(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114884801 B
(45)授权公告日 2024.09.24

(21)申请号 202210647322.X

(22)申请日 2022.06.09

(65)同一申请的已公布的文献号
申请公布号 CN 114884801 A

(43)申请公布日 2022.08.09

(73)专利权人 奇安信科技集团股份有限公司
地址 100032 北京市西城区新街口外大街28号102号楼3层332号
专利权人 奇安信网神信息技术(北京)股份有限公司

(72)发明人 赵伟

(74)专利代理机构 北京维飞联创知识产权代理有限公司 11857
专利代理师 樊阳阳

(51)Int.Cl.
H04L 41/0631(2022.01)
H04L 9/40(2022.01)

(56)对比文件
CN 114328139 A,2022.04.12
CN 114218577 A,2022.03.22
CN 113645232 A,2021.11.12

审查员 黎雨婷

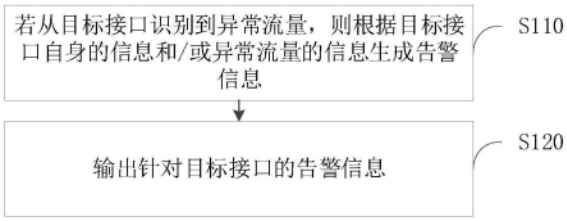
权利要求书2页 说明书9页 附图1页

(54)发明名称

告警方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种告警方法、装置、电子设备及存储介质，涉及安全技术领域。该方法在从目标接口识别到异常流量时，根据目标接口自身的信息和/或异常流量的信息来生成告警信息，并输出告警信息，如此的生成的告警信息可包含接口和/或异常流量的相关描述信息，实现更细粒度的告警，从而使得运维人员根据告警信息即可知晓接口的紧急处理程度，进而及时采取相应措施进行处理，有效提高了运维效率。



CN 114884801 B

1.一种告警方法,其特征在于,所述方法包括:

若从目标接口识别到异常流量,则根据所述目标接口自身的信息和所述异常流量的信息生成告警信息;

输出针对所述目标接口的所述告警信息;

其中,所述根据所述目标接口自身的信息和所述异常流量的信息生成告警信息,包括:

根据所述目标接口的业务属性确定对所述目标接口的处理优先级,以及,根据所述异常流量的异常情况确定所述异常流量的威胁等级;

根据所述处理优先级和所述威胁等级生成告警信息,所述告警信息包括所述处理优先级和所述威胁等级;

其中,所述根据所述异常流量的异常情况确定所述异常流量的威胁等级之后,所述输出针对所述目标接口的所述告警信息之前,还包括:

基于所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级;

其中,所述基于所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级,包括:

获取所述目标接口的历史访问信息;

根据所述历史访问信息以及所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级;

其中,所述根据所述历史访问信息以及所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级,包括:

根据所述历史访问信息确定初始优先级,其中,预先配置有所述历史访问信息与所述初始优先级的映射关系;

将所述初始优先级与所述威胁等级进行加权求和,得到调整量;

根据所述调整量对所述处理优先级进行调整,其中,调整后的处理优先级与所述威胁等级正相关。

2.根据权利要求1所述的方法,其特征在于,所述根据所述异常流量的异常情况确定所述异常流量的威胁等级,包括:

分析所述异常流量的攻击类别;

根据所述攻击类别确定所述异常流量的威胁等级。

3.根据权利要求1所述的方法,其特征在于,所述根据所述目标接口的业务属性确定对所述目标接口进行处理的处理优先级,包括:

根据所述目标接口的业务属性查找优先级映射表中所述业务属性对应的处理优先级,以获得对所述目标接口进行处理的处理优先级。

4.根据权利要求1所述的方法,其特征在于,通过以下方式获取所述目标接口的业务属性,包括:

获取所述目标接口的接口信息,所述接口信息包括接口命名和/或接口参数;

根据所述接口信息获取所述目标接口的业务属性。

5.根据权利要求1所述的方法,其特征在于,所述输出针对所述目标接口的所述告警信息,包括:

按照告警信息的处理优先级或威胁等级对告警信息进行排序输出。

6.根据权利要求1-5任一所述的方法,其特征在于,通过以下方式识别从所述目标接口接收到的流量是否为异常流量:

通过神经网络模型对从所述目标接口接收到的流量进行异常检测,以确定所述流量是否为异常流量。

7.一种告警装置,其特征在于,所述装置包括:

告警信息生成模块,用于若从目标接口识别到异常流量,则根据所述目标接口自身的信息和所述异常流量的信息生成告警信息;

