(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 108206830 B
(45)授权公告日 2019.09.24

(21)申请号 201711492203.7

(22)申请日 2017.12.30

(65)同一申请的已公布的文献号
申请公布号 CN 108206830 A

(43)申请公布日 2018.06.26

(73)专利权人 平安科技(深圳)有限公司
地址 518052 广东省深圳市福田区八卦岭八卦三路平安大厦六楼

(72)发明人 周圣龙

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 易皎鹤

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
US 2003065945 A1,2003.04.03,

审查员 鞠博

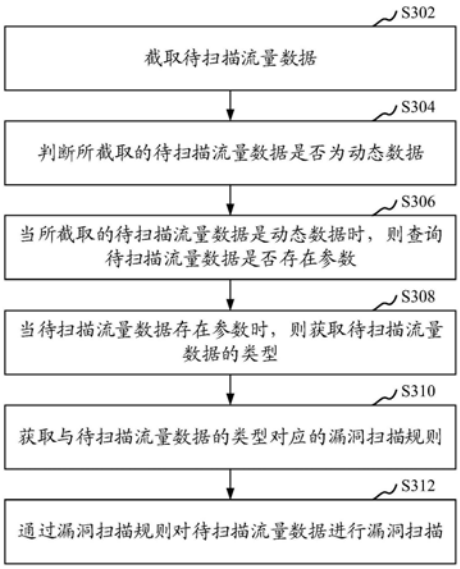
权利要求书2页 说明书10页 附图4页

(54)发明名称

漏洞扫描方法、装置、计算机设备和存储介质

(57)摘要

本申请涉及一种漏洞扫描方法、系统、计算机设备和存储介质，该方法包括截取待扫描流量数据；判断所截取的待扫描流量数据是否为动态数据；当所截取的待扫描流量数据是动态数据时，则查询待扫描流量数据是否存在参数；当扫描流量数据存在参数时，则获取待扫描流量数据的类型；获取与待扫描流量数据的类型对应的漏洞扫描规则；通过漏洞扫描规则对待扫描流量数据进行漏洞扫描。上述漏洞扫描方法、装置、计算机设备和存储介质，首先对不需要扫描的待扫描流量数据进行剔除，其次根据待扫描流量数据的类型获取到对应的漏洞扫描规则，而不需要将数据库中所有的漏洞扫描规则均执行一遍，可以大大降低漏洞扫描规则的执行数量，从而也提高了漏洞扫描的效率。



CN 108206830 B

1.一种漏洞扫描方法,所述方法包括:

截取待扫描流量数据;

判断所截取的待扫描流量数据是否为动态数据,所述动态数据为既可以看到,又有交互的数据;

当所截取的待扫描流量数据是动态数据时,则查询所述待扫描流量数据是否存在参数;

当所述扫描流量数据存在参数时,则获取所述待扫描流量数据的类型;

获取与所述待扫描流量数据的类型对应的漏洞扫描规则;

通过所述漏洞扫描规则对所述待扫描流量数据进行漏洞扫描。

2.根据权利要求1所述的方法,其特征在于,所述截取待扫描流量数据的步骤之后,还包括:

获取当前资源占用率;

若所述当前资源占用率超过阈值时,则获取备扫描服务器的资源占用率;

选取所述备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

3.根据权利要求2所述的方法,其特征在于,所述获取当前资源占用率的步骤之前,还包括:

判断当前扫描服务器是否出现故障;

若当前扫描服务器未出现故障,则继续执行获取当前资源占用率的步骤;

若当前扫描服务器出现故障,则获取备扫描服务器的资源占用率;

选取所述备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

4.根据权利要求1所述的方法,其特征在于,所述截取待扫描流量数据的步骤之后,还包括:

统计截取所述待扫描流量数据的截取次数;

根据所述截取次数启动对应数量的扫描服务器;

将所述待扫描流量数据分配至所启动的扫描服务器中以继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

5.根据权利要求1至4任意一项所述的方法,其特征在于,所述通过所述漏洞扫描规则对所述待扫描流量数据进行漏洞扫描的步骤之后,还包括:

接收针对所述待扫描流量数据的漏洞扫描规则调整指令;

根据所述漏洞扫描规则调整指令获取漏洞扫描补充规则;

通过所述漏洞扫描补充规则对所述待扫描流量数据进行漏洞扫描。

6.根据权利要求1至4任意一项所述的方法,其特征在于,所述截取待扫描流量数据的步骤,包括:

通过预先设置在客户端的代理程序截取待扫描流量数据。

7.根据权利要求1至4任意一项所述的方法,其特征在于,所述截取待扫描流量数据的步骤,包括:

接收核心交换机根据所截取到的待扫描流量数据生成的镜像流量数据作为待扫描流

量数据。

8.一种漏洞扫描装置,其特征在于,所述装置包括:

流量截取模块,用于截取待扫描流量数据;

数据判断模块,用于判断所截取的待扫描流量数据是否为动态数据,所述动态数据为既可以看到,又有交互的数据;

查询模块,用于当所截取的待扫描流量数据是动态数据时,则查询所述待扫描流量数据是否存在参数;

流量类型获取模块,用于当所述待扫描流量数据存在参数时,则获取所述待扫描流量数据的类型;

规则获取模块,用于获取与所述待扫描流量数据的类型对应的漏洞扫描规则;

扫描模块,用于通过所述漏洞扫描规则对所述待扫描流量数据进行漏洞扫描。

9.一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1至7中任一项所述方法的步骤。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

漏洞扫描方法、装置、计算机设备和存储介质

技术领域

[0001] 本申请涉及计算机技术领域，特别是涉及一种漏洞扫描方法、装置、计算机设备和存储介质。

背景技术

[0002] 随着计算机技术的发展，出现了漏洞扫描技术，传统的漏洞扫描技术是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测(渗透攻击)行为。

