端112的额外信息相关联的信息,如其地理位置、系统中的年龄(例如,自从客户端的第一份报告以来所经历的时间)、以及它曾提交的其他报告,等等。

[0032] 置信模块304确定客户端112的置信量度。如以上所提及的,置信量度表示在从一个客户端112接收的报告的真实性的置信度的量值。在一个实施方案中,该置信量度是从零到一(包括在内)的一个连续值并且存储在数据存储器104中。取决于该实施方案,该置信量度可以与除客户端112外的其他实体相关联。例如,该置信量度可以与客户端112的一个具体用户或与安全模块110的一个具体实例相关联。为了清晰起见,本说明书是指置信量度与客户端112相关联,但应该理解的是用在这个意义上的“客户端”也指置信量度可与之相关联的其他实体。

[0033] 置信模块304使用从客户端112接收的信息和/或从其他来源接收的有关客户端的信息来计算这些客户端的置信量度。置信模块304使用这些客户端的唯一性标识符去联系并关联来自客户端的信息。取决于该实施方案,置信模块304可以使用多种不同的因素来确定一个客户端的置信量度。

[0034] 置信模块304的一个实施方案使用一个客户端的系统年龄作为一个因素来计算该客户端的置信量度。一个客户端的系统年龄是一个客户端112一直处于活跃状态所经历的时间。例如,一个客户端112的系统年龄可以是从接收来自该客户端的第一份报告的时候起、从在该客户端上安装安全模块110的时候起、或者从用安全服务器102注册该安全模块的时候起所经历的时间。

[0035] 一般情况下,一个“较年长的”客户端112收到一个较高置信量度。仅最近才开始提交报告的一个客户端112可能是不可靠的或在其他方面是不可信赖的。例如,一个恶意实体可能伪造大量的合法的(并且是新的)客户端标识符,并且然后提交大量的报告,企图以此提升恶意软件的信誉分数。置信模块304可以辨认出这些报告是来自“年轻的”客户端112并且可以使用这个因素来降低这些客户端的置信量度。可以使用预定值来建立“年轻的”与“年长的”客户端之间的区别。例如,具有小于六个月年龄的客户端112可以被认为是“年轻的”而其他客户端可以被认为是“年长的”。

[0036] 置信模块304还可以基于除所经历时间外的其他特性来计算一个客户端的年龄。在一个实施方案中,一个客户端的年龄是基于该客户端已经提交的“流行的”对象的报告的数量来测量的。例如,某些软件应用程序在客户端112中是流行的或常见的。例如,很多客户端可能具有数目有限的安装的网页浏览应用程序至少之一。安全模块110将这种流行应用

程序连同其他被检测的对象一起上报给安全服务器102。置信模块304可以将已提交了流行对象的更多报告的一个客户端112处理为“年长”于已提交了此类对象的较少报告的客户端。这样的处理有助于降低客户端112的置信量度，这些客户端仅对非流行对象提交报告并且因此可能企图提升恶意软件的信誉分数。

[0037] 类似的，置信模块304可以基于对于流行对象提交的报告与对于“稀有”对象提交的报告的一个比率来计算一个客户端的年龄，其中“稀有”对象是由非常少的客户端上报的对象。如果一个客户端112对于稀有对象倾向于比对于流行对象提交更多的报告，那么该客户端可能正在企图提升恶意软件的信誉分数。因此，此类客户端112被处理为是“年轻的”并且将具有降低的置信量度。将系统上的一个客户端的年龄作为因素使得“欺骗”信誉系统变得昂贵，这是因为一个客户端必须是“年长的”才能具有一个较高置信量度。

[0038] 置信模块304的一个实施方案使用一个客户端112的地理位置作为一个因素来计算该客户端的置信量度。因为大多数客户端并不同时在世界的多个地方，所以在接近的时间内从不同地理位置接收的由同一客户端提交的有关同一对象的报告表明是一个可疑行为。此类报告可能表明例如该客户端的标识符是由多个恶意行为者用来行骗的。因此，置信模块304可以基于接收到此类报告来降低该客户端的置信量度。此外，不同的地理位置可能具有不同的置信量度。这样，从一个特别可疑的地理位置提交报告的一个客户端112可能具有低于从一个不太可疑的地理位置提交相同报告的另一个客户端的置信量度。