告警信息输出模块,用于输出针对所述目标接口的所述告警信息;

其中,所述告警信息生成模块,具体用于根据所述目标接口的业务属性确定对所述目标接口的处理优先级,以及,根据所述异常流量的异常情况确定所述异常流量的威胁等级;根据所述处理优先级和所述威胁等级生成告警信息,所述告警信息包括所述处理优先级和所述威胁等级;

其中,所述装置还包括:

优先级调整模块,用于基于所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级;

其中,所述优先级调整模块,具体用于获取所述目标接口的历史访问信息;根据所述历史访问信息以及所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级;

其中,所述优先级调整模块,具体用于根据所述历史访问信息确定初始优先级,其中,预先配置有所述历史访问信息与所述初始优先级的映射关系;将所述初始优先级与所述威胁等级进行加权求和,得到调整量;根据所述调整量对所述处理优先级进行调整,其中,调整后的处理优先级与所述威胁等级正相关。

8.一种电子设备,其特征在于,包括处理器以及存储器,所述存储器存储有计算机可读取指令,当所述计算机可读取指令由所述处理器执行时,运行如权利要求1-6任一所述的方法。

9.一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运行如权利要求1-6任一所述的方法。

告警方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及安全技术领域,具体而言,涉及一种告警方法、装置、电子设备及存储介质。

背景技术

[0002] 应用程序接口(Application Programming Interface,API)作为数据交互的重要接口,直接且纯粹的将数据与服务提供给用户,所以对API的数据安全、权限安全以及用户行为安全越来越重视。

[0003] 在API遭受攻击时,为了使得运维人员能够及时处理,一般系统会输出告警信息,但是目前输出的告警信息的含义比较笼统,比如接口访问频繁,这就使得运维人员经常无法明确其具体含义而容易将其忽略,可能导致对一些产生告警的重要的接口的处理滞后,运维效率较低。

发明内容

[0004] 本申请实施例的目的在于提供一种告警方法、装置、电子设备及存储介质,用以改善现有技术中输出的告警信息的含义不明确,无法使得运维人员及时对一些重要接口进行处理,运维效率低的问题。

[0005] 第一方面,本申请实施例提供了一种告警方法,所述方法包括:

[0006] 若从目标接口识别到异常流量,则根据所述目标接口自身的信息和/或所述异常流量的信息生成告警信息;

[0007] 输出针对所述目标接口的所述告警信息。

[0008] 在上述实现过程中,该方法在从目标接口识别到异常流量时,根据目标接口自身的信息和/或异常流量的信息来生成告警信息,并输出告警信息,如此的生成的告警信息可包含接口和/或异常流量的相关描述信息,实现更细粒度的告警,从而使得运维人员根据告警信息即可知晓接口的紧急处理程度,进而及时采取相应措施进行处理,有效提高了运维效率。

[0009] 可选地,所述根据所述目标接口自身的信息和/或所述异常流量的信息生成告警信息,包括:

[0010] 根据所述目标接口的业务属性确定对所述目标接口的处理优先级,和/或,根据所述异常流量的异常情况确定所述异常流量的威胁等级;

[0011] 根据所述处理优先级和/或所述威胁等级生成告警信息,所述告警信息包括所述处理优先级和/或所述威胁等级。

[0012] 在上述实现过程中,输出的告警信息中包含处理优先级和/或威胁等级,使得输出的告警信息的含义更加明确,这样运维人员可根据处理优先级和/或威胁等级即可知晓哪些告警信息应该优先处理,哪些告警信息可以靠后处理,进而可先对需要优先处理的接口进行处理,提高运维效率。

[0013] 可选地,所述根据所述异常流量的异常情况确定所述异常流量的威胁等级,包括:

[0014] 分析所述异常流量的攻击类别;

[0015] 根据所述攻击类别确定所述异常流量的威胁等级。

[0016] 在上述实现过程中,根据攻击类别确定威胁等级,如此可针对不同的攻击类别确定不同的威胁等级,从而可根据接口所遭受的实际攻击来判断接口当前受攻击的威胁程度。

[0017] 可选地,所述根据所述目标接口的业务属性确定对所述目标接口进行处理的处理优先级,包括:

[0018] 根据所述目标接口的业务属性查找优先级映射表中所述业务属性对应的处理优先级,以获得对所述目标接口进行处理的处理优先级。针对接口的业务属性设置不同的处理优先级,如此可针对业务重要性来选择处理顺序,针对一些重要的接口可设置较高的处理优先级,这样在运维过程中,可有效确保这些重要接口的安全性。

