(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 105793863 A
(43)申请公布日 2016.07.20

(21)申请号 201380081279.4

(22)申请日 2013.12.27

(85)PCT国际申请进入国家阶段日
2016.05.27

(86)PCT国际申请的申请数据
PCT/US2013/077935 2013.12.27

(87)PCT国际申请的公布数据
WO2015/099756 EN 2015.07.02

(71)申请人 迈克菲股份有限公司
地址 美国加利福尼亚州

(72)发明人 I·穆迪科

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 何焜

(51)Int.Cl.
G06F 21/55(2006.01)
G06F 21/56(2006.01)

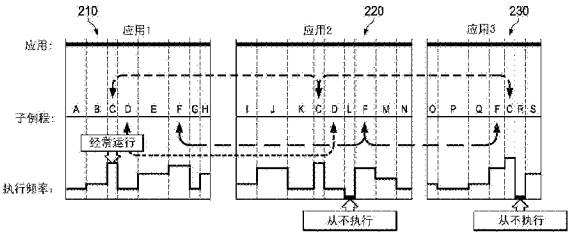
权利要求书4页 说明书15页 附图5页

(54)发明名称

基于频率的信誉

(57)摘要

在一个示例实施例中，公开了在子例程水平分析应用和其他可执行对象的防恶意软件系统和方法。可以给每一子例程指定执行频率评分，该执行频率评分可以基于隔离环境中的仿真执行、基于真实世界操作条件或基于静态分析。可以基于有多频繁地执行来给每一子例程指定执行频率评分。基于这种评分，也可以给每一子例程指定信誉评分。为了帮助对相同子例程在其他应用中发生进行交叉引用，也可以给子例程指定伪唯一标识符，例如模糊指纹。