[0039] 置信模块304还可以使用由一个客户端112提交报告的频率作为一个因素来计算该客户端的置信量度。通过追踪多个客户端提交报告的模式，置信模块304可以对由一个具体客户端提交的异常量进行检测。所构成对期望提交模式的一个“异常”偏差的阈值可以基于客户端以前的提交模式从一个客户端到另一个而有所变化。例如，在历史上仅提交少量报告而突然提交大量报告的一个客户端112可能受到危害。其结果是，置信模块304可以降低该客户端的置信量度。

[0040] 置信模块304还可以使用这些客户端标识符来确定置信量度。置信模块304可以将某些客户端标识符标识为无效、伪造、篡改、或以其他方式受到危害。例如，可以通过将在一个所接收的报告中的标识符与在数据存储器104中维护的一个标识符列表相关联来进行这一标识。置信模块304可以辨认出受到危害的标识符并且将该信息用作一个因素来计算那些受影响客户端的置信量度。因此，可以将一个较低置信量度赋予一个具有无效或受到危害的标识符的客户端。

[0041] 进一步地，置信模块304可以使用从其接收报告的客户端的IP地址来影响这些置信量度。某些IP地址可以被标识为属于恶意实体或者在其他方面与低信用有关联。因此，置信模块304可以降低从某些IP地址发送报告的客户端的置信量度。

[0042] 由置信模块304接收的其他信息还可以影响客户端的置信量度。如果一个客户端提交残缺的或虚假的报告，那么置信模块304有理由怀疑该客户端已经受到危害并且可以降低该客户端的置信量度。在多个实施方案中，其中客户端112与置信模块304访问的一个信用卡账户有关联(例如当该客户端的用户已使用信用卡从安全服务器102购买了安全模块110时)，置信模块304可以使用所观察到的信用活动(如退款请求)来影响该置信量度。在其他的实施方案中，基于上述一个或多个因素(如地理位置)对报告进行汇总还可以基于无规律的报告模式来对提交可疑报告的客户端进行标识并且影响客户端的置信量度。

[0043] 由置信模块304接收的额外因素与直接推断可以用于影响客户端的置信量度。例如，从多于一个IP地址接收由一个客户端(相同的客户端标识符)的同时提交可以表明该客户端已经受到危害。从一个客户端接收不寻常的高比率的提交、从多个客户端接收有关几个文件重复的报告、以及对提交不成比例地大量或少量文件的客户端进行标识(或者一个给定特征的不成比例数量的文件，例如客户端似乎提交的是其他客户端未曾提交过的文件)都会进一步影响那些客户端的置信量度。另外，在一个实施方案中，对已知发送垃圾邮件的客户端进行标识是置信模块304用来影响客户端的置信量度的另一个因素。

[0044] 置信模块304的一个实施方案使用上述一个或多个因素来确定一个客户端112的置信量度。在置信模块304使用多个因素的多个实施方案中，置信模块可以将不同的权重赋予不同的因素。例如，客户端112的年龄可以对该置信量度有显著的影响，而该客户端的地理位置可以仅具有非常小的影响。另外，一些实施方案使用多个置信量度，其中每个置信量度对应一个单一因素(例如，年龄)。

[0045] 在一个实施方案中，置信模块304使用计算好的置信量度来将这些客户端指定到一个白名单或黑名单中。总体来说，白名单列出了具有高置信量度并且因此推断是值得信赖的客户端112。相反，黑名单列出了具有低置信量度并且因此推断是不值得信赖的客户端112。在一些实施方案中，置信模块304使用多个阈值来将客户端112指定到这些名单中。如果一个客户端的置信量度低于某一阈值，那么该客户端被列入黑名单。同样，如果一个客户端的置信量度高于某一阈值，那么该客户端被列入白名单。在一些实施方案中，该阈值对于两个名单而言是相同的；在其他的实施方案中，每个名单具有一个单独的阈值。