[0019] 可选地,所述根据所述异常流量的异常情况确定所述异常流量的威胁等级之后,所述输出针对所述目标接口的所述告警信息之前,还包括:

[0020] 基于所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级。这样可根据接口所遭受的攻击程度来灵活调整处理优先级,使得处理优先级能够适配当前的攻击,如攻击程度严重,则处理优先级应该更高。

[0021] 可选地,所述基于所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级,包括:

[0022] 获取所述目标接口的历史访问信息;

[0023] 根据所述历史访问信息以及所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级。如此可以根据该接口的实际访问情况来确定一个更合适的处理优先级。

[0024] 可选地,通过以下方式获取所述目标接口的业务属性,包括:

[0025] 获取所述目标接口的接口信息,所述接口信息包括接口命名和/或接口参数;

[0026] 根据所述接口信息获取所述目标接口的业务属性。

[0027] 在上述实现过程中,通过接口命名和/或接口参数可快速获取到接口的业务属性。

[0028] 可选地,所述输出针对所述目标接口的所述告警信息,包括:

[0029] 按照告警信息的处理优先级或威胁等级对告警信息进行排序输出。如此运维人员可直接按照排序顺序进行处理,省去了手动筛选操作。

[0030] 可选地,通过以下方式识别从所述目标接口接收到的流量是否为异常流量:

[0031] 通过神经网络模型对从所述目标接口接收到的流量进行异常检测,以确定所述流量是否为异常流量。如此可实现异常流量的准确检测。

[0032] 第二方面,本申请实施例提供了一种告警装置,所述装置包括:

[0033] 告警信息生成模块,用于若从目标接口识别到异常流量,则根据所述目标接口自身的信息和/或所述异常流量的信息生成告警信息;

[0034] 告警信息输出模块,用于输出针对所述目标接口的所述告警信息。

[0035] 第三方面,本申请实施例提供一种电子设备,包括处理器以及存储器,所述存储器存储有计算机可读取指令,当所述计算机可读取指令由所述处理器执行时,运行如上述第一方面提供的所述方法中的步骤。

[0036] 第四方面,本申请实施例提供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运行如上述第一方面提供的所述方法中的步骤。

[0037] 第五方面,本申请实施例提供一种计算机程序产品,包括计算机程序指令,所述计算机程序指令被处理器读取并运行时,执行第一方面提供的方法中的步骤。

[0038] 本申请的其他特征和优点将在随后的说明书阐述,并且,部分地从说明书中变得显而易见,或者通过实施本申请实施例了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0039] 为了更清楚地说明本申请实施例的技术方案,下面将对本申请实施例中所需要使用的附图作简单地介绍,应当理解,以下附图仅示出了本申请的某些实施例,因此不应被看作是对范围的限定,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他相关的附图。

[0040] 图1为本申请实施例提供的一种告警方法的流程图;

[0041] 图2为本申请实施例提供的一种告警装置的结构框图;

[0042] 图3为本申请实施例提供的一种用于执行告警方法的电子设备的结构示意图。

具体实施方式

[0043] 下面将结合本申请实施例中附图,对本申请实施例中的技术方案进行清楚、完整地描述。

[0044] 需要说明的是,本发明实施例中的术语“系统”和“网络”可被互换使用。“多个”是指两个或两个以上,鉴于此,本发明实施例中也可以将“多个”理解为“至少两个”。“和/或”,描述关联对象的关联关系,表示可以存在三种关系,例如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况。另外,字符“/”,如无特殊说明,一般表示前后关联对象是一种“或”的关系。

[0045] 本申请实施例提供了一种告警方法,该方法在从目标接口识别到异常流量时,根据目标接口自身的信息和/或异常流量的信息来生成告警信息,并输出告警信息,如此的生成的告警信息可包含接口和/或异常流量的相关描述信息,实现更细粒度的告警,从而使得运维人员根据告警信息即可知晓接口的紧急处理程度,进而及时采取相应措施进行处理,避免接口因为遭受攻击而造成较大的损失,本方案可有效提高运维效率。

[0046] 请参照图1,图1为本申请实施例提供的一种告警方法的流程图,该方法包括如下步骤:

[0047] 步骤S110:若从目标接口识别到异常流量,则根据目标接口自身的信息和/或异常流量的信息生成告警信息。

[0048] 其中,目标接口可以是指检测设备上的任意一个接口,检测设备如网关、交换机、路由器等设备,本申请实施例中所指的接口均可以理解为是应用程序接口,即API。为了避免检测设备被非法攻击,以确保其安全性,可以对检测设备上的各个接口出入的流量进行安全检测,并在异常时进行相应告警,以使得运维人员可以及时采取相应措施进行处理。