CN 105793863 A

1.一种装置，其用于执行可执行对象的基于频率的分类，包括：

处理器，其通信上耦合到存储器；

网络接口；以及

信誉客户机引擎，其通信上耦合到所述处理器，且可操作为：

将可执行对象解析成多个子例程；以及

给每一子例程指定执行频率评分。

2.如权利要求1所述的信誉客户机，其特征在于，所述信誉客户机引擎还可操作为：

在所述网络接口上提供所述执行频率评分；以及

通过所述网络接口接收所述可执行对象的信誉评分。

3.如权利要求1所述的信誉客户机，其特征在于，所述给每一子例程指定执行频率评分进一步包括运行所述可执行对象和清点对所述各子例程的调用。

4.如权利要求1所述的信誉客户机，其特征在于，所述信誉客户机引擎还可以操作为在隔离环境中运行所述可执行对象。

5.如权利要求1所述的信誉客户机，其特征在于，将所述可执行对象解析成多个子例程进一步包括修改所述可执行对象的副本以便将频率计数器注入到所述各子例程。

6.一个或多个非暂态计算机可读介质，其上存储有可执行指令，所述可执行指令可操作为指示处理器提供如权利要求1-5中的任何一项所述的信誉客户机引擎。

7.一种信誉服务器，包括：

处理器，其通信上耦合到存储器；

网络接口；以及

信誉服务器引擎，其通信上耦合到所述处理器且可操作为：

将可执行对象解析成多个子例程；以及

给每一子例程指定信誉评分。

8.如权利要求7所述的信誉服务器，其特征在于，所述信誉服务器引擎还可操作为：

至少部分地基于所述多个子例程的所述信誉评分，计算所述可执行对象的信誉评分；以及

经由所述网络接口将所述各信誉评分中的至少一个分发给多个信誉客户机。

9.如权利要求8所述的信誉服务器，其特征在于，所述给每一子例程指定信誉评分进一步包括给每一子例程指定执行频率评分。

10.如权利要求8所述的信誉服务器，其特征在于，将所述可执行对象解析成多个子例程进一步包括从信誉客户机接收关于所述多个子例程的数据。

11.如权利要求8所述的信誉服务器，其特征在于，给每一子例程指定信誉评分进一步包括从信誉客户机接收每一子例程的执行频率评分。

12.如权利要求8所述的信誉服务器，其特征在于，给每一子例程指定信誉评分进一步包括：

给每一子例程指定伪唯一指纹；以及

使用所述伪唯一指纹在信誉数据库中查询匹配子例程的频率或信誉评分。

13.如权利要求8所述的信誉服务器，其特征在于，给每一子例程指定信誉评分进一步包括接收所述子例程的执行频率评分，所述执行频率评分包括跨越多个可执行对象的执行

频率。

14.如权利要求8所述的信誉服务器，其特征在于，所述信誉服务器引擎还可操作为：

在隔离环境中运行所述可执行对象；以及

基于各子例程的执行频率，给各子例程指定频率评分。

15.如权利要求8所述的信誉服务器，其特征在于，给每一子例程指定信誉评分进一步包括静态分析所述可执行对象。

16.如权利要求8所述的信誉服务器，其特征在于，所述信誉服务器引擎还可以操作为标记带有低信誉评分的可执行对象以供额外深入分析。

17.如权利要求8所述的信誉服务器，其特征在于，所述可执行对象的所述信誉至少部分地基于所述多个子例程的所述信誉。

18.如权利要求8所述的信誉服务器，其特征在于，所述信誉服务器引擎还可操作为：

确定所述可执行对象具有高信誉评分；以及

给所述多个子例程指定高信誉评分。

19.如权利要求8所述的信誉服务器，其特征在于，所述信誉服务器引擎还可操作为：

给至少一个子例程指定伪唯一指纹；

跨越多个可执行对象计算所述子例程的执行频率评分；以及

将所述信誉评分与所述执行频率评分相关起来。

20.如权利要求19所述的信誉服务器，其特征在于，给所述子例程指定伪唯一指纹包括计算模糊指纹。

21.如权利要求8所述的信誉服务器，其特征在于，所述信誉服务器引擎还可以操作为将具有执行频率评分0的子例程标识为安全风险。

22.如权利要求8所述的信誉服务器，其特征在于，所述信誉服务器引擎还可以操作为将带有低执行频率评分的子例程标识为可疑。

23.至少一个非暂态计算机可读存储介质，其上存储有可执行指令，所述可执行指令可操作为提供如权利要求8-22中的任何一项所述的信誉服务器引擎。

24.一种用于计算可执行对象的信誉的方法，所述方法可在计算设备上执行，且包括：

将可执行对象解析成多个子例程；

给每一子例程指定执行频率评分；

至少部分地基于所述执行频率评分，给每一子例程指定信誉评分；以及

至少部分地基于所述各子例程的所述信誉评分，给所述可执行对象指定信誉评分。

25.如权利要求24所述的方法，其特征在于，给所述可执行对象指定信誉评分进一步包括：

给子例程指定伪唯一标识符；

查找带有所述相同的伪唯一标识符的、具有先前计算的执行频率的子例程；以及

聚集所述子例程的所述执行频率。

26.一种提供信誉服务器引擎的方法，包括：

将可执行对象解析成多个子例程；以及

给每一子例程指定信誉评分。

27.如权利要求26所述的方法，进一步包括给所述可执行对象指定信誉，其特征在于，

所述可执行对象的所述信誉至少部分地基于所述各子例程的所述信誉。

28.如权利要求27所述的方法，进一步包括标记带有低信誉评分的可执行对象以供额外深入分析。

29.如权利要求26所述的方法，其特征在于，给每一子例程指定信誉评分包括给每一子例程指定执行频率评分。

30.如权利要求26所述的方法，其特征在于，可操作为给每一子例程指定信誉评分的所述各指令还可操作为：

确定所述可执行对象具有高信誉评分；以及

给所述各子例程指定高信誉评分。

31.如权利要求26所述的方法，其特征在于，可操作为给每一子例程指定信誉评分的所述各指令还可操作为：

给所述子例程指定伪唯一指纹；

跨越多个可执行对象计算所述子例程的执行频率评分；以及

将所述信誉评分与所述执行频率评分相关起来。

32.如权利要求31所述的方法，其特征在于，给所述子例程指定伪唯一指纹包括计算模糊指纹。

33.如权利要求26所述的方法，进一步包括标记带有低信誉评分的子例程以供额外深入分析。

34.如权利要求26所述的方法，进一步包括：

给每一子例程指定执行频率评分；以及

将带有执行频率评分0的子例程标记为安全风险。

35.如权利要求34所述的方法，进一步包括将带有低执行频率评分的子例程标识为可疑。

36.如权利要求26所述的方法，进一步包括在隔离环境中运行所述可执行对象。

37.一种设备，其包括用于执行如权利要求26-36中的任何一项所述的方法的装置。

38.如权利要求37所述的设备，其特征在于，所述装置包括处理器和存储器。

39.如权利要求38所述的设备，其特征在于，所述存储器包括机器可读指令，在被执行时，所述机器可读指令引起所述设备执行如权利要求26-36中的任何一项所述的方法。

40.如权利要求38所述的设备，其特征在于，所述设备是计算系统。

41.一个或多个非暂态计算机可读介质，其上存储有可执行指令，所述可执行指令可操作为指示处理器执行如权利要求26-36中的任何一项所述的方法。

42.一种计算设备，包括：

用于将可执行对象解析成多个子例程的装置；

用于给每一子例程指定执行频率评分的装置；

用于至少部分地基于所述执行频率评分给每一子例程指定信誉评分的装置；以及

用于至少部分地基于所述各子例程的所述信誉评分给所述可执行对象指定信誉评分的装置。

43.如权利要求42所述的所述计算设备，其特征在于，用于给所述可执行对象指定信誉评分的所述装置还包括：

用于给子例程指定伪唯一标识符的装置；

用于查找带有所述相同的伪唯一标识符的、具有先前计算的执行频率的子例程的装置；以及

用于聚集所述子例程的所述执行频率的装置。

44.如权利要求42或43所述的计算设备，其特征在于，所述各装置中的每一种都包括存储在非暂态计算机可读介质上的可执行指令。

基于频率的信誉

[0001] 本公开内容的领域

[0002] 本申请涉及计算机网络安全的领域，且尤其涉及用于为对象计算基于频率的信誉的系统、装置和方法。

[0003] 背景

[0004] 贯穿本说明书所使用的恶意软件(“malware”)包括任何病毒、木马、机器人、僵尸、黑客程序(rootkit)、后门、蠕虫、间谍软件、广告软件、勒索软件、拨号器、有效载荷、恶意浏览器辅助对象、cookie、记录器或被设计成采取可能不需要的动作的类似物，包括作为非限制性示例的数据破坏、隐蔽数据收集、浏览器劫持、网络代理或重定向、隐蔽跟踪、数据记录、键盘记录、过度或蓄意的障碍移除、联系人搜集以及未经许可的自我传播。在此称为防恶意软件系统某些系统聚焦于在应用或文件水平标识和打击恶意软件。“可执行对象”包括任何文件、程序、宏、脚本、文档、记录或包含用于执行程序的代码的类似物。除了被开发成作为单机程序操作之外，恶意软件也可以采取添加或注入到其他软件的恶意代码的形式。这种形式的一个示例可以是其中通过寄生复制计算机病毒引入恶意代码的“受感染文件”。也可以将恶意代码手动注入或将它添加到软件源，以使得在编译之后它将变成可执行对象的一部分，或者可以被添加到脚本且进行解释，脚本可以编译或者不编译。某些防恶意软件解决方案聚焦于标识受感染文件且然后移除、隔离或以其他方式阻断它们。

[0005] 附图简述

[0006] 在与附图一起阅读时，可从下列详细描述最佳理解本公开内容。要强调的是，根据本行业中的标准做法，各种特征没有按比例绘制，且仅用于阐释目的。事实上，出于讨论的清晰起见，可以任意增加或减少各种特征的尺度。

[0007] 图1是根据本说明书的一个或多个示例的分布式信誉环境的网络级图。

[0008] 图2是根据本说明书的一个或多个示例包含多个子例程(包括常见子例程)的多个可执行对象的框图。

[0009] 图3是根据本说明书的一个或多个示例的客户机设备130的框图。

[0010] 图4是根据本说明书的一个或多个示例由信誉客户机执行的示例过程的流程图。

[0011] 图5是根据本说明书的一个或多个示例的信誉服务器的框图。

[0012] 图6是根据本说明书的一个或多个示例的提供信誉服务器的一种方法的流程图。

[0013] 各实施例的详细描述

[0014] 概览

[0015] 在一种示例中，公开了在子例程水平分析应用和其他可执行对象的防恶意软件系统和方法。可以给每一子例程指定执行频率评分，该执行频率评分可以基于隔离环境中的仿真执行、基于真实世界操作条件或基于静态分析。可以基于有多频繁地执行来给每一子例程指定执行频率评分。基于这种评分，也可以给每一子例程指定信誉评分。为了辅助对在其他应用中发生的相同子例程的交叉引用，也可以给子例程指定伪唯一标识符，例如模糊指纹。

[0016] 本公开内容的各实施例

[0017] 一些软件生态系统已经向从“应用商店”如谷歌商店(Google Play)、苹果商店和微软商店分发的应用和其他可执行对象的模型迁移。在这种环境中，恶意软件作者可以通过隐藏恶意功能以免受应用商店筛选来改变适应。一些防恶意软件解决方案也可能难以检测的一种可能方法是构建有用的或期望的程序例如游戏并向其注入恶意子例程，这些恶意子例程仅在特定的相对罕见的条件下激活，例如，针对相对小的但期望的用户类别(这种类型的包含有时被称为“复活节彩蛋”)。在这种场景中，许多用户将发现该应用在预期边界内操作且看上去是有用和出现有用和有趣的。这些用户可能给予该应用良好评价，从而加剧了隐藏的恶意软件的散布。

[0018] 类似地，可以通过贿赂开发商或获得对源代码控制系统的未经授权的访问权的手段将恶意代码注入到合法软件，例如在入侵拥有对源代码储存库的“写”访问权的人的计算机之后。这种隐蔽的恶意软件传播可以用于大规模攻击以及有针对性的攻击，包括政府资助的攻击。

[0019] 因而，在一些情况中将恶意软件标识限制在可执行对象水平可能不是最优的。相反，新出现的威胁可能聚焦于新的攻击方法，例如包括：

[0020] 通过逆向工程或以其他方式修改现有可执行对象以注入恶意软件例程创建受感染文件，且向应用商店提供经修改的可执行对象。

[0021] 创建经由应用商店分发的大部分合法的可执行对象，但其中包括偶尔执行的恶意软件例程，使得难以将可执行对象标识为恶意软件。

[0022] 通过使用大型开发团队和第三方软件的加载项，可进一步加剧这些挑战。在一种示例攻击中，恶意软件作者以目标代码格式提供有用的第三方库。该库可以包括大部分合法的功能，加上仅偶尔执行的恶意软件有效载荷。这种偶尔执行可以帮助掩盖该库的恶意软件本质。例如，该库可以记录金融交易，且仅在用户访问具有多于100,000美元的可用资金的银行账户时激活，于是该账户被取空了。在另一示例中，恶意软件有效载荷从用户收集私有数据以供销售给营销实体，但仅在出现GPS信号时以及在发现用户处于从列表选择的一种邮政编码内时收集数据，该列表被配置成大到足以提供有用数据但小到足以确保仅偶尔执行恶意软件有效载荷。

[0023] 执行的这种偶发性可以帮助确保不能容易地检测到恶意软件库。如果该库提供通常使用的或非常有用的功能，且如果以宽松的授权条款免费或廉价提供它，那么，寻求满足紧迫的绝限的时间紧张的开发者可能被引诱到使用该库。因而，恶意软件库可能最终进入多种不同应用，且被分发给多种不同的设备。宽广、错杂的构分布也可能使得难以标识恶意软件库的所有实例，即使在发现恶意的有效载荷之后也是如此。例如，可以在第一可执行对象中标识有效载荷，以使得适当地隔离、清洗和重新部署第一可执行对象而不带有有效载荷。然而，由于不知道已经使用该库的每一供应商，难以标识每一受感染文件。此外，该库可能拥有执行或解释从外部源提供的代码的能力，作为非限制性示例，外部源例如来自Web页面的脚本或指令或经由网络连接接收的命令。在一些情况中，在执行在一些情况中等效于“僵尸”、“后门”、或“远程壳”功能的此类远程控制之前，静态和动态分析不能够检查攻击者的确切意图。

[0024] 在第二示例攻击场景中，恶意软件作者取得诸如应用之类的公开可获得的可执行对象的副本，并逆向工程或以其他方式修改该应用以插入恶意软件行为。然后，该作者可以

将该应用分发到例如用户可以可选地选择的未经验证第三方应用储存库。在这种情况中，最终用户可以发现可以在第三方应用储存库上免费获得流行的付费应用，且看上去具有所期望的应用的全部原始功能。因为恶意软件有效载荷仅在某些条件下激活，许多用户可能不会受到不良影响。在这种情况中，不需要将该应用的每一副本都标识为恶意软件。相反，仅需要标记已经修改的那些。

[0025] 在第三示例攻击场景中，恶意软件作者可能会被诸如应用之类的可执行对象的在其他方面合法的开发者合法雇佣。在这种情况中，用户可以隐蔽地将恶意软件行为注入在其他方面合法的应用，且可以通过将恶意软件有效载荷配置成仅在某些条件下激活来掩盖它们的存在。在这种情况中，可能难以标识哪些应用受到影响，这是因为可能不清楚恶意软件作者从事过或接触过哪些应用。

[0026] 作为其中可以有效地部署本说明书的系统和方法的非限制性示例提供前述内容。

[0027] 根据本说明书的一个示例，提供了用于标识在其他方面可能是(但不一定是)合法的可执行对象中的恶意软件有效载荷的系统和方法。在该示例中，信誉客户机将可执行对象解析成可识别的子例程，且给每一子例程指派伪唯一标识符例如模糊指纹。在本说明书中，“子例程”可以包括任何编程子例程、例程、过程、函数、方法、类、对象、模块或包含可执行指令的代码的类似可识别部分。应注意，子例程未必如同在明确过程中一样具有清晰定义的入口点和退出点。作为围绕实现本说明书的公开内容的系统的设计，恶意软件作者可以尝试将偶尔执行的恶意代码隐藏在频繁执行的过程内。因而，预测在一些情况中，可以将清晰定义的过程的分离的分支分离地标识为过程，以使得可以分离地评估它们的执行频率。

[0028] 一旦标识了每一子例程并给其指定标识符，信誉客户机要么将可执行对象传输给信誉服务器，要么执行本地分析，其中主动地或被动地分析可执行对象。分析可以是在集中式储存库中，或跨越多种现实世界用例而分布。有利的是，可以从多个个体客户机聚集关于细粒度子例程水平代码执行的数据。基于有多频繁地执行，给各子例程等级或评分。在频繁地执行子例程而没有值得注意的负面影响或来自用户的投诉时，可以将它标记成较不可疑。在偶尔执行子例程时，且尤其是在执行伴随着报告“古怪”行为或用户投诉的场合，可以将该子例程标记成可疑。可以隔离、清洗可疑子例程，或者在一些情况中可疑子例程可能经历额外的详尽分析，如操作人员的反编译和深入分析。有利的是，可以在任何可执行对象中通过其标识符标识该子例程。因而，恶意软件和恶意软件行为的标识可以与特定可执行对象的身份解耦。

[0029] 图1是根据本说明书的一个或多个示例的分布式信誉环境的网络级图。在这一示例中，多个用户132操作多个客户机设备130。应注意，每一客户机设备可以连接到网络120，如互联网、内联网、广域网(WAN)、局域网(LAN)、公司网络、受保护网络或类似网络。恶意软件作者170也经由客户机设备130-4连接到网络120。提供应用商店180，且其通信上耦合到网络120。信誉服务器110连接到网络120且通信上耦合到信誉数据库140。在这一实施例中，将信誉数据库140公开为直接连接到信誉服务器110，但应明白，其他配置是可能的，包括信誉数据库140可以由第三方提供、可以被在多个设备上分布以及可以例如经由应用编程接口(API)可访问。

