(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 114270347 A
(43)申请公布日 2022.04.01

(21)申请号 202080039806.5
(22)申请日 2020.03.19
(30)优先权数据
16/371,794 2019.04.01 US
(85)PCT国际申请进入国家阶段日
2021.11.29
(86)PCT国际申请的申请数据
PCT/US2020/023557 2020.03.19
(87)PCT国际申请的公布数据
WO2020/205258 EN 2020.10.08
(71)申请人 阿尔米斯安全有限公司
地址 以色列特拉维夫-雅法
(72)发明人 N·伊兹拉埃尔
S·拉德尔斯基·勒卢什
M·塞尔策
(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 郑勇
(51)Int.Cl.
G06F 21/50(2013.01)
H04L 69/40(2022.01)

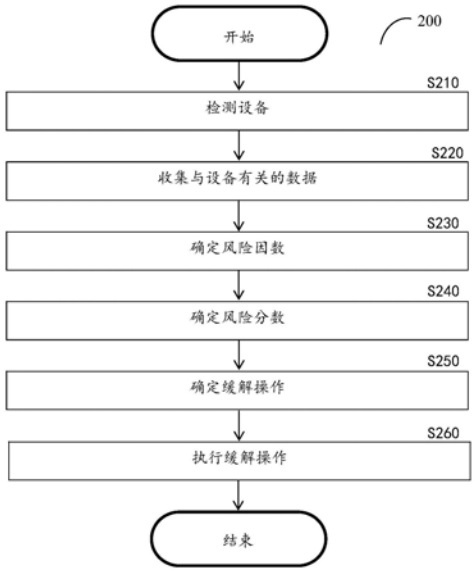
权利要求书3页 说明书10页 附图3页

(54)发明名称

缓解网络安全威胁的系统和方法

(57)摘要

本发明提供一种使用风险因数缓解设备的网络安全威胁的系统和方法。该方法包括:基于网络活动指示的多个风险行为和设备的信息来确定设备的多个风险因数;基于多个风险因数和多个权重来确定设备的风险分数,其中,将多个权重中的每一个应用于多个风险因数中的一个;以及基于风险分数执行至少一项缓解操作。



CN 114270347 A

1.一种使用风险因数缓解设备的网络安全威胁的方法,包括:

基于网络活动指示的多个风险行为和设备的信息,确定所述设备的多个风险因数;

基于所述多个风险因数和多个权重来确定所述设备的风险分数,其中将所述多个权重中的每一个应用于所述多个风险因数中的一个;以及

基于所述风险分数执行至少一项缓解操作。

2.根据权利要求1所述的方法,其中,所述多个风险行为包括观察到的风险行为和假设的风险行为,其中,所述观察到的风险行为由与所述设备的网络活动相关的数据指示,其中,所述假设的风险行为是基于与所述设备相关的已知上下文信息推断的。

3.根据权利要求1所述的方法,其中,当以下条件至少一个发生时,确定所述设备的所述多个风险因数:所述设备连接到网络,所述设备在物理上靠近网络的地方打开,并且所述设备在物理上靠近网络基础架构。

4.根据权利要求1所述的方法,其中,所述多个风险行为包括观察到的风险行为,其中确定所述多个风险因数还包括:

基于与以下中的至少一个相关的数据来确定所述观察到的风险行为:所述设备的配置、所述设备的网络活动、所述设备的地理移动、所述设备的信号强度和所述设备使用的协议。

5.根据权利要求1所述的方法,其中,所述多个风险行为包括观察到的风险行为,其中,确定所述多个风险因数还包括:

基于以下中的至少一个来确定所述假设的风险行为:制造商信誉信息、设备型号信誉信息、已知软件漏洞和已知操作系统漏洞。

6.根据权利要求1所述的方法,其中,所述至少一项缓解操作包括当所述风险分数低于阈值时监控所述设备的网络活动,还包括:

基于所述监控的网络活动更新所述风险分数;以及

基于所述更新后的风险分数执行至少一项后续缓解操作。

7.根据权利要求1所述的方法,其中,所述多个权重包括至少一个负权重。

8.根据权利要求1所述的方法,其中,所述多个风险因数包括制造商信誉风险因数,其中,所述制造商信誉风险因数基于所述设备的制造商造成的常见漏洞和暴露的数量与所述设备的制造商的员工数量的商来确定。

9.根据权利要求1所述的方法,其中,所述多个风险因数包括数据熵风险因数,其中,所述数据熵风险因数基于由所述设备接收的数据和由所述设备发送的数据中的至少一个的熵来确定。

10.根据权利要求1所述的方法,其中,所述多个风险因数包括以下风险因数中的至少一个:攻击表面暴露风险因数、云同步风险因数、连接安全风险因数、边界规避风险因数、第三方应用商店风险因数、恶意域风险因数、漏洞历史风险因数、静态数据风险因数、外部连接风险因数、用户认证风险因数、软件版本风险因数、证书重复使用风险因数、制造商信誉风险因数和设备型号信誉风险因数。

11.根据权利要求1所述的方法,其中,所述多个风险因数还基于多个已知设备行为来确定,其中,所述多个已知设备行为中的每一个与多个已知风险因数相关联,其中,所述多个已知风险因数中的每一个与至少一个风险行为相关联。

12.根据权利要求1所述的方法,其中,所述多个风险因数还基于至少一个其他设备的多个风险行为来确定。

13.一种非暂时性计算机可读介质,其上存储有用于使处理电路执行过程的指令,所述过程包括:

基于网络活动指示的多个风险行为和设备的信息,确定所述设备的多个风险因数;

基于所述多个风险因数和多个权重来确定所述设备的风险分数,其中,将所述多个权重中的每一个应用于所述多个风险因数中的一个;以及

基于所述风险分数执行至少一项缓解操作。

14.一种使用风险因数缓解设备的网络安全威胁的系统,包括:

处理电路;和

存储器,包含指令,所述指令在由所述处理电路执行时,将所述系统配置为:

基于网络活动指示的多个风险行为和设备的信息,确定所述设备的多个风险因数;

基于所述多个风险因数和多个权重来确定所述设备的风险分数,其中,将所述多个权重中的每一个应用于所述多个风险因数中的一个;以及

基于所述风险分数执行至少一项缓解操作。

15.根据权利要求14所述的系统,其中,所述多个风险行为包括观察到的风险行为和假设的风险行为,其中,所述观察到的风险行为由与所述设备的网络活动相关的数据指示,其中,所述假设的风险行为基于与所述设备相关的已知上下文信息来推断。

