(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 108989263 A
(43)申请公布日 2018.12.11

(21)申请号 201710399583.3

(22)申请日 2017.05.31

(71)申请人 中国移动通信集团公司
地址 100032 北京市西城区金融大街29号

(72)发明人 吴朝国

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 蒋雅洁 张颖玲

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/12(2009.01)
H04W 4/14(2009.01)

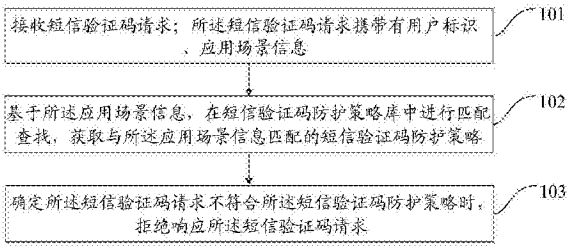
权利要求书1页 说明书13页 附图1页

(54)发明名称

短信验证码攻击防护方法、服务器和计算机可读存储介质

(57)摘要

本发明公开了一种短信验证码攻击防护方法，包括：接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。同时，本发明还公开了一种服务器和计算机可读存储介质。



CN 108989263 A

1.一种短信验证码攻击防护方法，其特征在于，所述方法包括：

接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；

基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；

确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

2.根据权利要求1所述的方法，其特征在于，当所述短信验证码请求为短信验证码获取请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

统计在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量；

当所述数量大于第一预设阈值时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

3.根据权利要求2所述的方法，其特征在于，所述方法还包括：

拒绝响应在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求。

4.根据权利要求1所述的方法，其特征在于，当所述短信验证码请求为短信验证码获取请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

确定所述短信验证码获取请求未携带有预设校验参数时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

5.根据权利要求2所述的方法，其特征在于，所述方法还包括：

确定所述短信验证码获取请求符合所述短信验证码防护策略时，响应所述短信验证码请求以生成短信验证码，并将数据库中所述短信验证码的状态标志位初始为有效状态。

6.根据权利要求1所述的方法，其特征在于，当所述短信验证码请求为短信验证码校验请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

基于所述用户标识，在数据库中进行匹配查找，获取与所述用户标识对应的短信验证码的状态标志位；

确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

7.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机可执行指令，所述计算机可执行指令用于执行权利要求1至6任一项所述的短信验证码攻击防护方法中的各个步骤。

8.一种服务器，其特征在于，所述服务器包括：存储器；一个或多个处理器；以及一个或多个模块；所述一个或多个模块被存储在所述存储器中并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行权利要求1至6任一项所述短信验证码攻击防护方法中各步骤的指令。

短信验证码攻击防护方法、服务器和计算机可读存储介质

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种短信验证码攻击防护方法、服务器和计算机可读存储介质。

背景技术

[0002] 近年来，由于在在线支付、网站登录、App用户注册等很多应用场景中需要对用户身份或手机号码真实性进行校验，此时通常需要用户通过输入手机号码以获取短信验证码而完成校验操作。例如，用户先在应用页面中选择“短信验证码”选项，然后点击“获取”按钮，从而获取短信验证码。因此，短信验证码的重要性与作用不容忽视。但与此同时，为了非法获取他人信息进行牟利等原因，针对短信验证码的攻击越来越多，使得短信验证码攻击的问题日趋严重。例如，攻击者通过程序调用短信发送接口向后台发送短信以获取短信验证码，这是因为http、https等接口暴露在公网下，脚本的代码都可以被黑客抓取到，而且参数都很透明，使得黑客比较容易就可以模拟浏览器给后台发送获取短信验证码请求。其中，短信验证码攻击中常用手段是暴力破解。例如，黑客通过脚本程序调用后台接口自动发送短信，以此来达到短信轰炸的目的；针对一个手机号码发送大量的验证码进行验证，并在验证成功后非法获取他人信息。

[0003] 现有技术中，应对短信验证码攻击的主要技术方案是每隔一定时间如每隔1～2分钟发送一次短信验证码，且该短信验证码在一段时间内如5～10分钟内有效，以拖延用户的攻击次数。但是，现有技术的缺点在于不能解决短信炸弹问题，因为攻击者通过程序等自动调用短信验证码，每隔一定时间给用户发送短信验证码，不但会给用户带来大量垃圾短信，而且也有一定的验证成功率。

发明内容

[0004] 有鉴于此，本发明实施例期望提供一种短信验证码攻击防护方法、服务器和计算机可读存储介质，能够有效阻止短信验证码攻击行为。

[0005] 为达到上述目的，本发明的技术方案是这样实现的：

[0006] 本发明实施例提供了一种短信验证码攻击防护方法，所述方法包括：

[0007] 接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；

[0008] 基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；

[0009] 确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0010] 上述方案中，当所述短信验证码请求为短信验证码获取请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0011] 统计在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量；