[0003] 然而，传统中的漏洞扫描技术是扫描服务器主动通过爬虫技术对服务器中的待扫描数据进行爬取，然后通过漏洞数据库中所有的漏洞匹配规则去判断所爬取的数据是否存在漏洞，扫描效率较低。

发明内容

[0004] 基于此，有必要针对上述技术问题，提供一种能够提高漏洞扫描效率的漏洞扫描方法、装置、计算机设备和存储介质。

[0005] 一种漏洞扫描方法，所述方法包括：

[0006] 截取待扫描流量数据；

[0007] 判断所截取的待扫描流量数据是否为动态数据；

[0008] 当所截取的待扫描流量数据是动态数据时，则查询所述待扫描流量数据是否存在参数；

[0009] 当所述扫描流量数据存在参数时，则获取所述待扫描流量数据的类型；

[0010] 获取与所述待扫描流量数据的类型对应的漏洞扫描规则；

[0011] 通过所述漏洞扫描规则对所述待扫描流量数据进行漏洞扫描。

[0012] 在其中一个实施例中，所述截取待扫描流量数据的步骤之后，还包括：

[0013] 获取当前资源占用率；

[0014] 若所述当前资源占用率超过阈值时，则获取备扫描服务器的资源占用率；

[0015] 选取所述备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0016] 在其中一个实施例中，所述获取当前资源占用率的步骤之前，还包括：

[0017] 判断当前扫描服务器是否出现故障；

[0018] 若当前扫描服务器未出现故障，则继续执行获取当前资源占用率的步骤；

[0019] 若当前扫描服务器出现故障，则获取备扫描服务器的资源占用率；

[0020] 选取所述备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0021] 在其中一个实施例中，所述截取待扫描流量数据的步骤之后，还包括：

[0022] 统计截取所述待扫描流量数据的截取次数；

[0023] 根据所述截取次数启动对应数量的扫描服务器；

[0024] 将所述待扫描流量数据分配至所启动的扫描服务器中以继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0025] 在其中一个实施例中，所述通过所述漏洞扫描规则对所述待扫描流量数据进行漏洞扫描的步骤之后，还包括：

[0026] 接收针对所述待扫描流量数据的漏洞扫描规则调整指令；

[0027] 根据所述漏洞扫描规则调整指令获取漏洞扫描补充规则；

[0028] 通过所述漏洞扫描补充规则对所述待扫描流量数据进行漏洞扫描。

[0029] 在其中一个实施例中，所述截取待扫描流量数据的步骤，包括：

[0030] 通过预先设置在客户端的代理程序截取待扫描流量数据。

[0031] 在其中一个实施例中，所述截取待扫描流量数据的步骤，包括：

[0032] 接收核心交换机根据所截取到的待扫描流量数据生成的镜像流量数据作为待扫描流量数据。

[0033] 一种漏洞扫描装置，所述装置包括：

[0034] 流量截取模块，用于截取待扫描流量数据；

[0035] 数据判断模块，用于判断所截取的待扫描流量数据是否为动态数据；

[0036] 查询模块，用于当所截取的待扫描流量数据是动态数据时，则查询所述待扫描流量数据是否存在参数；

[0037] 流量类型获取模块，用于当所述待扫描流量数据存在参数时，则获取所述待扫描流量数据的类型；

[0038] 规则获取模块，用于获取与所述待扫描流量数据的类型对应的漏洞扫描规则；

[0039] 扫描模块，用于通过所述漏洞扫描规则对所述待扫描流量数据进行漏洞扫描。

[0040] 一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述任一项所述方法的步骤。

[0041] 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述任一项所述的方法的步骤。

[0042] 上述漏洞扫描方法、装置、计算机设备和存储介质，首先是截取待扫描流量数据，即当客户端存在数据访问时，则就会截取流量数据，使得待扫描流量数据的覆盖范围变大；其次，在漏洞扫描前，对不需要扫描的待扫描流量数据进行剔除，减少了待扫描流量数据的扫描量，提高了漏洞扫描效率；最后，根据待扫描流量数据的类型获取到对应的漏洞扫描规则，而不需要将数据库中所有的漏洞扫描规则均执行一遍，可以大大降低漏洞扫描规则的执行数量，从而也提高了漏洞扫描的效率。

附图说明

[0043] 图1为一个实施例中漏洞扫描方法的应用场景图；

[0044] 图2为一实施例中扫描服务器的架构图；

[0045] 图3为一个实施例中漏洞扫描方法的流程示意图；

[0046] 图4为一个实施例中漏洞扫描装置的结构框图；

[0047] 图5为一个实施例中计算机设备的内部结构图。

具体实施方式

[0048] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0049] 本申请提供的漏洞扫描方法，可以应用于如图1所示的应用环境中。其中，终端可以通过核心交换机或路由器等访问网络上的资源，扫描服务器可以通过核心交换机或路由器截取到终端的流量数据，或者扫描服务器可以通过设置代理服务器的方式截取到终端的流量数据，从而扫描服务器可以在截取到流量数据的时候被动地对流量数据进行扫描，以判断该流量数据是否为漏洞数据，从而实现漏洞的检测。其中终端可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备，扫描服务器可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0050] 参见图2，图2为一实施例中扫描服务器的架构图，其中包括系统基础、调动引擎、web应用服务，调度引擎主要是为了被动式扫描服务，web应用服务则主要是为了查询记录服务器，UI界面则是可以进行显示。具体地，调度引擎可以采用分布式多线程的部署，其中设置有机器学习模型、扫描引擎以及系统升级程序等，该机器学习模型可以是决策树模型，扫描引擎主要存储有漏洞扫描规则，系统升级程序主要是针对系统的升级。Web应用服务主要包括报告模型、日志模块和配置模块，web应用服务则主要是为了查询记录服务，即每次漏洞扫描完成后可以生成日志存储至日志模块，并根据扫描结果生成对应的报告，例如存在漏洞的报告或不存在漏洞的报告，并显示在对应的UI界面上。