16.根据权利要求14所述的系统,其中,当以下条件至少一个发生时,确定所述设备的所述多个风险因数:所述设备连接到网络,所述设备在物理上靠近网络的地方打开,并且所述设备在物理上靠近网络基础架构。

17.根据权利要求14所述的系统,其中,所述多个风险行为包括观察到的风险行为,其中,所述系统还配置为:

基于与以下中的至少一个相关的数据来确定所述观察到的风险行为:所述设备的配置、所述设备的网络活动、所述设备的地理移动、所述设备的信号强度和所述设备使用的协议。

18.根据权利要求14所述的系统,其中,所述多个风险行为包括观察到的风险行为,其中,所述系统还配置为:

基于以下中的至少一个来确定所述假设的风险行为:制造商信誉信息、设备型号信誉信息、已知软件漏洞和已知操作系统漏洞。

19.根据权利要求14所述的系统,其中,所述至少一项缓解操作包括当所述风险分数低于阈值时,监控所述设备的网络活动,其中,所述系统还配置为:

基于所述监控的网络活动更新所述风险分数;以及

基于所述更新后的风险分数,执行至少一项后续缓解操作。

20.根据权利要求14所述的系统,其中,所述多个权重包括至少一个负权重。

21.根据权利要求14所述的系统,其中,所述多个风险因数包括制造商信誉风险因数,其中,所述制造商信誉风险因数基于所述设备的制造商造成的常见漏洞和暴露的数量与所述设备的制造商的员工数量的商来确定。

22.根据权利要求14所述的系统,其中,所述多个风险因数包括数据熵风险因数,其中,

所述数据熵风险因数基于由所述设备接收的数据和由所述设备发送的数据中的至少一个的熵来确定。

23.根据权利要求14所述的系统，其中，所述多个风险因数包括以下风险因数中的至少一个：攻击表面暴露风险因数、云同步风险因数、连接安全风险因数、边界规避风险因数、第三方应用商店风险因数、恶意域风险因数、漏洞历史风险因数、静态数据风险因数、外部连接风险因数、用户认证风险因数、软件版本风险因数、证书重复使用风险因数、制造商信誉风险因数和设备型号信誉风险因数。

24.根据权利要求14所述的系统，其中，所述多个风险因数还基于多个已知设备行为来确定，其中，所述多个已知设备行为中的每一个与多个已知风险因数相关联，其中，所述多个已知风险因数中的每一个与至少一个风险行为相关联。

25.根据权利要求14所述的系统，其中，所述多个风险因数还基于至少一个其他设备的多个风险行为来确定。

缓解网络安全威胁的系统和方法

技术领域

[0001] 本公开总体上涉及网络安全，更具体地说，涉及保护网络免受恶意设备构成的威胁。

背景技术

[0002] 每当有新设备连接到组织的网络或在靠近组织物理位置的位置被激活时，该新设备就有可能被恶意实体用来对组织、网络或两者造成损害。由于现在能够进行网络连接的新设备数量迅速增加，网络访问可能导致的潜在问题数量呈指数级增长。此外，这些新设备中的许多设备不仅能够连接到网络，而且还能够创建自己的网络或热点。

[0003] 针对恶意设备保护组织计算基础架构的一些解决方案包括要求登录网络的新设备进行认证，并阻止未知设备访问网络。但是，尽管有认证协议，要求认证并不一定会阻止恶意实体获得必要的凭证并访问网络。此外，阻止所有未知设备可能会导致良性设备被阻止。此外，先前良性设备可能在受到恶意软件感染时变成恶意设备。因此，这种受恶意软件感染的设备可能会被允许进行网络访问，从而可能被用于恶意目的。

[0004] 保护组织计算基础架构安全的其他解决方案包括监控网络活动以检测异常。但是，现有的检测工具可能无法检测到某些类型的异常行为，例如检测工具尚未识别的作为零日攻击一部分的新攻击模式。此外，不对网络构成直接威胁的设备(例如，不直接参与恶意行为但向其他恶意设备提供网络访问的设备)与参与更容易识别的恶意活动的设备相比，可能不会被检测为恶意，或者检测为恶意可能需要更长时间。

[0005] 因此，提供一种能够克服上述挑战的解决方案将是有益的。

发明内容

[0006] 以下是本公开的几个示例实施例的概述。提供本概述是为了方便读者，提供对这些实施例的基本理解，并不完全限定本公开的范围。本概述不是所有预期实施例的广泛综述，并且既不旨在标识所有实施例的关键或重要元素，也不旨在描绘任何或所有方面的范围。其唯一目的是以简化形式呈现一个或多个实施例的一些概念，作为稍后呈现的更详细描述的序言。为了方便起见，术语“一些实施例”或“某些实施例”在本文可以用来指本公开的单个实施例或多个实施例。

[0007] 本文公开的某些实施例包括一种使用风险因数缓解设备的网络安全威胁的方法。该方法包括：基于网络活动指示的多个风险行为和设备信息来确定设备的多个风险因数；基于所述多个风险因数和多个权重来确定所述设备的风险分数，其中将所述多个权重中的每一个应用于所述多个风险因数中的一个；以及基于风险分数执行至少一项缓解操作。

[0008] 本文公开的某些实施例还包括其上存储有使处理电路执行过程的非暂时性计算机可读介质，该过程包括：基于网络活动指示的多个风险行为和设备信息来确定设备的多个风险因数；基于所述多个风险因数和多个权重来确定所述设备的风险分数，其中将所述多个权重中的每一个应用于所述多个风险因数中的一个；以及基于风险分数执行至少一项

缓解操作。

[0009] 本文公开的某些实施例还包括一种使用风险因数缓解设备的网络安全威胁的系统。该系统包括:处理电路;以及存储器,所述存储器包含指令,当由处理电路执行时,所述指令将所述系统配置为:基于网络活动指示的多个风险行为和设备信息来确定设备的多个风险因数;基于所述多个风险因数和多个权重来确定所述设备的风险分数,其中将所述多个权重中的每一个应用于所述多个风险因数中的一个;以及基于风险分数执行至少一项缓解操作。

附图说明

[0010] 本文公开的主题在说明书结尾的权利要求中特别指出并明确要求保护。从下面结合附图的详细描述中,所公开的实施例的前述和其他目的、特征和优点将变得显而易见。