[0012] 当所述数量大于第一预设阈值时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0013] 上述方案中，所述方法还包括：

[0014] 拒绝响应在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求。

[0015] 上述方案中，当所述短信验证码请求为短信验证码获取请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0016] 确定所述短信验证码获取请求未携带有预设校验参数时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0017] 上述方案中，所述方法还包括：

[0018] 确定所述短信验证码获取请求符合所述短信验证码防护策略时，响应所述短信验证码请求以生成短信验证码，并将数据库中所述短信验证码的状态标志位初始为有效状态。

[0019] 上述方案中，当所述短信验证码请求为短信验证码校验请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0020] 基于所述用户标识，在数据库中进行匹配查找，获取与所述用户标识对应的短信验证码的状态标志位；

[0021] 确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0022] 本发明实施例提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机可执行指令，所述计算机可执行指令用于执行上述短信验证码攻击防护方法中的各个步骤。

[0023] 本发明实施例还提供了一种服务器，所述服务器包括：存储器；一个或多个处理器；以及一个或多个模块；所述一个或多个模块被存储在所述存储器中并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行上述短信验证码攻击防护方法中各步骤的指令。

[0024] 本发明实施例提供的短信验证码攻击防护方法、服务器和计算机可读存储介质，接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求；可见，本发明实施例提供的短信验证码攻击防护方法、服务器和计算机可读存储介质根据接收到的短信验证码请求所携带的应用场景信息，利用与所述应用场景信息匹配的短信验证码防护策略判断是否响应所述短信验证码请求，当所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求，能够有效阻止短信验证码攻击行为；并且，还能够有效减少因短信轰炸给用户带来的垃圾短信。

附图说明

[0025] 图1为本发明实施例一短信验证码攻击防护方法的实现流程示意图；

[0026] 图2为本发明实施例一服务器的组成结构示意图；

[0027] 图3为本发明实施例二服务器的组成结构示意图。

具体实施方式

[0028] 下面结合附图及具体实施例对本发明再作进一步详细的说明。

[0029] 实施例一

[0030] 图1为本发明实施例一短信验证码攻击防护方法的实现流程示意图，该方法包括以下步骤：

[0031] 步骤101：接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；

[0032] 具体地，服务器、后台管理平台等短信验证码管理系统或短信验证码管理设备接收短信验证码请求；其中，所述短信验证码请求中至少携带有用户标识、应用场景信息。

[0033] 这里，所述短信验证码请求可以是通过触发终端中的应用程序生成的，也可以是通过触发后台接口、应用程序接口等生成的；所述短信验证码请求包括短信验证码获取请求或短信验证码校验请求；当所述短信验证码请求为短信验证码获取请求时，终端向短信验证码管理系统或短信验证码管理设备发送短信验证码获取请求的目的是：请求短信验证码管理系统或短信验证码管理设备对所述短信验证码获取请求进行响应以生成短信验证码；当所述短信验证码请求为短信验证码校验请求时，所述短信验证码校验请求中携带有待校验短信验证码，终端向短信验证码管理系统或短信验证码管理设备发送短信验证码校验请求的目的是：请求短信验证码管理系统或短信验证码管理设备对待校验短信验证码进行校验。

[0034] 这里，所述终端可以是移动终端或固定终端；所述移动终端可以是移动电话、智能电话、笔记本电脑、平板电脑等；所述固定终端可以是数字电视机、台式计算机等；所述终端上可安装应用程序，终端通过有线网络或无线网络可与应用程序的提供方或管理方建立数据通信连接，也可理解为终端通过有线网络或无线网络可与应用程序的服务器、后台管理平台等进行数据传输。

[0035] 这里，所述用户标识用于指示短信验证码请求的发起方或短信验证码请求的响应结果的接收方；所述用户标识可以是用户手机号码、国际移动用户识别码、国际移动设备身份码、互联网协议地址(IP，Internet Protocol Address)等标识中的一种或多种；当然，所述用户标识也可以是用户名、密码等用户登录终端或应用程序的信息；例如，当用户通过手机向指定服务器发送短信验证码获取请求时，所述用户标识可以是用户的手机号码；当用户通过台式计算机向指定服务器发送短信验证码获取请求时，所述用户标识可以是该台式计算机的IP。

[0036] 这里，所述应用场景信息用于指示发送短信验证码请求的场景；其中，终端或接口发送短信验证码请求可以包括下述三种应用场景：

[0037] 场景一、用户在应用程序用户界面或网页界面中选择“短信验证码”选项后，再点击“获取”按钮，以获取短信验证码；

[0038] 场景二、攻击者通过程序调用短信发送接口发送短信而请求获取短信验证码；因为http接口、https接口暴露在公网下，使得脚本的代码都可以被攻击者比如黑客抓取到，而且参数都很透明，这样黑客比较容易就可以模拟浏览器给后台发送短信验证码获取请

