(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 12 月 7 日 (07.12.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/206605 A1

(51) 国际专利分类号:
H04L 29/02 (2006.01)

(21) 国际申请号: PCT/CN2017/080862

(22) 国际申请日: 2017 年 4 月 18 日 (18.04.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610377847.0 2016年5月31日 (31.05.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人; 及

(71) 申请人 (仅对*US*): 鲁亚然 (LU, Yaran) [CN/CN]; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲2号渔阳置业大厦B座605, Beijing 100029 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY,

(54) **Title:** METHOD AND DEVICE FOR PREVENTING SERVER FROM BEING ATTACKED

(54) **发明名称**: 防止服务器被攻击的方法及装置

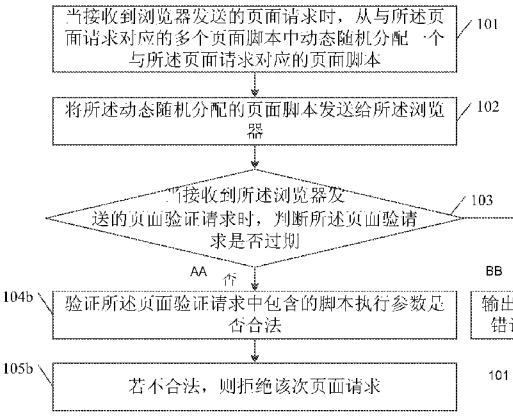

图 1

101 UPON RECEIVING A PAGE REQUEST SENT BY A BROWSER, DYNAMICALLY AND RANDOMLY ALLOCATE, FROM MULTIPLE PAGE SCRIPTS CORRESPONDING TO THE PAGE REQUEST, A PAGE SCRIPT CORRESPONDING TO THE PAGE REQUEST
102 SEND THE DYNAMICALLY AND RANDOMLY ALLOCATED PAGE SCRIPT TO THE BROWSER
103 UPON RECEIVING A PAGE VERIFICATION REQUEST SENT BY THE BROWSER, DETERMINE WHETHER THE PAGE VERIFICATION REQUEST HAS EXPIRED
104A OUTPUT ERROR PROMPT INFORMATION INDICATING PAGE EXPIRATION
104B VERIFY WHETHER THE SCRIPT EXECUTION PARAMETER COMPRISED IN THE PAGE VERIFICATION REQUEST IS LEGAL
105B IF THE SCRIPT EXECUTION PARAMETER IS ILLEGAL, REJECT THE CURRENT PAGE REQUEST
AA NO
BB YES

(57) **Abstract:** The present invention relates to the technical field of network security, and discloses a method and device for preventing a server from being attacked, solving the problem of low server security. The main technical solution of the present invention comprises: upon receiving a page request sent by a browser, dynamically and randomly allocating, from multiple page scripts corresponding to the page request, a page script corresponding to the page request; sending the dynamically and randomly allocated page script to the browser, so that the browser executes the page script to obtain a script execution parameter; upon receiving a page verification request

WO 2017/206605 A1

[见续页]

MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

sent by the browser, determining whether the page verification request is expired; if so, outputting error prompt information indicating page expiration; if not, verifying whether the script execution parameter comprised in the page verification request is legal; and if the script execution parameter is illegal, rejecting the current page request. The present invention mainly has application in preventing server attacks.

(57) 摘要：本发明公开了一种防止服务器被攻击的方法及装置，涉及网络安全技术领域，解决了服务器安全性低的问题。本发明的主要技术方案为：当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本；将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数；当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期；若过期，则输出页面过期的错误提示信息；若没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法；若不合法，则拒绝该次页面请求。本发明主要用于防止服务器被攻击。

防止服务器被攻击的方法及装置

技术领域

本发明涉及网络安全技术领域，尤其涉及一种防止服务器被攻击的方法及装置。

背景技术

随着互联网技术的快速发展，网络的安全保障越来越受到关注。而在一般情况下，网络的安全问题主要涉及如何防止网络中的服务器被攻击。一般的服务器被攻击，主要表现为攻击者通过服务请求占用服务器过多的服务资源，从而导致服务器运行超载，进而导致服务器无法响应其它的请求，最终造成服务器资源消耗殆尽，攻击者通过攻击服务器以达到服务器拒绝服务的目的。

目前，浏览器首先向服务器发送服务请求，该服务器请求中添加有经过 md5（Message Digest Algorithm，消息摘要算法第五版）加密的 cookie（服务器储存在用户本地终端上的数据）中的 token（令牌）值，服务器在接收到服务请求后，通过验证加密的 token 值判断浏览器发送的服务请求是否合法，以此实现防止服务器被攻击。然而，由于加密的 token 值是通过执行静态的脚本代码得到，且该静态的脚本代码是明文暴漏出来的，因此攻击者可用直接获得静态脚本代码中的逻辑，并从中解析出 token 的加密方式，从而可通过模拟正常用户的服务请求跳过服务器的检测机制，并以此对服务器进行攻击，进而现有的服务器的安全性低。