[0046] 类似地，置信模块304的一些实施方案基于预定的准则来将客户端的置信量度量化为零或一。例如，具有小于六个月年龄的“年轻的”一个客户端112，或者从两个不同的地理区域同时提交报告的一个客户端可以不管其他因素而接收到一个为零的置信量度。

[0047] 对象信誉模块306计算多个对象的信誉分数并且将这些信誉分数存储到数据存储器104中。如以上所提及的，一个对象的信誉分数代表对该对象的可信任度的一种评估。在一个实施方案中，该信誉分数是从零到一(包括在内)的一个数值。一低信誉分数表明该对象可能是恶意软件，而高信誉分数表明该对象可能是合法的。

[0048] 在一个实施方案中，对象信誉模块306至少部分地是基于在这些客户端中所上报对象的流行程度来计算多个对象的信誉分数。广泛分布在多个客户端中的对象(如流行的文字处理应用程序)更有可能是合法的，而这些客户端很少遇到的对象可能是恶意软件。因此，在一个实施方案中，一个具有高流行程度的对象收到较高的信誉分数。

[0049] 在一些实施方案中，多个对象的信誉分数还可以基于主要在其上发现这些对象的客户端112的保健分数。保健分数代表对客户端112的可信任度的一种评估。在保健背景下的“可信任度”是指对客户端对受到恶意软件感染的倾向，其中更经常被感染的客户端112是不太可信的。例如，经常在具有高保健分数的客户端112上发现的一个对象有可能收到表明良好信誉的高信誉分数。相反，主要在具有低保健分数的客户端112上发现的一个对象有可能收到表明不良信誉的低信誉分数。信誉分数还可以基于其他因素，如在其上发现多个对象的网站的信誉分数、这些对象的开发者和/或散布者的信誉分数、以及如这些对象是否被数字签名的其他特征。

[0050] 另外，对象信誉模块306基于曾提交了与对象相关联的报告的客户端的置信量度

来影响对象的信誉分数。在一个实施方案中，对象信誉模块306在计算对象的信誉分数时将来自具有低于一个阈值的置信量度的客户端112的报告排除。例如，可以将来自上述黑名单上的客户端112的报告排除。类似地，对象信誉模块306的一个实施方案在计算对象的信誉分数时使用仅来自具有高于一个阈值的置信量度的客户端的报告。例如，可以仅仅使用来自上述白名单上的客户端112的报告。

[0051] 在另一个实施方案中，对象信誉模块306在一个给定的时间段内使用低和/或高置信量度的客户端与报告一个对象的其他客户端的比率来影响该对象的信誉分数。在这个实施方案中，对象信誉模块306根据主要由具有低置信量度的客户端112上报的对象应当可能具有低信誉分数的原则来工作。同时，对象信誉模块306保留了足够的灵活性以便能够实时地检测信誉“欺骗”。对于这一实施方案，与信誉模块106的其他模块合作的对象信誉模306在每个对象的基础上追踪客户端112的置信量度。

[0052] 对于一个给定的对象，对象信誉模块306可以确定已上报该对象的具有低置信量度的客户端的数量以及已上报该对象的具有高置信量度的客户端的数量，其中“高”和“低”的置信水平是使用多个阈值来确定的。如果在一个给定的时间段内，高置信量度的客户端与其他置信量度的客户端(即非高置信量度客户端)的一个足够大的比率已经上报了该对象，那么对象信誉模块306提高该对象的信誉分数。相反地，如果在相同的时间段或在不同的时间段内，低置信量度的客户端与其他置信量度的客户端(低置信量度客户端)的一个足够大的比率已经上报了该对象，那么对象信誉模块306降低该对象的信誉分数。因此，能够对信誉“欺骗”进行实时检测，并且对象信誉模块306可以对恶意实体的信誉“欺骗”的恶意软件的攻击快速地做出响应。

[0053] 在一个实施方案中，对象信誉模块306使用这些置信量度来给这些报告加权。因此，当计算一个对象的信誉分数时，可以对具有1.0置信水平的一个报告比具有0.5置信水平的一个报告加权两倍。另一种说法就是，来自具有0.50置信量度的客户端的200个报告与来自具有1.0置信量度的客户端的100个报告可以对信誉分数有相同的影响。