求；

[0039] 场景三、黑客的脚本攻击；黑客通过脚本程序调用后台接口自动发送短信验证码请求，以此来达到短信轰炸的目的。

[0040] 步骤102：基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；

[0041] 这里，所述短信验证码防护策略库是预先设置的，用于存储针对不同应用场景的短信验证码防护策略，每一个短信验证码防护策略可以根据应用场景进行设置与更新。短信验证码防护策略可以是短信验证码单次有效即验证一次后自动失效、或同一手机号码发送短信验证码获取请求的频率过高即在X分钟内发送短信验证码获取请求的次数超过Y次，则在Z分钟内拒绝响应该手机号码发送的短信验证码获取请求等。例如，当所述应用场景信息为场景一所示的用户通过应用程序用户界面或网页界面请求获取短信验证码时，则在短信验证码防护策略库中获取与场景一匹配的短信验证码防护策略。

[0042] 步骤103：确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0043] 具体地，基于步骤102中确定的所述短信验证码防护策略，判断所述短信验证码请求是否符合所述短信验证码防护策略，确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0044] 这里，当所述短信验证码请求为短信验证码获取请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0045] 统计在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量；

[0046] 当所述数量大于第一预设阈值时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0047] 这里，所述第一预设时间段可以指一个具体的时间范围，包括以接收到所述短信验证码获取请求的当前时间为起点、且在所述当前时间之前的第一时间阈值范围；例如，当所述第一时间阈值为10分钟时，则第一预设时间段为在当前时间之前且包括当前时间在内的10分钟。

[0048] 这里，所述第一预设阈值可根据实际情况进行设置和调整；若在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量大于第一预设阈值，说明请求获取短信验证码的次数达到了一定频率，所述短信验证码获取请求可能是短信验证码攻击行为，则拒绝处理所述短信验证码获取请求，即不为所述短信验证码获取请求生成相应的短信验证码，从而限制短信发送次数，并阻止非正常用户获取短信验证码，有效解决短信验证码攻击行为。例如，当同一个手机号码在15分钟内请求获取短信验证码的次数超过8次，则根据用户使用习惯和制定的规则，可以将该手机号码对应的用户视为非正常用户，从而对该手机号码发送的短信验证码获取请求不予以响应。

[0049] 本实施例中，通过短信验证码防护策略限制短信验证码发送次数，阻止非正常用户获取短信验证码，能够有效解决或阻止短信验证码攻击行为；并且，还能够有效减少因短信轰炸给用户带来的垃圾短信。

[0050] 进一步地，该方法还可包括：

[0051] 拒绝响应在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求。

[0052] 这里，所述第二预设时间段可以指一个具体的时间范围，包括以接收到所述短信验证码获取请求的当前时间为起点、且在所述当前时间之后的第二时间阈值范围；例如，当所述第二时间阈值为20分钟时，则第二预设时间段为从当前时间开始的20分钟内。

[0053] 这里，由于所述用户标识对应的用户可能是非正常用户，则通过拒绝响应在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求，能够有效限制短信发送次数，并阻止非正常用户获取短信验证码，有效解决短信验证码攻击行为。例如，当同一个手机号码在15分钟内请求获取短信验证码的次数超过8次，则根据用户使用习惯和制定的规则，可以将该手机号码对应的用户视为非正常用户，从而对该手机号码在以后300分钟内发送的短信验证码获取请求都不予以响应，并且还可给相应的业务系统发送提示消息。

[0054] 进一步地，该方法还可包括：

[0055] 确定所述短信验证码获取请求符合所述短信验证码防护策略时，响应所述短信验证码请求以生成短信验证码，并将数据库中所述短信验证码的状态标志位初始为有效状态。

[0056] 这里，所述状态标志位用于指示短信验证码是否未被用于执行校验操作或已经被用于执行校验操作，也可以用于指示短信验证码是否还可被用于执行校验操作；所述状态标志位可以被设置为有效状态或无效状态；在实际应用中，有效状态可用“1”表示，无效状态可用“0”表示；当短信验证码的状态标志位为有效状态时，说明该短信验证码还可被用于执行校验操作；当短信验证码的状态标志位为无效状态时，说明该短信验证码不可被用于执行校验操作。此外，依据现有的数据库或设置一个新数据库来存储短信验证码的状态标志位；当根据接收到的短信验证码获取请求生成一个新短信验证码时，该新短信验证码的状态标志位初始为有效状态。

[0057] 这里，可设置一个次数阈值，用于指示短信验证码被用于执行校验操作的最大次数；当任意一个短信验证码被用于执行校验操作的次数小于所述次数阈值时，将该短信验证码的状态标志位设置为有效状态；而当任意一个短信验证码被用于执行校验操作的次数大于或等于所述次数阈值时，将该短信验证码的状态标志位设置为无效状态。例如，当一个短信验证码已经被用于执行一次校验操作时，则可将该短信验证码的状态标志位设置为无效状态。