[0030] 在一种示例中，用户132操作客户机设备130。“客户机设备”可以包括任何类型的

节点、用户设备，作为非限制性示例包括计算机、个人数字助理(PDA)、膝上型计算机或电子笔记本、蜂窝式电话、IP电话、iPhone™、iPad™、微软Surface™、安卓™电话、谷歌Nexus™或能够执行指令的任何其他设备、组件、元件或对象。“用户”可以包括能够操作、使用或以其他方式与客户机设备连接的任何个人、实体、软件或设备。在此明确预期，一些客户机设备130可以在没有人类用户交互的情况下操作，例如在远程控制的设备、传感器或嵌入式系统的情况下。例如，客户机设备130-5可以是嵌入式系统、远程传感器、网络控制器或通常不由人类用户操作的其他设备。在客户机设备130-5的情况中，用户132可以是嵌入式操作系统或受客户机设备130-5控制、向客户机设备130-5发送数据或从客户机设备130-5接收数据的外部系统。

[0031] 在一些情况中，具有多个信誉服务器110或将信誉服务器110配置成单独地处理多种类别的客户机设备130是有益的。例如，可在微软Windows7上执行的恶意软件有效载荷可能在上面列出的其他设备中的任何上不可执行。相反，可能需要将恶意软件有效载荷制作成专门针对特定架构。然而，本说明书明确预期其中单个恶意软件有效载荷可以针对多个客户机设备130平台的情况。例如，恶意软件有效载荷可以用跨平台语言如Java实现，且可以能够利用多个平台共有的安全弱点。

[0032] 在一种示例中，用户132-1操作客户机设备130-1，客户机设备130-1可以是安卓电话。在这一示例中，大量其他用户也可以操作类似地配置的安卓电话，且拥有对应用商店180的访问权，他们从应用商店接收可执行对象。恶意软件作者170可能想创建针对安卓电话的恶意软件，且可以通过上面提到的示例方法的其中之一或通过任何其他合适的方法来这样做。

[0033] 信誉服务器110可以例如由应用商店180的运营商或第三方安全提供商操作。进一步，信誉数据库可以由信誉服务器110的运营商操作，或者可以由第三方提供。笼统地说，在本说明书中公开的实体可以是或者不是分离的实体，这取决于具体配置。

[0034] 信誉服务器110可以被配置成为经由应用商店180分发的可执行对象或通过任何合适手段分发的其他可执行对象提供信誉。贯穿本说明书，“信誉”可以包括个别地或共同地表示与可执行对象或子例程是否恶意软件或是否包含恶意软件的判断相关的置信度水平的任何数据或多种数据。进一步，在本说明书的上下文中，可以给子例程或子例程组而不是整个可执行对象指定信誉。

[0035] 图2是根据本说明书的一个或多个示例包含多个子例程(包括常见子例程)的多个可执行对象的框图。在这一示例中，可执行对象210、220和230均包含多个子例程。在这一示例中，可执行对象210包括子例程A、B、C、D、E、F、G和H。如下图所指示，子例程C频繁地执行。子例程E、F和H适度频繁地执行。子例程B偶尔到适度频繁地执行。并且，子例程A和G偶尔执行。

[0036] 在可执行对象220中，出现了子例程I、J、K、C、D、L、F、M和N。值得注意的是，子例程C和D对可执行对象210来说是常见的。如同在可执行对象210中那样，子例程C频繁地执行。子例程I、J、F和M适度频繁地执行。子例程N偶尔执行。并且，子例程L从不执行。

[0037] 在可执行对象230中，出现了子例程O、P、Q、F、C、R和S。再次，子例程C非常频繁地执行。子例程F再次适度频繁地执行，子例程S也是如此。子例程O、P和Q偶尔执行。并且，子例程R从不执行。

[0038] 在前述的示例中，子例程C可以接收具有相对高的置信度的高的信誉(潜在地指示它是合法的)，这是因为它频繁地执行且出现在许多应用中。子例程F也可以接收相对高的信誉，这是因为它出现在许多应用中且适度频繁地执行。在本说明书的上下文中，“高的信誉”可以包括以高的置信度指示可执行对象或子例程是合法的和/或没有恶意软件的任何信誉。“低的信誉”对应于可执行对象或子例程是合法的和/或没有恶意软件的低的置信度，或相反地，可执行对象或子例程感染了恶意软件的高的置信度。在这里公开“高的信誉”和“低的信誉”的概念以表示至少一种或多种信誉尺度上的两个相对点，并且，除非在此明确指出，否则不旨在暗示简单二进制信誉分类。

[0039] 与子例程C相比，子例程D可以是相对可疑的，这是因为它在多于一个的应用中看上去是偶尔执行。因而，可以标记子例程D以供操作人员进一步分析。这可以涉及例如反编译、仿真和其他深入分析。如果在深入分析之后，发现子例程D是带有很少需要的合法子例程，则可以给它手动指定高的信誉，以使得遇到作为可执行对象的一部分的对象D的其他客户机设备知道可以安全地执行它。

[0040] 也可以给从未执行的子例程L和R指定相对低的信誉并标记以供进一步的深入分析或人工分析。在进一步分析时，可以发现子例程L包含恶意软件，且子例程R包含未经维护或不再有用的“死”代码。在这种情况中，两种子例程都可以接收低的信誉评分，且在其中可获得更精细调谐的信誉控制的一些实施例中，它们可以接收不同的类别的信誉评分(例如子例程R可以被标记成“已排除”)。例如，子例程L可以被标记成恶意代码。子例程R可以接收将其标识为非恶意但仍然属于潜在安全风险的不同标志，这是因为未使用或未维护的代码可以包含恶意软件作者的攻击载体。因而，可能仍然期望隔离、禁用、报告(例如作为软件脆弱性的可能来源)或以其他方式保护客户机免受子例程R影响。

[0041] 在另一示例中，可执行对象210可以具有非常高的总体信誉，例如因为它是由信誉好的软件供应商提供的广泛使用的软件，且已经使用了很长时间而没有实际恶意软件相关的用户投诉。在这种情况中，子例程A-H中的全部都可以继承来自可执行对象210的高的信誉。该信誉可以跟随那些子例程进入到其他可执行对象，例如220和230，即使其中那些子例程偶尔执行也是如此(例如可执行对象220中的子例程D)。因而，在这一示例中，只要子例程D不开始主动地显示出恶意软件行为，它就将继续具有高的信誉。

[0042] 图3是根据本说明书的一个或多个示例的客户机设备130的框图。客户机设备130受到处理器310的控制，处理器310通信上耦合到存储器元件320。在一种示例中，处理器310经由总线370通信上耦合到其他系统元件。作为非限制性示例，那些元件可以包括网络接口340和存储350(在一些情况中可以是某种存储器元件320)以及用户接口360。明确预期，上面的元素中的任何都可以以硬件、软件、固件或其任何组合来实现。

[0043] 可以例如经由可执行软件或固件指令将处理器310配置成控制客户机设备130。“处理器”可以包括提供可编程逻辑的硬件、软件或固件的任何组合，包括作为非限制性示例的微处理器、数字信号处理器、现场可编程门阵列、可编程逻辑阵列、专用集成电路或虚拟机处理器。

[0044] 在一些实施例中，存储器320可以是相对低等待时间的易失性存储器，且可以包括主存储器、高速缓存、片上存储器、L1存储器、L2存储器或类似物。注意，在这一实施例中，在带有存储器320的直接存储器存取布局中叙述处理器310，但在其他实施例中，存储器320可

以经由系统总线370、经由某种其他总线或经由某种其他装置与处理器310通信。此外，尽管在这一示例中将存储器320和存储350叙述成物理上或概念上分离的设备，但应明白，在一些实施例中，存储器320和存储350可以共享物理设备，该物理设备可以分割或不分割成分离的存储器区域。因而，应明白，在这里公开的布局仅仅是示例而非限制。相反，明确预期，除非明确地另外说明，否则，即使在分离地提到存储器和存储的场合，也可以在单个物理或逻辑的设备中实现它们。

[0045] 在这一示例中，网络接口340包括被配置成通信上将客户机设备130耦合到其他计算设备的任何通信介质，无论是模拟、数字还是混合信号。作为非限制性的示例，网络接口340可以包括Wi-Fi、以太网、火线、光纤、USB、串行接口、红外、蜂窝式网络、数字PC网络、2G数据网络、3G数据网络、4GWiMAX或4G LTE数据网络。

[0046] 在一些实施例中，可以提供用户接口360以辅助用户与客户机设备130交互。“用户接口”可以包括被配置成允许用户与客户机设备130交互(无论是否实时)的硬件、软件和固件的任何组合。在该示例中，作为非限制性示例，用户接口360可以包括键盘、鼠标、显示监视器、扬声器、话筒、可以充当组合输入/输出设备的触敏显示器和照相机。用户接口360可以包括诸如包括征求来自用户的输入或确认的实时对话框的图形用户界面之类的软件服务。

[0047] 作为非易失性存储器介质的示例公开存储350，它可以是某种类别的存储器320。在一些实施例中，存储器320和存储350可以是分离的设备，且存储器320是相对低等待时间的易失性存储器设备，且存储350是相对高等待时间的非易失性存储器设备。存储350也可以是另一设备，如硬盘驱动器、固态驱动器、外部存储、独立磁盘冗余阵列(RAID)、附加网络的存储、光存储、磁带机、备份系统或前述的任何组合。许多其他配置也是可能的，且旨在被包含在本说明书的宽广范围内。

