

(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2月2日 (02.02.2017)



(10) 国际公布号
WO 2017/016458 A1

- (51) 国际专利分类号:
G06F 21/64 (2013.01)
- (21) 国际申请号: PCT/CN2016/091539
- (22) 国际申请日: 2016年7月25日 (25.07.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510441013.7 2015年7月24日 (24.07.2015) CN
201510441257.5 2015年7月24日 (24.07.2015) CN
201510441057.X 2015年7月24日 (24.07.2015) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街28号D座112室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路6号院2号楼B座2层、3层301-306室, Beijing 100015 (CN)。
- (72) 发明人: 吴张树 (WU, Zhangshu); 中国北京市朝阳区酒仙桥路6号院2号楼B座2层、3层301-306

室, Beijing 100015 (CN)。李永剑 (LI, Yongjian); 中国北京市朝阳区酒仙桥路6号院2号楼B座2层、3层301-306室, Beijing 100015 (CN)。彭力扬 (PENG, Liyang); 中国北京市朝阳区酒仙桥路6号院2号楼B座2层、3层301-306室, Beijing 100015 (CN)。

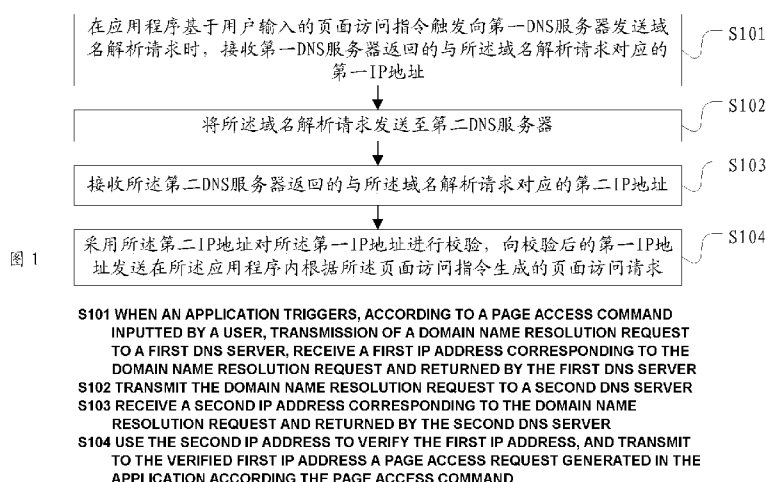
(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街31号神舟大厦702, Beijing 100081 (CN)。

(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, 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, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, 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。

[见续页]

(54) Title: APPLICATION INTERNAL PAGE PROCESSING METHOD AND DEVICE

(54) 发明名称: 应用程序内的页面处理方法和装置



(57) Abstract: The invention relates to the technical field of communications. Disclosed are an application internal page processing method and device. The invention uses a second IP address returned by a second DNS server to verify a first IP address returned by a first DNS server, and transmits to the verified first IP address a page access request generated in an application according to a page access command. Moreover, a sign-on function can be called to determine whether a jump in a first response page in the application occurs, thereby timely and accurately determining whether a jump in the first response page occurs. Further, a scan script embedded in the first response page can be loaded to detect whether the first response page in the application has been tampered with, thereby timely and accurately determining whether the first response page has been tampered with, improving user experience, and guaranteeing information and property security for a user.

(57) 摘要:

[见续页]



WO 2017/016458 A1

(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))。

本发明公开了一种应用程序内的页面处理方法和装置, 涉及通信技术领域。本发明通过第二 DNS 服务器返回的第二 IP 地址对第一 DNS 服务器返回的第一 IP 地址进行校验, 向校验后的第一 IP 地址发送在所述应用程序内根据页面访问指令生成的页面访问请求, 还可以通过调用签到函数来确定应用程序内第一响应页面是否发生跳转, 能够即时准确地确定所述第一响应页面是否发生跳转, 还可以通过加载第一响应页面中内嵌的扫描脚本, 以检测所述应用程序内第一响应页面是否被篡改, 能够即时准确地确定所述第一响应页面是否被篡改, 提高了用户体验, 保证了用户的信息安全及财产安全。

说明书

应用程序内的页面处理方法和装置

技术领域

5 本发明涉及通信技术领域，特别涉及一种应用程序内的页面处理方法和装置。

背景技术

DNS (Domain Name System, 域名系统)，因特网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。

10 用户通常需要通过运营商局域 DNS 服务器来实现页面访问，但现有技术中，由于运营商局域 DNS 服务器中的内容可能被篡改，又或是用户的路由器上 DNS 服务器地址被修改，可能导致不能正常访问页面，影响用户体验，也可能导致用户在正常访问页面时，被链接至钓鱼网站或木马网站等欺诈网站，影响用户的信息安全及财产安全。

发明内容

15 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一种应用程序内的页面访问方法及装置。

依据本发明的一个方面，提供了一种应用程序内的页面访问方法，所述方法包括：

在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址；

将所述域名解析请求发送至第二DNS服务器；

20 接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址；

采用所述第二IP地址对所述第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求。

依据本发明的另一个方面，提供了一种确定应用程序内页面跳转的方法，所述方法包括：

25 在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面；

通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转。

依据本发明的另一个方面，提供了一种检测应用程序内页面篡改方法，所述方法包括：

在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面；

30 加载所述第一响应页面中内嵌的扫描脚本，以检测所述应用程序内第一响应页面是否被篡改。

依据本发明的另一个方面，提供了一种应用程序内的页面访问装置，所述装置包括：

指令触发器，适于在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址；

请求发送器，适于将所述域名解析请求发送至第二DNS服务器；

35 地址接收器，适于接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址；

校验访问器，适于采用所述第二IP地址对所述第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求。

依据本发明的另一个方面，提供了一种确定应用程序内页面跳转的装置，所述装置包括：

40 页面接收器，适于在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面；

跳转确定器，适于通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转。

依据本发明的另一个方面，提供了一种检测应用程序内页面篡改装置，所述装置包括：

页面接收器，适于在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面；

45 篡改检测器，适于加载所述第一响应页面中内嵌的扫描脚本，以检测所述应用程序内第一响应页面是否被篡改。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行上述的任一个应用程序内的页面访问方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了执行上述的任一个应用程序内的页面访问方法的计算机程序。

5 根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行上述的任一个确定应用程序内页面跳转的方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了执行上述的任一个确定应用程序内页面跳转的方法的计算机程序。

10 根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行上述的任一个检测应用程序内页面篡改方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了执行上述的任一个检测应用程序内页面篡改方法的计算机程序。

15 本发明实施例的应用程序内的页面访问方法和装置，可以通过第二DNS服务器返回的第二IP地址对第一DNS服务器返回的第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据页面访问指令生成的页面访问请求，保证了页面的正常访问，提高了用户体验，另外，也保证了用户的信息安全及财产安全。

本发明实施例的确定应用程序内页面跳转的方法及装置，可以通过调用签到函数来确定应用程序内第一响应页面是否发生跳转，能够即时准确地确定所述第一响应页面是否发生跳转，提高了用户体验，并且保证了用户的信息安全及财产安全。

20 本发明实施例的检测应用程序内页面篡改方法及装置，可以通过加载第一响应页面中内嵌的扫描脚本，以检测所述应用程序内第一响应页面是否被篡改，能够即时准确地确定所述第一响应页面是否被篡改，提高了用户体验。

附图说明

25 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是本发明一种实施方式的应用程序内的页面访问方法的流程图；

图2是本发明一种实施方式的应用程序内的页面访问方法的流程图；

图3是本发明一种实施方式的应用程序内的页面访问方法的流程图；

30 图4是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图；

图5是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图；

图6是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图；

图7是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图；

图8是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；

35 图9是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；

图10是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；

图11是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；

图12是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；

图13是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；

40 图14是本发明一种实施方式的应用程序内的页面访问装置的结构框图；

图15是本发明一种实施方式的确定应用程序内页面跳转的装置的结构框图；

图16是本发明一种实施方式的检测应用程序内页面篡改装置的结构框图；

图17示出了用于执行根据本发明的方法的终端设备的框图；

图18示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。

45 具体实施方式

下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，

但不用来限制本发明的范围。

图1是本发明一种实施方式的应用程序内的页面访问方法的流程图；参照图1，所述方法包括：

S101：在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址；

5 需要说明的是，所述第一DNS服务器通常为运营商局域DNS服务器，但该DNS服务器中的内容可能被篡改，当然，也有可能为被黑客修改的DNS服务器（即应用程序的DNS服务器地址被修改）。

可理解的是，所述域名解析请求中包括有待解析域名，相应的，与所述域名解析请求对应的第一IP地址即为与所述待解析域名对应的IP地址。

S102：将所述域名解析请求发送至第二DNS服务器；

10 需要说明的是，所述第二DNS服务器可理解为第三方提供的DNS服务器，第二DNS服务器的链接地址可直接存储于本地，在需要执行步骤S102时，则直接从本地找到第二DNS服务器的链接地址，将所述域名解析请求根据链接地址发送至第二DNS服务器。

可理解的是，若直接将所述域名解析请求以明文方式（即HTTP协议等）发送至第二DNS服务器，则容易被黑客截获，从而难以保证所述第二DNS服务器所返回信息的真实性，为避免出现该问题，本实施方式
15 中，将所述域名解析请求通过加密协议（即HTTPS协议等）发送至第二DNS服务器；

在具体实现中，若将所有域名解析请求均向第一DNS服务器发送，又向第二DNS服务器发送，会对页面访问速度造成影响，为避免该问题，本实施方式中可以三个判断条件作为步骤S102的触发条件：

第一、判断本地是否第一次连接所述第一DNS服务器，若是，则执行步骤S102；

可理解的是，当本地是第一次连接所述第一DNS服务器时，无法确定该第一DNS服务器的域名解析
20 是否存在问题，故而，对该第一DNS服务器所返回的第一IP地址进行校验，则非常必要。

第二、判断本地连接的网络是否发生变化，若是，则执行步骤S102；

在具体实现中，在本地连接的网络发生变化（例如：所述应用程序为移动终端上的应用程序时，该移动终端的网络从3G网络变为WLAN网络）时，其所属的第一DNS服务器则很可能发生变化，故而，对该第一DNS服务器所返回的第一IP地址进行校验，则非常必要。

25 第三、判断本地IP地址是否发生变化，若是，则执行步骤S102。

在具体实现中，在本地IP地址发生变化时，其所属的第一DNS服务器也很可能发生变化，对该第一DNS服务器所返回的第一IP地址进行校验，则非常必要。

S103：接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址；

需要说明的是，若将所述域名解析请求是通过加密协议（即HTTPS协议等）发送至第二DNS服务器，
30 则所述第二DNS服务器通过加密协议返回所述第二IP地址。

S104：采用所述第二IP地址对所述第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求。

本实施方式通过第二DNS服务器返回的第二IP地址对第一DNS服务器返回的第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据页面访问指令生成的页面访问请求，保证了页面的正常
35 访问，提高了用户体验，另外，也保证了用户的信息安全及财产安全。

图2是本发明一种实施方式的应用程序内的页面访问方法的流程图；参照图2，所述方法包括：

S201：在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址；

S202：将所述域名解析请求发送至第二DNS服务器；

40 S203：接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址；

需要说明的是，步骤S201-S203与图1所示的实施方式的步骤S101-S103相同，在此不再赘述。

S204：判断所述第一IP地址是否与所述第二IP地址相同，若所述第一IP地址与所述第二IP地址相同，则认定所述第一IP地址校验通过，若所述第一IP地址与所述第二IP地址不相同，则认定所述第一IP地址未校验通过，并将所述第一IP地址修改为第二IP地址，向校验后的第一IP地址发送在所述应用程序内根
45 据所述页面访问指令生成的页面访问请求。

可理解的是，在所述第一IP地址与所述第二IP地址相同时，则认定所述第一IP地址校验通过，此时，

所述校验后的第一IP地址即为该第一IP地址本身；在所述第一IP地址与所述第二IP地址不相同，则认定所述第一IP地址未验证通过，并将所述第一IP地址修改为第二IP地址，此时，所述校验后的第一IP地址即为所述第二IP地址。

下面以一个具体的实例来说明，但不限定本发明的保护范围，设所述域名解析请求中包括的待解析域名为M.haoshou.com，将该域名解析请求发送至第一DNS服务器后，接收所述第一DNS服务器返回的第一IP地址为125.88.193.213，再将所述域名解析请求发送至第二DNS服务器后，若接收所述第二DNS服务器返回的第二IP地址为125.88.193.213时，则认为所述第一IP地址校验通过，校验后的第一IP地址即为125.88.193.213；