[0049] 例如,针对某个接口的流量,可以对其流量进行异常检测,若识别到该流量是异常

流量,则可根据接口自身的信息和/或异常流量的信息生成告警信息。这里可以理解为生成的告警信息中携带了接口自身的相关信息和/或异常流量的相关信息,如此运维人员在看到告警信息后即可知晓该接口的异常程度,如受威胁程度,进而可直接根据告警信息来选择是否紧急处理等。

[0050] 步骤S120:输出针对目标接口的告警信息。

[0051] 这里输出告警信息是指输出告警信息给运维人员,如将告警信息输出至运维人员的终端设备,使得运维人员可以看到告警信息,告警信息可携带有目标接口自身的信息,如目标接口的名称、参数等相关信息(这样运维人员可看到这些信息可知晓这个接口是否是需要紧急处理的接口),和/或携带有异常流量的相关信息,如异常流量的异常情况,包括异常类型、异常程度等,如对于登录接口来说,其异常情况可包含登录次数过多、登录IP异常等,对于数据接口,如异常情况可包括敏感数据爬取、数据攻击等。当然,从不同接口所接收到的异常流量的异常情况不同。

[0052] 在上述实现过程中,该方法在从目标接口识别到异常流量时,根据目标接口自身的信息和/或异常流量的信息来生成告警信息,并输出告警信息,如此的生成的告警信息可包含接口和/或异常流量的相关描述信息,实现更细粒度的告警,从而使得运维人员根据告警信息即可知晓接口的紧急处理程度,进而及时采取相应措施进行处理,有效提高了运维效率。

[0053] 在上述实施例的基础上,根据目标接口自身的信息和/或异常流量的信息生成告警信息,可以理解为,可以根据目标接口自身的信息生成告警信息,也可以根据异常流量的信息生成告警信息,也可以根据目标接口自身的信息和异常流量的信息生成告警信息。

[0054] 这里目标接口自身的信息可以是指目标接口的业务属性,业务属性可以理解为是接口的业务标签,如登录接口,其业务属性为登录,如数据下载接口,其业务属性为数据下载,如敏感数据接口,其业务属性为敏感数据。对于不同的接口可相应设置不同的业务属性,这里的业务属性可以是预先针对各个接口设置好的,即针对各个接口构建了一张业务属性表,业务属性表中存储了各个接口的名称或参数与其业务属性的对应关系,所以,在确定目标接口的业务属性时,可以直接从业务属性表中查找得到目标接口对应的业务属性。

[0055] 根据目标接口的业务属性可确定目标接口对应的处理优先级,这里的处理优先级也可以是预先配置的,如针对不同的业务属性配置了不同的处理优先级,其业务属性与处理优先级的对应关系可通过优先级映射表进行存储。如在一些实施方式中,可以根据目标接口的业务属性查找优先级映射表中业务属性对应的处理优先级,以获得对目标接口进行处理的处理优先级。

[0056] 针对不同的接口可配置不同的处理优先级,如针对一些重要监控的接口,如数据接口,数据安全性更重要,所以可以设置更高的处理优先级,而对于一些无关紧要的接口,可设置较低的处理优先级。处理优先级可表明对接口进行处理的紧急程度,如当前有多个接口的流量均为异常流量,此时针对这些接口都会产生告警信息,处理优先级高则表明其处理紧急程度高,处理优先级低表明其处理紧急程度低,告警信息中若包含处理优先级,此时运维人员可根据告警信息中的处理优先级来按照相应的顺序来进行处理,如处理优先级高的优先处理,处理优先级低的可后处理。

[0057] 另外,还可以根据异常流量的异常情况确定异常流量的威胁等级,这里的威胁等

级可表示异常流量对目标接口的威胁程度,如威胁等级越高表明威胁程度越高,威胁等级越低表明威胁程度越低。

[0058] 异常流量的异常情况可如上述举例所示,如登录接口,可统计同一IP的登录次数,如果登录次数超过设定次数,则确定其为异常流量,其异常情况即为登录次数过多,或者,还可以判断登录IP是否为黑名单IP,若是,则确定其为异常流量,其异常情况即为登录IP异常。所以,可以对流量进行异常分析,以获得其异常情况,在实际应用中,可根据实际需求选择不同的分析方法进行异常分析。然后可根据异常情况确定对应的威胁等级,例如,如果登录次数过多所对应的威胁等级较高,登录IP异常所对应的威胁等级较低。