[0048] 在一种示例中，存储器320中存储有可操作为提供在此描述的信誉客户机322的可执行指令。存储器320也可以具有处于执行状态的可执行对象，如正在运行的应用324。存储350也可以包括处于蛰伏或静态状态的可执行对象。信誉客户机引擎322可以被配置成根据在此公开的方法分析正在运行的应用324(在存储器320中)和所存储的应用352(在存储350中静止的数据)。在一些实施例中，可以通过从存储350(例如，作为所存储的应用352的一部分)载入到存储器320以供执行的可执行指令提供信誉客户机引擎322。各指令可以被配置成指示处理器310提供在此描述的客户机信誉服务，例如通过执行图4的方法。在进一步的其他实施例中，可以在管理程序中、在虚拟机或其他合适的虚拟平台上或作为被配置成携带执行诸如图4的方法之类的合适的方法的专有或专用硬件、软件和/或固件的任何组合提供信誉客户机引擎322。在相同实施例或另一实施例中，信誉客户机引擎322可以在专用存储器中操作且可以在分离的处理器或其他可信执行环境上执行，以提供与客户机设备130的其余部分的更好的隔离。这可以帮助防止恶意软件或软件恶意和意外操纵信誉客户机322两者。

[0049] 图4是根据本说明书的一个或多个示例提供信誉客户机引擎的示例方法的流程图。在图3中将信誉客户机322公开成运行在客户机设备130上，但应注意，信誉客户机可以运行在信誉服务器110或任何其他设备上。在某些实施例中，在此公开的步骤也可以跨越多个设备而拆分。例如，在此公开的步骤中的一些可以在客户机设备130上执行，同时可以将

其他卸载到信誉服务器110以节省客户机设备130上的电池或处理功率。

[0050] 在这一示例中，信誉客户机322在客户机设备130执行，表示“活性”筛选模型。在这种模型中，可执行对象可以被部署到多个客户机设备130而不带有现有信誉。当可执行对象在客户机设备130上执行时，构建执行档案以更新可执行对象的信誉。在其他实施例中信誉服务器110和客户机设备130，两者都可以执行图4的方法，其中，信誉服务器110执行静态分析以提供基线标识，且客户机设备130执行动态分析以指定信誉。

[0051] 本领域中的技术人员将想到许多其他组合，且预期它们被包含在本说明书的宽广范围内。还应注意，仅作为示例以具体次序公开图4的方法的步骤以及本说明书中的其他方法，除了另外明确说明或者在本公开内容的上下文中清楚指出一个步骤必须跟随另一步骤的场合之外，所采取的步骤的次序可以任意重排。此外，在其中一个步骤明确地或必然跟随另一步骤的情况中，不旨在暗示第二步骤必须在第一步骤之后直接地或立即发生、中间步骤必须发生、或第二步骤必须是第一步骤的直接的、立即的、不间断的结果、或没有第一步骤的话第二步骤就不能发生。

[0052] 在这一示例中，在框410中，信誉客户机322可以首先选择在客户机设备130上可供分析的所有可执行对象，包括例如应用。选择步骤410也可以包括基于至少一种性质、事件或上下文(例如在安装之前选择已下载应用)选择至少一个可执行对象。这可以包括正在运行应用324、已存储应用352或用户期望存储在存储350中的任何可执行对象中的一种或全部。选择也可以包括例如创建或更新驻留的应用的数据库，且可以包括每一可执行对象的初始整体信誉。在一个示例中，初始信誉可以被初始化为“0”状态，或者在另一非限制性示例中可以从信誉服务器110接收。编目也可以包括提供用于创建各个子例程的应用信誉并与之关联的存储器空间或结构。

[0053] 在框420中，每一可执行对象被解析成各个子例程。这可以包括作为非限制性示例，例如，经由钩住的函数入口点、经由其中记录了全部EIP的完整执行跟踪或经由记录对存储器页面的访问，收集表示可执行对象的执行档案的现场遥测。在一个示例中可以通过英特尔可信存储器服务层(TMSL)或可从McAfee有限公司商购的商用产品(包括DeepSAFE或DeepDefender)提供后者。解析各个子例程可以进一步包括经由函数的标准编译器骨架、经由反编译之后的调用流程图分析或其他合适的方法标识不止一次发现的代码段。

[0054] 解析的静态方法可以包括标识通常在子例程的入口点处执行的指令，例如后面跟着MOV BP、SP的PUSH BP。经由通常在子例程的结束出现的指令，例如后面跟着RET的POP BP，可以同样地标识子例程的结束。在另一示例中，信誉客户机322可以反编译可执行对象并重构流程图。

[0055] 进一步的动态方法可以包括监视CPU分支(CALL、RET、JMP指令)或监视栈区以便发现返回地址。也存在类似分支跟踪和断点(硬件和软件)机制，以辅助重构在某些处理器如英特尔处理器中构建的调用流。然而，应认识到，前述内容全部都是仅作为非限制性示例而公开的，且存在用于解析和标识子例程的多种其他可能的方法，它们预期被包含在本说明书的宽广的范围内。

[0056] 解析也可以涉及创建可执行对象的经修改副本以供分析。在这种情况下，可以修改某些子例程以便注入每当执行该子例程时就更新的频率计数器(或调用进行计数的例程)。

[0057] 一旦已经标识了每一子例程，在框430中，提取每一子例程的指纹，这意味着给它指定如上所述的伪唯一标识符。这可以包括例如计算每一子例程的密码散列。值得注意的是，密码散列将仅在子例程严格相同时匹配，这可能是借助于相同的编译器选项编译公共代码的多个单元的情况。诸如SHA2或SHA3之类的现代散列适于避免大多数冲突，这将有助于散列的伪唯一性质接近真正的唯一性。因而，应注意，如在本说明书中所使用的，“伪唯一”是指在其中使用标识符的应用的目的来说足够接近唯一的标识符，且不必是但可以是真正的唯一，或者由统计学上极低的冲突概率来表征。

[0058] 然而，强壮散列将不标识除了琐细修改之外相同的代码，包括以不同的编译器选项简单地编译相同的源代码。在一种示例中，为了改善基本相同但稍微不同的子例程的匹配，可以使用“模糊散列”或“模糊指纹提取”。例如，为了更好地匹配文本字符串，可以将它们转换成全部都是大写或者全部都是小写。为了匹配英特尔/AMD x32/x64代码，可以移除存储器引用并例如用0或连续数字替换，仅留下CPU操作码进行散列。例如，代替后面跟随着ADD AX,[2345]的MOV AX,[1234]，模糊指纹将散列后面跟随着ADD AX,[1]的MOV AX,[0]，这种方法和类似方法可以改善稍微修改的代码部分的匹配。

[0059] 也可以使用其他模糊散列技术，诸如例如SSDEEP，SSDEEP使用上下文触发的分段散列(CTPH)。也可以构建出现在不同子例程中的常见子串的字典，且可以基于常见子串的大小和频率匹配各子例程。

[0060] 为了使得子例程的标识更加稳健，执行免遭篡改的指纹提取以避免活动恶意软件干涉该过程的可能性可能是有益的。作为非限制性示例，例如通过在诸如管理程序、OS内核之类的可信执行环境(TEE)中或在英特尔安全守卫扩展(Intel Secure Guard Extension) SGX中、在英特尔vPro中、在安全元件中或者在固件中执行散列或指纹提取，可以实现这一点。增强散列步骤的另一方式可以包括经由到诸如信誉服务器110之类的另一可信计算机的安全网络连接来传送对象以供散列。在一些实施例中，整个信誉客户机322可以被放置到TEE中。

[0061] 应注意，仅作为非限制性示例给出在这里公开的指纹提取技术，且预期用于对子例程进行指纹提取的任何合适的技术都应被包括在本说明书的宽广范围内。

[0062] 在框440中，信誉客户机处理已知信誉。这些已知信誉可以是该方法先前的迭代的结果，或者可以从信誉服务器110接收。作为非限制性示例，该处理可以包括给某些子例程或可执行对象指定已知的或先前计算的信誉评分。对于被标记成恶意软件的可执行对象，可以隔离、删除、禁用或以其他方式补救该对象。对于包含恶意软件的在其它方面合法的可执行对象，可以采取补救步骤，包括例如从可执行对象去链接厌恶的子例程，重配置权限以阻止对敏感资源的访问，用剥除了恶意行为的子例程的“已清洗”版本代替该子例程，给子例程提供仿真数据以防止它执行，或以其他方式防止子例程提交有害动作。例如，如果子例程仅在发现用户处于某些邮政编码时激活，则可以给该子例程一贯地馈送不处于列表中的假的邮政编码。在已经以足够的粒度执行该方法的场合，即使在可执行对象以其他方式需要访问合法GPS数据以执行用户期望的功能时也可能这样做。在那些情况下，可以仅把假的地理数据馈送给受影响的子例程，而不是馈送给作为整体的可执行对象。

[0063] 在框450中，给已标识子例程指定频率评分。频率可以包括在使用期间执行子例程的次数，且也可以包括对在可执行对象内对该子例程的调用次数的静态分析。因而，在此明

确预期，频率可以包括多个因素且可以从那些多个因素的组合导出。还预期，信誉可以包括对不同的频率因素进行加权。例如，实际上执行子例程的次数可能比对该子例程的静态调用的数量相对而言更重要。因而，一种示例信誉算法可以包括给实际上执行的总的次数和静态调用的总的数量指定加权平均。在另一示例信誉算法中，可以分离地跟踪这两个因素，且置信度水平可以基于其中之一或两者是否高于或低于各自的阈值。在又一示例中，子例程出现在其中的不同应用的数量可以为子例程提供另一置信度指示符。例如，如果子例程出现在许多不同的应用中，且跨越所有应用执行得非常罕见，则可以将它标记成可疑子例程且应经受附加的人工分析。在另一示例中，出现在许多不同的应用中且跨越所有应用频繁地执行的子例程可以获得较不可疑的信誉。尤其是在与特定子例程的执行相关的场合，用户投诉的频率和严重程度也可以是本说明书中考虑的频率因素。应注意，在某些实施例中，信誉客户机322可以仅提供原始频率评分，而在其他实施例中，信誉客户机322可以基于频率评分计算信誉评分。