[0051] 在一个实施例中，如图3所示，提供了一种漏洞扫描方法，以该方法应用于图1中的扫描服务器为例进行说明，包括以下步骤：

[0052] S302：截取待扫描流量数据。

[0053] 具体地，流量数据是指终端在访问网络上的资源时所产生的数据，其包括访问请求的报文等。用户使用的终端可以访问Internet上的资源，当用户使用的终端进行访问时，可以在主干节点或链路节点中进行流量数据截取，截取到的流量存储在扫描服务器中，从而根据该流量数据判断是否存在漏洞。

[0054] S304：判断所截取的待扫描流量数据是否为动态数据。

[0055] 具体地，动态数据只是既可以看到，又可以交互的数据，并获得良好的体验效果，用户不再是被动的去浏览，比如说留言板，论坛，用户注册等这些就是动态的可以让用户与网站交互，而静态数据的则是仅供查看。具体地可以通过机器学习的方式将所截取到的待扫描流量数据中不需要漏洞检测的流量删除，例如可以通过决策树算法进行，当截取到待扫描流量数据时，则输入机器学习模型中，首先判断该待扫描的流量数据是否为动态数据，如果是动态数据，则表示该截取的待扫描流量数据需要继续扫描，如果是静态数据，则可以剔除掉，从而可以使得需要继续扫描的待扫描流量数据的量减少，提高扫描效率。其中机器学习的模型可以是预先设置好的，例如通过历史待扫描数据形成训练集和测试集等生成该机器学习的模型，其中训练集用于训练形成初始模型，测试集用于对初始模型进行修正，以保证模型的正确性。

[0056] S306：当所截取的待扫描流量数据是动态数据时，则查询待扫描流量数据是否存在参数。

[0057] 具体地，当第一步机器学习判断出该待扫描流量数据时动态数据时，则可以通过第二步机器学习判断该流量数据是否存在参数，只有存在参数的待扫描流量才会进行漏洞扫描，而没有参数的待扫描流量由于其一般不需要获取网络上服务器的资源等，因此不会进行漏洞扫描。在其他的实施例中，可以将两步机器学习集成在一个机器学习模型中，即待扫描流量数据当输入该集成的模型时，可以提出掉静态数据和无参数的待扫描流量数据。

[0058] S308：当待扫描流量数据存在参数时，则获取待扫描流量数据的类型。

[0059] 具体地，当待扫描流量数据为动态数据，且存在参数时，则标识该待扫描流量数据需要进行漏洞扫描，因此首先对获取到待扫描流量数据的类型，从而可以根据不同的类型获取到不同的漏洞扫描规则，进而减少漏洞扫描规则的执行。

[0060] S310：获取与待扫描流量数据的类型对应的漏洞扫描规则。

[0061] 具体地，待扫描流量数据的类型可以包括web流量或network流量等，根据该类型可以获取到对应的漏洞检测规则，从而可以减少漏洞检测规则的执行率。例如待扫描流量数据为web流量时，则直接获取到针对web流量的漏洞检测规则，而不需要执行全部的漏洞检测规则，提高漏洞检测规则的执行效率。

[0062] S312：通过漏洞扫描规则对待扫描流量数据进行漏洞扫描。

[0063] 具体地，漏洞扫描规则是指预先存储在扫描服务器中的规则，通过将待扫描流量数据与该漏洞扫描规则进行比较可以得到该待扫描流量数据是否为漏洞数据的结果，从而可以实现漏洞的扫描，例如当待扫描流量数据符合漏洞扫描规则时，则表示该待扫描流量数据为漏洞数据，因此需要后续拦截等以防止其正常访问，当待扫描流量数据不符合漏洞扫描规则时，则表示该待扫描流量数据不是漏洞数据，其可以正常进行访问，不需要后续进行拦截等操作。

[0064] 上述漏洞扫描方法，首先是截取待扫描流量数据，即当客户端存在数据访问时，则就会截取流量数据，使得待扫描流量数据的覆盖范围变大；其次，在漏洞扫描前，对不需要扫描的待扫描流量数据进行剔除，减少了待扫描流量数据的扫描量，提高了漏洞扫描效率；最后，根据待扫描流量数据的类型获取到对应的漏洞扫描规则，而不需要将数据库中所有的漏洞扫描规则均执行一遍，可以大大降低漏洞扫描规则的执行数量，从而也提高了漏洞扫描的效率。

[0065] 在其中一个实施例中，截取待扫描流量数据的步骤，即步骤S302之后，还可以包括：获取当前资源占用率；若当前资源占用率超过阈值时，则获取备扫描服务器的资源占用率；选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0066] 具体地，在该实施例中扫描服务器是以集群的形式存在的，设置一台主扫描服务器，当主扫描服务器截取到待扫描流量数据后，首先判断主扫描服务器的资源占用率，当主扫描服务器的当前资源占用率超过阈值时，则表示主扫描服务器的当前资源占用率较高，因此继续获取备扫描服务器的资源占用率，并获取到资源占用率最低的备扫描服务器来执行该漏洞扫描的方法，即判断所截取的待扫描流量数据是否为动态数据等。且在获取备扫描服务器的资源占用率时，还可以对该备扫描服务器的资源占用率进行排序，这样更加方便选取。其中当前资源占用率的阈值可以是根据经验进行确定，或者是根据系统压力测试时的测试峰值进行确定，例如根据所截取到的待扫描流量数据的量来确定不同的阈值等。