发明内容

鉴于上述问题，提出了本发明，以便提供一种克服上述问题或者至少部分地解决上述问题的防止服务器被攻击的方法及装置。

为达到上述目的，本发明主要提供如下技术方案：

一方面，本发明实施例提供了一种防止服务器被攻击的方法，该方法包括：

当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本；

将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数；

当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期；

若过期，则输出页面过期的错误提示信息；

若没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法；

若不合法，则拒绝该次页面请求。

另一方面，本发明实施例还提供一种防止服务器被攻击的装置，该装置包括：

分配单元，当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本；

发送单元，将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数；

判断单元，当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期；

输出单元，若所述页面验证请求过期，则输出页面过期的错误提示信息；

验证单元，若所述页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法；

拒绝单元，若所述页面验证请求中包含的脚本执行参数不合法，则拒绝该次页面请求。

借由上述技术方案，本发明实施例提供的技术方案至少具有下列优点：

本发明实施例提供的一种防止服务器被攻击的方法及装置，当接收到所述浏览器发送的页面验证请求时，首先判断所述页面验证请求是否过期，若页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法，若脚本执行参数不合法则拒绝该次页面请求，以此实现防止服务器被攻击。与目前通过验证加密的 token 值判断浏览器发送的服务请求是否合法，以实现防止服务器被攻击相比，本发明是通过验证脚本执行参数实现防止服务器被攻击的，由于脚本执行参数是根据与页面请求对应的多个页面脚本中动态随机分配的页面脚本得到的，且各页面脚本之间采用不同的脚本执行参数获取逻辑，因此即便攻击者获得动态代码中的脚本逻辑，也无法在预置时间内破解出其加密方式，且当页面验证请求的请求时间超过预置时间时，服务器将会拒绝该次页面请求，浏览器再次发送页面验证请求则需要从新加载页面验证请求，而从新加载的页面验证请求中的脚本执行参数则是通过执行重新抽取的页面脚本得到的，因此通过本发明实施例攻击者无法对服务器进行攻击，从而本发明实施例提高了服务器的安全性。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为本发明实施例提供的一种防止服务器被攻击的方法流程图;

图 2 为本发明实施例提供的另一种防止服务器被攻击的方法流程图;

图 3 为本发明实施例提供的一种防止服务器被攻击的装置的组成框图;

图 4 为本发明实施例提供的另一种防止服务器被攻击的装置的组成框图;

图 5 为本发明实施例提供的一种防止服务器被攻击的系统框图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明作详细说明。

本发明实施例提供了一种防止服务器被攻击的方法，如图 1 所示，所述方法包括:

101、当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本。

其中，所述页面请求中包括页面 URL，所述页面 URL 为浏览器请求页面脚本对应的页面。在本发明实施例中，一个页面 URL 对应多个页面脚本，同一个页面 URL 对应的页面脚本之间采用不同的脚本执行参数获取逻辑，执行同一个页面 URL 对应的多个页面脚本，将会得到多个不同的脚本执行参数。而同一页面 URL 对应的多个页面脚本之间的页面执行

结果是一样的，即对浏览器对各个页面脚本进行加载执行产生的页面是相同的。需要说明的是，本发明实施例可以根据系统当前时间生成的随机数，或根据发送页面请求的时间生成的随机数，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本，本发明实施例不做具体限定。

例如，若用户在浏览器地址栏中键入 Amazon 的 URL 并进行了回车确认，则服务器会接收到浏览器发送页面请求，该页面请求中的页面 URL 为 Amazon，然后从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本，即从与 Amazon 对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本。

102、将所述动态随机分配的页面脚本发送给所述浏览器。

进一步地，以使得所述浏览器执行所述页面脚本获取脚本执行参数，浏览器加载执行页面脚本之后会显示出对应的网页，并获取到脚本执行参数，脚本执行参数是网页当中的一些附加参数，本身并不会影响加载显示出来的网页。在本发明实施例中，执行同一页面 URL 分别对应的各页面脚本时，不同的页面脚本执行结果中会产生不同的脚本执行参数。

例如，某个页面 URL 对应有 3 个页面脚本，其中一个页面脚本中脚本执行参数获取逻辑是得到 Cookie 信息中 token 加密值，另一个页面脚本中脚本执行参数获取逻辑是得到用户当前鼠标坐标的加密值，再一个页面脚本中脚本执行参数获取逻辑是得到当前时间的加密值。需要说明的是，本发明实施例不限制页面脚本执行的逻辑，及脚本执行参数的加密方式，本发明中的各个页面脚本之间只需要采用不同的获取脚本执行参数逻辑即可，以此区分不同的页面脚本。

103、当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期。

其中，网页验证请求可以通过步骤 102 中加载执行得到的网页进行发送，具体可以在该页面中点击某个链接，或是选择某个命令按钮，输入某些关键字等，本发明实施例不做具体限定。所述页面验证请求中包括脚本执行参数，所述脚本执行参数是经过加密的参数。在本发明实施例中，判断所述页面验证请求是否过期具体过程可以为：首先获取从页面验证请求中获取页面验证请求的请求时间及浏览器执行页面脚本的时间，然后判断所述页面验证请求的请求时间是否晚于所述浏览器执行页面脚本的时间与预置时间的和，若页面验证请求的请求时间晚于浏览器执行页面脚本时间与预置时间的和，则确定页面验证请求过期；若页面验证请求的请求时间不晚于浏览器执行页面脚本时间与预置时间的和，则确定页面验证请求未过期。其中，所述预置时间可以根据实际需求进行配置，如 10 分钟、20 分钟、40 分钟等，本发明实施例不做具体限定。需要说明的是，由于攻击者可通过模拟正常用户的行为对服务器进行攻击，而攻击者模拟出正常用户的行为需要一定的时间，因此本发明实施例中在保证用户可正常向服务器发送请求的情况下，预置时间设置的越短，攻击者就越不容易攻击服务器。

例如，从页面验证请求中获取的页面验证请求的请求时间为 13:15，浏览器执行页面脚本的时间为 12:34，预置时间为 1 小时，则经过判断页面验证请求的请求时间早于浏览器执行页面脚本时间与预置时间的和，即 13:15 早于 13:34，因此该页面验证请求未过期。若页面验证请求的请求时间为 14:12，则经过上述判断方式可得出该页面验证请求已经过期。

104a、若过期，则输出页面过期的错误提示信息。

在本发明实施例中，若页面验证请求已经过期，则输出页面过期的错误提示信息，以提示用户当前页面已过了有效期，若用户想继续对该页面进行操作，则需要对该页面进行刷新操作。而对该页面进行刷新操作，相

当于向服务器发送页面请求，服务器接收到请求之后，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本。即在步骤 104a 之后，若接收到用户的刷新指令，则跳转至步骤 101 开始重新执行。

104b、若没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法。

其中，步骤 104b 为步骤 104a 的并列步骤，若页面验证请求没有过期，则验证页面验证请求中保护的脚本执行参数是否合法。在本发明实施例中，验证脚本执行参数是否合法，可以根据执行出该脚本执行参数的页面脚本来实现。步骤 104b 具体过程可以为：首先根据该页面脚本获取本地脚本参数，然后判断所述本地脚本参数和所述页面验证请求中包含的脚本执行参数是否相同，若相同则说明脚本执行参数合法，若不相同则说明脚本执行参数不合法。