[0011] 图1是描述各种公开实施例的网络图。

[0012] 图2是示出根据实施例的使用风险因数缓解设备的网络安全威胁的方法的流程图。

[0013] 图3是示出根据实施例的威胁缓解器的示意图。

具体实施方式

[0014] 重要的是要注意,本文公开的实施例仅仅是本文创新教导的许多有利用途的示例。总的来说,在本申请的说明书中做出的陈述不一定限制各种要求保护的实施例中的任何一个。此外,某些陈述可能适用于某些发明特征,但不适用于其他特征。一般来说,除非另有说明,单数元素可以是复数,反之亦然,不失一般性。在附图中,在几个视图中,相同的数字表示相同的部分。

[0015] 已经确定,每当设备连接到网络或在网络基础架构附近打开,都应快速评估新设备,以确定新设备是否以及在多大程度上对组织构成威胁。对任何恶意实体的反应必须迅速,因为恶意设备访问网络的时间越长,造成的损害就越大。此外,应持续评估设备,以确保活动或操作组合的变化没有显示出潜在威胁。

[0016] 然而,对潜在威胁的评估应当灵活,以便能够发现可能不构成直接、已知网络安全威胁的活动。例如,连接到网络的打印机可能会通过广播不受保护的Wi-Fi信号来充当后门。打印机本身可能不存在网络威胁检测工具检测到的任何网络威胁,但可能允许其他恶意设备访问网络。又如,没有适当防病毒软件的智能电视或带有过时软件的智能手机可能会带来网络安全威胁,即使设备本身尚未开始恶意行为。

[0017] 所公开的实施例允许快速检测和缓解设备的潜在网络安全威胁。与现有解决方案相比,根据所公开的实施例使用的风险因数提供了更灵活的方法来检测潜在的恶意设备,同时保持快速的反应时间。具体而言,风险因数允许在以下情况下检测潜在的恶意设备,例如但不限于,参与检测系统尚不知道的网络攻击的设备、参与攻击前阶段(例如,探索、感染或休眠阶段)活动的设备、不直接存在风险的设备(例如,提供对其他设备的后门网络访问的设备或可能容易被其他设备和系统利用的设备)以及还没有活动数据可用的完全未知的设备。

[0018] 为此,各种公开的实施例包括一种使用风险因数缓解设备的网络安全威胁的方法

和系统。对待检查风险的设备进行检测。接受检测的设备可以是连接到网络的设备、物理上接近网络基础架构(例如,路由器)的设备或者网络以其他方式可见的设备。

[0019] 根据风险相关行为(以下简称“风险行为”)确定设备的风险因数。基于一个或多个观察到的风险行为、一个或多个假设的风险行为或其组合来确定每个风险因数。观察到的风险行为是由从设备收集的数据(例如,设备配置数据、协议数据、信号强度数据等)指示的行为,由收集的关于设备在网络上的活动的数据指示的行为,或两者。基于与设备(诸如已经访问网络的其他设备)相关的上下文数据、公共信息(例如,关于制造或设计设备的公司的信息、与设备上安装的软件相关的信息等),去往或来自设备的流量中的数据的熵,或其组合来推断假设的风险行为。

[0020] 基于风险因数,确定设备的风险分数。风险分数可以是确定的风险因数的加权平均值。应用于每个风险因数的权重可以是预先确定的,并且可以基于被访问的网络部分、设备类型、具体设备等进一步变化。

[0021] 根据风险分数,执行一项或多项缓解操作。在示例实现方式中,缓解操作包括当风险分数高于阈值时主动干扰连接到网络或在网络上操作的设备,以及当风险分数低于阈值时被动监控设备的活动。

[0022] 一些风险因数可能被负加权,使得负风险因数降低设备的风险分数。例如,设备上安装的反病毒软件的存在可能会导致设备上安装的网络安全软件的风险因数被应用负权重。与在满足特定条件时确定设备安全与否的某些现有解决方案相比,负风险因数使得可以更全面地看待风险。

[0023] 所公开的实施例包括基于风险行为确定风险因数。以下是如何使用特定类型的风险行为来确定各种风险因数的解释,以及特定风险行为可能影响最终风险因数的示例。

[0024] 以下各种示例都提到了较高的数字。出于风险因数的目的,例如,如果数字高于阈值,则该数字可能很高。阈值可以随着时间变化,例如随着正常设备活动的变化而变化。以下各种示例也提到了更多、更高、更老或其他相关说法。对于这样的示例,风险因数的值可以随着相应数字或程度的增加而增加。

[0025] 可以基于风险行为来确定攻击表面暴露风险因数,例如但不限于漏洞、常见流量模式、威胁情报、流量漏洞、开放端口、特定协议的使用、云域访问、无线协议、开放热点以及设备提供的任何其他外部访问。可能导致更高攻击面暴露风险因数的风险行为可能包括但不限于大量开放端口、无线通信、热点或其组合;使用未加密的协议;偏离普通流量模式的流量模式;指示设备可能存在网络安全威胁的设备威胁情报;和大量已知漏洞。

[0026] 可以基于关于设备访问的云服务的风险行为来确定设备的云同步风险因数,例如但不限于设备使用的云服务的数量、设备传输到云服务的数据量、设备和云环境之间形成的隧道的数量、设备传输的数据的类型、设备访问的云环境的域的已知信誉等。会导致更高云同步风险因数的风险行为可能包括但不限于大量云端点、数据或凭证未加密、访问可疑云域等。

[0027] 可以基于关于设备连接的安全性和潜在漏洞的风险行为来确定设备的连接安全风险因数,例如但不限于与设备使用的协议相关的漏洞和威胁情报以及连接数据(例如,设备所连接的其他不同设备的数量、连接是否被加密等)。会导致更高连接安全风险因数的风险行为可以包括但不限于,与不同设备大量连接、使用未加密的连接、使用已知的潜在易受

攻击的协议等。

[0028] 可以基于关于设备连接到多个可信边界的风险行为来确定设备的边界规避风险因数，例如但不限于与不同边界的多个连接、与敏感边界(例如，公司网络的边界)的多个连接、已知的标准设备配置等。会导致更高边界规避风险因数的风险行为可以包括但不限于，与不同边界的更多连接、与敏感边界的更多连接、当类似设备的标准设备配置建议设备不应该连接到不止一个网络时该设备连接到不止一个网络等。