若接收所述第二DNS服务器返回的第二IP地址为125.88.192.144时，则认为所述第一IP地址未校验通过，并将所述第一IP地址修改为125.88.192.144，校验后的第一IP地址即为125.88.192.144。

在具体实现中，在所述第一IP地址未校验通过时，则说明第一DNS服务器的域名解析存在问题，故而，可先不通过第一DNS服务器进行域名解析，当然，若所有域名解析均直接通过第二DNS服务器，可能会导致第二DNS服务器的负荷过大，故而，可在第一预设时间内直接通过所述第二DNS服务器进行域名解析，在之后继续尝试通过第一DNS服务器进行域名解析。

图3是本发明一种实施方式的应用程序内的页面访问方法的流程图；参照图3，所述方法包括：

S300：接收用户输入的搜索词，根据所述搜索词查找与所述搜索词相关的网页信息，并将查找到的网页信息展示于所述应用程序内的显示界面中，接收用户在所述应用程序内的显示界面中输入的页面访问指令；

可理解的是，由于查找到的网页信息展示于应用程序内的显示界面中，此时，用户通常会输入与需要访问的网页信息对应的页面访问指令，故而，在步骤S301中域名解析请求中的待解析域名即为所述需要访问的网页信息的待解析域名。

S301：在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址；

S302：将所述域名解析请求发送至第二DNS服务器；

S303：接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址；

S304：采用所述第二IP地址对所述第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求；

需要说明的是，步骤S301-S304与图1所示的实施方式的步骤S101-S104相同，在此不再赘述。

S305：接收与所述页面访问请求对应的响应页面，在所述应用程序内的显示界面中展示所述响应页面。

在具体实现中，为了便于用户阅读响应页面，故而，在接收与所述页面访问请求对应的响应页面后，在所述应用程序内的显示界面中展示所述响应页面。

在以上实施方式中仅能保证校验后的第一IP地址的准确性，但若黑客通过修改所述响应页面，在所述响应页面中添加跳转代码，则会导致所述响应页面被跳转至其他页面，影响用户对页面的浏览，并且也可能导致跳转至钓鱼网站或木马网站等欺诈网站，影响用户的信息安全及财产安全，为避免出现该问题，本实施方式中，在步骤S305中，接收与所述页面访问请求对应的响应页面之后，所述方法还包括：

判断是否能够调用所述响应页面的签到函数，若能调用所述响应页面的签到函数，则执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤，若不能调用所述响应页面的签到函数，则通过加密协议重新向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求，接收与该页面访问请求对应的响应页面，并执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤。

在不能调用所述响应页面的签到函数时，说明所述响应页面中被添加跳转代码，为避免后续的响应页面被继续添加跳转代码，影响用户的正常使用，可通过加密协议向校验后的第一IP地址发送后续的页面访问请求。

当然，考虑到后续的页面访问速度，在通过加密协议向校验后的第一IP地址发送后续的页面访问请求达到第二预设时间（可设为1小时，当然，还可设置为其他时长）时，可执行所述向校验后的第一IP地

址发送后续的页面访问请求;

另外,在本地连接的网络发生变化或本地IP地址发生变化时,由于本地的网络环境发生了变化,可执行所述向校验后的第一IP地址发送后续的页面访问请求。

5 由于响应页面即使不被添加跳转代码,也可能被进行篡改,影响用户体验,为避免该问题,本实施方式中,在步骤S305中,接收与所述页面访问请求对应的响应页面之后,所述方法还包括:

通过加载于所述响应页面中的脚本扫描所述响应页面的DOM树,若所述DOM树中具有不在白名单中的外链,则通过加密协议重新向校验后的第一IP地址发送页面访问请求,接收与该页面访问请求对应的响应页面,并执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤;否则执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤。

10 当然,考虑到后续的页面访问速度,在通过加密协议向校验后的第一IP地址发送后续的页面访问请求达到第二预设时间(可设为1小时,当然,还可设置为其他时长)时,可执行所述向校验后的第一IP地址发送后续的页面访问请求;

另外,在本地连接的网络发生变化或本地IP地址发生变化时,由于本地的网络环境发生了变化,可执行所述向校验后的第一IP地址发送后续的页面访问请求。

15 在所述DOM树中具有不在白名单中的外链时,说明该响应页面中已经被篡改,可通过加密协议向校验后的第一IP地址发送后续的页面访问请求。

可理解的是,本实施方式中,在所述DOM树中具有不在白名单中的外链时,向后台服务器发送所述不在白名单中的外链,所述后台服务器即为所述应用程序的后台服务器,其可为云服务器,对接收到的所述不在白名单中的外链进行进一步分析,以更新所述白名单。

20 对于方法实施方式,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明实施方式并不受所描述的动作顺序的限制,因为依据本发明实施方式,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施方式均属于优选实施方式,所涉及的动作并不一定是本发明实施方式所必须的。

25 图4是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图;参照图4,所述方法包括:

S401:在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面;

可理解的是,所述应用程序在接收到第一响应页面后,即对所述第一响应页面进行加载。

S402:通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转。

30 需要说明的是,所述签到函数为内嵌于第一响应页面中的js脚本,在所述应用程序访问到第一响应页面的前端服务器或所述第一响应页面正常调用显示时,所述签到函数能够被调用,并在被调用后将签到标志进行置位。

因此,当所述应用程序在所述第一响应页面加载时,可先将签到标志设置为初始值(通常设置为0),只有在所述应用程序访问到第一响应页面的前端服务器及所述第一响应页面正常调用显示时,才能调用

35 签到函数,若所述第一响应页面中被添加跳转代码(通常为用于实现401跳转的代码),会使得第一响应页面跳转至其他页面,该签到函数无法被调用,签到标志仍为初始值,故而,可通过所述签到标志来判断所述签到函数是否被调用,相应地,即可通过所述签到标志来判断所述第一响应页面是否发生跳转。

当然,若所述第一响应页面未发生跳转,则直接在所述应用程序内的显示界面中展示所述第一响应页面。

40 本实施方式通过调用签到函数来确定应用程序内第一响应页面是否发生跳转,能够即时准确地确定所述第一响应页面是否发生跳转,提高了用户体验,并且保证了用户的信息安全及财产安全。

图5是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图;参照图5,所述方法包括:

S501:在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面;

45 S502:通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转;

需要说明的是,步骤S501-S502与图4所示的实施方式的步骤S401-S402相同,本实施方式不再赘

述。

S503: 在不能调用所述应用程序内第一响应页面的签到函数时, 认定所述应用程序内的第一响应页面发生跳转, 通过加密协议重新发送页面访问请求, 并接收与重新发送的页面访问请求对应的第二响应页面。

- 5 可理解的是, 为了提高页面访问速度, 通常的页面访问请求是通过明文方式 (即 HTTP 协议等) 进行发送的, 故而, 返回的第一响应页面是通过明文方式发送的, 故而, 容易被黑客截获, 从而在所述第一响应页面中添加跳转代码, 为避免与重新发送的页面访问请求对应的第二响应页面也被黑客截获, 本实施方式中, 通过加密协议 (即 HTTPS 协议等) 重新发送页面访问请求。

S504: 在所述应用程序内的显示界面中展示所述第二响应页面。

- 10 在具体实现中, 由于所述第二响应页面是通过加密协议发送的, 故而其被添加跳转代码的可能性非常小, 在此情况下, 则可停止在所述应用程序内加载所述第一响应页面, 直接在所述应用程序内的显示界面中展示所述第二响应页面。

图 6 是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图; 参照图 6, 所述方法包括:

- 15 S601: 在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

S602: 通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转;

S603: 在不能调用所述应用程序内第一响应页面的签到函数时, 认定所述应用程序内的第一响应页面发生跳转, 通过加密协议重新发送页面访问请求, 并接收与重新发送的页面访问请求对应的第二响应页面;

- 20 S604: 在所述应用程序内的显示界面中展示所述第二响应页面;

需要说明的是, 步骤 S601-S604 与图 5 所示的实施方式的步骤 S501-S504 相同, 本实施方式不再赘述。

S605: 通过所述加密协议发送后续的页面访问请求。

- 25 由于当前的第一响应页面发生跳转, 故而, 可理解为当前的网络环境并不安全, 故而可通过所述加密协议发送后续的页面访问请求。

若后续的所有页面访问请求都通过加密协议发送, 则会导致页面访问速度过慢, 影响用户体验, 为避免该问题, 可在达到预设时间时, 通过明文方式发送后续的页面访问请求。

另外, 在网络环境发生变化 (例如本地连接的网络发生变化或) 本地 IP 地址发生变化) 时, 通过明文方式发送后续的页面访问请求。

- 30 图 7 是本发明一种实施方式的确定应用程序内页面跳转的方法的流程图; 参照图 7, 所述方法包括:

S700: 接收用户输入的搜索词, 根据所述搜索词查找与所述搜索词相关的网页信息, 并将查找到的网页信息展示于所述应用程序内的显示界面中, 接收用户在所述应用程序内的显示界面中输入的页面访问指令。

- 35 可理解的是, 由于查找到的网页信息展示于应用程序内的显示界面中, 此时, 用户通常会输入与需要访问的网页信息对应的页面访问指令。

S701: 在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

S702: 通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转;

- 40 S703: 在不能调用所述应用程序内第一响应页面的签到函数时, 认定所述应用程序内的第一响应页面发生跳转, 通过加密协议重新发送页面访问请求, 并接收与重新发送的页面访问请求对应的第二响应页面;

S704: 在所述应用程序内的显示界面中展示所述第二响应页面;

需要说明的是, 步骤 S701-S704 与图 5 所示的实施方式的步骤 S501-S504 相同, 本实施方式不再赘述。

- 45 由于运营商局域 DNS 服务器中的内容可能被篡改, 又或是用户的路由器上 DNS 服务器地址被修改, 可能导致不能正常访问页面, 影响用户体验, 也可能导致用户在正常访问页面时, 被链接至钓鱼网站或

木马网站等欺诈网站，影响用户的信息安全及财产安全，本实施方式中，步骤 S700-S701 之间，所述方法还包括：

A：基于用户输入的页面访问指令触发向第一 DNS 服务器发送域名解析请求，并接收第一 DNS 服务器返回的与待解析域名对应的第一 IP 地址；

- 5 需要说明的是，所述第一 DNS 服务器通常为运营商局域 DNS 服务器，但该 DNS 服务器中的内容可能被篡改，当然，也有可能为被黑客修改的 DNS 服务器（即应用程序的 DNS 服务器地址被修改）。

B：将所述域名解析请求发送至第二 DNS 服务器；

- 需要说明的是，所述第二 DNS 服务器可理解为第三方提供的 DNS 服务器，第二 DNS 服务器的链接地址可直接存储于本地，在需要执行步骤 B 时，则直接从本地找到第二 DNS 服务器的链接地址，将所述域名解析
10 请求根据链接地址发送至第二 DNS 服务器。

可理解的是，若直接将所述域名解析请求以明文方式（即 HTTP 协议等）发送至第二 DNS 服务器，则容易被黑客截获，从而难以保证所述第二 DNS 服务器所返回信息的真实性，为避免出现该问题，本实施方式中，将所述域名解析请求通过加密协议（即 HTTPS 协议等）发送至第二 DNS 服务器；

C：接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址；

- 15 需要说明的是，若将所述域名解析请求是通过加密协议（即 HTTPS 协议等）发送至第二 DNS 服务器，则所述第二 DNS 服务器通过加密协议返回所述第二 IP 地址。

D：采用所述第二 IP 地址对所述第一 IP 地址进行校验；

- 可理解的是，在所述第一 IP 地址与所述第二 IP 地址相同时，则认定所述第一 IP 地址校验通过，此时，所述校验后的第一 IP 地址即为该第一 IP 地址本身；在所述第一 IP 地址与所述第二 IP 地址不相同，则认定
20 所述第一 IP 地址未验证通过，并将所述第一 IP 地址修改为第二 IP 地址，此时，所述校验后的第一 IP 地址即为所述第二 IP 地址。

- 下面以一个具体的实例来说明，但不限定本发明的保护范围，设所述域名解析请求中包括的待解析域名为 M.haoshou.com，将该域名解析请求发送至第一 DNS 服务器后，接收所述第一 DNS 服务器返回的第一 IP 地址为 125.88.193.213，再将所述域名解析请求发送至第二 DNS 服务器后，若接收所述第二 DNS 服务器
25 返回的第二 IP 地址为 125.88.193.213 时，则认为所述第一 IP 地址校验通过，校验后的第一 IP 地址即为 125.88.193.213；