例如，接收到浏览器发送的页面验证请求后，从与所述页面请求对应的多个页面脚本中动态随机抽取的页面脚本的脚本执行参数获取逻辑是获取 Cookie 信息中 token 的 MD5（Message-Digest Algorithm 5，消息摘要算法第五版）加密值，若页面验证请求在有效期内，则根据页面脚本中的脚本执行参数获取逻辑判断脚本参数是否能够验证成功，即根据服务器中存储对应 Cookie 信息中 token 的 MD5 加密值验证浏览器发送的脚本参数是否通过。

105b、若不合法，则拒绝该次页面请求。

在本发明实施例中，若验证脚本执行参数不合法，则拒绝该次页面请求之后，若用户想继续对该页面进行操作，则需要对该页面进行刷新操作。而对该页面进行刷新操作，相当于向服务器发送页面请求，服务器接收到请求之后，从与所述页面请求对应的多个页面脚本中动态随机分配一个与

所述页面请求对应的页面脚本。即在步骤 105b 之后，若接收到用户的刷新指令，则跳转至步骤 101 开始重新执行。

需要说明的是，本发明可以通过页面验证请求中的用户身份信息，拒绝该次页面请求，用户身份信息即服务器生成的 Cookie 信息。浏览器在接收到服务器发送的 Cookie 信息后，会将 Cookie 信息中的 key/value 保存到某个目录下的文本文件内，浏览器在下次请求网站时会将该 Cookie 信息发送给服务器。若浏览器发送的页面验证请求已经过期，或脚本执行参数验证不合法，则服务器可以通过将页面验证请求中的 Cookie 信息对应的服务设置为拒绝，以此实现拒绝该次页面请求。

本发明实施例提供的一种防止服务器被攻击的方法，当接收到所述浏览器发送的页面验证请求时，首先判断所述页面验证请求是否过期，若页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法，若脚本执行参数不合法则拒绝该次页面请求，以此实现防止服务器被攻击。与目前通过验证加密的 token 值判断浏览器发送的服务请求是否合法，以实现防止服务器被攻击相比，本发明是通过验证脚本执行参数实现防止服务器被攻击的，由于脚本执行参数是根据与页面请求对应的多个页面脚本中动态随机分配的页面脚本得到的，且各页面脚本之间采用不同的脚本执行参数获取逻辑，因此即便攻击者获得动态代码中的脚本逻辑，也无法在预置时间内破解出其加密方式，且当页面验证请求的请求时间超过预置时间时，服务器将会拒绝该次页面请求，浏览器再次发送页面验证请求则需要从新加载页面验证请求，而从新加载的页面验证请求中的脚本执行参数则是通过执行重新抽取的页面脚本得到的，因此通过本发明实施例攻击者无法对服务器进行攻击，从而本发明实施例提高了服务器的安全性。

本发明实施例提供了另一种防止服务器被攻击的方法，如图 2 所示，

所述方法包括:

201、当接收到浏览器发送的页面请求时，获取所述页面请求中的页面 URL。

202、从预置脚本库中存在的与所述页面 URL 对应的多个页面脚本中随机抽取一个页面脚本。

其中，所述多个页面脚本之间采用不同的脚本执行参数获取逻辑。在本发明实施例中，在步骤 202 之前，所述方法还包括：配置所述预置脚本库中各页面 URL 分别对应的页面脚本。所述预置脚本库中存储有不同 URL 分别对应的多个页面脚本，每个 URL 对应的页面脚本之间采用不同的脚本参数获取逻辑。在本发明实施例中，页面脚本用于执行加载浏览器请求的页面，并从执行的结果中获取脚本执行参数。执行同一页面 URL 分别对应的各页面脚本时，执行不同页面脚本将会产生不同的脚本执行参数。

需要说明的是，由于各个页面脚本之间的区别仅是采用不同的脚本执行参数获取逻辑，因此对各个页面脚本进行加载执行产生的网页页面是相同的，执行各个页面脚本出现的差别仅是执行页面时所产生的脚本执行参数的不同。

203、将所述动态随机分配的页面脚本发送给所述浏览器。

进一步地，以使得所述浏览器执行所述页面脚本获取脚本执行参数。浏览器执行加载执行页面脚本之后会显示出对应的网页，并获取到脚本执行参数，脚本执行参数是网页当中的一些附加参数，本身并不会影响加载显示出来的网页。

204、当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期。

对于本发明实施例，所述步骤 204 包括：判断所述网页验证请求的请求时间是否晚于所述浏览器执行页面脚本的时间与预置时间的和；若是，

则确认所述网页验证请求过期；若否，则确认所述网页验证请求未过期。其中，所述预置时间用于限制浏览器可向服务器发送验证页面请求的时间，所述预置时间可以根据实际需求进行配置。

需要说明的是，由于攻击者可通过模拟正常用户的行为对服务器进行攻击，而攻击者模拟出正常用户的行为需要一定的时间，因此本发明实施例中在保证用户可正常向服务器送请求的情况下，预置时间设置的越短，攻击者就越不容易攻击服务器。

205a、若过期，则输出页面过期的错误提示信息。

205b、若没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法。

其中，步骤205b为步骤205a的并列步骤，若页面验证请求没有过期，则验证页面验证请求中保护的脚本执行参数是否合法。在本发明实施例中，所述网页请求中还包括被所述浏览器执行页面脚本的标识信息，步骤205b包括：从所述预置脚本库中查找与所述标识信息对应的页面脚本，所述预置脚本库中还存储有与各个页面脚本分别对应的标识信息；根据与所述标识信息对应的页面脚本，验证所述页面验证请求中包含的脚本执行参数是否合法。其中，被所述浏览器执行页面脚本即为步骤203中服务器发送给浏览器的页面脚本，服务器将页面脚本发送给浏览器时，也会将该页面脚本对应的标识信息一同发送给浏览器。当浏览器向服务器发送页面验证请求时，会将页面脚本的标识信息一同发送给服务器，然后服务器根据页面脚本标识信息从预置脚本库中获取对应的页面脚本，并根据获取的页面脚本验证脚本执行参数是否正确。