[0029] 可以基于关于设备访问的第三方应用商店的数量和风险的风险行为来确定设备的第三方应用商店风险因数，例如但不限于访问的第三方应用商店的数量、托管访问的第三方应用商店的域的信誉、所访问的第三方应用商店的安全特征(例如防火墙、流量阻挡等)等。会导致更高的第三方应用商店风险因数的风险行为可以包括但不限于，访问更多第三方应用商店、威胁情报关于已知攻击指示的更高风险远程域、没有检测到防火墙或流量阻挡等。

[0030] 可以基于关于设备访问的域的数量和风险的风险行为来确定设备的恶意域风险因数，例如但不限于访问的已知恶意或可疑域的数量、威胁情报关于已知攻击指示的更高风险远程域、访问域的安全特征(例如防火墙、流量阻挡等)等。会导致更高恶意域风险因数的风险行为可包括但不限于，与已知恶意或可疑域进行更多连接、威胁情报关于已知攻击指示的更高风险远程域、没有检测到防火墙或流量阻挡等。

[0031] 可以基于关于检测到的设备漏洞的数量和严重性的风险行为来确定设备的漏洞历史风险因数，例如但不限于检测到的漏洞的数量、漏洞的严重性、漏洞是否可被远程利用、设备是否已经执行了缓解等。会导致更高的漏洞历史风险因数的风险行为可以包括但不限于漏洞更多、漏洞风险更高、可远程利用漏洞的风险更高、缺少缓解等。

[0032] 可以基于关于设备囤积或存储数据的风险行为来确定设备的静态数据风险因数，例如但不限于发送到设备和由设备接收的数据量、发送到设备的数据的重要性或敏感性、设备是否具有加密盘等。会导致更高静态数据风险因数的风险行为可能包括但不限于，进入设备的数据多于流出的数据、进入设备的业务更重要或更敏感、设备缺少未加密盘等。重要或敏感数据的示例可以包括但不限于客户关系管理数据、设备数据、扫描数据、患者数据、指示身份信息的数据等。

[0033] 可以基于关于设备打开外部连接的风险行为来确定设备的外部连接风险因数，例如但不限于热点的数量、开放无线协议的数量、设备的访问是否被加密、设备的访问是否需要认证、任何外部连接的已知漏洞等。会导致更高外部连接风险因数的风险行为可能包括但不限于热点更多、无线协议更开放、访问未加密、访问未经认证、外部连接存在已知漏洞等。

[0034] 可以基于关于设备上不同的用户认证以及这些用户认证的凭证安全性的风险行为来确定设备的用户认证风险因数，例如但不限于使用同一设备的用户数量、凭证是否被加密、认证用户是否符合已知的组织结构等。会导致更高用户认证风险因数的风险行为可以包括但不限于更多用户使用同一设备、凭证未加密、用户不符合组织中用户结构等。

[0035] 可以基于关于设备上安装的操作系统和软件应用的数量和年限的设备风险行为来确定软件版本风险因数，该风险行为，例如但不限于应用的年限、操作系统的年限、应用的数量、操作系统的数量、应用的版本号、操作系统的版本号、具有已知更高风险的可远程

利用的漏洞的应用或操作系统、操作系统或软件缺少对网络威胁的缓解等。会导致更高软件版本风险因数的风险行为可包括但不限于应用或操作系统较旧、应用或操作系统更多、应用或操作系统具有更高风险的可远程利用漏洞、缺少检测到的缓解等。

[0036] 可以基于关于设备重复使用证书的风险行为来确定设备的证书重复使用风险因数，例如但不限于多个设备使用相同证书、设备使用的证书是基于用户的还是基于设备的、共享证书的设备的品牌和型号等。会导致更高证书重复使用风险因数的风险行为可以包括但不限于，更多设备使用相同证书、使用基于用户的证书、不同品牌和型号的设备共享证书等。

[0037] 可以基于关于设备制造商的风险行为来确定制造商信誉风险因数，例如但不限于影响制造商的已知违规数量、制造商的原产地地理位置的已知信誉、制造商制造的设备的漏洞的已知数量等。会导致更高制造商信誉风险因数的风险行为可包括但不限于，影响制造商的已知违规数量更多、原产国信誉不佳、制造商制造的设备的漏洞数量更多等。

[0038] 可以基于与设备型号相关的风险行为来确定设备型号信誉风险因数，例如但不限于设备型号的通用性程度(例如，相同型号的设备的用户或所有者的相对数量)、设备型号的已知威胁情报、设备型号的已知漏洞数量等。会导致更高设备型号信誉风险因数的风险行为可包括但不限于设备型号不太常见、关于设备型号的威胁情报暗示设备型号可能不安全、设备型号存在大量漏洞等。

[0039] 图1示出了用于描述各种公开实施例的示例网络图100。在示例网络图100中部署有威胁缓解器120，使得其可以访问网络110。网络110可以是但不限于无线、蜂窝或有线网络、局域网(LAN)、广域网(WAN)、城域网(MAN)、类似网络及其任意组合。

[0040] 设备130访问网络110(示出)或部署在物理上靠近网络110的地方(未示出)。设备130可以是但不限于个人计算机、笔记本电脑、平板计算机、智能手机、可穿戴计算设备、打印机或连接到网络110或部署在物理上靠近网络110的网络基础架构(例如，路由器，未示出)的地方的任何其他设备。

[0041] 在示例实现方式中，网络110包括数据库111和一个或多个网络活动检测工具112。威胁缓解器120配置为访问数据库111、检测工具112或两者，以获得与用于确定风险因数的风险行为相关的数据。

[0042] 数据库111可以存储与假设的风险行为相关的上下文数据，例如但不限于制造商信誉信息、设备型号信誉信息、制造商或设计者与产品相关联的常见漏洞和暴露的数量、制造商或设计者的员工数量、流行的操作系统等。数据库111还可以存储由网络活动检测工具112收集的数据，使得威胁缓解器112可以从数据库111检索这样的信息。

[0043] 数据库111还可存储与已知设备行为相关的数据，这些数据可用于确定风险因数。因此，数据库111可以充当已知设备行为简档的知识库。与已知设备行为相关的数据可以定义设备的代表正常行为的基线行为和基于与基线行为的偏差的风险因数的值(或用于计算值的公式)。作为非限制性示例，安全摄像机的基线行为可以是与网络上固定地理位置的单个内部服务器通信。安全摄像头的风险因数可以针对包括与不止一个服务器通信、与外部服务器通信、停止与服务器通信或改变地理位置的行为来定义。