资源占用率可以是指扫描服务器的cpu的占用率等。

[0067] 上述实施例中，在截取到待扫描流量数据后，首先判断主扫描服务器的资源占用率，当主扫描服务器的资源占用率未超过阈值时，才会通过主扫描服务器进行漏洞扫描，当主扫描服务器的资源占用率超过阈值时，则启动备扫描服务器，由备扫描服务器进行漏洞扫描，可以保证系统的协调一致，正常运行。

[0068] 在其中一个实施例中，获取当前资源占用率的步骤之前还可以包括：判断当前扫描服务器是否出现故障；若当前扫描服务器未出现故障，则继续执行获取当前资源占用率的步骤；若当前扫描服务器出现故障，则获取备扫描服务器的资源占用率；选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0069] 具体地，在获取当前资源占用率的步骤之前，首先判断当前扫描服务器是否出现故障，如果未出现故障，则可以进一步判断当前资源占用率，并根据当前资源占用率来判断是否由当前扫描服务器来执行漏洞检测。如果当前扫描服务器出现故障，则选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤，而不需要先判断当前资源占用率，可以减少执行步骤，其中，资源占用率最低可以是指资源占用率小于资源占用率预设值，且最低的一个资源占用率；例如三台备扫描服务器：备扫描服务器A、备扫描服务器B、备扫描服务器C，其中备扫描服务器A的资源占用率为a，备扫描服务器B的资源占用率为b，备扫描服务器C的资源占用率为c，a大于资源占用率预设值m，b和c小于资源占用率预设值m，且b小于c，因此需要选取资源占用率b所对应的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤，且在本实施例中不对该资源占用率预设值进行具体限定，其可以是根据经验进行设置的。

[0070] 在实际使用时，扫描服务器采用分布式架构，多线程队列形式进行插件扫描或者规则匹配。例如可以设置一台主扫描服务器和多台备扫描服务器，接收到截取的流量时，首先判断主扫描服务器是否故障，如果主扫描服务器故障，则通过备扫描服务器进行扫描，其中也可以首先判断被扫描服务器是否出现故障，例如可以按照备扫描服务器的顺序一台一台地进行判断，当当前备扫描服务器出现故障，则按照顺序对下一台进行判断，直至出现没有故障的备扫描服务器。如果主扫描服务器未出现故障，则获取主扫描服务器当前的资源占用率，当资源占用率超过阈值时，则通过备扫描服务器进行扫描，例如可以首先获取到备扫描服务器当前的资源占用率，然后进行排序，选择资源占用率低的备扫描服务器进行扫描。

[0071] 上述实施例中，在截取待扫描流量数据后，首先判断当前扫描服务器是否出现故障，如果出现故障，则直接选取备扫描服务器进行漏洞扫描，如果没有出现故障，则首先判断当前扫描服务器的资源占用率，当当前扫描服务器的资源占用率未超过阈值时，才会通过当前扫描服务器进行漏洞扫描，当当前扫描服务器的资源占用率超过阈值时，则启动其他扫描服务器，由其他扫描服务器进行漏洞扫描，可以保证系统的协调一致，正常运行。

[0072] 在其中一个实施例中，截取待扫描流量数据的步骤，即步骤S302之后，还包括：统计截取待扫描流量数据的截取次数；根据截取次数启动对应数量的扫描服务器；将待扫描流量数据分配至所启动的扫描服务器中以继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0073] 具体地，待扫描流量的截取次数是指扫描服务器所收到的漏洞扫描请求的次数，即通过核心交换机或路由器或代理服务器截取到待扫描流量后，该核心交换机或路由器或代理服务器则向扫描服务器发送漏洞扫描请求，该请求中携带有待扫描流量数据。扫描服务器控制系统根据截取次数启动对应数量的扫描服务器，将待扫描流量数据分配至所启动的扫描服务器中，从而多台扫描服务器一起对待扫描流量数据进行扫描。

[0074] 其中，根据所截取到的待扫描流量数据的截取次数，即获取针对待扫描流量数据进行扫描的请求的数量，根据该请求的数量启动对应的扫描服务器，然后根据负载均衡策略将所接收到的请求分配给对应的扫描服务器。例如，有3000个请求需要进行处理时，则开启的扫描服务器的数量是3个，根据负载均衡策略将这3000个请求按顺序的分配给这3台扫描服务器，3台扫描服务器将同时对请求进行处理，提高了扫描效率。且每台扫描服务器在扫描的时，可以采用多线程扫描，即每台扫描服务器接收到1000个请求时，开启50条线程，每条线程对20个请求中的待扫描流量数据进行扫描，这样可以进一步地提高效率。其中可以预设每台扫描服务器的处理峰值，并为每台扫描服务器预设处理等级，根据所接收到的请求的数量选取处理等级，例如当接收到的请求为第一数量，则处理等级为一级，当接收到的请求为第二数量，则处理等级为二级，一级时扫描服务器的处理请求的量为A，二级时扫描服务器的处理请求的量为B；根据所接收到的请求的数量选取处理等级，假设选取的处理等级为一级，则根据所接收到的请求的数量N与一级时扫描服务器的处理请求的量为A得到需要启动的扫描服务器的台数＝N/A；然后根据数量A确定每台扫描服务器需要启动的线程数，从而实现对请求的并行处理，提高处理效率。

[0075] 上述实施例中，根据所截取到的流量的次数，即获取针对流量进行扫描的请求的数量，根据该请求的数量启动对应的扫描服务器，然后根据负载均衡策略将所接收到的请求分配给对应的扫描服务器，提高了处理效率。