[0058] 如此，只有确认短信验证码获取请求符合相应的短信验证码防护策略时，才对短信验证码请求进行响应以生成短信验证码，能够有效减少发送给用户的垃圾短信，并更好的实现短信验证码的服务。

[0059] 进一步地，当所述短信验证码请求为短信验证码获取请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0060] 确定所述短信验证码获取请求未携带有预设校验参数时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0061] 这里，可以预先通过在应用程序或网页界面中设置校验参数，并在生成短信验证码获取请求时写入校验参数，以标识所述短信验证码获取请求是正常用户发送的；所述校

验参数可以是用户名、密码等。例如，可以在打开网页界面时在浏览器端写入一些cookie作为预设校验参数，以使通过浏览器端发出的短信验证码获取请求中携带所述预设校验参数，使得黑客等攻击者无法直接用脚本模拟发送短信验证码获取请求，从而最大化的阻止黑客的攻击行为。

[0062] 这里，当所述短信验证码获取请求携带有预设校验参数时，还可判断所述预设校验参数是否与存储的参数一致，进而决定是否响应所述短信验证码获取请求，即还要判断出所述预设校验参数与存储的参数一致时，才允许响应所述短信验证码获取请求。

[0063] 如此，能够使得黑客等攻击者无法直接用脚本模拟发送短信验证码获取请求，从而最大化的阻止黑客的攻击行为。

[0064] 进一步地，当所述短信验证码请求为短信验证码校验请求时，所述确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0065] 基于所述用户标识，在数据库中进行匹配查找，获取与所述用户标识对应的短信验证码的状态标志位；

[0066] 确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0067] 具体地，基于短信验证码校验请求中携带的用户标识，在数据库中进行匹配查找；当在数据库中查找到所述用户标识时，获取与所述用户标识对应的短信验证码的状态标志位；确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0068] 这里，当确定所述短信验证码的状态标志位为无效状态时，说明所述短信验证码不可被用于执行校验操作，因此拒绝响应所述短信验证码校验请求。

[0069] 这里，当确定所述短信验证码的状态标志位为有效状态时，响应所述短信验证码校验请求，即将所述短信验证码与所述短信验证码校验请求中携带的待校验短信验证码进行比对，判断两者是否一致，若一致，则说明对所述短信验证码校验请求的校验通过；若不一致，则说明对所述短信验证码校验请求的校验不通过；然后，可将所述短信验证码的状态标志位设置为无效状态。

[0070] 假设，设置短信验证码单次有效，即短信验证码只可被用于执行一次校验操作，并在执行一次校验操作后自动失效，不可继续用于执行校验操作；因此，如果对用户第一次输入的待校验短信验证码的验证失败，则用户后续输入的待校验短信验证码是正确的短信验证码，也是校验不通过的。

[0071] 这样，通过限定短信验证码被用于执行校验操作的次数，能够提高用户手机短信验证码的安全性。

[0072] 为实现上述方法，本发明实施例还提供了一种服务器，图2为本发明实施例服务器的组成结构示意图，该服务器包括通信接口11和处理器12；其中，

[0073] 所述通信接口11，用于接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；

[0074] 所述处理器12，用于基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0075] 这里，所述短信验证码请求可以是通过触发终端中的应用程序生成的，也可以是

通过触发后台接口、应用程序接口等生成的；所述短信验证码请求包括短信验证码获取请求或短信验证码校验请求；当所述短信验证码请求为短信验证码获取请求时，终端向所述通信接口11发送短信验证码获取请求的目的是：请求对所述短信验证码获取请求进行响应以生成短信验证码；当所述短信验证码请求为短信验证码校验请求时，所述短信验证码校验请求中携带有待校验短信验证码，终端向所述通信接口11发送短信验证码校验请求的目的是：请求对待校验短信验证码进行校验。

[0076] 这里，所述终端可以是移动终端或固定终端；所述移动终端可以是移动电话、智能电话、笔记本电脑、平板电脑等；所述固定终端可以是数字电视机、台式计算机等；所述终端上可安装应用程序，终端通过有线网络或无线网络可与应用程序的提供方或管理方建立数据通信连接，也可理解为终端通过有线网络或无线网络可与应用程序的服务器、后台管理平台等进行数据传输。

[0077] 这里，所述用户标识用于指示短信验证码请求的发起方或短信验证码请求的响应结果的接收方；所述用户标识可以是用户手机号码、国际移动用户识别码、国际移动设备身份码、IP等标识中的一种或多种；当然，所述用户标识也可以是用户名、密码等用户登录终端或应用程序的信息；例如，当用户通过手机向指定服务器发送短信验证码获取请求时，所述用户标识可以是用户的手机号码；当用户通过台式计算机向指定服务器发送短信验证码获取请求时，所述用户标识可以是该台式计算机的IP。