[0044] 制造商信誉信息可以包括与以前连接到网络的设备相关的信息、与公司规模相关的公共源信息以及显著的安全违规，或者两者都有。与先前设备相关的信息可以基于针对

具有相同制造商的其他设备确定的风险分数，使得这种先前设备的高风险分数将增加最终的风险因数。规模和安全违规信息可以包括，例如，CVE的数量、每个CVE的严重程度和公司的规模，使得相对于公司的员工数量，CVE的数量高和CVE的严重程度高将导致更高的风险因数。

[0045] 流行的操作系统信息可以包括安装在其他设备上的常见操作系统、设备可用的最小和最大(即最早和最新或最不安全和最安全)操作系统版本，或者两者都有。不使用通用操作系统的设备会导致更高的风险因数。操作系统版本更接近最低版本的设备会比操作系统版本最接近最高版本的设备导致更高的风险因数。

[0046] 检测工具112配置为收集与设备、设备130的网络活动或两者相关的数据。这种数据可以包括与观察到的风险行为相关的数据，例如但不限于，包括在去往或来自设备130的流量中的数据、由设备130发送的流量的量、从设备130接收流量的端点的数量、由设备130发送的流量的类型(例如，加密或未加密、重复或不重复等)、设备130表现出的常见漏洞和暴露(例如，对于设备130、对于在设备130上运行的软件或两者)、设备130寻址和访问的域和互联网协议(IP)、安装在设备130上的软件的类型和版本、安装在设备130上的操作系统的类型和版本、外部通信选项的数量和类型(例如，端口、协议、广播的服务集标识符的数量、不同天线的数量等)、设备的地理位置、设备的地理移动等。网络活动数据可以针对设备130、设备130上运行的操作系统、设备130上运行的每个应用或其组合来收集。

[0047] 威胁缓解器120配置为确定设备130的风险分数，并基于所确定的风险分数执行缓解操作。风险分数根据风险因数确定。风险因数基于风险行为(包括观察到的风险行为和假设的风险行为)确定。观察到的风险行为可以在从设备130、从网络活动检测工具112收集的关于设备130的网络活动的数据中指示，或者在两者中指示。假设的风险行为基于与设备相关的上下文数据来推断，所述上下文数据为例如但不限于访问网络110的其他设备(未示出)的活动、与设备相关的公共信息(例如，关于设备制造商的信息、设备130使用的假设操作系统、传输到设备或由设备传输的数据等)，或者两者都有。每个风险因数可以基于观察到的风险行为、假设的风险行为或其组合来确定。

[0048] 应当注意，所公开的实施例不限于图1所示的特定布局。例如，威胁缓解器120在图1中示为部署在网络110之外，但是威胁缓解器120可以同样地部署在网络110中，而不脱离本公开的范围。另外，为了简单起见，威胁缓解器120和检测工具112分开示出，但是威胁缓解器120可以包括在检测工具112之一中，或者以其他方式充当检测工具112之一，而不脱离本公开的范围。

[0049] 图2是示出根据实施例的使用风险因数缓解设备的网络安全威胁的方法的示例流程图200。在一个实施例中，该方法由威胁缓解器120执行。

[0050] 在可选步骤S210，对待检查风险设备进行检测。该检测可以包括检测设备到网络的连接、检测在物理上靠近网络基础架构的地方开启的设备、或者检测对网络可见的设备(例如，已经开启的设备在距离网络基础架构的任何部分的阈值物理距离内移动)。在一些实现方式中，可以检查网络已经可见的设备的风险。具体而言，可以如关于从连接到网络到从网络断开的以下步骤所描述的那样持续分析设备。

[0051] 在步骤S220，收集与设备相关的数据。与设备相关的数据包括与设备直接相关的数据(例如，设备的配置数据、设备的识别信息等)和设备的网络活动(例如，从设备收集的

或通过监控设备的活动收集的数据)以及指示与设备相关的上下文信息的数据。

[0052] 收集的数据可包括但不限于网络活动数据(例如,指示进入或离开设备的流量的数据、流量数据(即,由设备传输或传输到设备的数据、流量的量、设备所连接的网络部分等)、设备的识别信息(例如,设备的名称、型号、标识符、制造商等)、寿命终止或服务终止数据、与设备相关的软件数据(例如,安装在设备上的程序)、连接数据(例如,开放端口、无线通信、热点、设备作为端点连接到的网络数量、连接是否加密、设备连接到的系统的域和互联网协议地址等)、指示设备使用的协议的协议数据、设备访问的网站、设备的地理位置、设备的类型(例如,智能手机、智能手表、笔记本电脑、安全摄像头、个人计算机等)、指示与如上所述确定风险因数相关的其他信息的数据等。

[0053] 在步骤S230,基于收集的数据,确定风险因数。风险因数基于风险行为确定,如观察到的风险行为和假设的风险行为。在一个实施例中,每个风险因数基于预定风险因数和相关风险行为的列表来确定,作为表示风险行为的一个或多个数值或其组合的函数(例如,预定数值可以与相关风险行为相关联,并且预定数值可以用作多个风险行为值的函数的输入)。在示例实现方式中,每个风险因数都是1-10范围内的数字。

[0054] 每个风险因数可以基于观察到的风险行为、假设的风险行为或其组合来确定,并且可以基于代表不同风险行为的多个值来聚集。为此,S230还可以包括确定每个风险行为的值,并且聚集这些值以确定风险因数。

[0055] 在一个实施例中,可以基于已知正常设备行为的知识库来确定风险因数。这样的知识库可以存储在数据库(例如,图1的数据库111)中,并且包括设备的已知正常行为。知识库还定义了偏离已知正常行为的风险因数。为此,知识库可以定义特定偏离行为的预定值,基于表示偏离正常行为的值来计算风险因数值的公式,或者两者都定义。已知正常行为还可以包括不同设备、设备类型、设备用户等的不同组的已知正常行为。

[0056] 在另一个实施例中,可以基于设备之间的行为比较来确定风险因数。例如,可以将设备的行为与连接到网络的其他设备的行为进行比较。更具体地,可以基于是否存在行为差异、行为差异程度、具有相同行为的其他设备的数量、具有不同行为的其他设备的数量、具有不同行为差异程度的设备的数量等来确定基于与网络上的其他设备的比较而为设备确定的风险因数。