对于本发明实施例，所述根据与所述标识信息对应的页面脚本，验证所述页面验证请求中包含的脚本执行参数是否合法包括：根据与所述标识信息对应的页面脚本获取本地脚本参数；判断所述本地脚本参数和所述页

面验证请求中包含的脚本执行参数是否相同；若相同，则确认所述脚本执行参数合法；若不相同，则确认所述脚本执行参数不合法。

206b、若不合法，则拒绝该次页面请求。

本发明实施例中，若验证脚本执行参数不合法，则拒绝该次页面请求之后，若用户想继续对该页面进行操作，则需要对该页面进行刷新操作。而对该页面进行刷新操作，相当于向服务器发送页面请求，服务器接收到请求之后，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本。即在拒绝该次页面请求之后，若接收到用户的刷新指令，则跳转至步骤201开始重新执行，而从新执行步骤201之后又将会重新随机抽取页面脚本，因此通过本发明实施例攻击者无法对服务器进行攻击，从而通过本发明实施例提高了服务器的安全性。

对于本发明实施例，可以应用的场景如图5所示，但不仅限于此，包括：如图5中的步骤1，浏览器首先向服务器发送页面请求，所述页面请求中包括页面URL，服务器在接收到页面请求后从所述预置脚本库中随机抽取出一个与所述页面 URL 对应的页面脚本，然后将所述页面脚本发送给所述浏览器，即服务器通过图5当中的步骤2服务器向浏览器发送随机抽取的页面脚本；浏览器在接收到服务器发送的页面脚本之后，执行所述页面脚本并获取通过执行所述页面脚本得到的脚本执行参数，之后向服务器发送页面验证请求，所述页面验证请求中携带有脚本执行参数，即浏览器通过图5当中的步骤3向服务器发送页面验证请求，服务器在接收到页面验证请求后，首先判断所述页面验证请求的时间是否晚于所述浏览器执行页面脚本的时间与所述预置时间的和，若所述页面验证请求的时间早于所述浏览器执行页面脚本的时间与所述预置时间的和，则验证所述脚本执行参数是否合法，若不合法，则拒绝该次页面请求。由于本发明中的脚本执行参数是通过执行从预置脚本库中随机抽取的与页面 URL 对应的页面

脚本得到的，且页面脚本之间采用不同的脚本执行参数获取逻辑，因此即便攻击者获得动态代码中的脚本逻辑，也无法在预置时间内破解出其加密方式，且当页面验证请求的时间过期时，浏览器则需要从新加载，从新加载的页面验证请求中的脚本执行参数则是通过执行重新抽取的与页面URL对应的页面脚本得到的，因此通过本发明实施例攻击者无法对服务器进行攻击，从而通过本发明实施例提高了服务器的安全性。

本发明实施例提供的另一种防止服务器被攻击的方法，当接收到所述浏览器发送的页面验证请求时，首先判断所述页面验证请求是否过期，若页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法，若脚本执行参数不合法则拒绝该次页面请求，以此实现防止服务器被攻击。与目前通过验证加密的 token 值判断浏览器发送的服务请求是否合法，以实现防止服务器被攻击相比，本发明是通过验证脚本执行参数实现防止服务器被攻击的，由于脚本执行参数是根据与页面请求对应的多个页面脚本中动态随机分配的页面脚本得到的，且各页面脚本之间采用不同的脚本执行参数获取逻辑，因此即便攻击者获得动态代码中的脚本逻辑，也无法在预置时间内破解出其加密方式，且当页面验证请求的请求时间超过预置时间时，服务器将会拒绝该次页面请求，浏览器再次发送页面验证请求则需要从新加载页面验证请求，而从新加载的页面验证请求中的脚本执行参数则是通过执行重新抽取的页面脚本得到的，因此通过本发明实施例攻击者无法对服务器进行攻击，从而本发明实施例提高了服务器的安全性。

进一步地，本发明实施例提供一种防止服务器被攻击的装置，如图 3 所示，所述装置包括：分配单元 31、发送单元 32、判断单元 33、输出单元 34、验证单元 35、拒绝单元 36。

分配单元 31，当接收到浏览器发送的页面请求时，从与所述页面请求

对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本;

发送单元 32，将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数;

判断单元 33，若所述页面验证请求过期，则输出页面过期的错误提示信息;

输出单元 34，若过期，则输出页面过期的错误提示信息;

验证单元 35，若所述页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法;

拒绝单元 36，若所述页面验证请求中包含的脚本执行参数不合法，则拒绝该次页面请求。

需要说明的是，本发明实施例提供的一种防止服务器被攻击的装置所涉及各功能单元的其他相应描述，可以参考图 1 所示方法的对应描述，在此不再赘述，但应当明确，本实施例中的装置能够对应实现前述方法实施例中的全部内容。

本发明实施例提供的一种防止服务器被攻击的方法及装置，当接收到所述浏览器发送的页面验证请求时，首先判断所述页面验证请求是否过期，若页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法，若脚本执行参数不合法则拒绝该次页面请求，以此实现防止服务器被攻击。与目前通过验证加密的 token 值判断浏览器发送的服务请求是否合法，以实现防止服务器被攻击相比，本发明是通过验证脚本执行参数实现防止服务器被攻击的，由于脚本执行参数是根据与页面请求对应的多个页面脚本中动态随机分配的页面脚本得到的，且各页面脚本之间采用不同的脚本执行参数获取逻辑，因此即便攻击者获得动态代码中的脚本逻辑，也无法在预置时间内破解出其加密方式，且当页面验证请求的

请求时间超过预置时间时，服务器将会拒绝该次页面请求，浏览器再次发送页面验证请求则需要从新加载页面验证请求，而从新加载的页面验证请求中的脚本执行参数则是通过执行重新抽取的页面脚本得到的，因此通过本发明实施例攻击者无法对服务器进行攻击，从而本发明实施例提高了服务器的安全性。

进一步地，本发明实施例提供另一种防止服务器被攻击的装置，如图4所示，所述装置包括：分配单元41、发送单元42、判断单元43、输出单元44、验证单元45、拒绝单元46。