[0054] 对象信誉模块306的一个实施方案使用机器学习来计算对象的信誉分数。统计性机器学习算法可以使用置信量度、报告的流行程度、以及其他有关客户端112的信息作为特征来建立一个用于确定信誉分数的分类器。可以使用一组已知其实际配置的对象(即，已知这些对象是合法的或是恶意软件)的特征来训练该分类器。

[0055] 调节模块308对客户端112的置信量度与多个对象的信誉分数进行修改，当这些值随时间变化时。置信量度可以影响信誉分数，并且在一些实施方案中，信誉分数可以影响置信量度。调节模块308将这些置信量度与信誉分数修改为随时间推移由安全服务器102接收的额外的报告。取决于该实施方案，调节模块308可以在周期性的基础上和/或在其他时间内不断地修改这些量度与分数。

[0056] 例如，在一个轻视来自年轻客户端的报告的实施方案中(例如，不到六个月大的客户端收到为零的置信量度)，一个主要在年轻客户端中发现的对象可能收到低信誉分数，因为它看起来并不流行。一旦这些客户端不再“年轻”，那么来自这些客户端的报告将不再被轻视并且该对象现在看起来更流行了。调节模块308由此提高该对象的信誉分数。类似地，具有高置信量度的一个客户端112可能受到危害并且提交随后被发现是恶意软件的对象的很多报告。在这样的情况下，调节模块308可以下调客户端112的置信量度。

[0057] 训练模块310可以生成一个或多个信誉分类器用于支持信誉分数的基于机器学习的计算。在一个实施方案中，训练模块基于与客户端112以及对象相关联的特征的一个数据集来生成一个信誉分类器。这些特征可以包括客户端112的置信量度、客户端的保健分数、对象的信誉、以及对象的流行程度，等等。信誉分类器是一个具体指明多个值(如与用于确定信誉分数的特征相关联的权重或系数)的统计模型。用作信誉分类器的适当类型的统计模型包括但不局限于：神经网络、贝叶斯模型、基于回归的模型以及支持向量机(SVM)。可以通过对已知的恶意软件及合法软件情况的对象进行标识并且使用那些对象的历史客户端报告作为基本实况来训练信誉分类器。根据该实施方案，训练模块310可以在一个周期性的基础上或在其他时间内生成该信誉分类器。训练模块310将生成的信誉分类器进行存储以供对象信誉模块306使用。

[0058] 图4是一个流程图，展示了根据一个实施方案的信誉模块106的操作，该信誉模块使用来自从多个客户端112中接收的报告的信息来确定有关多个对象的信誉分数。应当理解的是这些步骤仅是示意性的。信誉模块106的不同的实施方案能够以不同的顺序执行这些步骤、省略某些步骤、和/或执行未在图4中示出的额外步骤。

[0059] 如图4所示，在402中，信誉模块106接收由多个客户端112提交的有关多个对象的报告。这些报告对在客户端处所检测到的多个对象进行标识并且可以伴随有这些对象的信誉分数的多个请求。在404中，信誉模块106确定提交这些报告的客户端112的信息。如以上所说明的，这些信息可以包括该客户端的一个标识符、该对象的一个散列或其他标识符、以及有关该客户端的其他信息。信誉模块106使用报告中的信息来确定有关该客户端的其他信息，如该客户端的年龄、地理位置、IP地址，等等。在406中，信誉模块106使用所确定的信息来生成客户端112的置信量度。在408中，信誉模块106基于例如这些对象在这些客户端处的流行程度来生成这些对象的信誉分数。所生成的信誉分数受这些客户端的置信量度的影响。在410中，信誉模块106将对象的信誉分数提供给客户端112。客户端112可以使用这些信誉分数来检测这些客户端处的恶意软件。

[0060] 如上所述的技术可以应用于不同其他类型的检测系统，如用于消息传送应用程序的垃圾邮件过滤器、以及被设计为利用对象的信誉分数和客户端的置信量度来检测恶意软件的其他机制。