[0057] 还可以进行如下比较:在可比设备之间、设备类型之间(例如,笔记本电脑的行为可以相互比较,但不能与服务器或安全摄像头的行为进行比较)、设备所有者之间(例如,设备的行为可以在入门级员工之间、管理层之间、高管或其他高级官员之间进行比较等)、设备品牌之间等进行比较。作为非限制性示例,如果网络上的其他ABC品牌笔记本计算机具有操作系统版本10.1,并且该设备是网络上具有操作系统版本9.0的笔记本电脑,则可以基于该偏差来确定风险因数。

[0058] 确定风险因数的一些示例如下。第一,指示设备正在移动的数据与预定的观察行为风险因数2相关联,并且指示设备不动的数据与预定的观察行为风险因数8相关联。第二,将公司常见漏洞和暴露(CVE)历史的假设行为风险因数确定为商(CVE数量)/(员工数量)的函数,使得相对于以员工数量表示的公司规模,CVE数量越高,得到的风险因数越高,并且该函数还可以基于每个CVE的严重程度。第三,用于数据可预测性的假设风险行为可以是基于数据计算的熵的函数,使得熵越高得到的风险因数越低,反之亦然。第四,与可疑云域的连

接(例如,来自可疑云域的预定列表)可以与值7相关联,并且与20个云端点的连接可以与值9相关联,使得将聚集风险因数确定为8。

[0059] 以上描述了额外的示例风险因数及确定这些风险因数时所依据的风险行为。

[0060] 在一个实施例中,S230还包括确定观察到的风险行为。观察到的风险行为直接基于设备的网络活动数据、配置数据或两者来确定。作为非限制性示例,可以分析与流量相关的网络活动数据,以确定进出设备的流量。作为另一个非限制性示例,可以分析设备的配置数据以确定设备是否具有加密盘。

[0061] 在一个实施例中,S230还包括确定假设的风险行为。假设的风险行为通过基于与设备相关的上下文信息进行推断而间接确定。为此,上下文信息可以包括例如与设备相关的数据所指示的某些情况和假设的风险行为之间的预定关联。可以基于与设备相关的数据来确定环境,所述数据例如但不限于设备的配置数据、设备的识别数据(例如,通过名称、类型、型号、制造商、品牌等来识别设备)。作为非限制性示例,可以分析设备的配置数据来确定设备的操作系统版本(例如,ABC OS v.5.4),并且可以基于操作系统的已知版本列表来确定操作系统的已知年限(例如,实际年限或相对于其他版本的年限)。作为另一个非限制性示例,可以分析该设备的识别数据以确定该设备的制造商(例如,XYZ电话制造商公司),并且可以基于制造商列表和已知信誉(例如,信誉表示为相对于该制造商的员工数量而言,该制造商造成的常见漏洞和暴露的数量)来确定该设备的制造商信誉。

[0062] 在步骤S240,基于风险因数,为设备确定风险分数。在一个实施例中,通过将权重值应用于每个风险因数来确定风险分数。风险分数是加权风险因数的总和。权重可以预先确定,并且可以根据设备(例如,设备类型、型号、具体设备等)、设备的活动(例如,设备连接到的网络部分)、或者这两者而不同。作为非限制性示例,当设备是笔记本电脑时,可将0.1的低权重应用于所访问的域数量的风险因数,而当设备是安全摄像机时,可将0.8的高权重应用于该风险因数。

[0063] 在一些实现方式中,至少一些权重可以是负的,使得其相应的风险因数降低总体风险分数。这使得可以整体考虑与风险相关的加重和缓解情况(即,分别增加设备有风险的可能性和降低设备有风险的可能性的情况)。

[0064] 在步骤S250,基于风险分数,确定适当的缓解操作。适当的缓解操作可以包括但不限于,将设备从网络断开、防止设备连接到网络(例如,通过重新配置网络基础架构的访问控制设置)、限制设备在网络上的活动(例如,防止设备上传数据到网络)、限制设备可以连接到的网络部分(例如,仅允许设备连接到访客网络而不是私用网络)等。例如,基于风险分数的一个或多个阈值,要执行的缓解操作可能会有所不同。

[0065] 在一些实现方式中,适当的缓解操作可以包括对设备活动进行被动监控,而不是对设备活动进行主动干扰,例如,当风险分数低于阈值时。在这样的实现方式中,设备的风险因数和风险分数可以基于通过被动监控获得的新信息随着时间(例如,周期性地)而更新。这允许向尚未被确定为具有足够风险的设备提供网络访问,以基于网络活动缓解和重新评估设备带来的风险。例如,长时间未连接到网络的设备最初可能具有较低的风险分数,但是随着时间的推移,当设备在网络内操作时,该设备可能具有更高的风险分数。因此,最初可以允许这种设备操作,但是一旦确定该设备存在可能的网络安全威胁,就可以断开连接或以其他方式阻止其访问网络。

[0066] 在步骤S260,执行缓解操作。在一些实现方式中,当检测到可疑活动时(例如,通过一个或多个网络安全检测工具,例如图1的检测工具112,或者两者),可以周期性地更新设备的风险因数和风险分数。在这样的实现方式中(未示出),执行继续到步骤S220。

[0067] 应该注意的是,图2是针对关于风险因数的设备的离散单一评估来描述的,这仅仅是为了简单起见,并不限制所公开的实施例。所公开的实施例同样可以应用于重复执行、持续执行或以其他方式在网络上或物理上接近网络的设备的整个会话期间更新设备的评估的实现方式。

[0068] 图3是根据实施例的威胁缓解器120的示例示意图。威胁缓解器120包括耦合到存储器320、存储装置330和网络接口340的处理电路310。在一个实施例中,威胁缓解器120的组件可以经由总线350通信连接。

[0069] 处理电路310可以实现为一个或多个硬件逻辑组件和电路。例如,但不限于,可以使用的说明性类型的硬件逻辑组件包括现场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、片上系统(SOC)、通用微处理器、微控制器、数字信号处理器(DSP)等,或者可以执行计算或其他信息操作的任何其他硬件逻辑组件。

[0070] 存储器320可以是易失性的(例如,RAM等)、非易失性的(例如,ROM、闪存等)或其组合。在一种配置中,实现本文公开的一个或多个实施例的计算机可读指令可以存储在存储装置330中。