[0076] 在其中一个实施例中，通过漏洞扫描规则对待扫描流量数据进行漏洞扫描的步骤之后，还可以包括：接收针对待扫描流量数据的漏洞扫描规则调整指令；根据漏洞扫描规则调整指令获取漏洞扫描补充规则；通过漏洞扫描补充规则对待扫描流量数据进行漏洞扫描。

[0077] 具体地，一般情况下对不同类型的待扫描流量数据只需要通过与之对应的漏洞扫描规则进行扫描即可，但是在特殊情况下，该待扫描流量数据的扫描结果可能存在问题，为了避免该问题的出现，可以将待扫描流量数据的扫描结果均展示在UI界面上，通过该UI界面可以接收到针对待扫描流量数据的漏洞扫描规则调整指令，例如针对web流量，扫描服务器可能首先通过web流量漏洞扫描规则进行扫描后，输出扫描结果，但是测试人员可能认为本次扫描不够完善，则可以再调用network流量扫描规则对该web流量进行再次扫描，即根据漏洞扫描规则调整指令获取漏洞扫描补充规则；通过漏洞扫描补充规则对待扫描流量数据进行漏洞扫描，从而可以提高漏洞扫描规则的准确率。

[0078] 上述实施例中，还可以包括接收漏洞扫描规则调整指令，根据漏洞扫描规则调整指令获取其他类型的漏洞扫描规则对该流量进行进一步的扫描。即通过web应用服务对系统进行配置，该实施例中，不仅支持流量的动态扫描，还支持人工干预，从而可以对重点流量进行全方位的扫描，提高漏洞扫描的准确率。

[0079] 在其中一个实施例中，截取待扫描流量数据的步骤可以包括通过预先设置在客户

端的代理程序截取待扫描流量数据。或者截取待扫描流量数据的步骤可以包括：接收核心交换机根据所截取到的待扫描流量数据生成的镜像流量数据作为待扫描流量数据。

[0080] 具体地，可以在主干或主链路节点中进行流量截取，利于可以预先在客户端设置代理，当终端安装的客户端存在流量数据的发送时，则通过该预先设置在客户端的代理程序截取到待扫描流量数据。或者在核心交换机或路由器接收到客户端发送的流量数据时，核心交换机或路由器将该流量数据进行镜像，并将流量数据的镜像发送到待扫描服务器以实现待扫描流量数据的截取。

[0081] 上述实施例中，通过在主干或主链路节点中进行流量截取，并将该截取到的待扫描流量数据发送到扫描服务器，实现扫描服务器对待扫描流量数据的被动扫描，而不需要像传统中爬取流量数据，从而可以保证待扫描流量数据的完整性。

[0082] 应该理解的是，虽然图3的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图3中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0083] 在一个实施例中，如图4所示，提供了一种漏洞扫描装置，包括：流量截取模块、数据判断模块、查询模块、流量类型获取模块、规则获取模块和扫描模块，其中：

[0084] 流量截取模块100，用于截取待扫描流量数据。

[0085] 数据判断模块200，用于判断所截取的待扫描流量数据是否为动态数据。

[0086] 查询模块300，用于当所截取的待扫描流量数据是动态数据时，则查询待扫描流量数据是否存在参数。

[0087] 流量类型获取模块400，用于当待扫描流量数据存在参数时，则获取待扫描流量数据的类型。

[0088] 规则获取模块500，用于获取与待扫描流量数据的类型对应的漏洞扫描规则。

[0089] 扫描模块600，用于通过漏洞扫描规则对待扫描流量数据进行漏洞扫描。

[0090] 在其中一个实施例中，装置还可以包括：

[0091] 资源占用率获取模块，用于在截取待扫描流量数据之后，获取当前资源占用率；若当前资源占用率超过阈值时，则获取备扫描服务器的资源占用率。

[0092] 扫描模块还用于选取备扫描服务器的资源占用率最低的备扫描服务器继续判断所截取的待扫描流量数据是否为动态数。

[0093] 在其中一个实施例中，装置还可以包括：

[0094] 故障判断模块，用于在获取当前资源占用率之前，判断当前扫描服务器是否出现故障。

[0095] 资源占用率获取模块还用于若当前扫描服务器未出现故障，则继续获取当前资源占用率；若当前扫描服务器出现故障，则获取备扫描服务器的资源占用率。

[0096] 扫描模块还用于选取备扫描服务器的资源占用率最低的备扫描服务器继续判断所截取的待扫描流量数据是否为动态数据。

[0097] 在其中一个实施例中，装置还可以包括：

[0098] 统计模块，用于在截取待扫描流量数据之前，统计截取待扫描流量数据的截取次数。

[0099] 启动模块，用于根据截取次数启动对应数量的扫描服务器。

[0100] 数据判断模块还用于将待扫描流量数据分配至所启动的扫描服务器中以继续判断所截取的待扫描流量数据是否为动态数据。

[0101] 在其中一个实施例中，装置还可以包括：

[0102] 接收模块，用于在通过漏洞扫描规则对待扫描流量数据进行漏洞扫描之后，接收针对待扫描流量数据的漏洞扫描规则调整指令。

[0103] 补充规则获取模块，用于根据漏洞扫描规则调整指令获取漏洞扫描补充规则。

[0104] 补充扫描模块，用于通过漏洞扫描补充规则对待扫描流量数据进行漏洞扫描。

[0105] 在其中一个实施例中，截取模块还可以用于通过预先设置在客户端的代理程序截取待扫描流量数据。

[0106] 在其中一个实施例中，截取模块还可以用于接收核心交换机根据所截取到的待扫描流量数据生成的镜像流量数据作为待扫描流量数据。

[0107] 关于漏洞扫描装置的具体限定可以参见上文中对于漏洞扫描方法的限定，在此不再赘述。上述漏洞扫描装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0108] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图5所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储漏洞扫描规则数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种漏洞扫描方法。