若接收所述第二 DNS 服务器返回的第二 IP 地址为 125.88.192.144 时，则认为所述第一 IP 地址未校验通过，并将所述第一 IP 地址修改为 125.88.192.144，校验后的第一 IP 地址即为 125.88.192.144。

相应地，步骤 S701 进一步包括：

- 30 在应用程序基于用户输入的页面访问指令触发向校验后的第一 IP 地址发送页面访问请求时，接收与页面访问请求对应的第一响应页面。

图 8 是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；参照图 8，所述方法包括：

- S801：在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的
35 第一响应页面；

可理解的是，所述第一响应页面中内嵌有扫描脚本。

S802：加载所述第一响应页面中内嵌的扫描脚本，以检测所述应用程序内第一响应页面是否被篡改。

- 需要说明的是，所述扫描脚本可在检测所述应用程序内第一响应页面被篡改时，将篡改标志置位，故而，所述应用程序在加载所述第一响应页面中内嵌的扫描脚本时，先将篡改标志设置为初始值（通常
40 设置为 0），可根据所述篡改标志来判断所述第一响应页面是否被篡改。

当然，若所述第一响应页面未被篡改，则直接在所述应用程序内的显示界面中展示所述第一响应页面。

本实施方式通过加载第一响应页面中内嵌的扫描脚本，以检测所述应用程序内第一响应页面是否被篡改，能够即时准确地确定所述第一响应页面是否被篡改，提高了用户体验。

- 45 图 9 是本发明一种实施方式的检测应用程序内页面篡改方法的流程图；参照图 9，所述方法包括：

S901：在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的

第一响应页面;

需要说明的是, 步骤S901与图8所示的实施方式的步骤S801相同, 在此不再赘述。

S902: 加载所述第一响应页面中内嵌的扫描脚本, 由所述扫描脚本对所述应用程序内第一响应页面的DOM树进行扫描, 将所述应用程序内第一响应页面中的外链作为扫描结果;

5 S903: 根据扫描结果来检测所述应用程序内第一响应页面是否被篡改。

可理解的是, 所述外链即为用于在第一响应页面中发起的向外链接, 由于对第一响应页面的篡改通常是通过添加类似于广告等信息, 而广告等信息一般是通过在页面中发起的向外链接来体现, 故而, 本实施方式中将所述应用程序内第一响应页面中的外链作为扫描结果, 并根据扫描结果来检测所述应用程序内第一响应页面是否被篡改, 能够保证检测的准确性。

10 图10是本发明一种实施方式的检测应用程序内页面篡改方法的流程图; 参照图10, 所述方法包括:

S1001: 在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

S1002: 加载所述第一响应页面中内嵌的扫描脚本, 由所述扫描脚本对所述应用程序内第一响应页面的DOM树进行扫描, 将所述应用程序内第一响应页面中的外链作为扫描结果;

15 需要说明的是, 步骤S1001-S1002与图9所示的实施方式的步骤S901-S902相同, 在此不再赘述。

S1003: 检测所述扫描结果中的各外链是否在白名单中, 在所述扫描结果中具有不在白名单中的外链时, 认定所述应用程序内第一响应页面被篡改。

在具体实现中, 有些外链为第一响应页面中自带的, 若直接将具有外链的第一响应页面均认为是被篡改的, 容易导致检测的准确性过低, 影响用户体验, 故而, 本实施方式中, 通过检测所述扫描结果中的各外链是否在白名单中, 在所述扫描结果中具有不在白名单中的外链时, 认定所述应用程序内第一响

20 应页面被篡改, 从而有效提高了检测的准确性。

由于外链是不断变化地, 为保证白名单能够进行更新, 从而保证实时性, 本实施方式中, 在步骤S303之后, 所述方法还包括:

将不在白名单中的外链发送至后台服务器, 所述后台服务器即为所述应用程序的后台服务器, 其可为云服务器, 能够对接收到的不在白名单中的外链进行进一步分析, 以更新所述白名单。

25

图11是本发明一种实施方式的检测应用程序内页面篡改方法的流程图; 参照图11, 所述方法包括:

S1101: 在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

30 S1102: 加载所述第一响应页面中内嵌的扫描脚本, 由所述扫描脚本对所述应用程序内第一响应页面的DOM树进行扫描, 将所述应用程序内第一响应页面中的外链作为扫描结果;

S1103: 检测所述扫描结果中的各外链是否在白名单中, 在所述扫描结果中具有不在白名单中的外链时, 认定所述应用程序内第一响应页面被篡改。

需要说明的是, 步骤S1101-S1103与图10所示的实施方式的步骤S1001-S1003相同, 在此不再赘述。

S1104: 通过加密协议重新发送页面访问请求, 接收与重新发送的页面访问请求对应的第二响应页面。

35 可理解的是, 为了提高页面访问速度, 通常的页面访问请求是通过明文方式(即HTTP协议等)进行发送的, 故而, 返回的第一响应页面页是通过明文方式发送的, 故而, 容易被黑客截获, 从而对所述第一响应页面进行篡改, 为避免与重新发送的页面访问请求对应的第二响应页面也被黑客截获, 本实施方式中, 通过加密协议(即HTTPS协议等)重新发送页面访问请求。

S1105: 在所述应用程序内的显示界面中展示所述第二响应页面。

40 在具体实现中, 由于所述第二响应页面是通过加密协议发送的, 故而其被篡改的可能性非常小, 在此情况下, 则直接在所述应用程序内的显示界面中展示所述第二响应页面。

图12是本发明一种实施方式的检测应用程序内页面篡改方法的流程图; 参照图12, 所述方法包括:

S1201: 在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

45 S1202: 加载所述第一响应页面中内嵌的扫描脚本, 由所述扫描脚本对所述应用程序内第一响应页面的DOM树进行扫描, 将所述应用程序内第一响应页面中的外链作为扫描结果;

S1203: 检测所述扫描结果中的各外链是否在白名单中, 在所述扫描结果中具有不在白名单中的外链时, 认定所述应用程序内第一响应页面被篡改。

S1204: 通过加密协议重新发送页面访问请求, 接收与重新发送的页面访问请求对应的第二响应页面。

S1205: 在所述应用程序内的显示界面中展示所述第二响应页面。

5 需要说明的是, 步骤 S1201-S1205 与图 11 所示的实施方式的步骤 S1101-S1105 相同, 在此不再赘述。

S506: 通过所述加密协议发送后续的页面访问请求。

由于当前的第一响应页面被篡改, 故而, 可理解为当前的网络环境并不安全, 故而可通过所述加密协议发送后续的页面访问请求。

10 若后续的所有页面访问请求都通过加密协议发送, 则会导致页面访问速度过慢, 影响用户体验, 为避免该问题, 可在达到预设时间时, 通过明文方式发送后续的页面访问请求。

另外, 在网络环境发生变化 (例如本地连接的网络发生变化或) 本地 IP 地址发生变化) 时, 通过明文方式发送后续的页面访问请求。

图13是本发明一种实施方式的检测应用程序内页面篡改方法的流程图; 参照图13, 所述方法包括:

15 S1300: 接收用户输入的搜索词, 根据所述搜索词查找与所述搜索词相关的网页信息, 并将查找到的网页信息展示于所述应用程序内的显示界面中, 接收用户在所述应用程序内的显示界面中输入的页面访问指令。

可理解的是, 由于查找到的网页信息展示于应用程序内的显示界面中, 此时, 用户通常会输入与需要访问的网页信息对应的页面访问指令。

20 S1301: 在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

S1302: 加载所述第一响应页面中内嵌的扫描脚本, 由所述扫描脚本对所述应用程序内第一响应页面的 DOM 树进行扫描, 将所述应用程序内第一响应页面中的外链作为扫描结果;

S1303: 检测所述扫描结果中的各外链是否在白名单中, 在所述扫描结果中具有不在白名单中的外链时, 认定所述应用程序内第一响应页面被篡改。

25 S1304: 通过加密协议重新发送页面访问请求, 接收与重新发送的页面访问请求对应的第二响应页面。

S1305: 在所述应用程序内的显示界面中展示所述第二响应页面。

需要说明的是, 步骤 S1301-S1305 与图 11 所示的实施方式的步骤 S1101-S1105 相同, 在此不再赘述。

30 由于运营商局域 DNS 服务器中的内容可能被篡改, 又或是用户的路由器上 DNS 服务器地址被修改, 可能导致不能正常访问页面, 影响用户体验, 也可能导致用户在正常访问页面时, 被链接至钓鱼网站或木马网站等欺诈网站, 影响用户的信息安全及财产安全, 本实施方式中, 步骤 S1300-S1301 之间, 所述方法还包括:

A: 基于用户输入的页面访问指令触发向第一 DNS 服务器发送域名解析请求, 并接收第一 DNS 服务器返回的与待解析域名对应的第一 IP 地址;

35 需要说明的是, 所述第一 DNS 服务器通常为运营商局域 DNS 服务器, 但该 DNS 服务器中的内容可能被篡改, 当然, 也有可能为被黑客修改的 DNS 服务器 (即应用程序的 DNS 服务器地址被修改)。

B: 将所述域名解析请求发送至第二 DNS 服务器;

需要说明的是, 所述第二 DNS 服务器可理解为第三方提供的 DNS 服务器, 第二 DNS 服务器的链接地址可直接存储于本地, 在需要执行步骤 B 时, 则直接从本地找到第二 DNS 服务器的链接地址, 将所述域名解析请求根据链接地址发送至第二 DNS 服务器。

40 可理解的是, 若直接将所述域名解析请求以明文方式 (即 HTTP 协议等) 发送至第二 DNS 服务器, 则容易被黑客截获, 从而难以保证所述第二 DNS 服务器所返回信息的真实性, 为避免出现该问题, 本实施方式中, 将所述域名解析请求通过加密协议 (即 HTTPS 协议等) 发送至第二 DNS 服务器;

C: 接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址;

45 需要说明的是, 若将所述域名解析请求是通过加密协议 (即 HTTPS 协议等) 发送至第二 DNS 服务器, 则所述第二 DNS 服务器通过加密协议返回所述第二 IP 地址。

D: 采用所述第二 IP 地址对所述第一 IP 地址进行校验;

可理解的是,在所述第一IP地址与所述第二IP地址相同时,则认定所述第一IP地址校验通过,此时,所述校验后的第一IP地址即为该第一IP地址本身;在所述第一IP地址与所述第二IP地址不相同,则认定所述第一IP地址未验证通过,并将所述第一IP地址修改为第二IP地址,此时,所述校验后的第一IP地址即为所述第二IP地址。

5 下面以一个具体的实例来说明,但不限定本发明的保护范围,设所述域名解析请求中包括的待解析域名为M.haoshou.com,将该域名解析请求发送至第一DNS服务器后,接收所述第一DNS服务器返回的第一IP地址为125.88.193.213,再将所述域名解析请求发送至第二DNS服务器后,若接收所述第二DNS服务器返回的第二IP地址为125.88.193.213时,则认为所述第一IP地址校验通过,校验后的第一IP地址即为125.88.193.213;

10 若接收所述第二DNS服务器返回的第二IP地址为125.88.192.144时,则认为所述第一IP地址未校验通过,并将所述第一IP地址修改为125.88.192.144,校验后的第一IP地址即为125.88.192.144。

相应地,步骤1301进一步包括:

在应用程序基于用户输入的页面访问指令触发向校验后的第一IP地址发送页面访问请求时,接收与页面访问请求对应的第一响应页面。

15 对于方法实施方式,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明实施方式并不受所描述的动作顺序的限制,因为依据本发明实施方式,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施方式均属于优选实施方式,所涉及的动作并不一定是本发明实施方式所必须的。

20 图14是本发明一种实施方式的应用程序内的页面访问装置的结构框图;参照图14,所述装置包括:指令触发器1401,适于在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时,接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址;

请求发送器1402,适于将所述域名解析请求发送至第二DNS服务器;

地址接收器1403,适于接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址;

25 校验访问器1404,适于采用所述第二IP地址对所述第一IP地址进行校验,向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求。

在本发明的一种可选实施方式中,所述校验访问器,进一步适于判断所述第一IP地址是否与所述第二IP地址相同,若所述第一IP地址与所述第二IP地址相同,则认定所述第一IP地址校验通过,若所述第一IP地址与所述第二IP地址不相同,则认定所述第一IP地址未校验通过,并将所述第一IP地址修改为第二IP地址。