[0064] 在一些实施例中，计算频率评分也可以涉及专用装备或仪器。例如，某些设备可以配备有支持处理器或存储器监视(包括例如英特尔TMSL库、断点或CPU分支历史)的适当的硬件。在另一示例中，经由代码覆盖遥测收集频率数据。在这一示例中，可以从客户机设备130或在隔离环境中的预筛选过程期间收集频率数据，作为非限制性示例，包括虚拟化环境、在沙箱或管理程序中或在仿真器中。这可以将可执行对象与目标系统隔离开来，这在可执行对象还不具有信誉评分的场合中特别有用。在一个实施例中，隔离环境可以直接耦合到信誉服务器110且对未知应用执行分析，以便为它们创建信誉。可以通过提供仿真的私有用户数据或用户输入来增强在隔离环境中的执行，这可帮助标识恶意软件行为。在共同待决的、于2012年12月21日提交的标题为“用户驱动的应用仿真”的美国申请13/723,495中提供了这样的仿真的一个示例，该申请通过引用合并于此。例如，尽管处于隔离环境，但可以给可执行对象提供仿真的私有用户数据，包括位置数据、联系人列表、键击或个人细节。仿真的私有用户数据也可以包括可执行对象可能试图“窥探”的仿真的后台任务，例如访问银行、金融、医疗或社交网站或资源。

[0065] 为了节省移动设备上的电池电源，可以将频率计算限制在设备插入到外部电源的时候。

[0066] 在又一示例中，除了来自代码的大量“叶子”部分之外(或替换为来自代码的大量“叶子”部分)，频率评分可以与调用流程图的所选择的分支(从一个更高级的子例程调用的叶子的集合)相关联。这可以提供用于父例程及其孩子两者的额外分层频率跟踪。这可以帮助计算包括多个组件的软件例如对动态链接库或共享对象文件做出调用的可执行文件的信誉。在一种示例中，可以用频率解释可执行对象和所有库以及它们的函数和输出。

[0067] 在框460中，将频率评分提供给信誉服务器110。然而，应注意，在此仅作为非限制性示例公开原始频率评分的提供，且在一些实施例中，框450可以包括实际信誉评分的计算，在这种情况中可以严格地内部使用信誉，或者计算信誉以供转发给信誉服务器110。

[0068] 在框460中，可以将所计算的频率评分(或信誉评分)提供给信誉服务器110，以供与从其他设备接收的其他评分聚集起来。

[0069] 在某些实施例中，该方法可以返回到框410，供选择附加的可执行对象，或者进一步提炼在现有的可执行对象上收集的数据。

[0070] 图5是根据本说明书的一个或多个示例的信誉服务器110的框图。在这一示例中，信誉服务器110受到处理器510的控制。存储器520通信上耦合到处理器510。信誉服务器110的其他系统组件经由系统总线570连接到处理器510。信誉服务器110也可以包括存储550和网络接口540。处理器510可以类似于图3的处理器310。同样地，存储器520可以类似于存储器320，存储550可以类似于存储350，且网络接口540可以类似于网络接口340。

[0071] 在这一示例中，网络接口540可以被配置成将信誉服务器110通信上耦合到网络120。在一些情况中，存储550可以包括信誉数据库140，而在其他情况中可以分离地提供信誉数据库140。

[0072] 存储器520其中存储有信誉服务器软件522。在一些实施例中，可以由从存储550加载到存储器520以供执行的可执行指令提供信誉服务器引擎522。各指令可以被配置成指示处理器510提供在此描述的客户机服务器服务，例如通过执行图6的方法。在进一步的其他实施例中，可以在管理程序中、在虚拟机或其他合适的虚拟平台上或作为被配置成执行诸如图6的方法之类的合适的方法的专有或专用硬件、软件和/或固件的任何组合提供信誉服务器引擎522。在相同实施例或另一实施例中，信誉服务器引擎522可以在专用存储器中操作且可以在分离的处理器或其他可信执行环境上执行，以提供与信誉服务器110的其余部分的更好的隔离。

[0073] 图6是根据本说明书的一个或多个示例提供信誉服务器引擎的一种方法的流程图。根据该示例，在框610中，信誉服务器110从一个或多个客户机设备130接收数据。该数据可以包括例如可执行对象和子例程的频率评分或信誉评分。

[0074] 在框620中，可以更新例如被包含在信誉数据库140中的主目录(在一种示例中，主目录覆盖完整的可执行对象和子例程两者)。更新可以包括添加先前未出现在主应用目录中的应用或子例程，或以其他方式准备主目录以便保存关于从客户机设备130接收的可执行对象和子例程的数据。

[0075] 在框630中，可以将可执行对象和子例程交叉引用到信誉数据库140中现有的可执行对象和子例程，允许将它们标识为匹配。在框640中，基于频率计算信誉评分，且可以以新的信誉评分更新信誉数据库140。如上所述，在一些情况中，客户机设备130可能已经本地计算信誉评分。在这种情况中，可以基于由客户机设备提供的信誉评分计算“全局”信誉评分。在其他实施例中，为便于由信誉服务器110计算的全局信誉评分，可以丢弃由客户机设备130提供的信誉评分。应明白，许多算法都可能用于在信誉服务器110上计算信誉评分，且除非明确地说明，否则包括所附权利要求的本说明书的范围不旨在限于任何特定的算法。

[0076] 在一些实施例中，信誉评分也可以考虑相应的开发者或团队的信誉。例如，离开公司、受到怀疑、已被逮捕、已知与恶意软件组织有联系或者以其他方式其个人信誉可疑的开发者可能因他或她开发的代码而应经受附加详细审查。在一些情况中，来自软件开发公司的合作是有益的。类似的考虑可以应用到代码的第三方源，作为非限制性示例，例如外部库、转包商和开源工程。例如，来自并发版本管理系统(CVS)的提交记录可以用来确定哪些开发者提交哪些子例程。也可以经由API将频率和信誉数据返回给软件开发公司，这可以帮助公司改善它们的开发进程并获得它们的自己开发进程的更大的洞察。

[0077] 在框650，例如基于具有低的基于频率的信誉评分，可以将某些类别的子例程或可执行对象指定为“可疑”。可指定这些以供例如由操作人员深入分析。如果来自操作人员的

深入分析揭示了这些子例程和可执行对象包含恶意代码，则可以将它们标记成恶意软件，且可以采取补救步骤。

[0078] 在框660中，可以将已知对象的信誉数据分发回去给客户机设备130。也可以经由API以及作为经由网络的服务提供信誉信息。在一些实施例中，然后，执行可以返回到框610，以供处理附加的子例程和可执行对象。

[0079] 前述内容概述了若干实施例的特征，以使得本领域中的技术人员可以更好理解本公开内容的各方面。本领域中的技术人员应明白，他们可以容易地将本公开内容用作设计或修改用于执行在此介绍的各实施例的相同目的和/或取得相同优点的其他过程和结构的基础。本领域中的技术人员也应认识到，这样的等效构造并不偏离本公开内容的精神和范围，且他们可以在不偏离本公开内容的精神和范围的前提下在此做出各种改变、替换和变更。

[0080] 本公开内容的具体实施例可以容易地包括片上系统(SOC)中央处理单元(CPU)封装。SOC表示将计算机或其他电子系统集成到单个芯片的集成电路(IC)。它可以包含数字、模拟、混合信号和射频功能：所有这些都可以在单个芯片基板上提供。其他实施例可以包括多芯片模块(MCM)，具有位于单个电子封装内和且配置成通过该电子封装相互紧密交互的多个芯片。在各种其他实施例中，可以在专用集成电路(ASIC)、现场可编程门阵列(FPGA)和其他半导体芯片的一个或多个硅核中实现数字信号处理功能。

[0081] 在示例实现中，也可以用软件实现在此略述的处理活动中的至少一些部分。在一些实施例中，可以用在所公开的图的元素之外提供的硬件实现这些特征中的一种或多种，或者以任何适当的方式合并以便实现预期功能。各种组件可以包括可以协作以便实现在此略述的操作的软件(或往复式软件)。在进一步的其他实施例中，这些元素可以包括促进其操作的任何合适的算法、硬件、软件、组件、模块、接口或对象。

[0082] 另外，可以移除或以其他方式合并与所描述的微处理器相关联的组件中的一些。在一般意义上，各图中所叙述的布局在它们的表示方面可能更符合逻辑，而物理架构可以包括这些元素的各种排列、组合和/或混合。当务之急是要注意，无数可能的设计配置都可以用来实现在此略述的操作目标。因此，关联的基础设施具有无数中替代布局、设计选择、设备可能性、硬件配置、软件实现、装备选项等等。

[0083] 任何合适地配置的处理器组件都可以执行与数据相关联的任何类型的指令以实现在此详述的操作。在此公开的任何处理器都可以将元素或制品(例如，数据)从一个状态或事物变换成另一状态或事物。在另一示例中，可以借助于固定逻辑或可编程逻辑(例如，由处理器执行的软件和/或计算机指令)实现在此略述的一些活动，且在此标识的元素可以是某种类型的可编程处理器、可编程数字逻辑(例如现场可编程门阵列(FPGA)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM))、包括数字逻辑的ASIC、软件、代码、电子指令、闪速存储器、光盘、CD-ROM、DVD ROM、磁或光卡、适用于存储电子指令的其他类型的机器可读介质或其任何合适的组合。在操作时，在适当的场合且基于具体的需要，处理器可以将信息存储在任何合适的类型的非暂态存储介质(例如随机存取存储器(RAM)、只读存储器(ROM)、现场可编程门阵列(FPGA)、可擦除可编程只读存储器(EPROM)、电可擦除可编程ROM(EEPROM)等等)、软件、硬件或任何其他合适的组件、设备、元素或对象。进一步，基于具体的需要和实现，可以在任何数据库、寄存器、表、高速缓存、队列、控制列表或