[0071] 在另一个实施例中,存储器320配置为存储软件。软件应广义地解释为任何类型的指令,无论是指软件、固件、中间件、微码、硬件描述语言还是其他形式。指令可以包括代码(例如,源代码格式、二进制代码格式、可执行代码格式或任何其他合适的代码格式)。当由处理电路310执行时,指令使得处理电路310执行本文描述的各种过程。具体而言,指令在被执行时,使得处理电路310生成车队行为模型,并检测车队或子车队中的异常行为,如本文所述。

[0072] 存储装置330可以是磁存储装置、光存储装置等,并且可以实现为例如闪存或其他存储技术、CD-ROM、数字多功能盘(DVD)或任何其他可以用于存储期望信息的介质。

[0073] 网络接口340允许威胁缓解器120与数据库111通信,用于例如检索与设备130相关的假设行为数据等目的。此外,网络接口340允许威胁缓解器120与检测工具112通信,用于例如检索与设备130相关的网络活动数据的目的。

[0074] 应当理解,本文描述的实施例不限于图3所示的特定架构,并且在不脱离所公开的实施例的范围的情况下,可以同样地使用其他架构。

[0075] 本文公开的各种实施例可以实现为硬件、固件、软件或其任意组合。此外,软件优选地被实现为有形地包含在程序存储单元或计算机可读介质上的应用程序,该程序存储单元或计算机可读介质由一些部件、某些设备和/或设备的组合组成。该应用程序可以被上传到包括任何合适架构的机器,并由该机器执行。优选地,机器在计算机平台上实现,该计算机平台具有硬件,例如一个或多个中央处理单元(“CPU”)、存储器和输入/输出接口。计算机平台还可以包括操作系统和微指令代码。本文描述的各种过程和功能可以是微指令代码的一部分或应用程序的一部分,或其任意组合,其可以由CPU执行,无论是否明确示出了这样的计算机或处理器。此外,各种其他外围单元可以连接到计算机平台,例如附加数据存储单元和打印单元。此外,非暂时性计算机可读介质是除暂时性传播信号之外的任何计算机可

读介质。

[0076] 本文列举的所有示例和条件语言都是为了教学目的，以帮助读者理解所公开的实施例的原理和发明人为促进本领域所贡献的概念，并且应该解释为不限于这些具体列举的示例和条件。此外，本文叙述所公开的实施例的原理、方面和实施例及其具体示例的所有陈述旨在包括其结构和功能等同物。此外，这种等同物旨在包括当前已知的等同物以及将来开发的等同物，即，无论结构如何，开发的执行相同功能的任何元件。

[0077] 应当理解，本文中使用诸如“第一”、“第二”等名称对元件的任何引用通常不限制这些元件的数量或顺序。相反，这些名称在本文中通常用作区分两个或更多元件或元件示例的便利方法。因此，对第一和第二元件的引用并不意味着在那里只能使用两个元件，或者第一元件必须以某种方式在第二元件之前。此外，除非另有说明，否则一组元件包括一个或多个元件。

[0078] 如本文所用，短语“至少一个”后跟项目列表意味着可以单独使用任何列出的项目，或者可以使用两个或多个列出的项目的任意组合。例如，如果一个系统被描述为包括“A、B和C中的至少一个”，则该系统可以单独包括A；单独包括B；单独包括C；2A；2B；2C；3A；A和B的组合；B和C的组合；A和C的组合；A、B、C的组合；2A和C的组合；A、3B、2C的组合；等等。