[0059] 在一些实施方式中,可以预先针对某个接口的流量的不同异常情况配置不同的威胁等级,这样可以在确定目标接口为异常流量后,分析异常流量的异常情况,然后根据异常情况来查找获得对应的威胁等级。

[0060] 可以理解地,这里的异常情况可包括攻击类别,即可分析异常流量的攻击类别,然后根据攻击类别来确定异常流量的威胁等级。

[0061] 其中攻击类别可理解为是异常类别,如上述的登录次数过多、登录IP异常等类别,由于不同的接口的业务属性不同,所以其所遭受的攻击类别也可能不同,如对于数据接口,其所遭受的攻击类别可为分敏感数据下载、非权限数据下载等,所以可以针对不同的攻击类别设置不同的威胁等级,当然这里的威胁等级可视某种攻击类别对接口的威胁程度来确定。如数据接口,如果敏感数据下载是内部比较重视的,则其对数据接口的威胁程度可能就较大,那么在设置威胁等级时,则可设置敏感数据下载的威胁等级大于非权限数据下载的威胁等级。

[0062] 若告警信息中包含威胁等级,则运维人员可根据告警信息中的威胁等级来判断该接口所受到的威胁程度,进而可及时采取相应的措施进行处理。

[0063] 若告警信息中包含处理优先级和威胁等级,则运维人员也可视处理优先级或威胁等级来选择是否进行紧急处理,如此本方案可实现对告警信息的明确输出,使得运维人员可以第一时间知晓其告警含义以及告警紧急程度。当然,为了细化告警信息,使得运维人员能够更明确其告警含义,告警信息中还可以包含接口的业务属性,如对于数据接口,其告警信息示例可如:数据接口遭受敏感数据下载攻击,威胁等级1,处理优先级1。相比于针对各个接口进行笼统的告警如“接口高频访问”来说,本方案可以细化对各个接口进行细化告警,使得运维人员无需自己筛选即可知晓哪些告警需要优先处理,进而提高运维效率。

[0064] 在上述实现过程中,输出的告警信息中包含处理优先级和/或威胁等级,使得输出的告警信息的含义更加明确,这样运维人员可根据处理优先级和/或威胁等级即可知晓哪些告警信息应该优先处理,哪些告警信息可以靠后处理,进而可先对需要优先处理的接口进行处理,提高了运维效率。

[0065] 在上述实施例的基础上,目标接口的业务属性也可以是实时确定的,如检测设备在识别到从目标接口接收到的流量为异常流量时,获取目标接口的接口信息,其接口信息包括接口命名和/或接口参数等,然后根据接口信息可获取目标接口的业务属性。

[0066] 其中,接口命名是指接口的名称,如“login”可表示是的登录接口,接口参数如username、password等字段,也可表示是登录接口,通过识别接口命名和/或接口参数即可知晓接口的业务属性,如示例中其接口的业务属性为“登录”。当然结合接口命名和接口参

数能够更准确地确定其接口的业务属性。

[0067] 或者,其业务属性也可以是第一次从接口接收到流量后就对接口进行识别,然后为该接口标识上该业务属性,这样在识别到接口的异常流量后,通过标识的业务属性即可确定该接口的业务属性。或者也可以是预先就通过接口命名和/或接口参数这些接口信息识别到接口的业务属性后,为接口标识对应的业务属性,如此后续也可直接确定接口的业务属性。

[0068] 在上述实施例的基础上,检测设备可以通过一些配置好的规则来识别从接口接收到的流量是否为异常流量,如登录接口,可判断其登录次数是否超过设定次数,若是,则为异常流量,或者判断其登录IP是否在黑名单中,若是,则为异常流量,反之,则不是异常流量。

[0069] 而为了更准确地进行异常流量的检测,还可以通过神经网络模型对从目标接口接收到的流量进行异常检测,以确定该流量是否为异常流量。

[0070] 这里的神经网络模型的类型可以根据实际需求灵活选择,如长短期记忆网络模型、生成式对抗网络模型等。神经网络模型可以预先通过大量的流量进行训练,在训练过程中可使得神经网络模型学习到流量中的异常特征,从而实现异常检测。对于其具体的检测过程在此不再过多赘述。

[0071] 在上述实施例的基础上,由于处理优先级是预先人为根据接口的业务属性所设置的,其包含了一些主观考虑因素,但是在实际情况中,接口所受的攻击程度跟其处理优先级是紧密关联的,所以还可以在根据业务属性确定目标接口的处理优先级以及根据异常流量的异常情况确定异常流量的威胁等级之后,还包括:基于威胁等级对处理优先级进行调整,获得调整后的处理优先级。