分配单元41，当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本；

发送单元42，将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数；

判断单元43，若所述页面验证请求过期，则输出页面过期的错误提示信息；

输出单元44，若过期，则输出页面过期的错误提示信息；

验证单元45，若所述页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法；

拒绝单元46，若所述页面验证请求中包含的脚本执行参数不合法，则拒绝该次页面请求。

进一步地，所述分配单元41包括：

获取模块411，获取所述页面请求中的页面URL；

抽取模块412，从预置脚本库中存在的与所述页面URL对应的多个页面脚本中随机抽取一个页面脚本，所述多个页面脚本之间采用不同的脚本执行参数获取逻辑。

进一步地，所述判断单元 43 包括;

判断模块 431，判断所述网页验证请求的请求时间是否晚于所述浏览器执行页面脚本的时间与预置时间的和;

确定模块 432，若所述网页验证请求的请求时间晚于所述浏览器执行页面脚本的时间与预置时间的和，则确认所述网页验证请求过期;

确定模块 432，若所述网页验证请求的请求时间不晚于所述浏览器执行页面脚本的时间与预置时间的和，则确认所述网页验证请求没有过期。

对于本发明实施例，所述网页请求中还包括被所述浏览器执行页面脚本的标识信息，所述验证单元 45 包括:

查找模块 451，从所述预置脚本库中查找与所述标识信息对应的页面脚本，所述预置脚本库中还存储有与各个页面脚本分别对应的标识信息;

验证模块 452，根据与所述标识信息对应的页面脚本，验证所述页面验证请求中包含的脚本执行参数是否合法。

对于本发明实施例，所述根据与所述标识信息对应的页面脚本，

所述验证模块 452，根据与所述标识信息对应的页面脚本获取本地脚本参数;

所述验证模块 452，判断所述本地脚本参数和所述页面验证请求中包含的脚本执行参数是否相同;

所述验证模块 452，若本地脚本参数和所述页面验证请求中包含的脚本执行参数相同，则确认所述脚本执行参数合法;

所述验证模块 452，若本地脚本参数和所述页面验证请求中包含的脚本执行参数不相同，则确认所述脚本执行参数不合法。

进一步地，所述装置还包括:

配置单元 47，配置所述预置脚本库中各页面 URL 分别对应的页面脚本。

需要说明的是，本发明实施例提供的另一种防止服务器被攻击的装置所涉及各功能单元的其他相应描述，可以参考图 2 所示方法的对应描述，在此不再赘述，但应当明确，本实施例中的装置能够对应实现前述方法实施例中的全部内容。

本发明实施例提供的一种防止服务器被攻击的方法及装置，当接收到所述浏览器发送的页面验证请求时，首先判断所述页面验证请求是否过期，若页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法，若脚本执行参数不合法则拒绝该次页面请求，以此实现防止服务器被攻击。与目前通过验证加密的 token 值判断浏览器发送的服务请求是否合法，以实现防止服务器被攻击相比，本发明是通过验证脚本执行参数实现防止服务器被攻击的，由于脚本执行参数是根据与页面请求对应的多个页面脚本中动态随机分配的页面脚本得到的，且各页面脚本之间采用不同的脚本执行参数获取逻辑，因此即便攻击者获得动态代码中的脚本逻辑，也无法在预置时间内破解出其加密方式，且当页面验证请求的请求时间超过预置时间时，服务器将会拒绝该次页面请求，浏览器再次发送页面验证请求则需要从新加载页面验证请求，而从新加载的页面验证请求中的脚本执行参数则是通过执行重新抽取的页面脚本得到的，因此通过本发明实施例攻击者无法对服务器进行攻击，从而本发明实施例提高了服务器的安全性。

所述防止服务器被攻击的装置包括处理器和存储器，上述分配单元、发送单元、判断单元、输出单元、验证单元、拒绝单元和配置单元等均作为程序单元存储在存储器中，由处理器执行存储在存储器中的上述程序单元来实现相应的功能。

处理器中包含内核，由内核去存储器中调取相应的程序单元。内核可以设置一个或以上，通过调整内核参数来提高服务器的安全性。

存储器可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)，存储器包括至少一个存储芯片。

本申请还提供了一种计算机程序产品，当在数据处理设备上执行时，适于执行初始化有如下方法步骤的程序代码：当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本；将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数；当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期；若过期，则输出页面过期的错误提示信息；若没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法；若不合法，则拒绝该次页面请求。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的防止服务器被攻击方法及装置、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个

方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

存储器可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。存储器是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号

和载波。

以上仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理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权利要求范围之内。

权 利 要 求 书

1、一种防止服务器被攻击的方法，其特征在于，包括:

当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本;

将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数;

当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期;

若过期，则输出页面过期的错误提示信息;

若没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法;

若不合法，则拒绝该次页面请求。

2、根据权利要求 1 所述的方法，其特征在于，所述从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本包括:

获取所述页面请求中的页面 URL;

从预置脚本库中存在的与所述页面 URL 对应的多个页面脚本中随机抽取一个页面脚本，所述多个页面脚本之间采用不同的脚本执行参数获取逻辑。

3、根据权利要求 1 所述的方法，其特征在于，所述判断所述页面验证请求是否过期包括:

判断所述网页验证请求的请求时间是否晚于所述浏览器执行页面脚本的时间与预置时间的和;

若是，则确认所述网页验证请求过期;

若否，则确认所述网页验证请求未过期。

4、根据权利要求 1-3 任一所述的方法，其特征在于，所述网页请求中还包括被所述浏览器执行页面脚本的标识信息，所述验证所述页面验证请求中包含的脚本执行参数是否合法包括:

从所述预置脚本库中查找与所述标识信息对应的页面脚本，所述预置脚本库中还存储有与各个页面脚本分别对应的标识信息;

根据与所述标识信息对应的页面脚本，验证所述页面验证请求中包含的脚本执行参数是否合法。

5、根据权利要求 4 所述的方法，其特征在于，所述根据与所述标识信息对应的页面脚本，验证所述页面验证请求中包含的脚本执行参数是否合法包括:

根据与所述标识信息对应的页面脚本获取本地脚本参数;

判断所述本地脚本参数和所述页面验证请求中包含的脚本执行参数是否相同;

若相同，则确认所述脚本执行参数合法;

若不相同，则确认所述脚本执行参数不合法。

6、根据权利要求 2 所述的方法，其特征在于，所述从预置脚本库中存在的与所述页面 URL 对应的多个页面脚本中随机抽取一个页面脚本之前，所述方法还包括:

配置所述预置脚本库中各页面 URL 分别对应的页面脚本，及所述页面脚本对应的标识信息。

7、一种防止服务器被攻击的装置，其特征在于，包括:

分配单元，当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本;

发送单元，将所述动态随机分配的页面脚本发送给所述浏览器，以使得所述浏览器执行所述页面脚本获取脚本执行参数;

判断单元，当接收到所述浏览器发送的页面验证请求时，判断所述页面验证请求是否过期;

输出单元，若所述页面验证请求过期，则输出页面过期的错误提示信息;

验证单元，若所述页面验证请求没有过期，则验证所述页面验证请求中包含的脚本执行参数是否合法;

拒绝单元，若所述页面验证请求中包含的脚本执行参数不合法，则拒绝该次页面请求。

8、根据权利要求 7 所述的装置，其特征在于，所述分配单元包括:

获取模块，获取所述页面请求中的页面 URL;

抽取模块，从预置脚本库中存在的与所述页面 URL 对应的多个页面脚本中随机抽取一个页面脚本，所述多个页面脚本之间采用不同的脚本执行参数获取逻辑。

9、根据权利要求 7 所述的装置，其特征在于，所述判断单元包括;

判断模块，判断所述网页验证请求的请求时间是否晚于所述浏览器执行页面脚本的时间与预置时间的和;

确定模块，若所述网页验证请求的请求时间晚于所述浏览器执行页面脚本的时间与预置时间的和，则确认所述网页验证请求过期;

确定模块，若所述网页验证请求的请求时间不晚于所述浏览器执行页面脚本的时间与预置时间的和，则确认所述网页验证请求没有过期。

10、根据权利要求 7-9 任一所述的装置，其特征在于，所述网页请求中还包括被所述浏览器执行页面脚本的标识信息，所述验证单元包括:

查找模块，从所述预置脚本库中查找与所述标识信息对应的页面脚本，所述预置脚本库中还存储有与各个页面脚本分别对应的标识信息;

验证模块，根据与所述标识信息对应的页面脚本，验证所述页面验证

请求中包含的脚本执行参数是否合法。

11、根据权利要求 10 所述的装置，其特征在于，

所述验证模块，根据与所述标识信息对应的页面脚本获取本地脚本参数；

所述验证模块，判断所述本地脚本参数和所述页面验证请求中包含的脚本执行参数是否相同；

所述验证模块，若所述本地脚本参数和所述页面验证请求中包含的脚本执行参数相同，则确认所述脚本执行参数合法；

所述验证模块，若所述本地脚本参数和所述页面验证请求中包含的脚本执行参数不相同，则确认所述脚本执行参数不合法。

12、根据权利要求 8 所述的装置，其特征在于，所述装置还包括：

配置单元，配置所述预置脚本库中各页面 URL 分别对应的页面脚本，及所述页面脚本对应的标识信息。

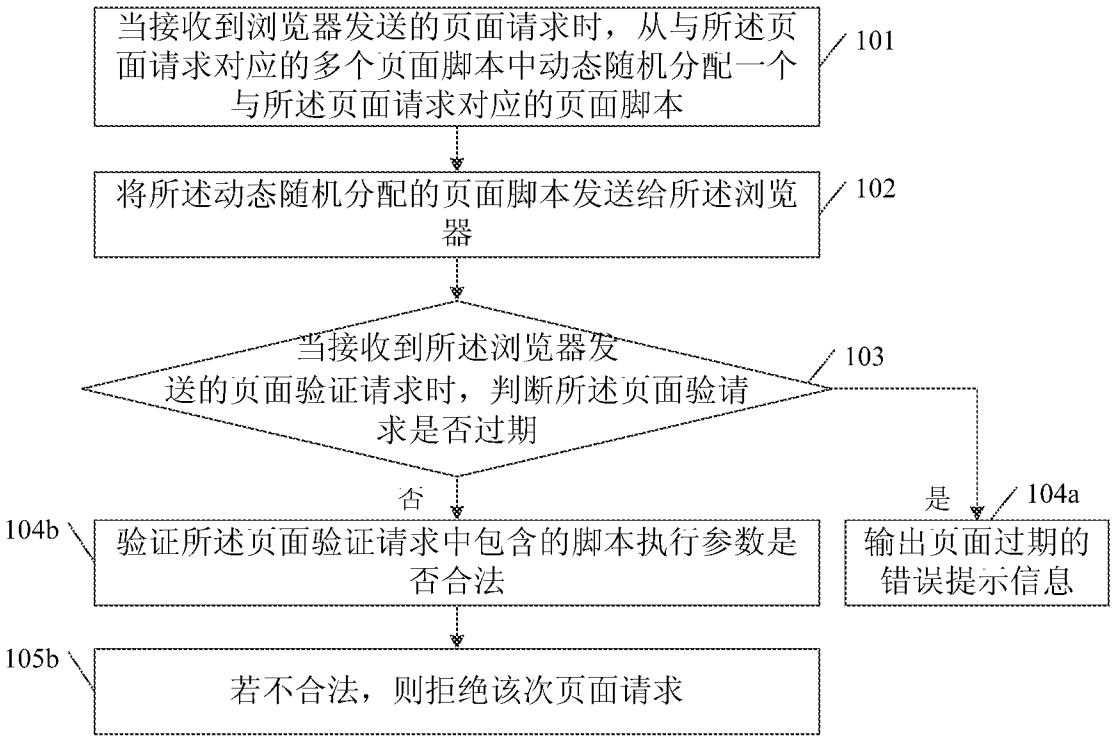
当接收到浏览器发送的页面请求时，从与所述页面请求对应的多个页面脚本中动态随机分配一个与所述页面请求对应的页面脚本
101
将所述动态随机分配的页面脚本发送给所述浏览器
102
当接收到所述浏览器发送的页面验证请求时，判断所述页面验请求是否过期
103
否
是
104a
输出页面过期的错误提示信息
104b
验证所述页面验证请求中包含的脚本执行参数是否合法
105b
若不合法，则拒绝该次页面请求