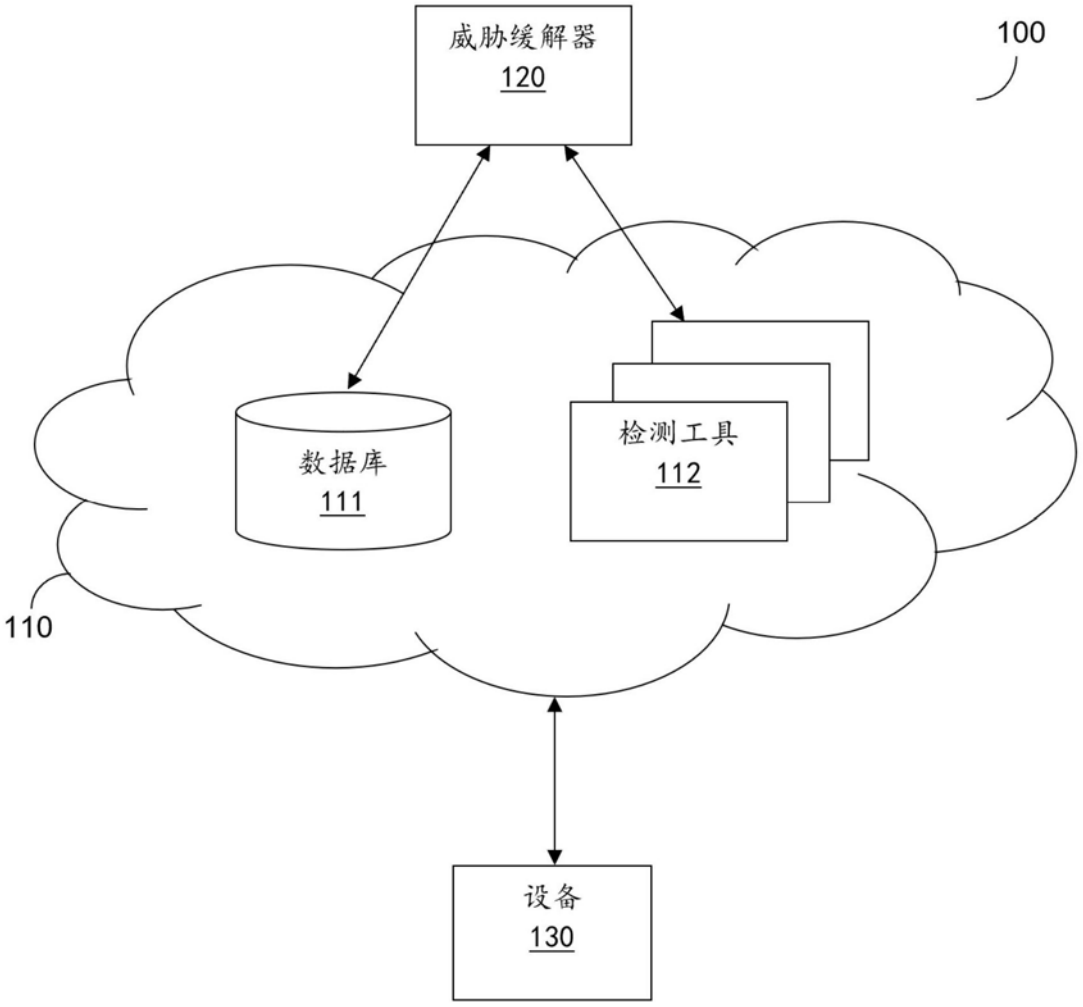


图1

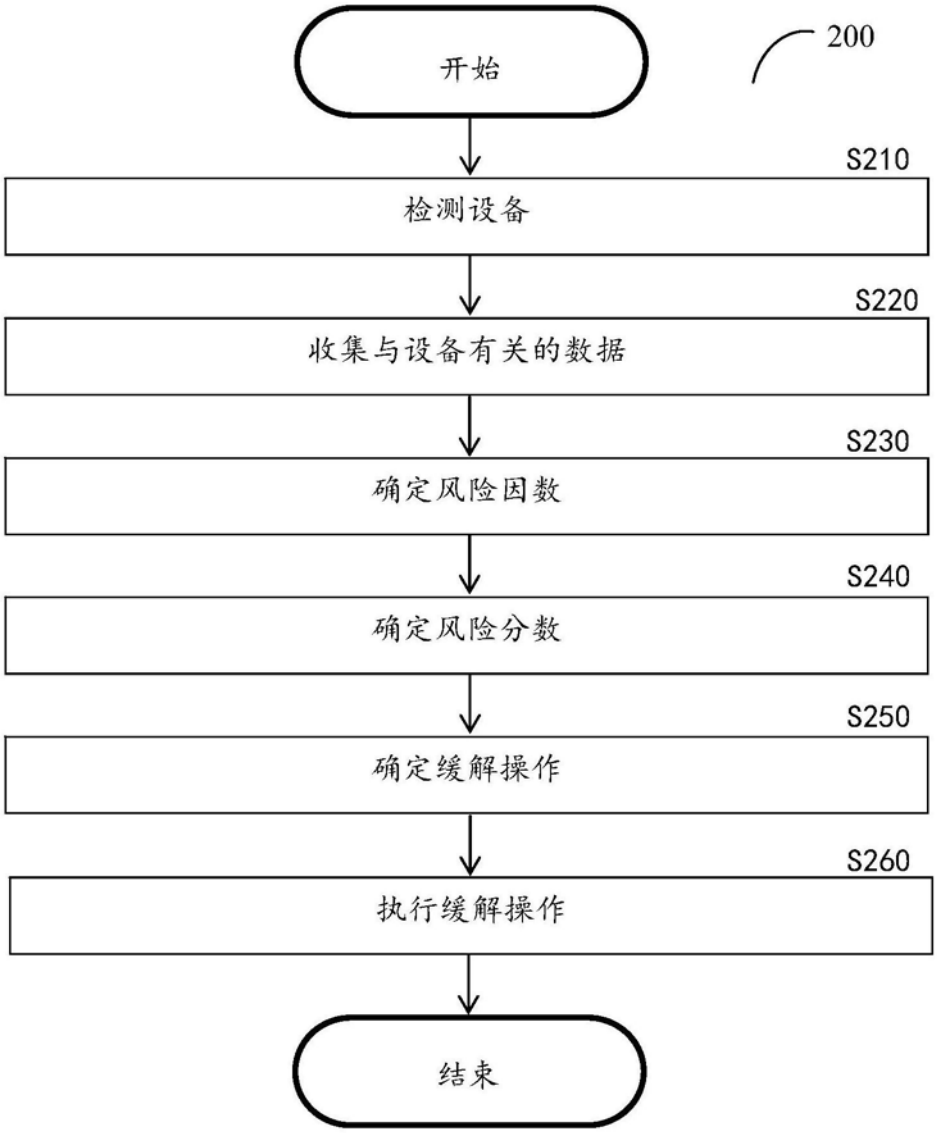

开始
200
S210
检测设备
S220
收集与设备有关的数据
S230
确定风险因数
S240
确定风险分数
S250
确定缓解操作
S260
执行缓解操作
结束

图2

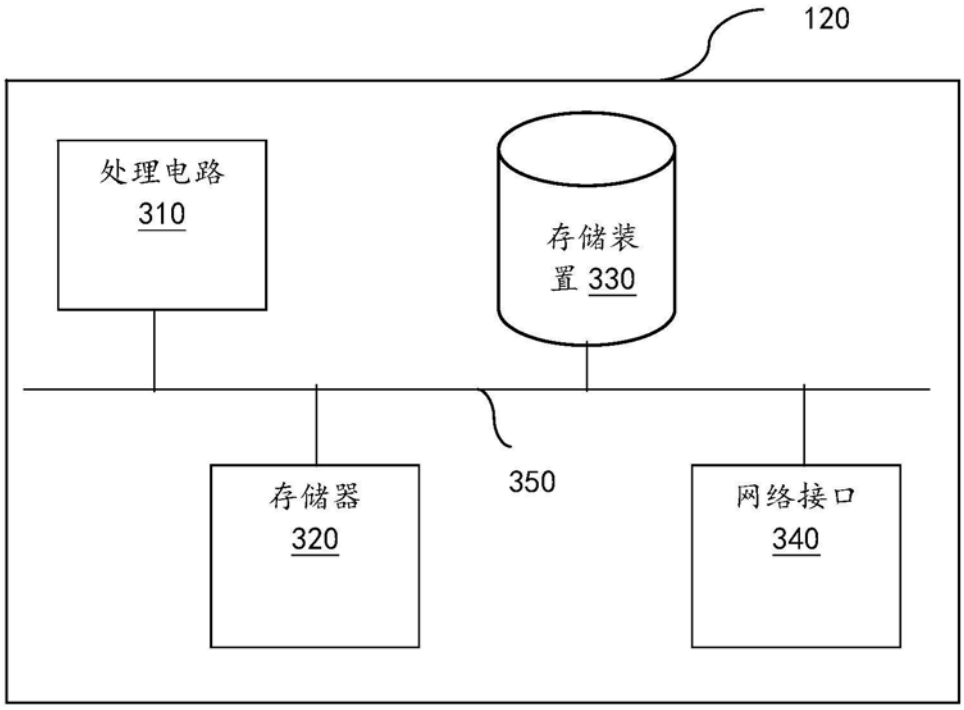


图3