[0109] 本领域技术人员可以理解，图5中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0110] 在一个实施例中，提供了一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行计算机程序时实现以下步骤：截取待扫描流量数据；判断所截取的待扫描流量数据是否为动态数据；当所截取的待扫描流量数据是动态数据时，则查询待扫描流量数据是否存在参数；当待扫描流量数据存在参数时，则获取待扫描流量数据的类型；获取与待扫描流量数据的类型对应的漏洞扫描规则；通过漏洞扫描规则对待扫描流量数据进行漏洞扫描。

[0111] 在其中一个实施例中处理器执行计算机程序时所实现的截取待扫描流量数据的步骤之后，还可以包括：获取当前资源占用率；若当前资源占用率超过阈值时，则获取备扫描服务器的资源占用率；选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0112] 在其中一个实施例中处理器执行计算机程序时所实现的获取当前资源占用率的

步骤之前，还可以包括：判断当前扫描服务器是否出现故障；若当前扫描服务器未出现故障，则继续执行获取当前资源占用率的步骤；若当前扫描服务器出现故障，则获取备扫描服务器的资源占用率；选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0113] 在其中一个实施例中处理器执行计算机程序时所实现的截取待扫描流量数据的步骤之后，还可以包括：统计截取待扫描流量数据的截取次数；根据截取次数启动对应数量的扫描服务器；将待扫描流量数据分配至所启动的扫描服务器中以继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0114] 在其中一个实施例中处理器执行计算机程序时所实现的通过漏洞扫描规则对待扫描流量数据进行漏洞扫描的步骤之后，还可以包括：接收针对待扫描流量数据的漏洞扫描规则调整指令；根据漏洞扫描规则调整指令获取漏洞扫描补充规则；通过漏洞扫描补充规则对待扫描流量数据进行漏洞扫描。

[0115] 在其中一个实施例中处理器执行计算机程序时所实现的截取待扫描流量数据的步骤，可以包括：通过预先设置在客户端的代理程序截取待扫描流量数据。

[0116] 在其中一个实施例中处理器执行计算机程序时所实现的截取待扫描流量数据的步骤，可以包括：接收核心交换机根据所截取到的待扫描流量数据生成的镜像流量数据作为待扫描流量数据。

[0117] 在一个实施例中，提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现以下步骤：截取待扫描流量数据；判断所截取的待扫描流量数据是否为动态数据；当所截取的待扫描流量数据是动态数据时，则查询待扫描流量数据是否存在参数；当待扫描流量数据存在参数时，则获取待扫描流量数据的类型；获取与待扫描流量数据的类型对应的漏洞扫描规则；通过漏洞扫描规则对待扫描流量数据进行漏洞扫描。

[0118] 在一个实施例中，计算机程序被处理器执行时所实现的截取待扫描流量数据的步骤之后，还可以包括：获取当前资源占用率；若当前资源占用率超过阈值时，则获取备扫描服务器的资源占用率；选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0119] 在一个实施例中，计算机程序被处理器执行时所实现的获取当前资源占用率的步骤之前，还可以包括：判断当前扫描服务器是否出现故障；若当前扫描服务器未出现故障，则继续执行获取当前资源占用率的步骤；若当前扫描服务器出现故障，则获取备扫描服务器的资源占用率；选取备扫描服务器的资源占用率最低的备扫描服务器继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0120] 在一个实施例中，计算机程序被处理器执行时所实现的截取待扫描流量数据的步骤之后，还可以包括：统计截取待扫描流量数据的截取次数；根据截取次数启动对应数量的扫描服务器；将待扫描流量数据分配至所启动的扫描服务器中以继续执行判断所截取的待扫描流量数据是否为动态数据的步骤。

[0121] 在一个实施例中，计算机程序被处理器执行时所实现的通过漏洞扫描规则对待扫描流量数据进行漏洞扫描的步骤之后，还可以包括：接收针对待扫描流量数据的漏洞扫描规则调整指令；根据漏洞扫描规则调整指令获取漏洞扫描补充规则；通过漏洞扫描补充规

则对待扫描流量数据进行漏洞扫描。

[0122] 在一个实施例中，计算机程序被处理器执行时所实现的截取待扫描流量数据的步骤，可以包括：通过预先设置在客户端的代理程序截取待扫描流量数据。

[0123] 在一个实施例中，计算机程序被处理器执行时所实现的截取待扫描流量数据的步骤，可以包括：接收核心交换机根据所截取到的待扫描流量数据生成的镜像流量数据作为待扫描流量数据。

[0124] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0125] 以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0126] 以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