[0078] 这里，所述应用场景信息用于指示发送短信验证码请求的场景；其中，终端或接口发送短信验证码请求可以包括下述三种应用场景：

[0079] 场景一、用户在应用程序用户界面或网页界面中选择“短信验证码”选项后，再点击“获取”按钮，以获取短信验证码；

[0080] 场景二、攻击者通过程序调用短信发送接口发送短信而请求获取短信验证码；因为http接口、https接口暴露在公网下，使得脚本的代码都可以被攻击者比如黑客抓取到，而且参数都很透明，这样黑客比较容易就可以模拟浏览器给后台发送短信验证码获取请求；

[0081] 场景三、黑客的脚本攻击；黑客通过脚本程序调用后台接口自动发送短信验证码请求，以此来达到短信轰炸的目的。

[0082] 这里，所述短信验证码防护策略库是预先设置的，用于存储针对不同应用场景的短信验证码防护策略，每一个短信验证码防护策略可以根据应用场景进行设置与更新。短信验证码防护策略可以是短信验证码单次有效即验证一次后自动失效、或同一手机号码发送短信验证码获取请求的频率过高即在X分钟内发送短信验证码获取请求的次数超过Y次，则在Z分钟内拒绝响应该手机号码发送的短信验证码获取请求等。例如，当所述应用场景信息为场景一所示的用户通过应用程序用户界面或网页界面请求获取短信验证码时，则所述处理器12在短信验证码防护策略库中获取与场景一匹配的短信验证码防护策略。

[0083] 所述处理器12，具体用于：基于所述短信验证码防护策略，判断所述短信验证码请求是否符合所述短信验证码防护策略，确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0084] 这里，当所述短信验证码请求为短信验证码获取请求时，所述处理器12确定所述短信验证码请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码请求，包括：

[0085] 统计在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量；

[0086] 当所述数量大于第一预设阈值时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0087] 这里，所述第一预设时间段可以指一个具体的时间范围，包括以接收到所述短信验证码获取请求的当前时间为起点、且在所述当前时间之前的第一时间阈值范围；例如，当所述第一时间阈值为10分钟时，则第一预设时间段为在当前时间之前且包括当前时间在内的10分钟。

[0088] 这里，所述第一预设阈值可根据实际情况进行设置和调整；若在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量大于第一预设阈值，说明请求获取短信验证码的次数达到了一定频率，所述短信验证码获取请求可能是短信验证码攻击行为，则拒绝处理所述短信验证码获取请求，即不为所述短信验证码获取请求生成相应的短信验证码，从而限制短信发送次数，并阻止非正常用户获取短信验证码，有效解决短信验证码攻击行为。例如，当同一个手机号码在15分钟内请求获取短信验证码的次数超过8次，则根据用户使用习惯和制定的规则，可以将该手机号码对应的用户视为非正常用户，从而对该手机号码发送的短信验证码获取请求不予以响应。

[0089] 本发明实施例提供的服务器通过短信验证码防护策略限制短信验证码发送次数，阻止非正常用户获取短信验证码，能够有效解决或阻止短信验证码攻击行为；并且，还能够有效减少因短信轰炸给用户带来的垃圾短信。

[0090] 进一步地，所述处理器12，还用于拒绝响应通信接口11在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求。

[0091] 这里，所述第二预设时间段可以指一个具体的时间范围，包括以接收到所述短信验证码获取请求的当前时间为起点、且在所述当前时间之后的第二时间阈值范围；例如，当所述第二时间阈值为20分钟时，则第二预设时间段为从当前时间开始的20分钟内。

[0092] 这里，由于所述用户标识对应的用户可能是非正常用户，则所述处理器12通过拒绝响应通信接口11在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求，能够有效限制短信发送次数，并阻止非正常用户获取短信验证码，有效解决短信验证码攻击行为。例如，当同一个手机号码在15分钟内请求获取短信验证码的次数超过8次，则根据用户使用习惯和制定的规则，可以将该手机号码对应的用户视为非正常用户，从而对该手机号码在以后300分钟内发送的短信验证码获取请求都不予以响应，并且还可给相应的业务系统发送提示消息。

[0093] 进一步地，所述处理器12，还用于定所述短信验证码获取请求符合所述短信验证码防护策略时，响应所述短信验证码请求以生成短信验证码，并将数据库中所述短信验证码的状态标志位初始为有效状态。

[0094] 这里，所述状态标志位用于指示短信验证码是否未被用于执行校验操作或已经被用于执行校验操作，也可以用于指示短信验证码是否还可被用于执行校验操作；所述状态标志位可以被设置为有效状态或无效状态；在实际应用中，有效状态可用“1”表示，无效状态可用“0”表示；当短信验证码的状态标志位为有效状态时，说明该短信验证码还可被用于执行校验操作；当短信验证码的状态标志位为无效状态时，说明该短信验证码不可被用于