[0061] 本发明的这些实施方案的前述说明已经为了进行说明而给出；它并不打算是穷进的或将本发明限于所披露的确切形式。相关领域的技术人员可以认识到对以上披露的许多修改和变更是可能的。

[0062] 最后，在本说明书中的语言主要是为了可读性和指导性而选择的，选择这些语言并非用于描述或限定本发明的主题。因此，在此的意图是本发明的范围不受限于这种详细的说明，而是由基于本申请而授权的任何权利要求所限定。因此，本发明的实施方案的披露是旨在是说明性的、并非限制以下权利要求中给出的本发明的范围。

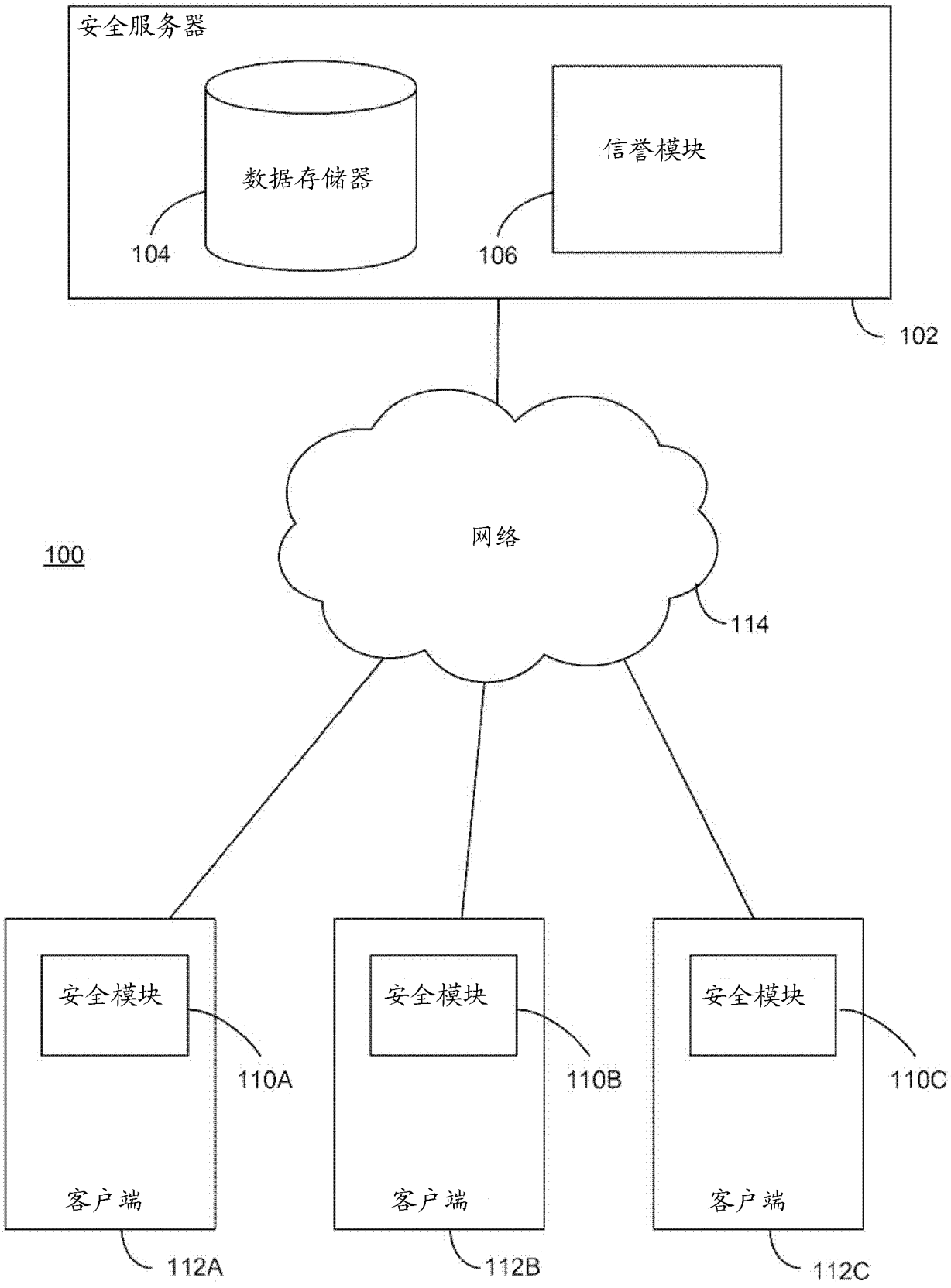

安全服务器
数据存储器
104
信誉模块
106
102
网络
100
114
安全模块
110A
客户端
112A
安全模块
110B
客户端
112B
安全模块
110C
客户端
112C