存储结构中提供被跟踪、发送、接收或存储在处理器中的信息，所有这些都可以在任何合适的时间范围内引用。在此讨论的存储器项中的任何应被解释成被包含在广义术语‘存储器’内。类似地，在此描述的任何潜在的处理元件、模块和机器应被解释成被包含在广义术语‘微处理器’或‘处理器’内。

[0084] 以各种形式来具体现实现在此描述的功能的全部或部分的计算机程序逻辑，这些形式包括但绝不限于源代码形式、计算机可执行形式和各种中间形式(例如，由汇编器、编译器、链接器或定位器生成的形式)。在一种示例中，源代码包括用各种编程语言实现的一系列计算机程序指令，这些编程语言例如目标代码、汇编语言或与各种操作系统或操作环境一起使用的诸如OpenCL、Fortran、C、C++、JAVA、Python、Perl、JavaScript或HTML之类的高级语言。源代码可以定义和使用各种数据结构并传输消息。源代码可以是以计算机可执行的形式(例如，经由解释器)，或者源代码可以被转换(例如，经由翻译器、汇编器或编译器)成计算机可执行的形式。

[0085] 在上面的各实施例的讨论中，可以容易地替换、取代或以其他方式修改电容器、缓冲器、图形元件、互连板、时钟、DDR、照相机传感器、驱动器、电感器、电容器、放大器、开关、数字核、晶体管和/或其他组件，以便适应具体的电路需要。此外，应注意，使用补充的电子设备、硬件、非暂态软件等等提供用于实现本公开内容的教导的同样可行的选项。

[0086] 在一个示例中，可以在关联电子设备的板上实现各图中任何数量的电子电路。该板可以是可以容纳电子设备的内部电子系统的各种组件且进一步为其他外围设备提供连接器的常见的电路板。更具体地，该板可以提供系统的其他组件可以通过其进行电气通信的电连接。基于具体的配置需要、处理需求、计算机设计等等，任何合适的处理器(包括数字信号处理器、微处理器、支持芯片组等等)、存储器元件等等都可以合适地耦合到该板。诸如外部存储、附加的传感器、用于音频/视频显示器的控制器和外围设备之类的其他组件可以作为插件卡经由电缆附加到该板，或被集成到该板本身。在另一示例中，各图的电子电路可以作为独立模块(例如，被配置成执行特定应用或功能的带有关联组件和电路的设备)或作为插入式模块被实现到电子设备的专用硬件中。

[0087] 注意，借助于在此提供的众多示例，可以利用二、三、四或更多个电气组件描述交互。然而，仅出于清晰和示例的目的这样做。应明白，可以以任何合适的方式合并该系统。连同相似的设计备选方案一起，可以以各种可能的配置组合，各图中所阐释的组件、模块和元素中的任何，所有这些都清楚地处于本说明书的宽广范围内。在某些情况中，通过仅引用有限数量的电子元件，可能容易描述给定的一组流的功能中的一种或多种。应明白，各图及其教导的电子电路容易可扩展，且可以容纳大量组件，以及更复杂/精密的布局和配置。因此，所提供的示例不应限制潜在地应用到无数其他架构的电子电路的范围或约束这些电子电路的广义教导。

[0088] 本领域中的技术人员可以确定众多其他改变、取代、变化、变更和修改，且预期本公开内容包含落在所附权利要求的范围内的所有这样的改变、取代、变化、变更和修改。为了帮助美国专利和商标局(United States Patent and Trademark Office,USPTO)且另外帮助本申请提出的任何专利的任何读者解释所附权利要求，申请人希望声明，申请人:(a)除非词语词“用于……的手段”或“用于……的步骤”专门用于特定权利要求，否则不预期任何所附的权利要求援引从其提交日期开始存在的35U.S.C.第112节第六(6)段;以及(b)不

预期由本说明书中的任何语句以在所附权利要求中不能反映的任何方式限制本公开内容限制。

[0089] 示例实施例实现

[0090] 作为非限制性示例，在此作为示例1公开一种用于执行可执行对象的基于频率的分类的装置，包括处理器，其通信上耦合到存储器；网络接口；以及信誉客户机引擎，其通信上耦合到所述处理器，且可操作为将可执行对象解析成多个子例程；以及给每一子例程指定执行频率评分。

[0091] 在此作为示例2公开示例1所述的信誉客户机，其中，所述信誉客户机引擎还可操作为：在所述网络接口上提供所述执行频率评分；以及通过所述网络接口接收所述可执行对象的信誉评分。

[0092] 在此作为示例3公开示例1或2所述的信誉客户机，其中，所述给每一子例程指定执行频率评分进一步包括运行所述可执行对象和清点对所述各子例程的调用。

[0093] 在此作为示例4公开示例1-3中的任何所述的信誉客户机，其中，所述信誉客户机引擎还可以操作为在隔离环境中运行所述可执行对象。

[0094] 在此作为示例公开5示例1-4中的任何所述的信誉客户机，其中，将所述可执行对象解析成多个子例程进一步包括修改所述可执行对象的副本以便将频率计数器注入到所述各子例程。

[0095] 在此作为示例6公开一个或多个非暂态计算机可读介质，其上存储有可执行指令，所述可执行指令可操作为指示处理器提供示例1-5中的任何所述的信誉客户机引擎。

[0096] 在此作为示例7公开信誉服务器，所述信誉服务器包括：处理器，其通信上耦合到存储器；网络接口；以及信誉服务器引擎，其通信上耦合到所述处理器且可操作为：将可执行对象解析成多个子例程；以及给每一子例程指定信誉评分；

[0097] 在此作为示例8公开示例7所述的信誉服务器，其中，所述信誉服务器引擎还可以操作为：至少部分地基于所述多个子例程的所述信誉评分，计算所述可执行对象的信誉评分；以及经由所述网络接口将所述各信誉评分中的至少一个分发给多个信誉客户机。

[0098] 在此作为示例9公开示例8或9所述的信誉服务器，其中，所述给每一子例程指定信誉评分进一步包括给每一子例程指定执行频率评分。

[0099] 在此作为示例10公开示例8-9中的任何所述的信誉服务器，其中，将所述可执行对象解析成多个子例程进一步包括从信誉客户机接收关于所述多个子例程的数据。

[0100] 在此作为示例11公开示例8-10中的任何所述的信誉服务器，其中，给每一子例程指定信誉评分进一步包括从信誉客户机接收每一子例程的执行频率评分。

[0101] 在此作为示例公开12示例8-11中的任何所述的信誉服务器，其中，给每一子例程指定信誉评分进一步包括：给每一子例程指定伪唯一指纹；以及使用所述伪唯一指纹在信誉数据库中查询匹配子例程的频率或信誉评分。

[0102] 在此作为示例13公开示例8-12中的任何所述的信誉服务器，其中，给每一子例程指定信誉评分进一步包括接收所述子例程的执行频率评分，所述执行频率评分包括跨越多个可执行对象的执行频率。

[0103] 在此作为示例14公开示例8-13中的任何所述的信誉服务器，其中，所述信誉服务器引擎还可以操作为：在隔离环境中运行所述可执行对象；以及基于各子例程的执行频率，

给各子例程指定频率评分。

[0104] 在此作为示例15公开示例8-14中的任何所述的信誉服务器，其中，给每一子例程指定信誉评分进一步包括静态分析所述可执行对象。

[0105] 在此作为示例16公开示例8-15中的任何所述的信誉服务器，其中，所述信誉服务器引擎还可以操作为标记带有低信誉评分的可执行对象以供额外深入分析。

[0106] 在此作为示例17公开示例8-16中的任何所述的信誉服务器，其中，所述可执行对象的所述信誉至少部分地基于所述多个子例程的所述信誉。

[0107] 在此作为示例18公开示例8-17中的任何所述的信誉服务器，其中，所述信誉服务器引擎还可操作为：判断所述可执行对象具有高信誉评分；以及给所述多个子例程指定高信誉评分。

[0108] 在此作为示例19公开示例8-18中的任何所述的信誉服务器，其中，所述信誉服务器引擎还可以操作为：给至少一个子例程指定伪唯一指纹；跨越多个可执行对象计算所述子例程的执行频率评分；以及将所述信誉评分与所述执行频率评分相关起来。

[0109] 在此作为示例20公开示例19所述的信誉服务器，其中，给所述子例程指定伪唯一指纹包括计算模糊指纹。

[0110] 在此作为示例21公开示例8-20中的任何所述的信誉服务器，其中，所述信誉服务器引擎还可以操作为将具有执行频率评分0的子例程标识为安全风险。

[0111] 在此作为示例22公开示例8-21中的任何所述的信誉服务器，其中，所述信誉服务器引擎还可以操作为将带有低执行频率评分的子例程标识为可疑。

[0112] 在此作为示例23公开至少一个非暂态计算机可读的存储介质，其上存储有可执行指令，所述可执行指令可操作为提供示例8-22中的任何所述的信誉服务器引擎。

[0113] 在此作为示例24公开一种用于计算可执行对象的信誉的方法，所述方法可在计算设备上执行，且包括：将可执行对象解析成多个子例程；给每一子例程指定执行频率评分；至少部分地基于所述执行频率评分，给每一子例程指定信誉评分；以及至少部分地基于所述各子例程的所述信誉评分给所述可执行对象指定信誉评分。

[0114] 在此作为示例25公开示例24所述的方法，其中，给所述可执行对象指定信誉评分进一步包括：给子例程指定伪唯一标识符；查找带有所述相同的伪唯一标识符的、具有先前计算的执行频率的子例程；以及聚集所述子例程的所述执行频率。