30 在本发明的一种可选实施方式中,所述校验访问器,还适于在所述第一IP地址未校验通过时,在第一预设时间内直接通过所述第二DNS服务器进行域名解析。

在本发明的一种可选实施方式中,所述装置还包括:

连接判断器,适于判断本地是否第一次连接所述第一DNS服务器。

35 在本发明的一种可选实施方式中,所述装置还包括:

网络判断器,适于判断本地连接的网络是否发生变化。

在本发明的一种可选实施方式中,所述装置还包括:

地址判断器,适于判断本地IP地址是否发生变化。

40 在本发明的一种可选实施方式中,所述请求发送器,进一步适于将所述域名解析请求通过加密协议发送至第二DNS服务器。

在本发明的一种可选实施方式中,所述装置还包括:

指令接收器,适于接收用户输入的搜索词,根据所述搜索词查找与所述搜索词相关的网页信息,并将查找到的网页信息展示于所述应用程序内的显示界面中,接收用户在所述应用程序内的显示界面中输入的页面访问指令。

45 在本发明的一种可选实施方式中,所述装置还包括:

页面展示器,适于接收与所述页面访问请求对应的响应页面,在所述应用程序内的显示界面中展示

所述响应页面。

在本发明的一种可选实施方式中,所述装置还包括:

函数判断器,适于判断是否能够调用所述响应页面的签到函数,若能调用所述响应页面的签到函数,则调用所述页面展示器,若不能调用所述响应页面的签到函数,则通过加密协议重新向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求,接收与该页面访问请求对应的响应页面,并调用所述页面展示器。

在本发明的一种可选实施方式中,所述函数判断器,还适于在不能调用所述响应页面的签到函数时,通过HTTPS协议向校验后的第一IP地址发送后续的页面访问请求。

在本发明的一种可选实施方式中,所述装置还包括:

外链扫描器,适于通过加载于所述响应页面中的脚本扫描所述响应页面的DOM树,若所述DOM树中具有不在白名单中的外链,则通过加密协议重新向校验后的第一IP地址发送页面访问请求,接收与该页面访问请求对应的响应页面,并调用所述页面展示器;否则调用所述页面展示器。

在本发明的一种可选实施方式中,所述外链扫描器,还适于在所述DOM树中具有不在白名单中的外链时,通过加密协议向校验后的第一IP地址发送后续的页面访问请求。

在本发明的一种可选实施方式中,所述外链扫描器,还适于在所述DOM树中具有不在白名单中的外链时,向后台服务器发送所述不在白名单中的外链。

图15是本发明一种实施方式的确定应用程序内页面跳转的装置的结构框图;参照图15,所述装置包括:

页面接收器1501,适于在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面;

跳转确定器1502,适于通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转。

在本发明的一种可选实施方式中,所述装置还包括:

跳转认定器,适于在不能调用所述应用程序内第一响应页面的签到函数时,认定所述应用程序内的第一响应页面发生跳转。

在本发明的一种可选实施方式中,所述装置还包括:

请求重发器,适于通过加密协议重新发送页面访问请求,并接收与重新发送的页面访问请求对应的第二响应页面。

在本发明的一种可选实施方式中,所述装置还包括:

页面展示器,适于在所述应用程序内的显示界面中展示所述第二响应页面。

在本发明的一种可选实施方式中,所述装置还包括:

加密发送器,适于通过所述加密协议发送后续的页面访问请求。

在本发明的一种可选实施方式中,所述装置还包括:

时间判断器,适于判断是否达到预设时间,若否,则调用所述加密发送器。

在本发明的一种可选实施方式中,所述装置还包括:

网络判断器,适于判断本地连接的网络是否发生变化,若否,则调用所述加密发送器。

在本发明的一种可选实施方式中,所述装置还包括:

地址判断器,适于判断本地IP地址是否发生变化,若否,则调用所述加密发送器。

在本发明的一种可选实施方式中,所述装置还包括:

指令接收器,适于接收用户输入的搜索词,根据所述搜索词查找与所述搜索词相关的网页信息,并将查找到的网页信息展示于所述应用程序内的显示界面中,接收用户在所述应用程序内的显示界面中输入的页面访问指令。

在本发明的一种可选实施方式中,所述方法还包括:

指令触发器,适于基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求,并接收第一DNS服务器返回的与待解析域名对应的第一IP地址;

请求发送器,适于将所述域名解析请求发送至第二DNS服务器;

地址接收器,适于接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址;

地址校验器, 适于采用所述第二 IP 地址对所述第一 IP 地址进行校验;

相应地, 所述页面接收器, 进一步适于在应用程序基于用户输入的页面访问指令触发向校验后的第一 IP 地址发送页面访问请求时, 接收与页面访问请求对应的第一响应页面。

图16是本发明一种实施方式的检测应用程序内页面篡改装置的结构框图; 参照图16, 所述装置包括:

5 页面接收器1601, 适于在应用程序基于用户输入的页面访问指令触发页面访问请求时, 接收与页面访问请求对应的第一响应页面;

篡改检测器 1602, 适于加载所述第一响应页面中内嵌的扫描脚本, 以检测所述应用程序内第一响应页面是否被篡改。

10 在本发明的一种可选实施方式中, 所述篡改检测器, 进一步适于加载所述第一响应页面中内嵌的扫描脚本, 由所述扫描脚本对所述应用程序内第一响应页面的 DOM 树进行扫描, 将所述应用程序内第一响应页面中的外链作为扫描结果, 并根据扫描结果来检测所述应用程序内第一响应页面是否被篡改。

在本发明的一种可选实施方式中, 所述篡改检测器, 进一步适于检测所述扫描结果中的各外链是否在白名单中, 在所述扫描结果中具有不在白名单中的外链时, 认定所述应用程序内第一响应页面被篡改。

在本发明的一种可选实施方式中, 所述装置还包括:

15 外链发送器, 适于将不在白名单中的外链发送至后台服务器。

在本发明的一种可选实施方式中, 所述装置还包括:

请求重发器, 适于通过加密协议重新发送页面访问请求, 接收与重新发送的页面访问请求对应的第二响应页面。

在本发明的一种可选实施方式中, 所述装置还包括:

20 页面展示器, 适于在所述应用程序内的显示界面中展示所述第二响应页面。

在本发明的一种可选实施方式中, 所述装置还包括:

加密发送器, 适于通过所述加密协议发送后续的页面访问请求。

在本发明的一种可选实施方式中, 所述装置还包括:

时间判断器, 适于判断是否达到预设时间, 若否, 则调用所述加密发送器。

25 在本发明的一种可选实施方式中, 所述装置还包括:

网络判断器, 适于判断本地连接的网络是否发生变化, 若否, 则调用所述加密发送器。

在本发明的一种可选实施方式中, 所述装置还包括:

地址判断器, 适于判断本地 IP 地址是否发生变化, 若否, 则调用所述加密发送器。

在本发明的一种可选实施方式中, 所述装置还包括:

30 指令接收器, 适于接收用户输入的搜索词, 根据所述搜索词查找与所述搜索词相关的网页信息, 并将查找到的网页信息展示于所述应用程序内的显示界面中, 接收用户在所述应用程序内的显示界面中输入的页面访问指令。

在本发明的一种可选实施方式中, 所述装置还包括:

指令触发器, 适于基于用户输入的页面访问指令触发向第一 DNS 服务器发送域名解析请求, 并接收

35 第一 DNS 服务器返回的与待解析域名对应的第一 IP 地址;

请求发送器, 适于将所述域名解析请求发送至第二 DNS 服务器;

地址接收器, 适于接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址;

地址校验器, 适于采用所述第二 IP 地址对所述第一 IP 地址进行校验;

40 相应地, 所述页面接收器, 进一步适于在应用程序基于用户输入的页面访问指令触发向校验后的第一 IP 地址发送页面访问请求时, 接收与页面访问请求对应的第一响应页面。

对于装置实施方式而言, 由于其与方法实施方式基本相似, 所以描述的比较简单, 相关之处参见方法实施方式的部分说明即可。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述, 构造这类系统所要求的结构是显而易见的。此外, 本发明也不针对任何特定编程语言。应当明白, 可以利用各种编程语言实现在此描述的本发明的内容, 并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的应用程序内的页面访问设备、确定应用程序内页面跳转的设备、检测应用程序内页面篡改设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图17示出了可以实现根据本发明的一种应用程序内的页面访问的终端设备。该终端设备传统上包括处理器1710和以存储器1720形式的计算机程序产品或者计算机可读介质。存储器1720可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者ROM之类的电子存储器。存储器1720具有用于执行上述方法中的任何方法步骤的程序代码1731的存储空间1730。例如，用于程序代码的存储空间1730可以包括分别用于实现上面的方法中的各种步骤的各个程序代码1731。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘、紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图18所述的便携式或者固定存储单元。该存储单元可以具有与图17的终端设备中的存储器1720类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码1731'，即可以由例如诸如1710之类的处理器读取的代码，这些代码当由终端设备运行时，导致该终端设备执行上面所描述的方法中的各个步骤。

当然，对于确定应用程序内页面跳转的终端设备、检测应用程序内页面篡改的终端设备类似图17和图18的结构。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求 书

- 1、一种应用程序内的页面访问方法，其特征在于，所述方法包括：
在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址；
- 5 将所述域名解析请求发送至第二DNS服务器；
接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址；
采用所述第二IP地址对所述第一IP地址进行校验，向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求。
- 2、如权利要求1所述的方法，其特征在于，所述采用所述第二IP地址对所述第一IP地址进行校验，
10 进一步包括：
判断所述第一IP地址是否与所述第二IP地址相同，若所述第一IP地址与所述第二IP地址相同，则认定所述第一IP地址校验通过，若所述第一IP地址与所述第二IP地址不相同，则认定所述第一IP地址未校验通过，并将所述第一IP地址修改为第二IP地址。
- 3、如权利要求2所述的方法，其特征在于，在所述第一IP地址未校验通过时，在第一预设时间内直接通过所述第二DNS服务器进行域名解析。
- 15 4、如权利要求1所述的方法，其特征在于，所述将所述域名解析请求发送至第二DNS服务器之前，所述方法还包括：
判断本地是否第一次连接所述第一DNS服务器，若是，则执行所述将所述域名解析请求发送至第二DNS服务器的步骤。
- 20 5、如权利要求1所述的方法，其特征在于，所述将所述域名解析请求发送至第二DNS服务器之前，所述方法还包括：
判断本地连接的网络是否发生变化，若是，则执行所述将所述域名解析请求发送至第二DNS服务器的步骤。
- 6、如权利要求5所述的方法，其特征在于，所述将所述域名解析请求发送至第二DNS服务器之前，
25 所述方法还包括：
判断本地IP地址是否发生变化，若是，则执行所述将所述域名解析请求发送至预设DNS服务器的步骤。
- 7、如权利要求5所述的方法，其特征在于，所述将所述域名解析请求发送至第二DNS服务器，进一步包括：
将所述域名解析请求通过加密协议发送至第二DNS服务器。
- 30 8、如权利要求5所述的方法，其特征在于，所述在应用程序基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求时，接收第一DNS服务器返回的与所述域名解析请求对应的第一IP地址之前，所述方法还包括：
接收用户输入的搜索词，根据所述搜索词查找与所述搜索词相关的网页信息，并将查找到的网页信息展示于所述应用程序内的显示界面中，接收用户在所述应用程序内的显示界面中输入的页面访问指令。
- 35 9、如权利要求1-8任一项所述的方法，其特征在于，所述向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求之后，所述方法还包括：
接收与所述页面访问请求对应的响应页面，在所述应用程序内的显示界面中展示所述响应页面。
- 10、如权利要求9所述的方法，其特征在于，所述接收与所述页面访问请求对应的响应页面之后，所述方法还包括：
40 判断是否能够调用所述响应页面的签到函数，若能调用所述响应页面的签到函数，则执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤，若不能调用所述响应页面的签到函数，则通过加密协议重新向校验后的第一IP地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求，接收与该页面访问请求对应的响应页面，并执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤。
- 45 11、如权利要求10所述的方法，其特征在于，在不能调用所述响应页面的签到函数时，通过加密协议向校验后的第一IP地址发送后续的页面访问请求。

12、如权利要求9所述的方法，其特征在于，所述接收与所述页面访问请求对应的响应页面之后，所述方法还包括：

通过加载于所述响应页面中的脚本扫描所述响应页面的DOM树，若所述DOM树中具有不在白名单中的外链，则通过加密协议重新向校验后的第一IP地址发送页面访问请求，接收与该页面访问请求对应的响应页面，并执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤；否则执行所述在所述应用程序内的显示界面中展示所述响应页面的步骤。