[0072] 可以认为先根据业务属性确定的目标接口的处理优先级是初始的处理优先级,然后可以根据实际所确定的威胁等级来对处理优先级进行相应调整。例如,初始的处理优先级为5,其等级较低,表示对目标接口的优先处理顺序靠后,而根据异常情况确定异常流量的威胁等级为1,其威胁等级较高,表示此时该接口正在遭受比较严重的攻击,需要引起运维人员的重视,所以可以根据威胁等级提高处理优先级,如将处理优先级调整为4或3等,即提高处理优先级的优先处理程度,而如果威胁等级也较低,如威胁等级为4,此时则表示接口遭受的攻击程度不严重,可不调整对应的处理优先级。

[0073] 或者,在调整时,可以根据威胁等级与处理优先级的适配程度来确定是否调整,比如可以预先设置威胁等级与处理优先级范围的对应关系,比如,威胁等级1,其对应处理优先级范围为1-2,表示正常的情况下,如果威胁等级是1,其处理优先级为1或2,如果当前确定的处理优先级不在这个范围,这可以将当前的处理优先级调整到这个范围,如当前确定的处理优先级为4,则其调整量可以为-2或-3,即将处理优先级调整为1或2,如果当前确定的处理优先级在这个范围,则不进行调整。所以,可以针对每个威胁等级配置对应的处理优先级范围,然后判断根据业务属性确定的处理优先级是否在当前确定的威胁等级对应的处理优先级范围内,如果是,则不进行调整,即调整量为0,如果不是,则将当前的处理优先级调整到威胁等级对应的处理优先级范围内即可。

[0074] 需要说明的是,具体的调整方式可以根据实际需求灵活设置,具体原则为威胁等级较高,但是处理优先级较低时,适当提高处理优先级,而威胁等级较低,但是处理优先级

较高时,适当降低处理优先级,两者均是中等等级时,则不进行调整。

[0075] 在上述实现过程中,可根据接口所遭受的攻击程度来灵活调整处理优先级,使得处理优先级能够适配当前的攻击,如攻击程度严重,则处理优先级应该更高。

[0076] 在上述实施例的基础上,在调整时,还可以考虑到接口的访问信息,如获取目标接口的历史访问信息,然后根据历史访问信息以及威胁等级对处理优先级进行调整,获得调整后的处理优先级。

[0077] 其历史访问信息可以包括历史访问量等,当然也可以包括在一段时间内的访问均值、访问方差、访问标准差等数据,这些数据可以间接反映该接口的历史访问情况。比如可以根据历史访问信息、威胁等级确定出一个调整量,其调整量的确定方式,可以是先将历史访问信息映射到一个初始优先级,然后再将初始优先级和威胁等级进行加权求和,然后确定出一个调整量,根据该调整量来对当前确定的处理优先级进行调整。

[0078] 其中,历史访问信息与初始优先级的映射关系可以是预先配置好的,如不同的历史访问量对应相应的初始优先级,历史访问量高,表示该接口比较重要,其优先级应该更高,所以可以配置高一点的初始优先级,历史访问量低,表示该接口可能不重要,可以配置低一点的初始优先级,这里初始优先级的配置可以根据不同的历史访问量范围来灵活配置。在将初始优先级与威胁等级进行加权求和时,其权重的设置可以根据实际需求设置,如威胁等级所占的权重可以大一点,而初始优先级所占的权重可以相对小一点,如此可根据威胁等级和初始优先级算出一个调整量,然后来对当前确定的处理优先级进行调整,当然这里在调整时,其根据调整量进行调高或降低处理优先级的原则可以是调整后的处理优先级与威胁等级正相关,即威胁等级越高,调整后的处理优先级也应越高,威胁等级越低,调整后的处理优先级也越低。

[0079] 例如,初始优先级为1,威胁等级为1,初始优先级的权重为0.6,威胁等级的权重为0.4,则加权求和后的调整量为1,如果当前确定的处理优先级为3,则其调整后的处理优先级为2,即将处理优先级调高。又如初始优先级为2,威胁等级为1,则加权求和后的调整量为1.6,当前确定的处理优先级为3,则调整后的处理优先级为1.4,四舍五入取整后为1。又如,初始优先级为2,威胁等级为3,则加权求和后的调整量为2.4,当前确定的处理优先级为2,由于此时威胁等级较低,所以应将处理优先级调低,则调整后的处理优先级为4.4,四舍五入取整后为4。

[0080] 需要说明的是,在实际应用中,根据历史访问信息和威胁等级来对处理优先级进行调整的方式不限于上述举例的方式,具体的调整方式可以根据实际需求灵活设置,其调整的目的是为了使得调整后的处理优先级与其威胁等级和历史访问信息适配,进而可获得一个更合适的处理优先级。