图1

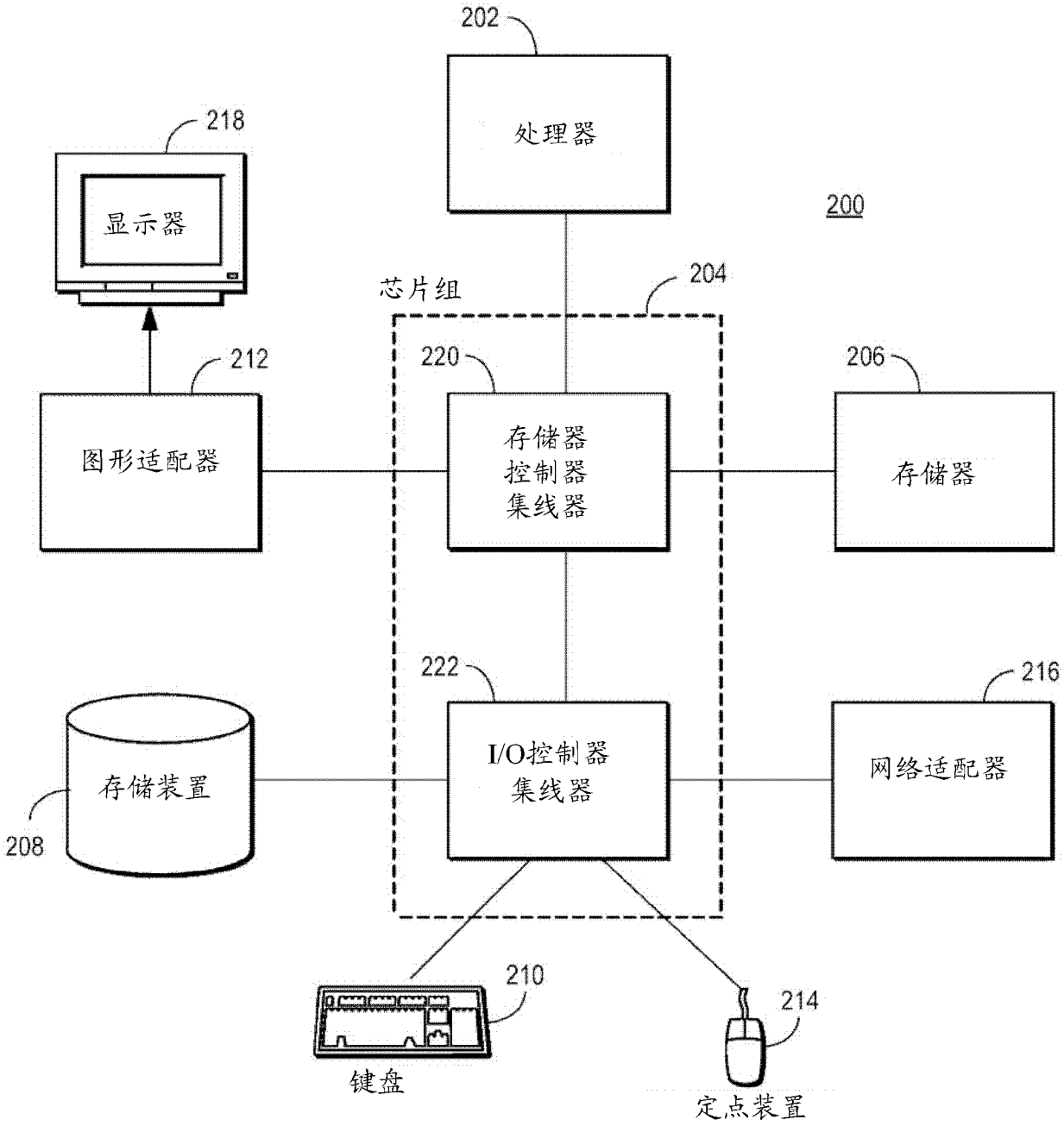

202
处理器
218
显示器
200
芯片组
204
212
220
206
图形适配器
存储器
控制器
集线器
存储器
222
216
存储装置
I/O控制器
集线器
网络适配器
208
210
214
键盘
定点装置