13、如权利要求12所述的方法，其特征在于，在所述DOM树中具有不在白名单中的外链时，通过加密协议向校验后的第一IP地址发送后续的页面访问请求。

14、如权利要求12所述的方法，其特征在于，在所述DOM树中具有不在白名单中的外链时，向后台服务器发送所述不在白名单中的外链。

15、一种确定应用程序内页面跳转的方法，其特征在于，所述方法包括：

在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面；

通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转。

16、如权利要求15所述的方法，其特征在于，所述通过调用签到函数来确定所述应用程序内的第一响应页面是否发生跳转之后，所述方法还包括：

在不能调用所述应用程序内第一响应页面的签到函数时，认定所述应用程序内的第一响应页面发生跳转。

17、如权利要求16所述的方法，其特征在于，所述认定所述应用程序内的第一响应页面发生跳转之后，所述方法还包括：

通过加密协议重新发送页面访问请求，并接收与重新发送的页面访问请求对应的第二响应页面。

18、如权利要求17所述的方法，其特征在于，所述接收与重新发送的页面访问请求对应的第二响应页面之后，所述方法还包括：

在所述应用程序内的显示界面中展示所述第二响应页面。

19、如权利要求16所述的方法，其特征在于，所述认定所述应用程序内的第一响应页面发生跳转之后，所述方法还包括：

通过所述加密协议发送后续的页面访问请求。

20、如权利要求19所述的方法，其特征在于，所述通过所述加密协议发送后续的页面访问请求之后，所述方法还包括：

判断是否达到预设时间，若否，则执行所述通过所述加密协议发送后续的页面访问请求的步骤。

21、如权利要求19所述的方法，其特征在于，所述通过所述加密协议发送后续的页面访问请求之后，所述方法还包括：

判断本地连接的网络是否发生变化，若否，则执行所述通过所述加密协议发送后续的页面访问请求的步骤。

22、如权利要求19所述的方法，其特征在于，所述通过所述加密协议发送后续的页面访问请求之后，所述方法还包括：

判断本地IP地址是否发生变化，若否，则执行所述通过所述加密协议发送后续的页面访问请求的步骤。

23、如权利要求15-22中任一项所述的方法，其特征在于，所述在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面之前，所述方法还包括：

接收用户输入的搜索词，根据所述搜索词查找与所述搜索词相关的网页信息，并将查找到的网页信息展示于所述应用程序内的显示界面中，接收用户在所述应用程序内的显示界面中输入的页面访问指令。

24、如权利要求23所述的方法，其特征在于，所述在应用程序基于用户输入的页面访问指令触发页面访问请求时，接收与页面访问请求对应的第一响应页面之前，所述方法还包括：

基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求，并接收第一DNS服务器返回的与待解析域名对应的第一IP地址；

将所述域名解析请求发送至第二 DNS 服务器;

接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址;

采用所述第二 IP 地址对所述第一 IP 地址进行校验;

相应地,所述在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求
5 对应的第一响应页面,进一步包括:

在应用程序基于用户输入的页面访问指令触发向校验后的第一 IP 地址发送页面访问请求时,接收与
页面访问请求对应的第一响应页面。

25、一种检测应用程序内页面篡改方法,其特征在于,所述方法包括:

在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响
10 应页面;

加载所述第一响应页面中内嵌的扫描脚本,以检测所述应用程序内第一响应页面是否被篡改。

26、如权利要求 25 所述的方法,其特征在于,所述加载所述第一响应页面中内嵌的扫描脚本,以检
测所述应用程序内第一响应页面是否被篡改,进一步包括:

加载所述第一响应页面中内嵌的扫描脚本,由所述扫描脚本对所述应用程序内第一响应页面的 DOM
15 树进行扫描,将所述应用程序内第一响应页面中的外链作为扫描结果;

根据扫描结果来检测所述应用程序内第一响应页面是否被篡改。

27、如权利要求 26 所述的方法,其特征在于,所述根据扫描结果来检测所述应用程序内第一响应页
面是否被篡改,进一步包括:

检测所述扫描结果中的各外链是否在白名单中,在所述扫描结果中具有不在白名单中的外链时,认
20 定所述应用程序内第一响应页面被篡改。

28、如权利要求 27 所述的方法,其特征在于,所述认定所述应用程序内第一响应页面被篡改之后,
所述方法还包括:

将不在白名单中的外链发送至后台服务器。

29、如权利要求 27 所述的方法,其特征在于,所述认定所述应用程序内第一响应页面被篡改之后,
25 所述方法还包括:

通过加密协议重新发送页面访问请求,接收与重新发送的页面访问请求对应的第二响应页面。

30、如权利要求 29 所述的方法,其特征在于,所述接收与重新发送的页面访问请求对应的第二响应
页面之后,所述方法还包括:

在所述应用程序内的显示界面中展示所述第二响应页面。

31、如权利要求 27 所述的方法,其特征在于,所述认定所述应用程序内第一响应页面被篡改之后,
30 所述方法还包括:

通过所述加密协议发送后续的页面访问请求。

32、如权利要求 31 所述的方法,其特征在于,所述通过所述加密协议发送后续的页面访问请求之后,
所述方法还包括:

35 判断是否达到预设时间,若否,则执行所述通过所述加密协议发送后续的页面访问请求的步骤。

33、如权利要求 32 项所述的方法,其特征在于,所述通过所述加密协议发送后续的页面访问请求之
后,所述方法还包括:

判断本地连接的网络是否发生变化,若否,则执行所述通过所述加密协议发送后续的页面访问请求
的步骤。

34、如权利要求 31 所述的方法,其特征在于,所述通过所述加密协议发送后续的页面访问请求之后,
40 所述方法还包括:

判断本地 IP 地址是否发生变化,若否,则执行所述通过所述加密协议发送后续的页面访问请求的步
骤。

35、如权利要求 25-34 中任一项所述的方法,其特征在于,所述在应用程序基于用户输入的页面访
45 问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面之前,所述方法还包括:

接收用户输入的搜索词,根据所述搜索词查找与所述搜索词相关的网页信息,并将查找到的网页信

息展示于所述应用程序内的显示界面中,接收用户在所述应用程序内的显示界面中输入的页面访问指令。

36、如权利要求 35 所述的方法,其特征在于,所述在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面之前,所述方法还包括:

基于用户输入的页面访问指令触发向第一 DNS 服务器发送域名解析请求,并接收第一 DNS 服务器返回的与待解析域名对应的第一 IP 地址;

将所述域名解析请求发送至第二 DNS 服务器;

接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址;

采用所述第二 IP 地址对所述第一 IP 地址进行校验;

相应地,所述在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面,进一步包括:

在应用程序基于用户输入的页面访问指令触发向校验后的第一 IP 地址发送页面访问请求时,接收与页面访问请求对应的第一响应页面。

37、一种应用程序内的页面访问装置,其特征在于,所述装置包括:

指令触发器,适于在应用程序基于用户输入的页面访问指令触发向第一 DNS 服务器发送域名解析请求时,接收第一 DNS 服务器返回的与所述域名解析请求对应的第一 IP 地址;

请求发送器,适于将所述域名解析请求发送至第二 DNS 服务器;

地址接收器,适于接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址;

校验访问器,适于采用所述第二 IP 地址对所述第一 IP 地址进行校验,向校验后的第一 IP 地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求。

38、如权利要求 37 所述的装置,其特征在于,所述校验访问器,进一步适于判断所述第一 IP 地址是否与所述第二 IP 地址相同,若所述第一 IP 地址与所述第二 IP 地址相同,则认定所述第一 IP 地址校验通过,若所述第一 IP 地址与所述第二 IP 地址不相同,则认定所述第一 IP 地址未校验通过,并将所述第一 IP 地址修改为第二 IP 地址。

39、如权利要求 38 所述的装置,其特征在于,所述校验访问器,还适于在所述第一 IP 地址未校验通过时,在第一预设时间内直接通过所述第二 DNS 服务器进行域名解析。

40、如权利要求 37 所述的装置,其特征在于,所述装置还包括:

连接判断器,适于判断本地是否第一次连接所述第一 DNS 服务器。

41、如权利要求 37 所述的装置,其特征在于,所述装置还包括:

网络判断器,适于判断本地连接的网络是否发生变化。

42、如权利要求 37 所述的装置,其特征在于,所述装置还包括:

地址判断器,适于判断本地 IP 地址是否发生变化。

43、如权利要求 37 所述的装置,其特征在于,所述请求发送器,进一步适于将所述域名解析请求通过加密协议发送至第二 DNS 服务器。

44、如权利要求 37 所述的装置,其特征在于,所述装置还包括:

指令接收器,适于接收用户输入的搜索词,根据所述搜索词查找与所述搜索词相关的网页信息,并将查找到的网页信息展示于所述应用程序内的显示界面中,接收用户在所述应用程序内的显示界面中输入的页面访问指令。

45、如权利要求 37-44 中任一项所述的装置,其特征在于,所述装置还包括:

页面展示器,适于接收与所述页面访问请求对应的响应页面,在所述应用程序内的显示界面中展示所述响应页面。

46、如权利要求 45 所述的装置,其特征在于,所述装置还包括:

函数判断器,适于判断是否能够调用所述响应页面的签到函数,若能调用所述响应页面的签到函数,则调用所述页面展示器,若不能调用所述响应页面的签到函数,则通过加密协议重新向校验后的第一 IP 地址发送在所述应用程序内根据所述页面访问指令生成的页面访问请求,接收与该页面访问请求对应的响应页面,并调用所述页面展示器。

47、如权利要求 46 所述的装置,其特征在于,所述函数判断器,还适于在不能调用所述响应页面的

签到函数时,通过HTTPS协议向校验后的第一IP地址发送后续的页面访问请求。

48、如权利要求45所述的装置,其特征在于,所述装置还包括:

外链扫描器,适于通过加载于所述响应页面中的脚本扫描所述响应页面的DOM树,若所述DOM树中具有不在白名单中的外链,则通过加密协议重新向校验后的第一IP地址发送页面访问请求,接收与该页面访问请求对应的响应页面,并调用所述页面展示器;否则调用所述页面展示器。

49、如权利要求48所述的装置,其特征在于,所述外链扫描器,还适于在所述DOM树中具有不在白名单中的外链时,通过加密协议向校验后的第一IP地址发送后续的页面访问请求。

50、如权利要求48所述的装置,其特征在于,所述外链扫描器,还适于在所述DOM树中具有不在白名单中的外链时,向后台服务器发送所述不在白名单中的外链。

51、一种确定应用程序内页面跳转的装置,其特征在于,所述装置包括:

页面接收器,适于在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面;

跳转确定器,适于通过调用签到函数来确定所述应用程序内第一响应页面是否发生跳转。

52、如权利要求51所述的装置,其特征在于,所述装置还包括:

跳转认定器,适于在不能调用所述应用程序内第一响应页面的签到函数时,认定所述应用程序内的第一响应页面发生跳转。

53、如权利要求52所述的装置,其特征在于,所述装置还包括:

请求重发器,适于通过加密协议重新发送页面访问请求,并接收与重新发送的页面访问请求对应的第二响应页面。

54、如权利要求53所述的装置,其特征在于,所述装置还包括:

页面展示器,适于在所述应用程序内的显示界面中展示所述第二响应页面。

55、如权利要求51所述的装置,其特征在于,所述装置还包括:

加密发送器,适于通过所述加密协议发送后续的页面访问请求。

56、如权利要求55所述的装置,其特征在于,所述装置还包括:

时间判断器,适于判断是否达到预设时间,若否,则调用所述加密发送器。

57、如权利要求55所述的装置,其特征在于,所述装置还包括:

网络判断器,适于判断本地连接的网络是否发生变化,若否,则调用所述加密发送器。

58、如权利要求55所述的装置,其特征在于,所述装置还包括:

地址判断器,适于判断本地IP地址是否发生变化,若否,则调用所述加密发送器。

59、如权利要求51-58中任一项所述的装置,其特征在于,所述装置还包括:

指令接收器,适于接收用户输入的搜索词,根据所述搜索词查找与所述搜索词相关的网页信息,并将查找到的网页信息展示于所述应用程序内的显示界面中,接收用户在所述应用程序内的显示界面中输入的页面访问指令。

60、如权利要求59所述的装置,其特征在于,所述方法还包括:

指令触发器,适于基于用户输入的页面访问指令触发向第一DNS服务器发送域名解析请求,并接收第一DNS服务器返回的与待解析域名对应的第一IP地址;

请求发送器,适于将所述域名解析请求发送至第二DNS服务器;

地址接收器,适于接收所述第二DNS服务器返回的与所述域名解析请求对应的第二IP地址;

地址校验器,适于采用所述第二IP地址对所述第一IP地址进行校验;

相应地,所述页面接收器,进一步适于在应用程序基于用户输入的页面访问指令触发向校验后的第一IP地址发送页面访问请求时,接收与页面访问请求对应的第一响应页面。

61、一种检测应用程序内页面篡改装置,其特征在于,所述装置包括:

页面接收器,适于在应用程序基于用户输入的页面访问指令触发页面访问请求时,接收与页面访问请求对应的第一响应页面;

篡改检测器，适于加载所述第一响应页面中内嵌的扫描脚本，以检测所述应用程序内第一响应页面是否被篡改。

62、如权利要求 61 所述的装置，其特征在于，所述篡改检测器，进一步适于加载所述第一响应页面中内嵌的扫描脚本，由所述扫描脚本对所述应用程序内第一响应页面的 DOM 树进行扫描，将所述应用程序内第一响应页面中的外链作为扫描结果，并根据扫描结果来检测所述应用程序内第一响应页面是否被篡改。

63、如权利要求 62 所述的装置，其特征在于，所述篡改检测器，进一步适于检测所述扫描结果中的各外链是否在白名单中，在所述扫描结果中具有不在白名单中的外链时，认定所述应用程序内第一响应页面被篡改。

10 64、如权利要求 62 所述的装置，其特征在于，所述装置还包括：

外链发送器，适于将不在白名单中的外链发送至后台服务器。

65、如权利要求 62 所述的装置，其特征在于，所述装置还包括：

请求重发器，适于通过加密协议重新发送页面访问请求，接收与重新发送的页面访问请求对应的第二响应页面。

15 66、如权利要求 65 所述的装置，其特征在于，所述装置还包括：

页面展示器，适于在所述应用程序内的显示界面中展示所述第二响应页面。

67、如权利要求 62 所述的装置，其特征在于，所述装置还包括：

加密发送器，适于通过所述加密协议发送后续的页面访问请求。

68、如权利要求 67 所述的装置，其特征在于，所述装置还包括：

20 时间判断器，适于判断是否达到预设时间，若否，则调用所述加密发送器。

69、如权利要求 68 所述的装置，其特征在于，所述装置还包括：

网络判断器，适于判断本地连接的网络是否发生变化，若否，则调用所述加密发送器。

70、如权利要求 67 所述的装置，其特征在于，所述装置还包括：

地址判断器，适于判断本地 IP 地址是否发生变化，若否，则调用所述加密发送器。

25 71、如权利要求 61-70 中任一项所述的装置，其特征在于，所述装置还包括：

指令接收器，适于接收用户输入的搜索词，根据所述搜索词查找与所述搜索词相关的网页信息，并将查找到的网页信息展示于所述应用程序内的显示界面中，接收用户在所述应用程序内的显示界面中输入的页面访问指令。

72、如权利要求 71 所述的装置，其特征在于，所述装置还包括：

30 指令触发器，适于基于用户输入的页面访问指令触发向第一 DNS 服务器发送域名解析请求，并接收第一 DNS 服务器返回的与待解析域名对应的第一 IP 地址；

请求发送器，适于将所述域名解析请求发送至第二 DNS 服务器；

地址接收器，适于接收所述第二 DNS 服务器返回的与所述域名解析请求对应的第二 IP 地址；

地址校验器，适于采用所述第二 IP 地址对所述第一 IP 地址进行校验；

35 相应地，所述页面接收器，进一步适于在应用程序基于用户输入的页面访问指令触发向校验后的第一 IP 地址发送页面访问请求时，接收与页面访问请求对应的第一响应页面。

73、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行根据权利要求 1-14 中的任一个所述的应用程序内的页面访问方法。

74、一种计算机可读介质，其中存储了如权利要求 73 所述的计算机程序。

40 75、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行根据权利要求 15-24 中的任一个所述的应用程序内页面跳转的方法。

76、一种计算机可读介质，其中存储了如权利要求 75 所述的计算机程序。

77、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行根据权利要求 25-36 中的任一个所述的检测应用程序内页面篡改方法。

45 78、一种计算机可读介质，其中存储了如权利要求 77 所述的计算机程序。

说明书附图

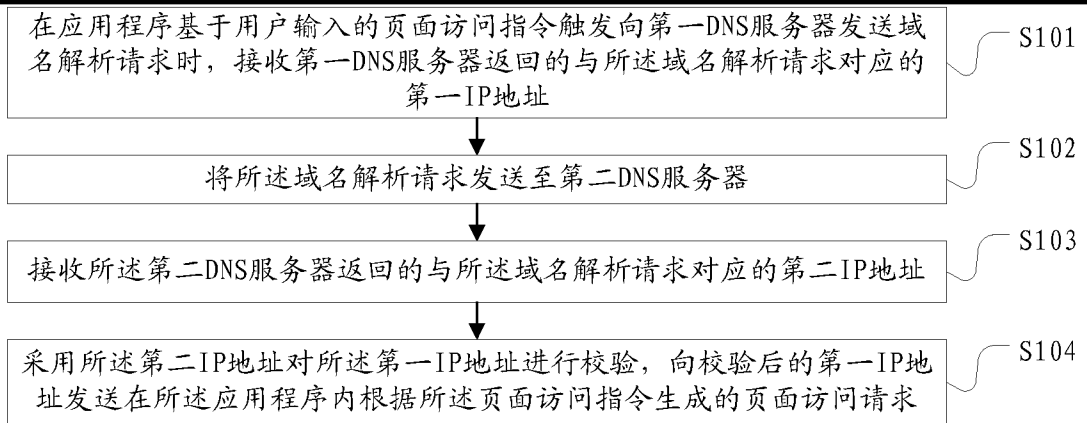


图 1

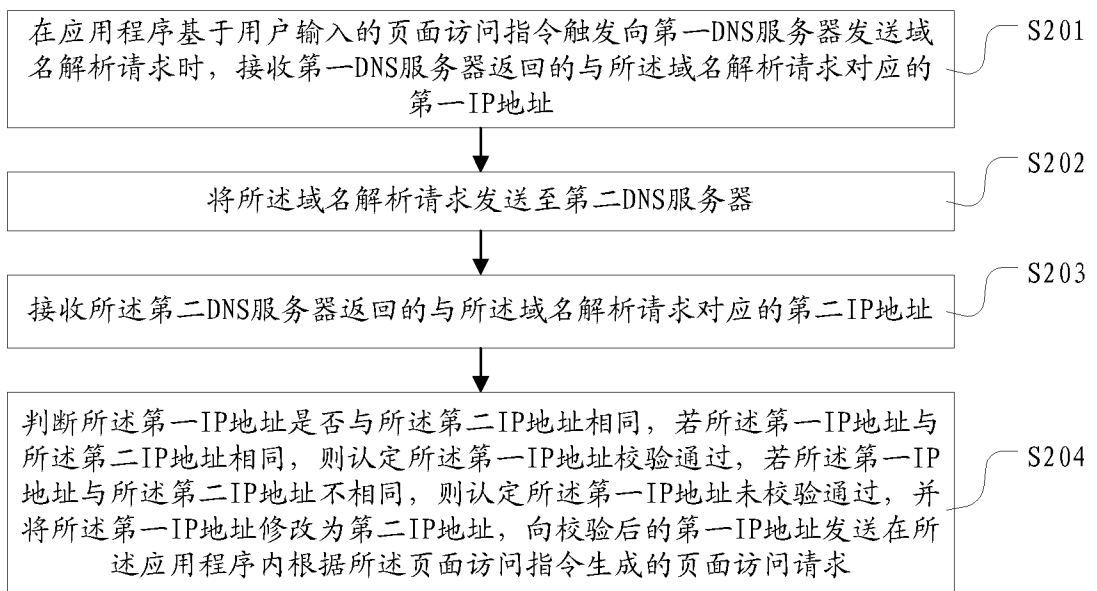
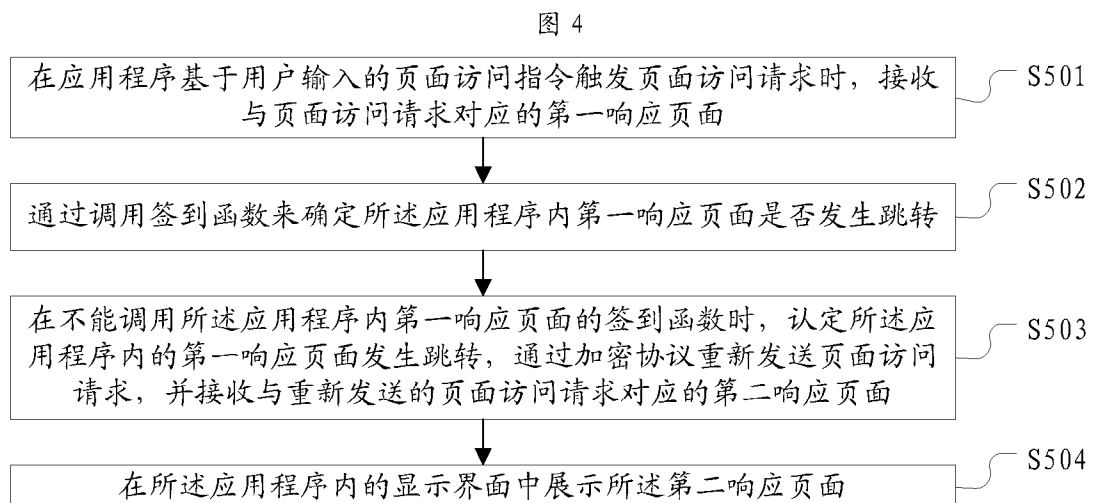
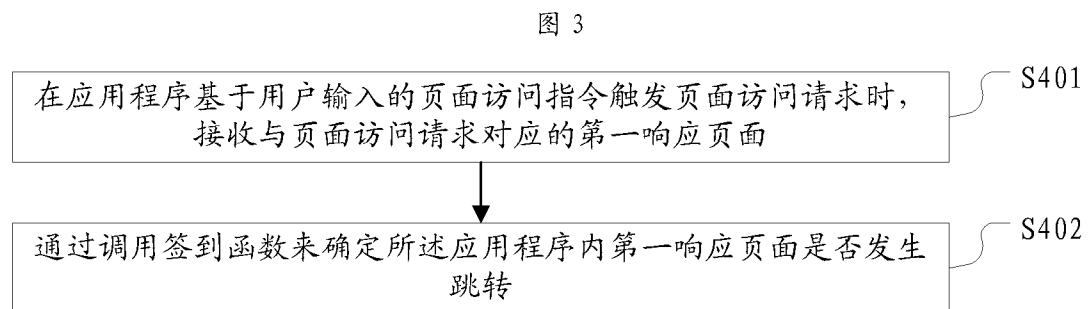
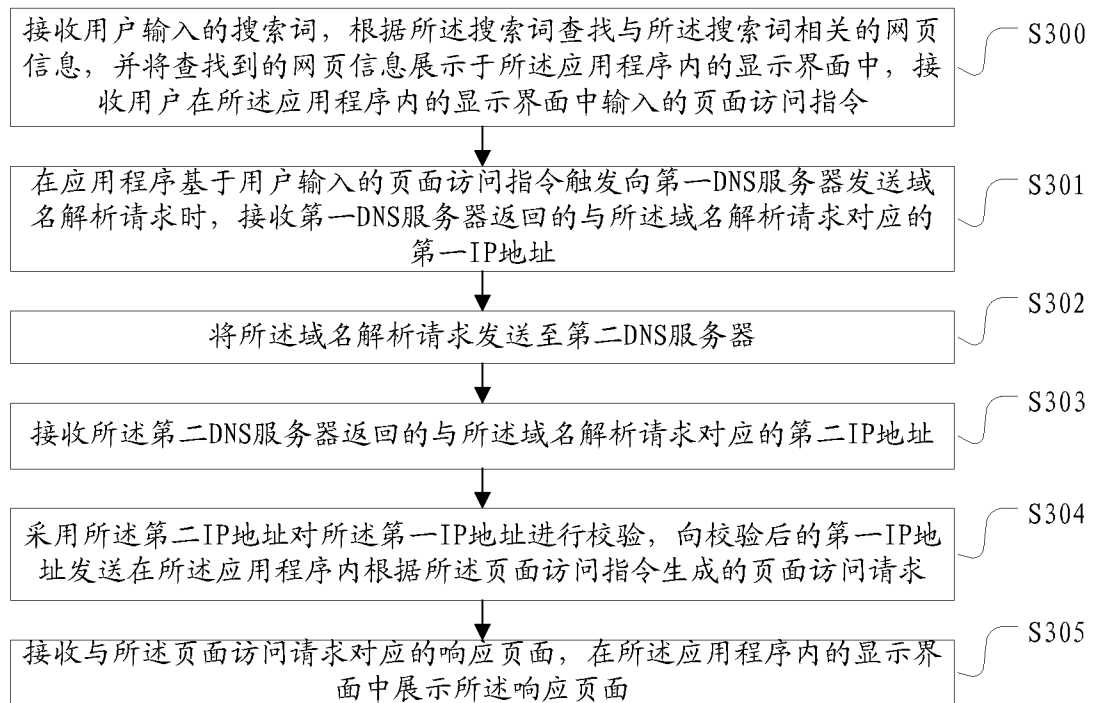