[0115] 在此作为示例26公开一种提供信誉服务器引擎的方法，包括：将可执行对象解析成多个子例程；以及给每一子例程指定信誉评分。

[0116] 在此作为示例27公开示例26所述的方法，进一步包括给所述可执行对象指定信誉，其中，所述可执行对象的所述信誉至少部分地基于所述各子例程的所述信誉。

[0117] 在此作为示例28公开示例26或27所述的方法，进一步包括标记带有低信誉评分的可执行对象以供额外深入分析。

[0118] 在此作为示例29公开示例26-28中的任何所述的方法，其中，给每一子例程指定信誉评分包括给每一子例程指定执行频率评分。

[0119] 在此作为示例30公开示例26-29中的任何所述的方法，其中，可操作为给每一子例程指定信誉评分的所述各指令还可操作为：判断所述可执行对象具有高信誉评分；以及给所述各子例程指定高信誉评分。

[0120] 在此作为示例31公开示例26-30中的任何所述的方法，其中，可操作为给每一子例程指定信誉评分的所述各指令还可以操作为：给所述子例程指定伪唯一指纹；跨越多个可执行对象计算所述子例程的执行频率评分；以及将所述信誉评分与所述执行频率评分相关起来。

[0121] 在此作为示例32公开示例31所述的方法，其中，给所述子例程指定伪唯一指纹包括计算模糊指纹。

[0122] 在此作为示例公开33示例26-32中的任何所述的方法，进一步包括标记带有低信誉评分的子例程以供额外深入分析。

[0123] 在此作为示例34公开示例26-33中的任何所述的方法，进一步包括：给每一子例程指定执行频率评分；以及将带有执行频率评分0的子例程标记为安全风险。

[0124] 在此作为示例35公开示例34所述的方法，进一步包括将带有低执行频率评分的子例程标识为可疑。

[0125] 在此作为示例36公开示例26-34中的任何所述的方法，进一步包括在隔离环境中运行所述可执行对象。

[0126] 在此作为示例37公开一种装置，其包括用于执行示例26-36中的任何所述的方法的工具。

[0127] 在此作为示例38公开示例37所述的装置，其中，所述工具包括处理器和存储器。

[0128] 在此作为示例39公开示例37或38所述的装置，其中，所述存储器包括机器可读指令，在被执行时，所述机器可读指令引起所述装置执行示例26-36中的任何所述的方法。

[0129] 在此作为示例40公开示例37-39中的任何所述的装置，其中，所述装置是计算系统。

[0130] 在此作为示例41公开一个或多个非暂态计算机可读介质，其上存储有可执行指令，所述可执行指令可操作为指示处理器执行示例26-36中的任何所述的方法。

[0131] 在此作为示例42公开一种计算设备，其包括：用于将可执行对象解析成多个子例程的装置；用于给每一子例程指定执行频率评分的装置；用于至少部分地基于所述执行频率评分给每一子例程指定信誉评分的装置；以及用于至少部分地基于所述各子例程的所述信誉评分给所述可执行对象指定信誉评分的装置。

[0132] 在此作为示例43公开示例42所述的计算设备，其中，用于给所述可执行对象指定信誉评分的所述装置还包括：用于给子例程指定伪唯一标识符的装置；用于查找带有所述相同的伪唯一标识符的、具有先前计算的执行频率的子例程的装置；以及用于聚集所述子例程的所述执行频率的装置。

[0133] 在此作为示例44公开示例42或43所述的计算设备，其中，所述装置中的每一种包括存储在非暂态计算机可读介质上的可执行指令。

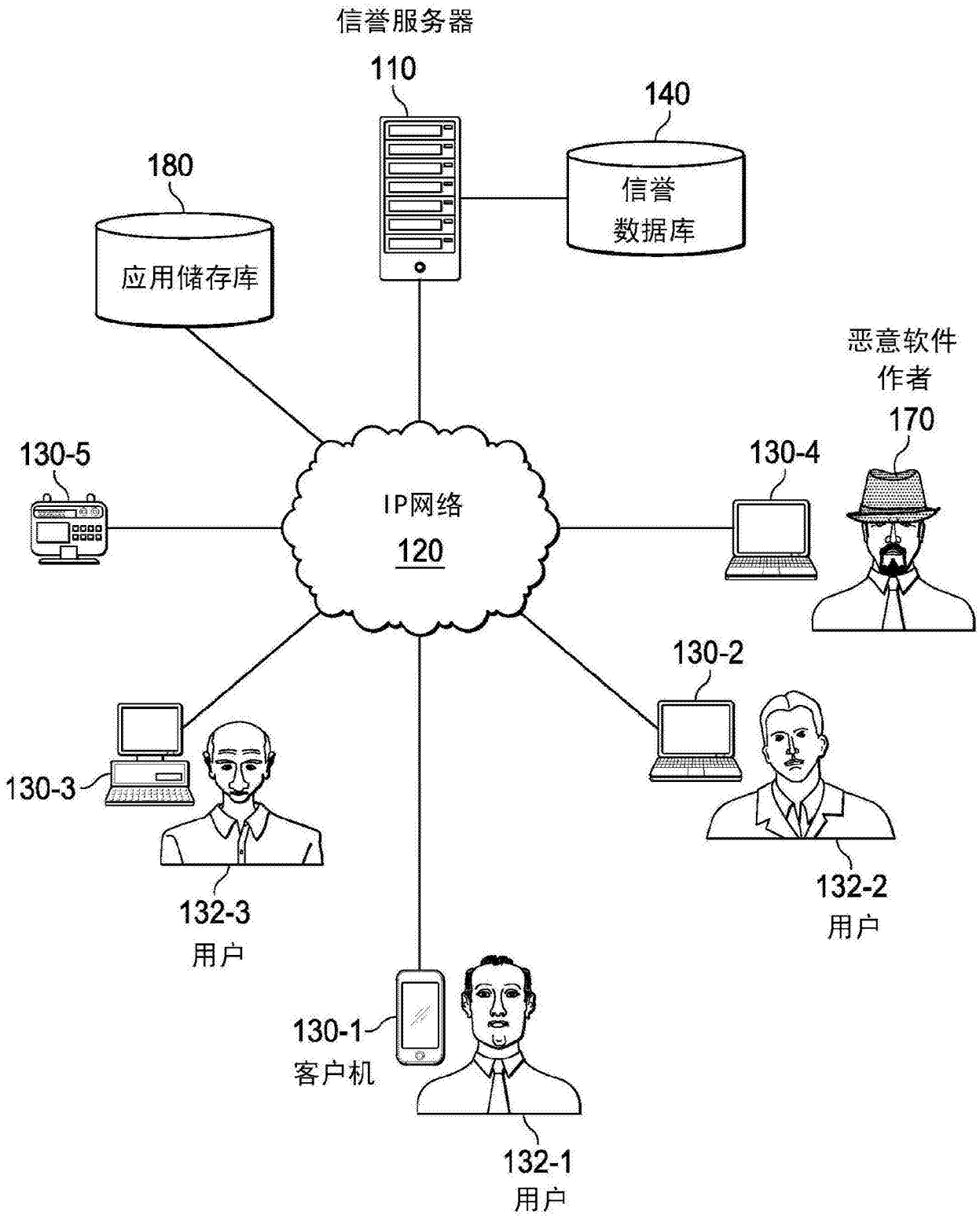

信誉服务器
110
140
信誉
数据库
180
应用储存库
恶意软件
作者
170
130-5
IP网络
120
130-4
130-2
130-3
132-3
用户
132-2
用户
130-1
客户机
132-1
用户

图1

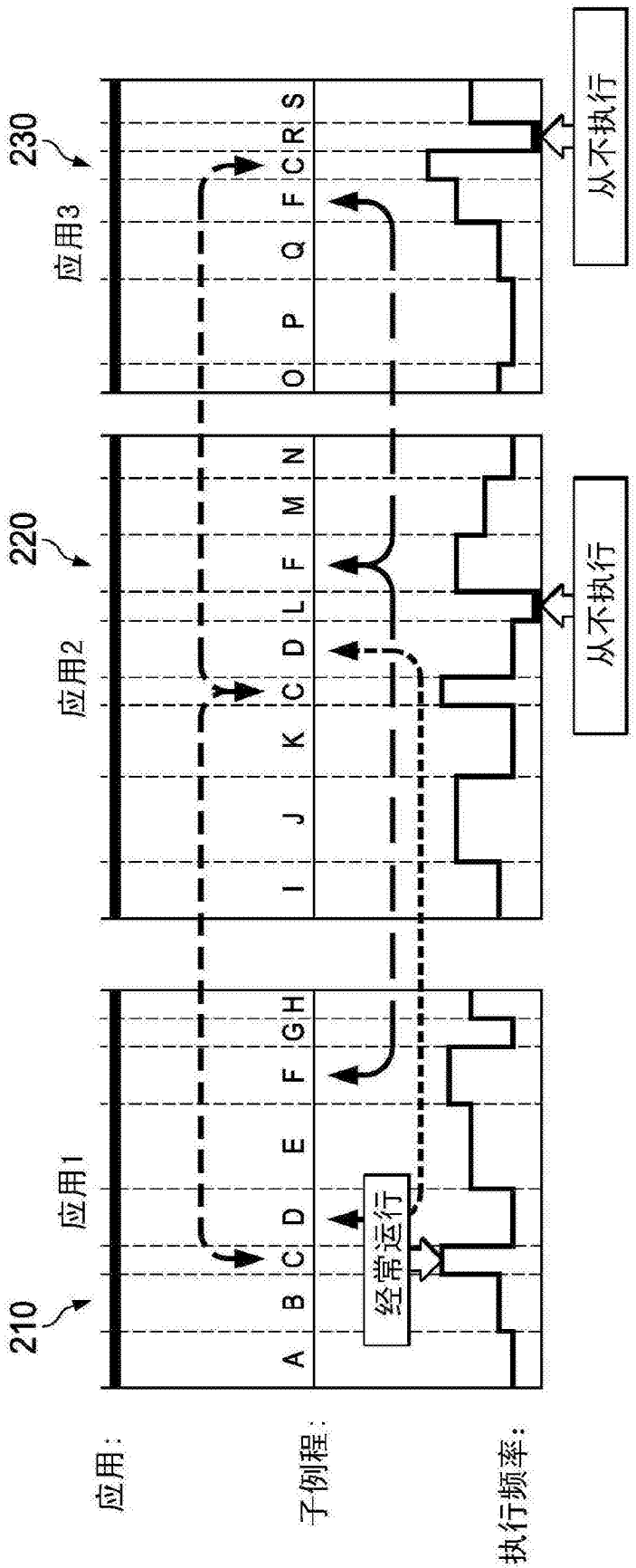

210
应用1
A
B
C
D
E
F
G
H
经常运行
220
应用2
I
J
K
C
D
L
F
M
N
从不执行
230
应用3
O
P
Q
F
C
R
S
从不执行
应用：
子例程：
执行频率：