图 1

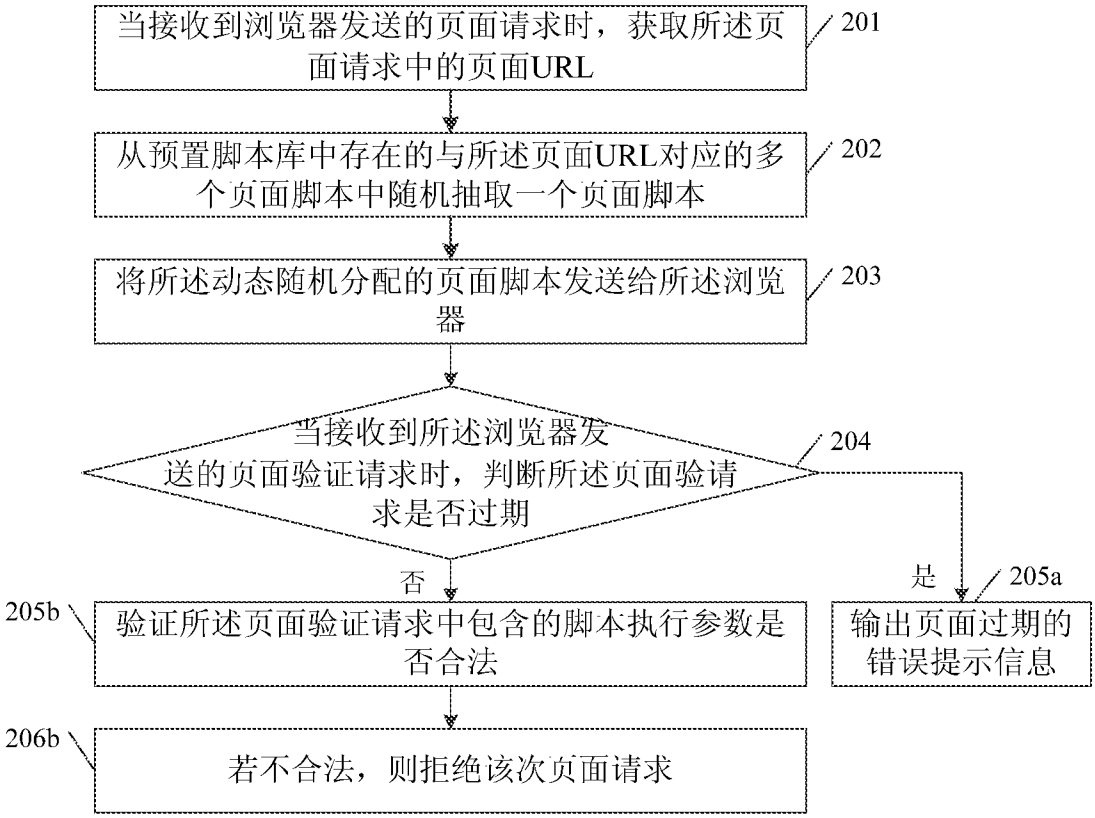
当接收到浏览器发送的页面请求时，获取所述页面请求中的页面URL
201
从预置脚本库中存在的与所述页面URL对应的多个页面脚本中随机抽取一个页面脚本
202
将所述动态随机分配的页面脚本发送给所述浏览器
203
当接收到所述浏览器发送的页面验证请求时，判断所述页面验请求是否过期
204
否
是
205a
输出页面过期的错误提示信息
205b
验证所述页面验证请求中包含的脚本执行参数是否合法
206b
若不合法，则拒绝该次页面请求

图 2

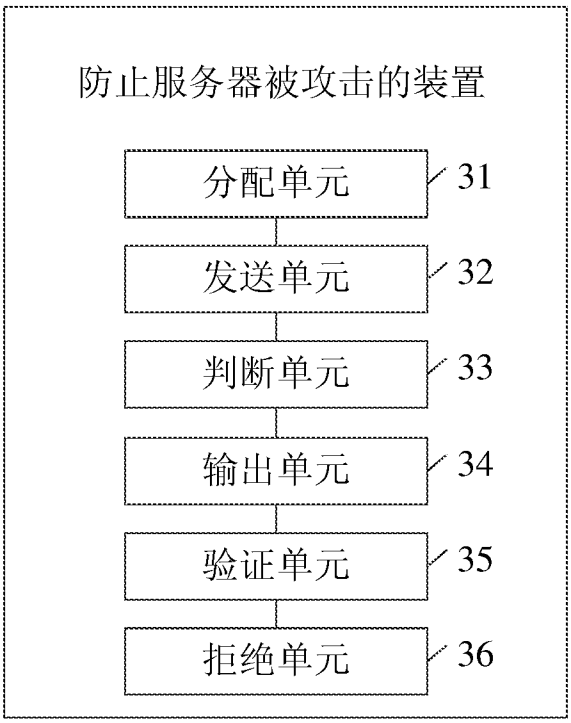
防止服务器被攻击的装置
分配单元
31
发送单元
32
判断单元
33
输出单元
34
验证单元
35
拒绝单元
36