执行校验操作。此外，依据现有的数据库或设置一个新数据库来存储短信验证码的状态标志位；当根据接收到的短信验证码获取请求生成一个新短信验证码时，该新短信验证码的状态标志位初始为有效状态。

[0095] 这里，可设置一个次数阈值，用于指示短信验证码被用于执行校验操作的最大次数；当任意一个短信验证码被用于执行校验操作的次数小于所述次数阈值时，将该短信验证码的状态标志位设置为有效状态；而当任意一个短信验证码被用于执行校验操作的次数大于或等于所述次数阈值时，将该短信验证码的状态标志位设置为无效状态。例如，当一个短信验证码已经被用于执行一次校验操作时，则可将该短信验证码的状态标志位设置为无效状态。

[0096] 如此，只有确认短信验证码获取请求符合相应的短信验证码防护策略时，才对短信验证码请求进行响应以生成短信验证码，能够有效减少发送给用户的垃圾短信，并更好的实现短信验证码的服务。

[0097] 进一步地，当所述短信验证码请求为短信验证码获取请求时，所述处理器12，具体用于：确定所述短信验证码获取请求未携带有预设校验参数时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0098] 这里，可以预先通过在应用程序或网页界面中设置校验参数，并在生成短信验证码获取请求时写入校验参数，以标识所述短信验证码获取请求是正常用户发送的；所述校验参数可以是用户名、密码等。例如，可以在打开网页界面时在浏览器端写入一些cookie作为预设校验参数，以使通过浏览器端发出的短信验证码获取请求中携带所述预设校验参数，使得黑客等攻击者无法直接用脚本模拟发送短信验证码获取请求，从而最大化的阻止黑客的攻击行为。

[0099] 这里，当所述短信验证码获取请求携带有预设校验参数时，还可判断所述预设校验参数是否与存储的参数一致，进而决定是否响应所述短信验证码获取请求，即还要判断出所述预设校验参数与存储的参数一致时，才允许响应所述短信验证码获取请求。

[0100] 如此，能够使得黑客等攻击者无法直接用脚本模拟发送短信验证码获取请求，从而最大化的阻止黑客的攻击行为。

[0101] 进一步地，当所述短信验证码请求为短信验证码校验请求时，

[0102] 所述处理器12，还用于基于所述用户标识，在数据库中进行匹配查找，获取与所述用户标识对应的短信验证码的状态标志位；确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0103] 具体地，所述处理器12基于短信验证码校验请求中携带的用户标识，在数据库中进行匹配查找；当在数据库中查找到所述用户标识时，所述处理器12获取与所述用户标识对应的短信验证码的状态标志位；所述处理器12确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0104] 这里，当确定所述短信验证码的状态标志位为无效状态时，说明所述短信验证码不可被用于执行校验操作，因此所述处理器12拒绝响应所述短信验证码校验请求。

[0105] 这里，当所述处理器12确定所述短信验证码的状态标志位为有效状态时，响应所述短信验证码校验请求，即将所述短信验证码与所述短信验证码校验请求中携带的待校验短信验证码进行比对，判断两者是否一致，若一致，则说明对所述短信验证码校验请求的校

验通过；若不一致，则说明对所述短信验证码校验请求的校验不通过；然后，可将所述短信验证码的状态标志位设置为无效状态。

[0106] 假设，设置短信验证码单次有效，即短信验证码只可被用于执行一次校验操作，并在执行一次校验操作后自动失效，不可继续用于执行校验操作；因此，如果对用户第一次输入的待校验短信验证码的验证失败，则用户后续输入的待校验短信验证码是正确的短信验证码，也是校验不通过的。

[0107] 这样，通过限定短信验证码被用于执行校验操作的次数，能够提高用户手机短信验证码的安全性。

[0108] 上述实施例提供的服务器在进行短信验证码攻击防护时，仅以上述划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的处理器完成，即将装置的内部结构划分成不同的处理器，以完成以上描述的全部或者部分处理。另外，上述实施例提供的服务器与短信验证码攻击防护方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0109] 实施例二

[0110] 本发明实施例提供了一种服务器，图3为本发明实施例服务器的组成结构示意图，该服务器200包括：一个或多个处理器201、存储器202、以及一个或多个模块；其中，图3中示意的处理器201并非用于指代处理器的个数为一个，而是仅用于指代处理器相对其他器件的位置关系，在实际应用中，处理器的个数可以为一个或多个；同样，图3中示意的存储器202也是同样的含义，即：仅用于指代存储器相对其他器件的位置关系，在实际应用中，存储器的个数可以为一个或多个。

[0111] 所述一个或多个模块被存储在所述存储器202中并被配置成由所述一个或多个处理器201执行，所述一个或多个模块用于执行如下步骤：

[0112] 接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；

[0113] 基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；

[0114] 确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0115] 在本发明实施例一实施方式中，所述一个或多个模块还用于执行如下步骤：