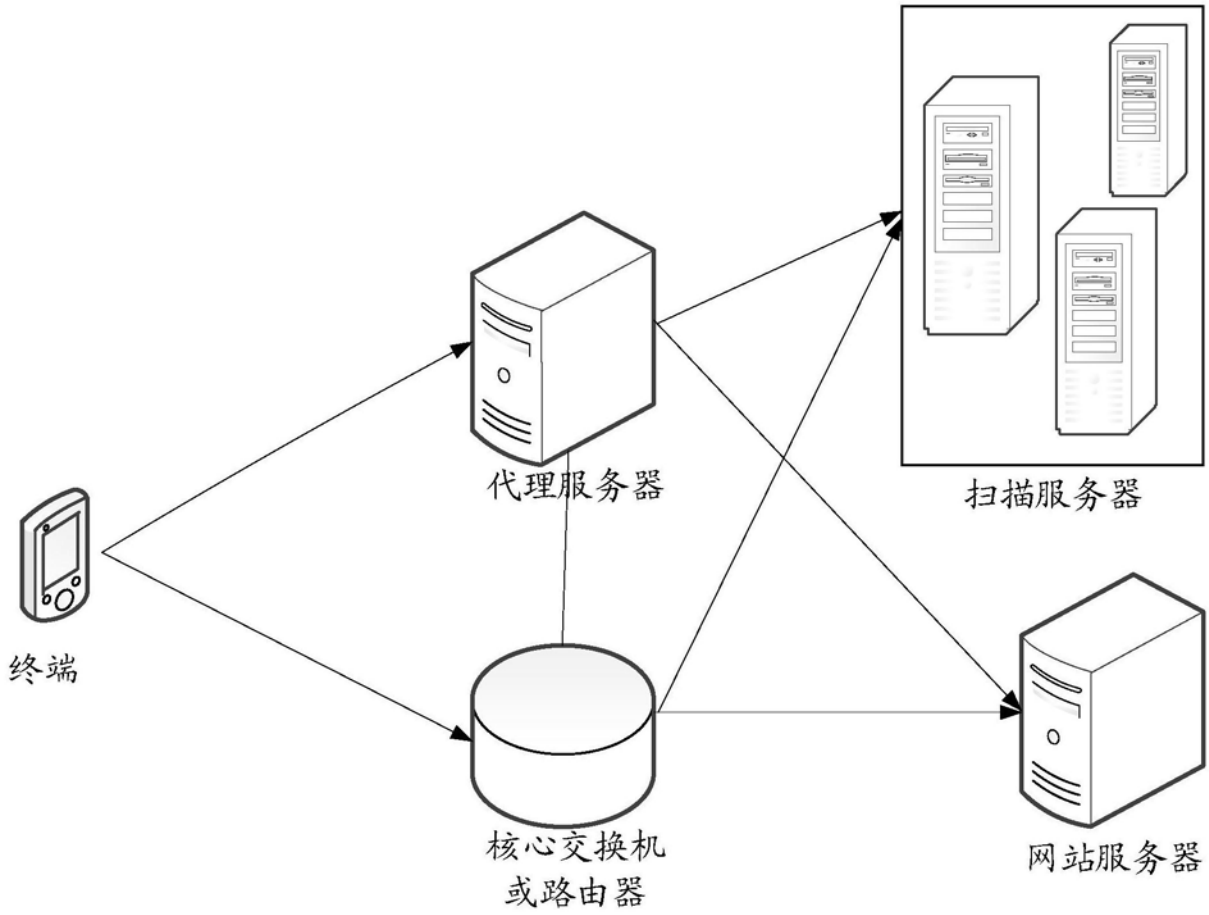


图1

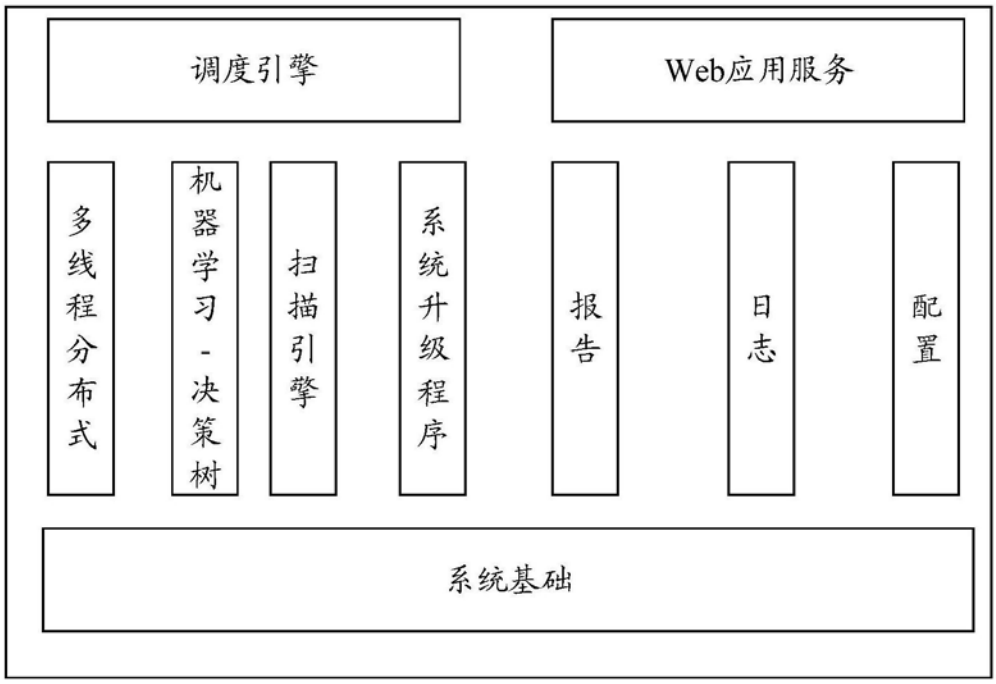


图2

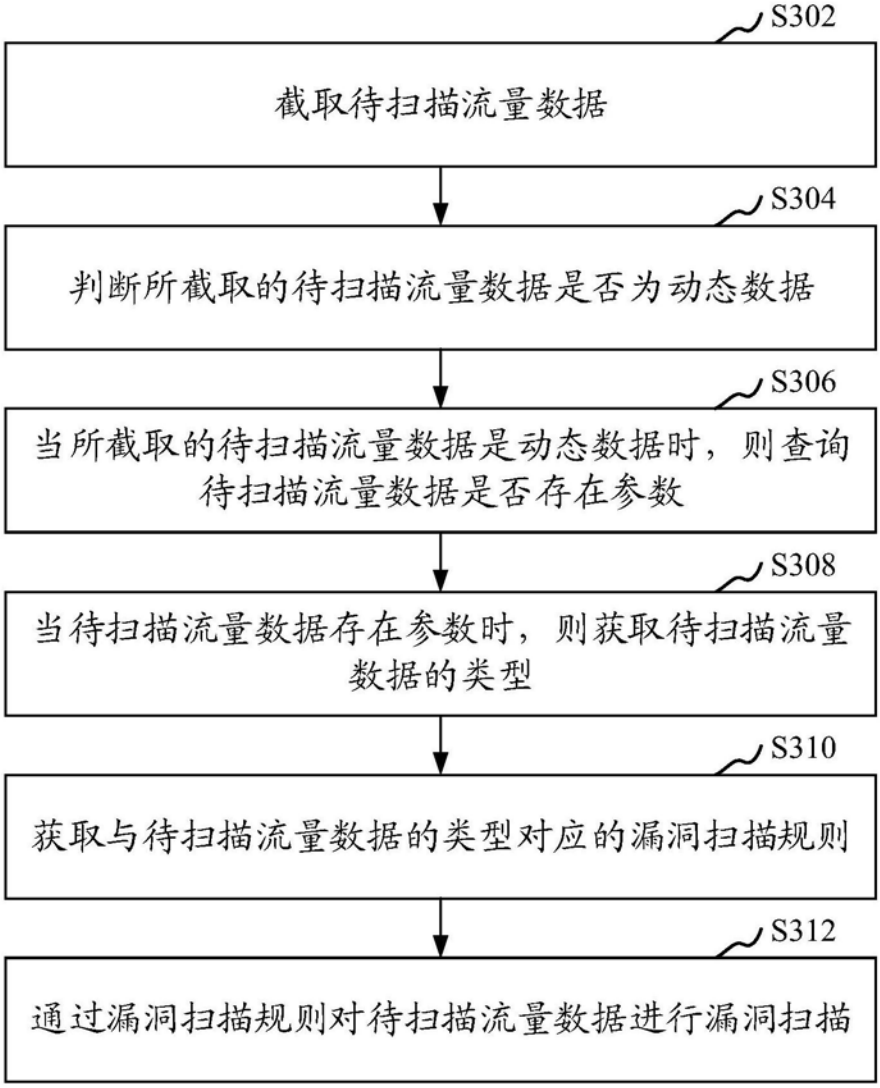

S302
截取待扫描流量数据
S304
判断所截取的待扫描流量数据是否为动态数据
S306
当所截取的待扫描流量数据是动态数据时，则查询待扫描流量数据是否存在参数
S308
当待扫描流量数据存在参数时，则获取待扫描流量数据的类型