图 3

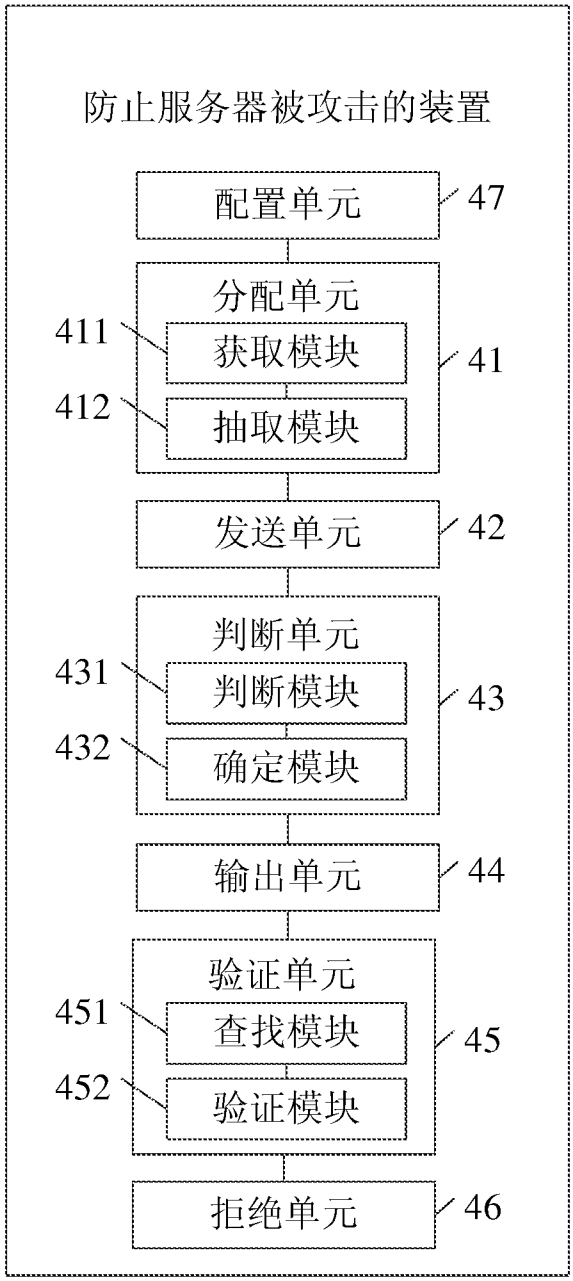
防止服务器被攻击的装置
配置单元
47
分配单元
411
获取模块
41
412
抽取模块
发送单元
42
判断单元
431
判断模块
43
432
确定模块
输出单元
44
验证单元
451
查找模块
45
452
验证模块
拒绝单元
46

图 4

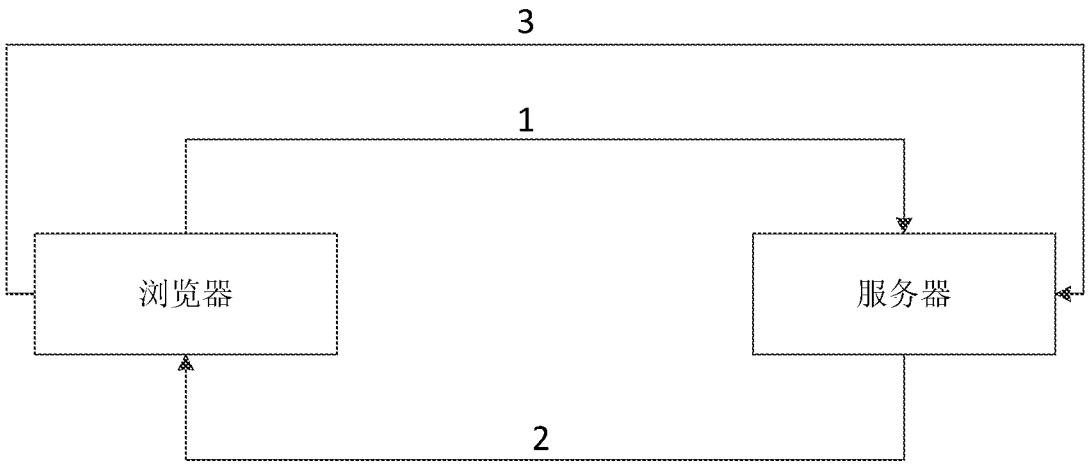

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/080862

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/02 (2006. 01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; H04L; H04Q; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: web, script, authen+, verif???, access control, time out, time, threshold, dynamic+, random, stochastic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101834866 A (BEIJING LAIAN TECHNOLOGY CO., LTD.) 15 September 2010 (15.09.2010) description, paragraphs [0007]-[0013] and [0033]-[0039]	1-12
A	CN 103139138 A (FORTINET, INC.) 05 June 2013 (05.06.2013) the whole document	1-12
A	CN 103795786 A (HANGZHOU PAX ELECTRONIC TECHNOLOGY CO., LTD.) 14 May 2014 (14.05.2014) the whole document	1-12
A	US 2015365397 A1 (VIVOTEK INC.) 17 December 2015 (17.12.2015) the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 June 2017	12 July 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer ZHANG,, Feng Telephone No. (86-10) 62413247

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/080862

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101834866 A	15 September 2010	None	
CN 103139138 A	05 June 2013	None	
CN 103795786 A	14 May 2014	None	
US 2015365397 A1	17 December 2015	TW 201547247 A	16 December 2015

国际检索报告

国际申请号
PCT/CN2017/080862

A. 主题的分类

H04L 29/02(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F; H04L; H04Q; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC：网页，页面，脚本，验证，认证，鉴权，访问控制，过期，超时，超期，时间，阈值，动态，随机，web, script, authen+, verif???, access control, time out, time, threshold, dynamic+, random, stochastic

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 101834866 A (北京来安科技有限公司) 2010年 9月 15日 (2010 - 09 - 15) 说明书第[0007]-[0013]、[0033]-[0039]段	1-12
A	CN 103139138 A (飞塔公司) 2013年 6月 5日 (2013 - 06 - 05) 全文	1-12
A	CN 103795786 A (杭州百富电子技术有限公司) 2014年 5月 14日 (2014 - 05 - 14) 全文	1-12
A	US 2015365397 A1 (VIVOTEK INC.) 2015年 12月 17日 (2015 - 12 - 17) 全文	1-12

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 6月 21日	2017年 7月 12日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张枫 电话号码 (86-10)62413247

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/080862

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 101834866 A	2010年 9月 15日	无	
CN 103139138 A	2013年 6月 5日	无	
CN 103795786 A	2014年 5月 14日	无	
US 2015365397 A1	2015年 12月 17日	TW 201547247 A	2015年 12月 16日