图2

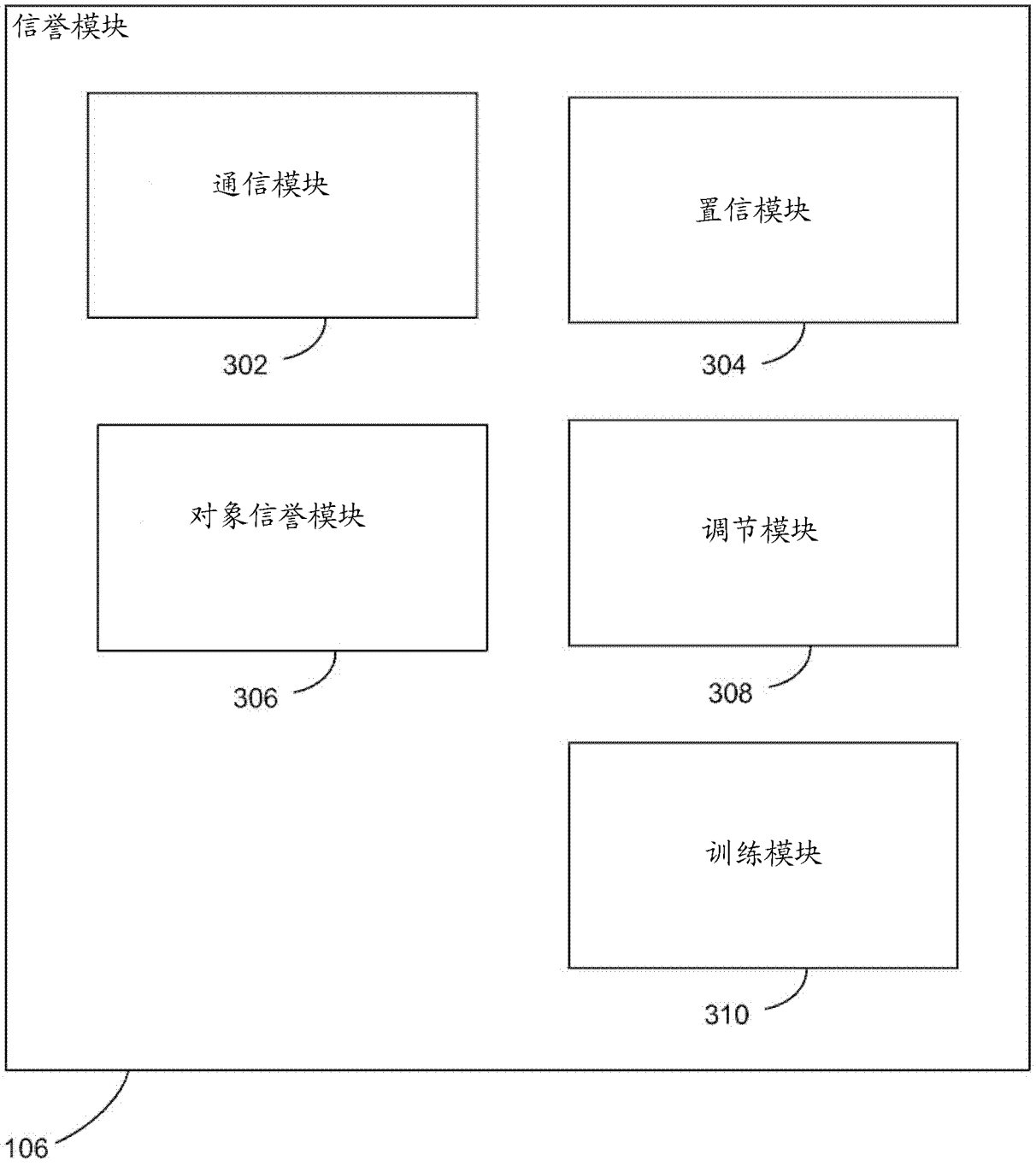


图3

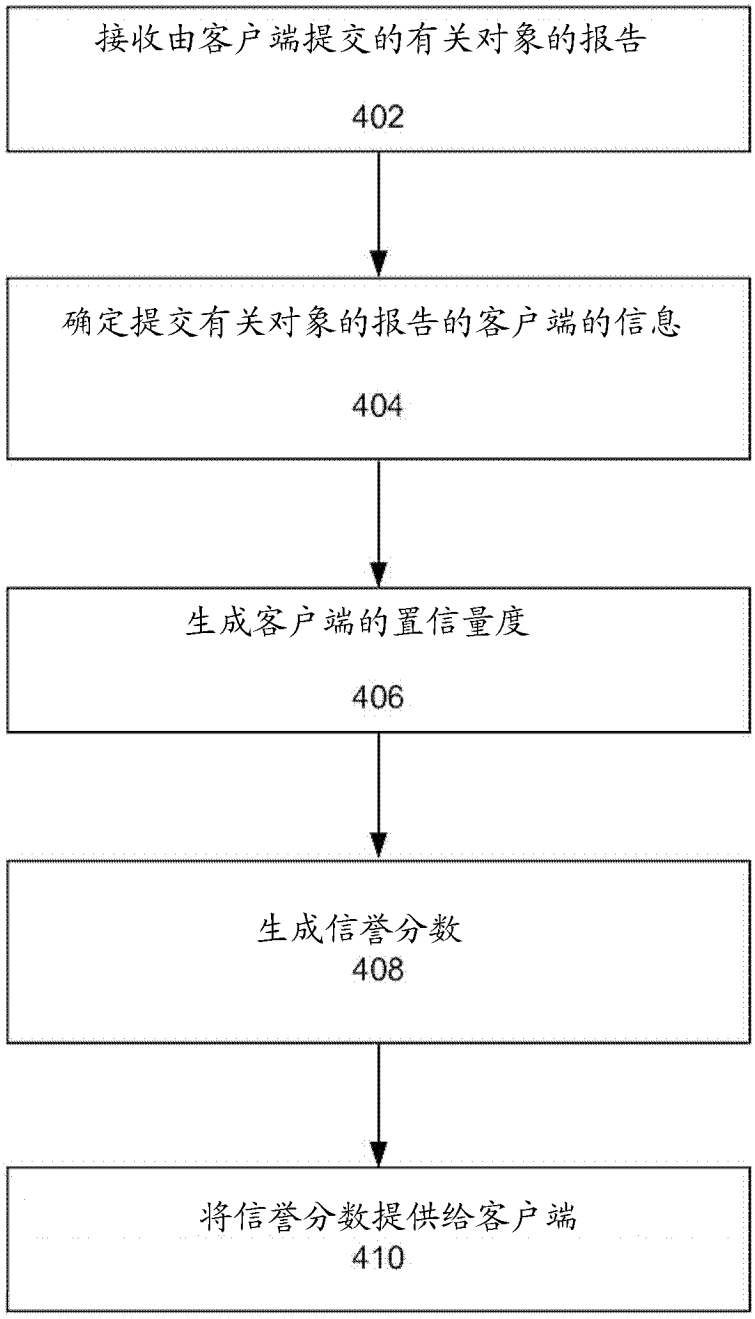

接收由客户端提交的有关对象的报告
402
确定提交有关对象的报告的客户端的信息
404
生成客户端的置信量度
406
生成信誉分数
408
将信誉分数提供给客户端
410

图4