图2

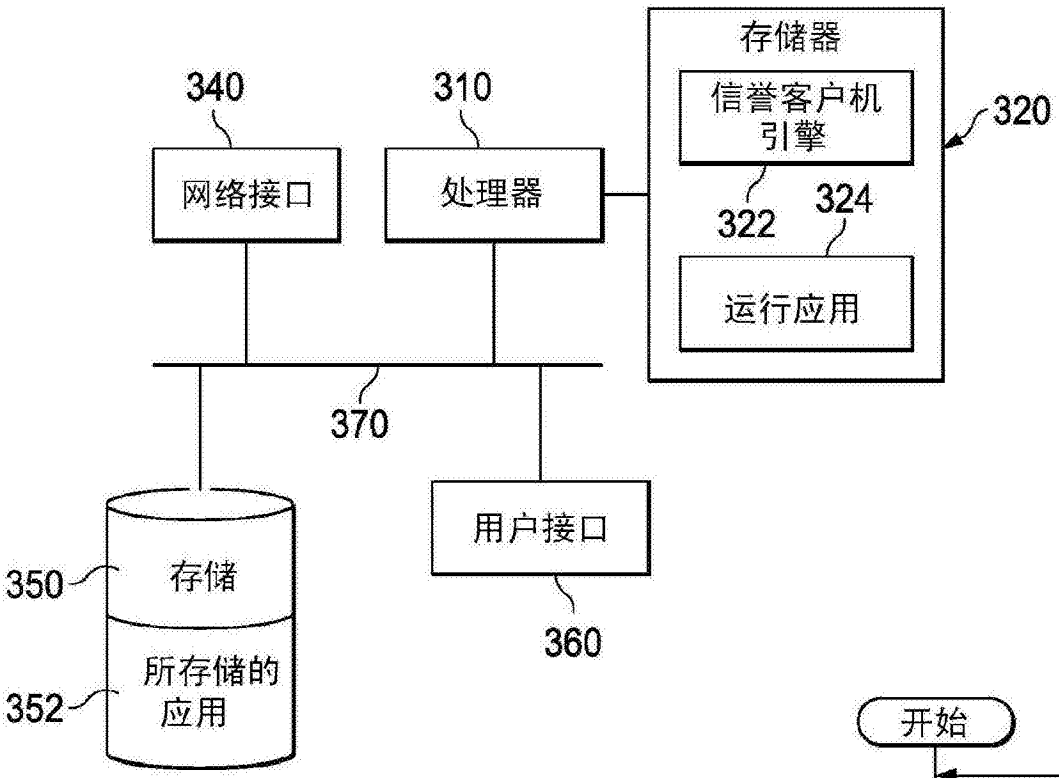

存储器
信誉客户机引擎
320
340
310
网络接口
处理器
322
324
运行应用
370
用户接口
350
存储
所存储的应用
352
360

图 3

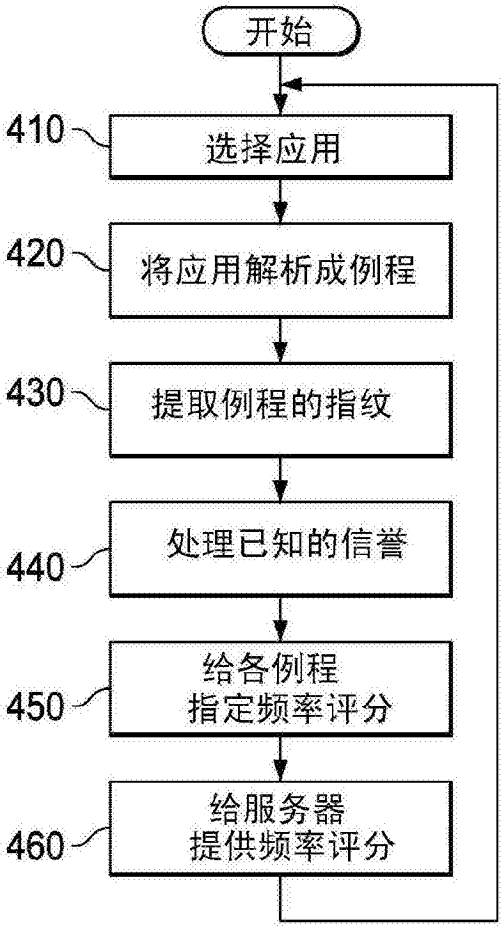

开始
410
选择应用
420
将应用解析成例程
430
提取例程的指纹
440
处理已知的信誉
450
给各例程指定频率评分
460
给服务器提供频率评分

图 4

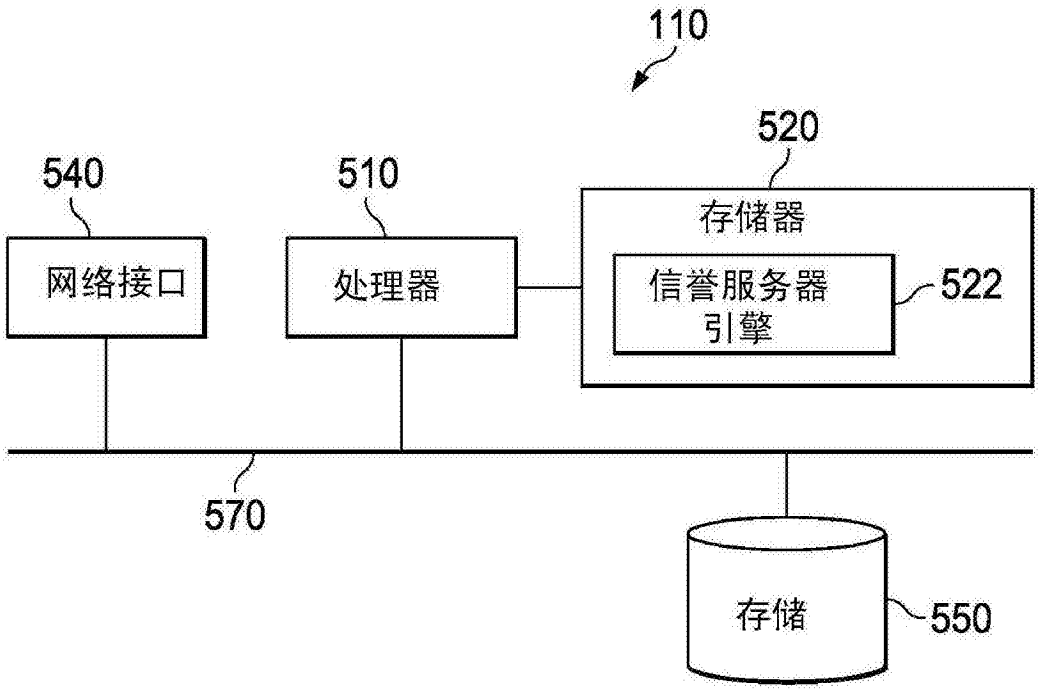


图5

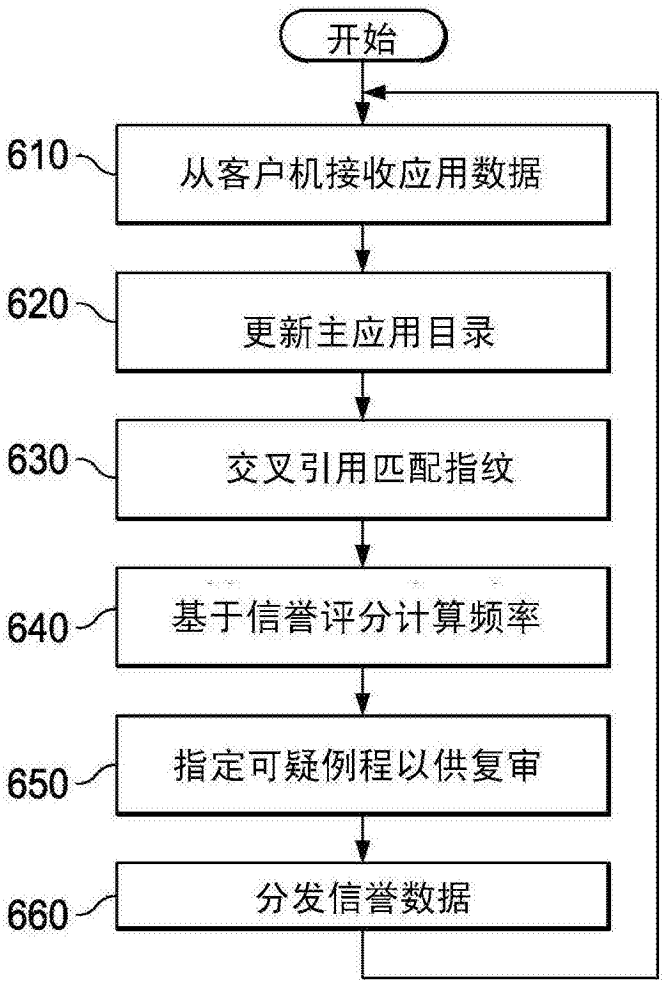

开始
610
从客户机接收应用数据
620
更新主应用目录
630
交叉引用匹配指纹
640
基于信誉评分计算频率
650
指定可疑例程以供复审
660
分发信誉数据

图6