图 2



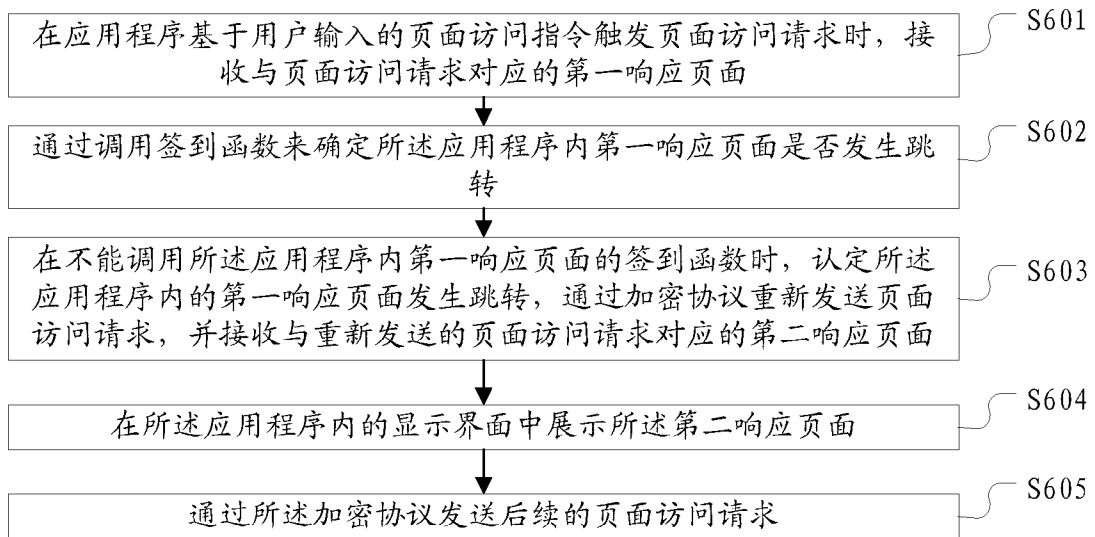


图 6

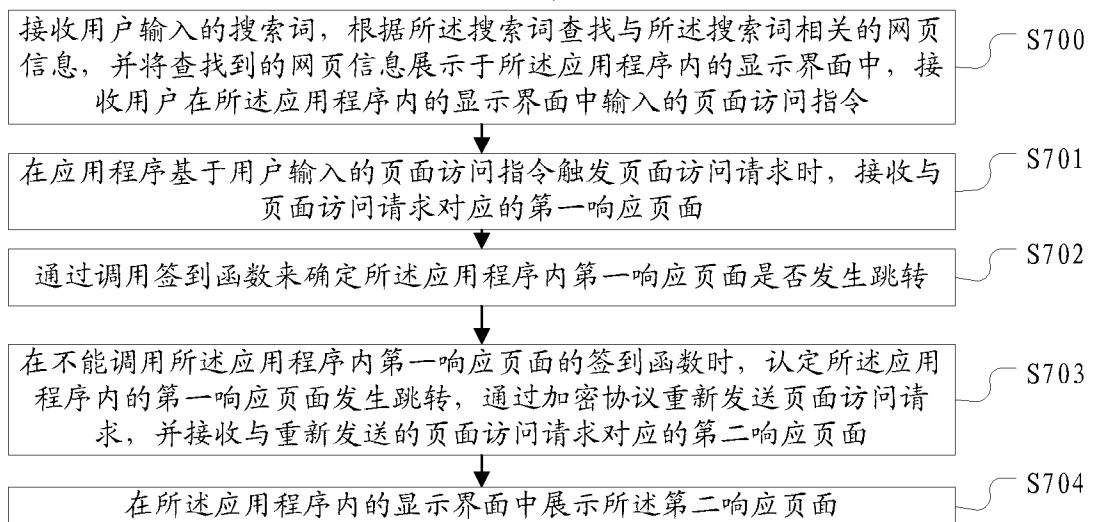


图 7

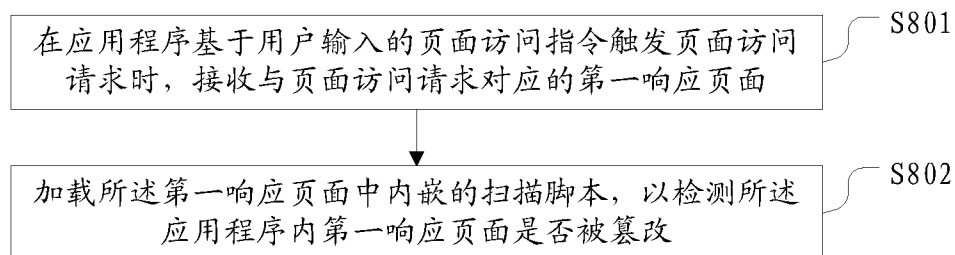
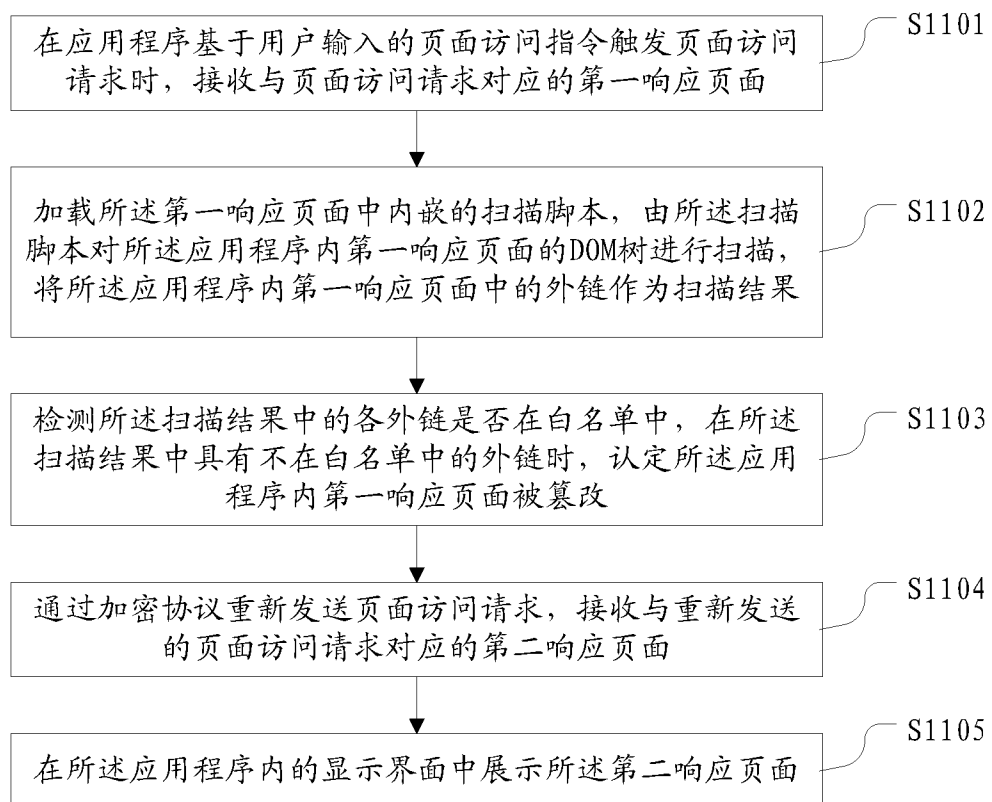
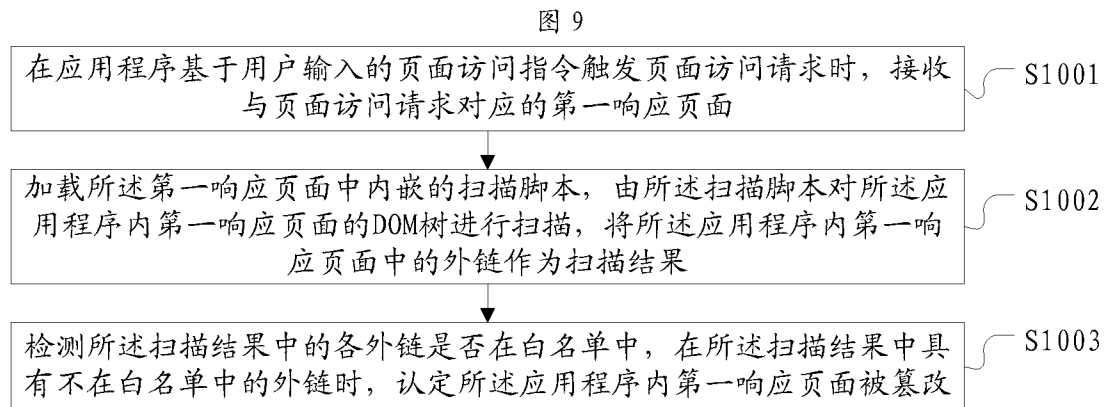
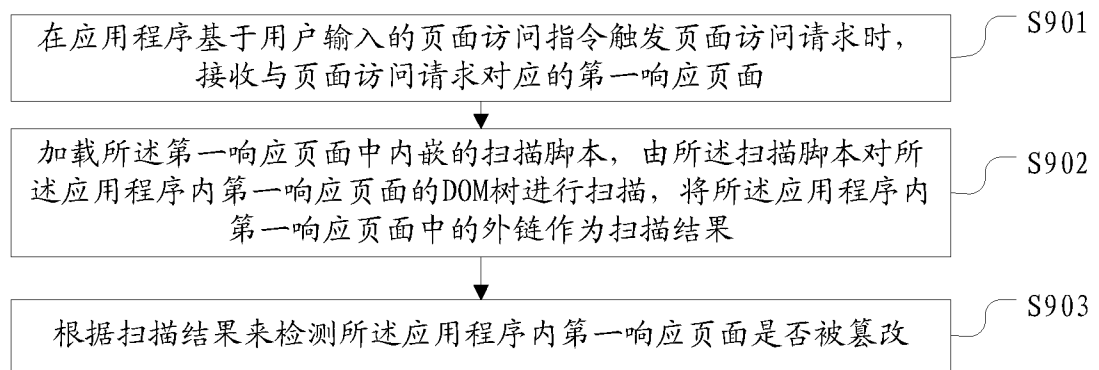