[0116] 统计在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量；

[0117] 当所述数量大于第一预设阈值时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0118] 在本发明实施例一实施方式中，所述一个或多个模块还用于执行如下步骤：拒绝响应在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求。

[0119] 在本发明实施例一实施方式中，所述一个或多个模块还用于执行如下步骤：

[0120] 确定所述短信验证码获取请求未携带有预设校验参数时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0121] 在本发明实施例一实施方式中，所述一个或多个模块还用于执行如下步骤：

[0122] 确定所述短信验证码获取请求符合所述短信验证码防护策略时，响应所述短信验

证码请求以生成短信验证码，并将数据库中所述短信验证码的状态标志位初始为有效状态。

[0123] 在本发明实施例一实施方式中，所述一个或多个模块还用于执行如下步骤：

[0124] 基于所述用户标识，在数据库中进行匹配查找，获取与所述用户标识对应的短信验证码的状态标志位；

[0125] 确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0126] 这里，服务器200还可包括通信模组203；服务器200中的各个组件通过总线系统204耦合在一起。可理解，总线系统204用于实现这些组件之间的连接通信。总线系统204除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图3中将各种总线都标为总线系统204。

[0127] 其中，存储器202可以是易失性存储器或非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(ROM，Read Only Memory)、可编程只读存储器(PROM，Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM，Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM，Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM，ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM，Compact Disc Read-Only Memory)；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM，Random Access Memory)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(SRAM，Static Random Access Memory)、同步静态随机存取存储器(SSRAM，Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM，Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM，Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM，Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM，Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM，SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM，Direct Rambus Random Access Memory)。本发明实施例描述的存储器102旨在包括但不限于这些和任意其它适合类型的存储器。

[0128] 本发明实施例中的存储器202用于存储各种类型的数据以支持服务器200的操作。这些数据的示例包括：用于在服务器200上操作的任何计算机程序，如操作系统和应用程序；联系人数据；电话簿数据；消息；图片；视频等。其中，操作系统包含各种系统程序，例如框架层、核心库层、驱动层等，用于实现各种基础业务以及处理基于硬件的任务。应用程序可以包含各种应用程序，例如媒体播放器(Media Player)、浏览器(Browser)等，用于实现各种应用业务。这里，实现本发明实施例方法的程序可以包含在应用程序中。

[0129] 上述本发明实施例揭示的方法可以应用于处理器201中，或者由处理器201实现。处理器201可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器201中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器201可以是通用处理器、数字信号处理器(DSP，Digital Signal Processor)，或者其他可

编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器201可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本发明实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器202，处理器201读取存储器202中的信息，结合其硬件完成前述方法的步骤。

[0130] 在示例性实施例中，本发明实施例还提供了一种计算机可读存储介质，例如包括计算机程序的存储器202，上述计算机程序可由服务器200中的处理器201执行，以完成前述方法所述步骤。计算机可读存储介质可以是FRAM、ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或CD-ROM等存储器；也可以是包括上述存储器之一或任意组合的各种设备，如移动电话、计算机、平板设备、个人数字助理等。

[0131] 一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，所述计算机程序被处理器运行时，执行如下步骤：

[0132] 接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息；

[0133] 基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略；

[0134] 确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求。

[0135] 在本发明实施例一实施方式中，所述计算机程序被处理器运行时，还执行如下步骤：

[0136] 统计在第一预设时间段内接收到携带有所述用户标识的短信验证码获取请求的数量；

[0137] 当所述数量大于第一预设阈值时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0138] 在本发明实施例一实施方式中，所述计算机程序被处理器运行时，还执行如下步骤：

[0139] 拒绝响应在第二预设时间段内接收到的、且携带有所述用户标识的短信验证码获取请求。

[0140] 在本发明实施例一实施方式中，所述计算机程序被处理器运行时，还执行如下步骤：

[0141] 确定所述短信验证码获取请求未携带有预设校验参数时，判定所述短信验证码获取请求不符合所述短信验证码防护策略，拒绝响应所述短信验证码获取请求。

[0142] 在本发明实施例一实施方式中，所述计算机程序被处理器运行时，还执行如下步骤：

[0143] 确定所述短信验证码获取请求符合所述短信验证码防护策略时，响应所述短信验证码请求以生成短信验证码，并将数据库中所述短信验证码的状态标志位初始为有效状态。

[0144] 在本发明实施例一实施方式中，所述计算机程序被处理器运行时，还执行如下步骤：

[0145] 基于所述用户标识，在数据库中进行匹配查找，获取与所述用户标识对应的短信验证码的状态标志位；

[0146] 确定所述短信验证码的状态标志位为无效状态时，拒绝响应所述短信验证码校验请求。

[0147] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和范围之内所作的任何修改、等同替换和改进等，均包含在本发明的保护范围之内。