[0081] 在上述实施例的基础上,将告警信息输出给运维人员后,运维人员可根据处理优先级和/或威胁等级来对告警信息进行筛选,因为运维人员可能在短时间内会收到大量的告警信息,所以,通过处理优先级和/或威胁等级对告警信息进行筛选,可以快速筛选出需要优先处理的告警信息,进而对需要优先处理的接口及时进行处理。

[0082] 当然,为了减少运维人员的筛选操作,在输出告警信息时,还可以按照告警信息的处理优先级或威胁等级对告警信息进行排序输出。如按照处理优先级由高到低的顺序排序输出多个告警信息,或者按照威胁等级由高到低的顺序排序输出多个告警信息,如此运维

人员在处理告警信息时,可直接按照排序的顺序进行处理即可,无需自己筛选,因为排在前面的是需要优先处理的,如此可进一步提高运维效率。

[0083] 请参照图2,图2为本申请实施例提供的一种告警装置200的结构框图,该装置200可以是电子设备上的模块、程序段或代码。应理解,该装置200与上述图1方法实施例对应,能够执行图1方法实施例涉及的各个步骤,该装置200具体的功能可以参见上文中的描述,为避免重复,此处适当省略详细描述。

[0084] 可选地,所述装置200包括:

[0085] 告警信息生成模块210,用于若从目标接口识别到异常流量,则根据所述目标接口自身的信息和/或所述异常流量的信息生成告警信息;

[0086] 告警信息输出模块220,用于输出针对所述目标接口的所述告警信息。

[0087] 可选地,所述告警信息生成模块210,用于根据所述目标接口的业务属性确定对所述目标接口的处理优先级;和/或,根据所述异常流量的异常情况确定所述异常流量的威胁等级;根据所述处理优先级和/或所述威胁等级生成告警信息,所述告警信息包括所述处理优先级和/或所述威胁等级。

[0088] 可选地,所述告警信息生成模块210,用于分析所述异常流量的攻击类别;根据所述攻击类别确定所述异常流量的威胁等级。

[0089] 可选地,所述告警信息生成模块210,用于根据所述目标接口的业务属性查找优先级映射表中所述业务属性对应的处理优先级,以获得对所述目标接口进行处理的处理优先级。

[0090] 可选地,所述装置200还包括:

[0091] 优先级调整模块,用于基于所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级。

[0092] 可选地,所述优先级调整模块,用于获取所述目标接口的历史访问信息;根据所述历史访问信息以及所述威胁等级对所述处理优先级进行调整,获得调整后的处理优先级。

[0093] 可选地,所述告警信息生成模块210,用于获取所述目标接口的接口信息,所述接口信息包括接口命名和/或接口参数;根据所述接口信息获取所述目标接口的业务属性。

[0094] 可选地,所述告警信息输出模块220,用于按照告警信息的处理优先级或威胁等级对告警信息进行排序输出。

[0095] 可选地,所述告警信息生成模块210,用于通过神经网络模型对从所述目标接口接收到的流量进行异常检测,以确定所述流量是否为异常流量。

[0096] 需要说明的是,本领域技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的装置的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再重复描述。

[0097] 请参照图3,图3为本申请实施例提供的一种用于执行告警方法的电子设备的结构示意图,所述电子设备可以包括:至少一个处理器310,例如CPU,至少一个通信接口320,至少一个存储器330和至少一个通信总线340。其中,通信总线340用于实现这些组件直接的连接通信。其中,本申请实施例中设备的通信接口320用于与其他节点设备进行信令或数据的通信。存储器330可以是高速RAM存储器,也可以是非易失性的存储器(non-volatile memory),例如至少一个磁盘存储器。存储器330可选的还可以是至少一个位于远离前述处理器的存储装置。存储器330中存储有计算机可读取指令,当所述计算机可读取指令由所述

处理器310执行时,电子设备执行上述图1所示方法过程。

[0098] 可以理解,图3所示的结构仅为示意,所述电子设备还可包括比图3中所示更多或者更少的组件,或者具有与图3所示不同的配置。图3中所示的各组件可以采用硬件、软件或其组合实现。

[0099] 本申请实施例提供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,执行如图1所示方法实施例中电子设备所执行的方法过程。

[0100] 本实施例公开一种计算机程序产品,所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序,所述计算机程序包括程序指令,当所述程序指令被计算机执行时,计算机能够执行上述各方法实施例所提供的方法,例如,包括:若从目标接口识别到异常流量,则根据所述目标接口自身的信息和/或所述异常流量的信息生成告警信息;输出针对所述目标接口的所述告警信息。