图 8



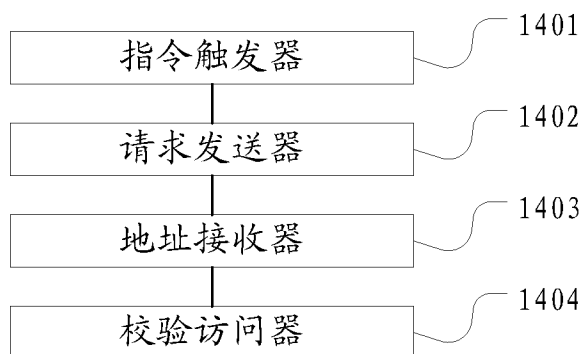
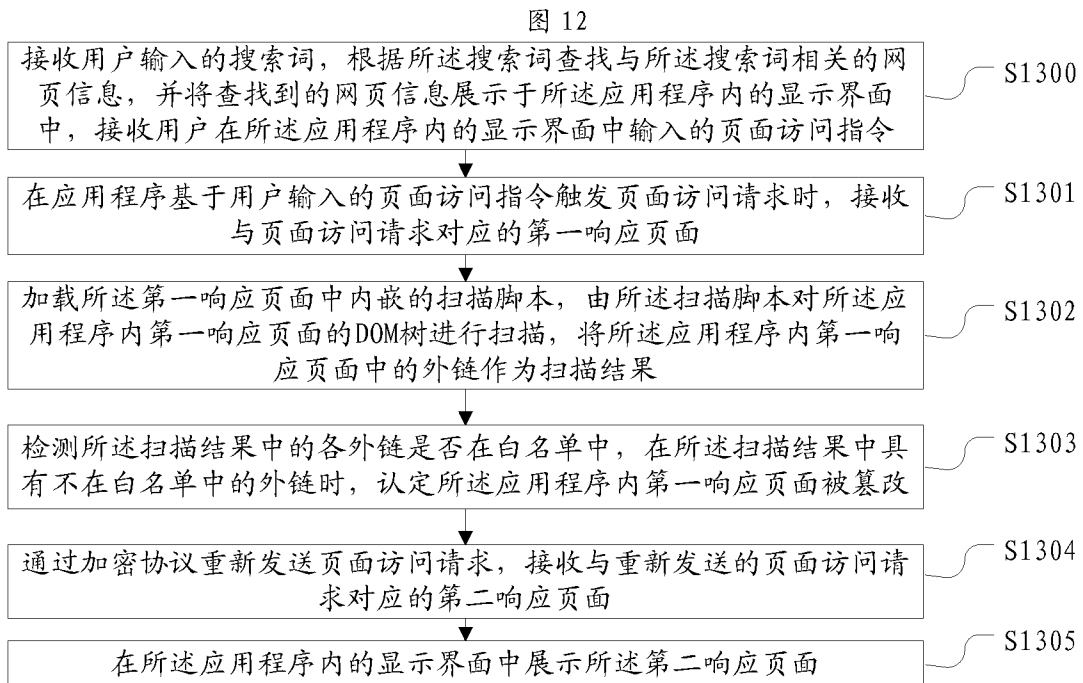
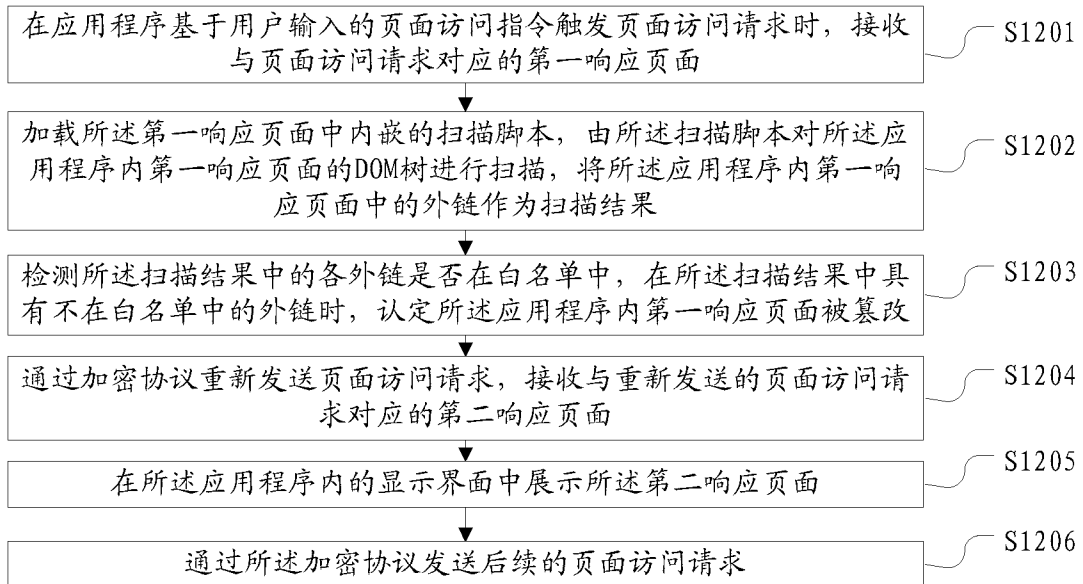




图 15

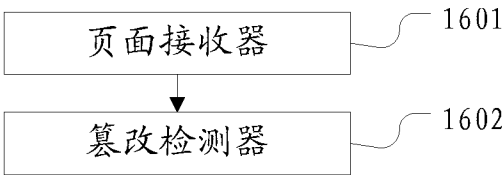


图 16

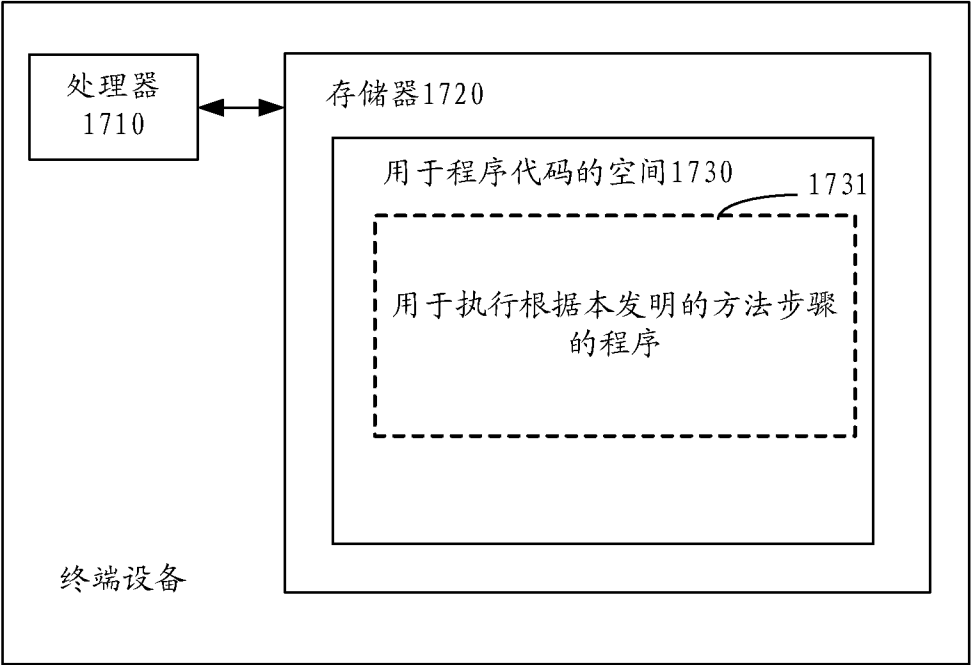


图 17

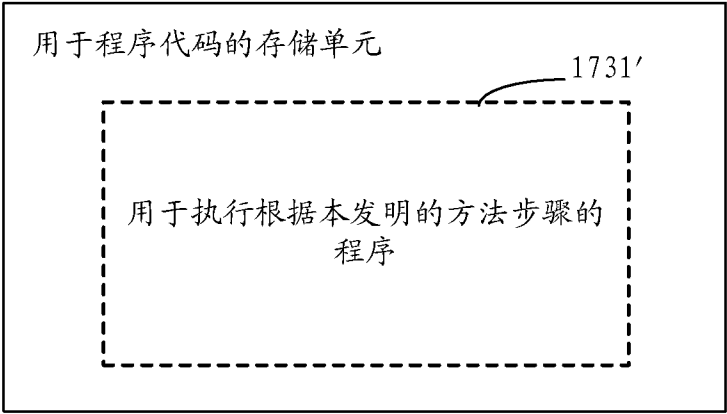


图 18

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/091539

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64 (2013.01) 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

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: domain name, application program, local IP address, DOMAIN, NAME, ANALYSE, VERIF+, REQUEST, TRANSMIT, SEND, INFORMATION, PERFORMANCE, EXECUTE, APPLICATION, PROGRAM, PAGE, TAMPER, DETECT, RECEIV+, ACCESS+, EMBED, RESPOND+, USER, INPUT, JUMP+, DETERMIN+, TRIGGER, LOCAL, IP, ADDRESS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105100298 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 25 November 2015 (25.11.2015), claims 1-10, and description, pages 1-4	1-14, 37-50, 73-74
PX	CN 105141709 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 09 December 2015 (09.12.2015), claims 1-10, and description, pages 1-3	15-24, 51-60, 75-76
PX	CN 105354511 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 24 February 2016 (24.02.2016), claims 1-10, and description, pages 1-4	25-36, 61-72, 77-78
X	CN 103605926 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 26 February 2014 (26.02.2014), description, paragraphs 28-44, and claims 4 and 6	25, 35, 61, 71, 77-78
Y	CN 103605926 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 26 February 2014 (26.02.2014), description, paragraphs 28-44, and claims 4 and 6	15, 23, 51, 59, 75-76

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 22 October 2016 (22.10.2016)	Date of mailing of the international search report 02 November 2016 (02.11.2016)
Name and mailing address of the ISA/CN: 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 LIU, Huan Telephone No.: (86-10) 62411853

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/091539

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104408204 A (BEIJING GRIDSUM TECHNOLOGY CO., LTD.), 11 March 2015 (11.03.2015), claims 1-2	15, 23, 51, 59, 75-76
A	CN 103605926 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 26 February 2014 (26.02.2014), the whole document	16-22, 24, 26-34, 36, 52-58, 60, 62-70, 72
A	CN 103561121 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 05 February 2014 (05.02.2014), the whole document	1-14, 37-50, 73-74
A	US 2014331304 A1 (WONG, J.), 06 November 2014 (06.11.2014), the whole document	1-14, 37-50, 73-74

International application No.
PCT/CN2016/091539

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 G06F 21/64 (2013.01) 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 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; EPDOC; 域名, 解析, 校验, 请求, 发送, 信息, 执行, 应用程序, 页面, 篡改, 检测, 接收, 访问, 内嵌, 响应, 用户, 输入, 跳转, 确定, 触发, 本地 IP 地址, DOMAIN, NAME, ANALYSE, VERIF+, REQUEST, TRANSMIT, SEND, INFORMATION, PERFORMANCE, EXECUTE, APPLICATION, PROGRAM, PAGE, TAMPER, DETECT, RECEIV+, ACCESS+, EMBED, RESPOND+, USER, INPUT, JUMP+, DETERMIN+, TRIGGER, LOCAL, IP, ADDRESS		
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
PX	CN 105100298 A (北京奇虎科技有限公司等) 2015年 11月 25日 (2015 - 11 - 25) 权利要求1-10, 说明书第1-4页	1-14, 37-50, 73-74
PX	CN 105141709 A (北京奇虎科技有限公司等) 2015年 12月 9日 (2015 - 12 - 09) 权利要求1-10, 说明书第1-3页	15-24, 51-60, 75-76
PX	CN 105354511 A (北京奇虎科技有限公司等) 2016年 2月 24日 (2016 - 02 - 24) 权利要求1-10, 说明书第1-4页	25-36, 61-72, 77-78
X	CN 103605926 A (北京奇虎科技有限公司等) 2014年 2月 26日 (2014 - 02 - 26) 说明书第28-44段、权利要求4, 6	25, 35, 61, 71, 77-78
Y	CN 103605926 A (北京奇虎科技有限公司等) 2014年 2月 26日 (2014 - 02 - 26) 说明书第28-44段、权利要求4, 6	15, 23, 51, 59, 75-76
☒ 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
2016年 10月 22日		2016年 11月 2日
ISA/CN的名称和邮寄地址		受权官员
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		刘欢
		电话号码 (86-10) 62411853

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
Y	CN 104408204 A (北京国双科技有限公司) 2015年 3月 11日 (2015 - 03 - 11) 权利要求1-2	15, 23, 51, 59, 75-76
A	CN 103605926 A (北京奇虎科技有限公司等) 2014年 2月 26日 (2014 - 02 - 26) 全文	16-22, 24, 26- 34, 36, 52-58, 60, 62-70, 72
A	CN 103561121 A (北京奇虎科技有限公司等) 2014年 2月 5日 (2014 - 02 - 05) 全文	1-14, 37-50, 73-74
A	US 2014331304 A1 (WONG JOHN) 2014年 11月 6日 (2014 - 11 - 06) 全文	1-14, 37-50, 73-74

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/091539

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	105100298	A	2015年 11月 25日	无	
CN	105141709	A	2015年 12月 9日	无	
CN	105354511	A	2016年 2月 24日	无	
CN	103605926	A	2014年 2月 26日	无	
CN	104408204	A	2015年 3月 11日	无	
CN	103561121	A	2014年 2月 5日	无	
US	2014331304	A1	2014年 11月 6日	US 9294483 B2	2016年 3月 22日