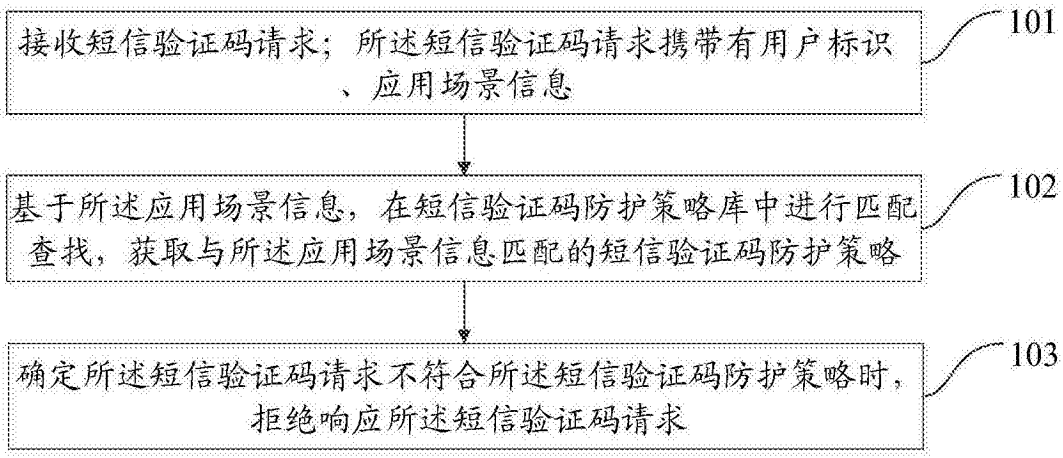

接收短信验证码请求；所述短信验证码请求携带有用户标识、应用场景信息
101
基于所述应用场景信息，在短信验证码防护策略库中进行匹配查找，获取与所述应用场景信息匹配的短信验证码防护策略
102
确定所述短信验证码请求不符合所述短信验证码防护策略时，拒绝响应所述短信验证码请求
103

图1

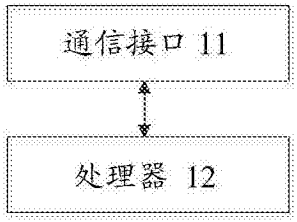

通信接口 11
处理器 12

图2

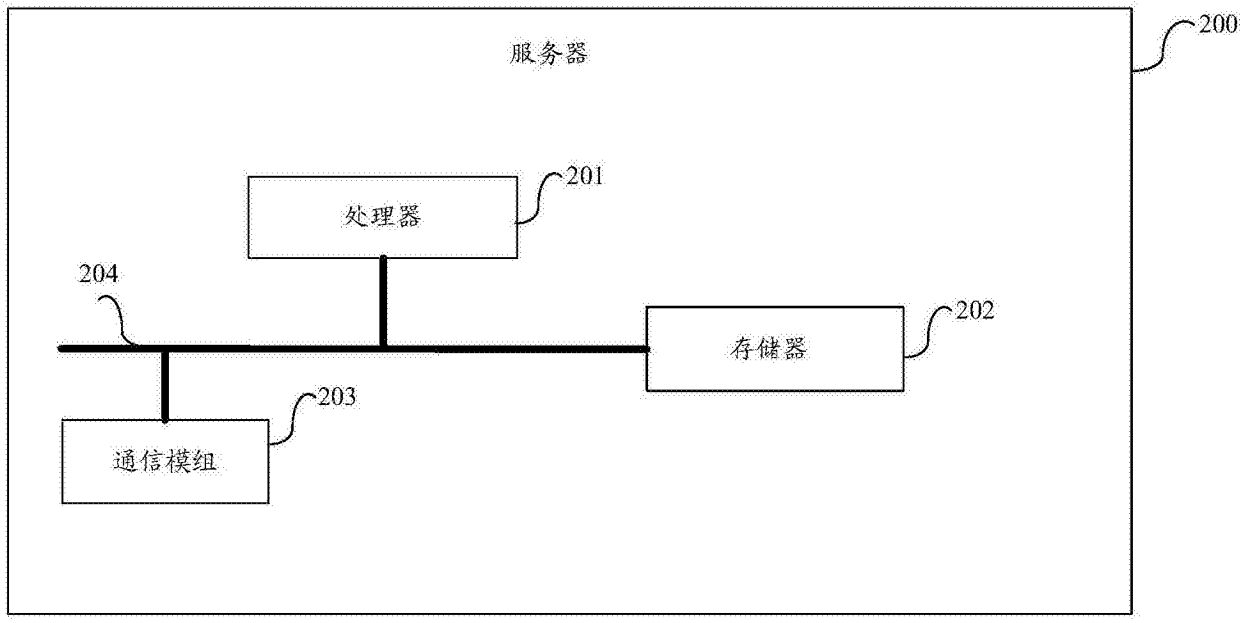

服务器
200
处理器
201
204
存储器
202
通信模组
203

图3