[0101] 综上所述,本申请实施例提供了一种告警方法、装置、电子设备及存储介质,该方法在从目标接口识别到异常流量时,根据目标接口自身的信息和/或异常流量的信息来生成告警信息,并输出告警信息,如此的生成的告警信息可包含接口和/或异常流量的相关描述信息,实现更细粒度的告警,从而使得运维人员根据告警信息即可知晓接口的紧急处理程度,进而及时采取相应措施进行处理,有效提高了运维效率。

[0102] 在本申请所提供的实施例中,应该理解到,所揭露装置和方法,可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,又例如,多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0103] 另外,作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0104] 再者,在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分,也可以是各个模块单独存在,也可以两个或两个以上模块集成形成一个独立的部分。

[0105] 在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0106] 以上所述仅为本申请的实施例而已,并不用于限制本申请的保护范围,对于本领域的技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

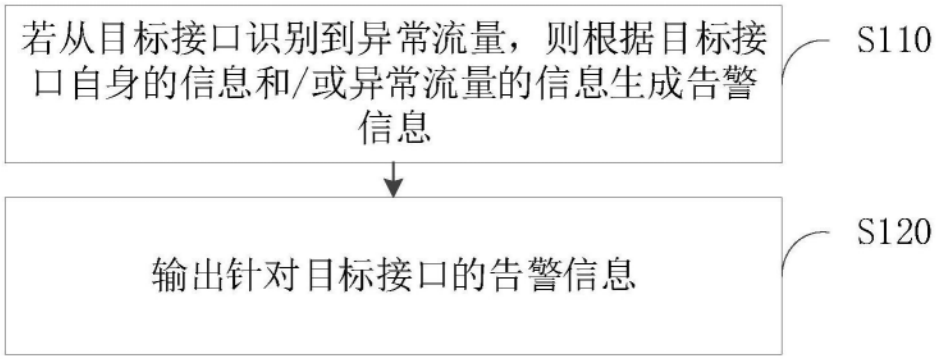

若从目标接口识别到异常流量，则根据目标接口自身的信息和/或异常流量的信息生成告警信息
S110
输出针对目标接口的告警信息
S120

图1

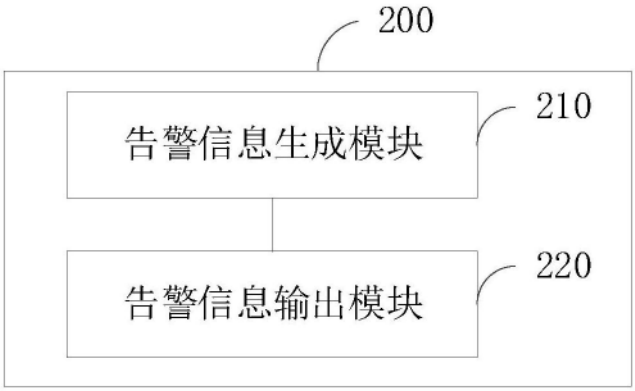

200
告警信息生成模块
210
告警信息输出模块
220

图2

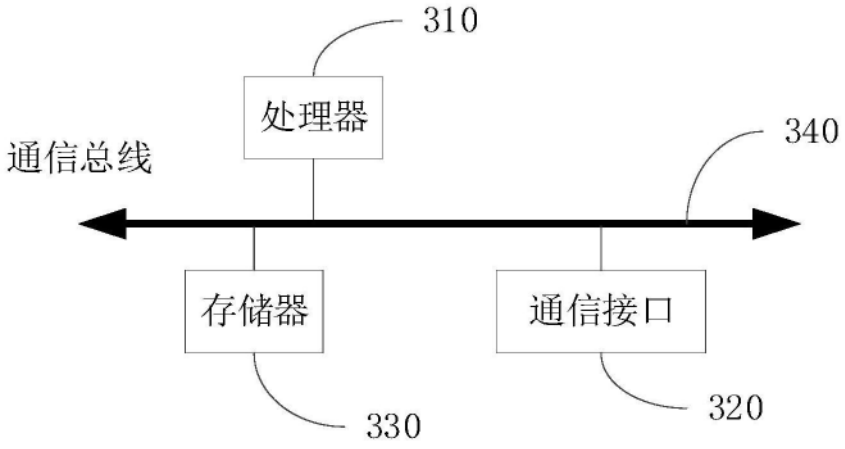

310
处理器
通信总线
340
存储器
通信接口
330
320

图3