S310
获取与待扫描流量数据的类型对应的漏洞扫描规则
S312
通过漏洞扫描规则对待扫描流量数据进行漏洞扫描

图3

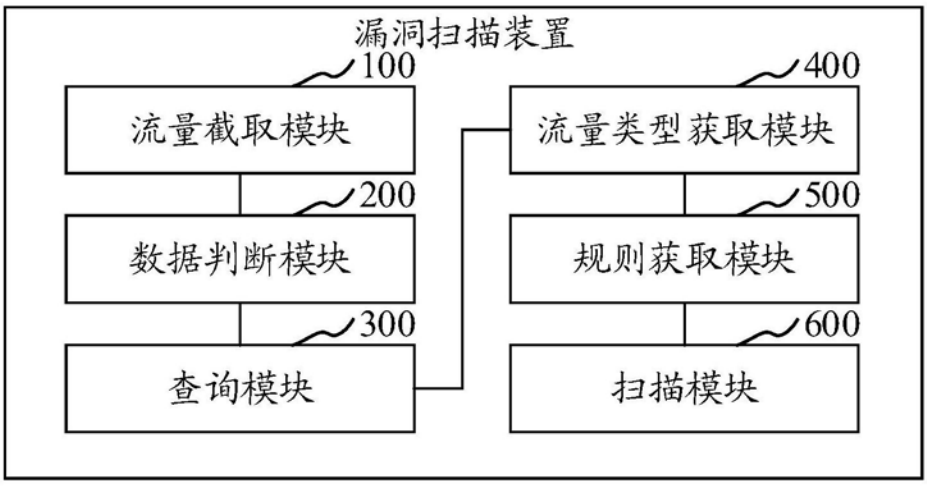

漏洞扫描装置
100
流量截取模块
200
数据判断模块
300
查询模块
400
流量类型获取模块
500
规则获取模块
600
扫描模块

图4

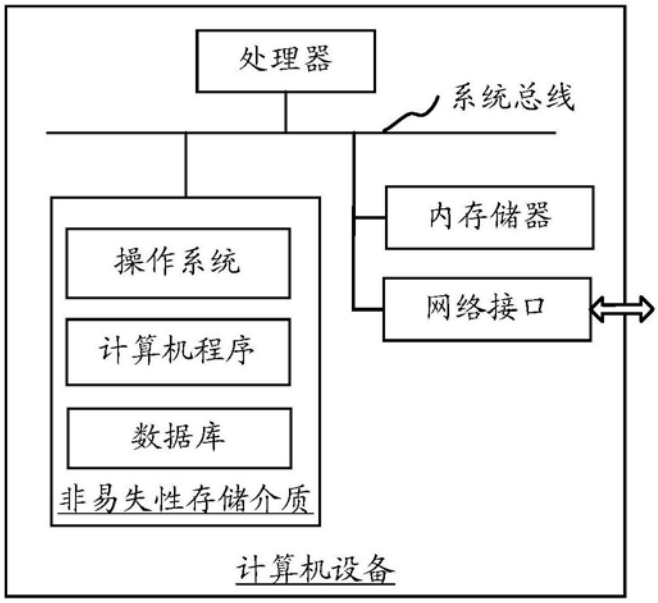


图5