

(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
2012 年 9 月 27 日 (27.09.2012)



(10) 国际公布号
WO 2012/126263 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2011/083807
- (22) 国际申请日: 2011 年 12 月 12 日 (12.12.2011)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201110070193.4 2011 年 3 月 23 日 (23.03.2011) CN
- (71) 申请人 (对除美国外的所有指定国): **腾讯科技 (深圳) 有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。
- (72) 发明人; 及
- (75) 发明人/申请人 (仅对美国): **胡鹏 (HU, Peng)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。 **张子璠 (ZHANG, Zijun)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。 **葛文兵 (GE, Wenbing)** [CN/CN]; 中国广东

省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。

- (74) 代理人: **北京德琦知识产权代理有限公司 (DEQI INTELLECTUAL PROPERTY LAW CORPORATION)**; 中国北京市海淀区知春路 1 号学院国际大厦 7 层, Beijing 100083 (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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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,

[见续页]

(54) Title: DEVICE, SYSTEM AND METHOD FOR ACCESSING INTERNET WEB PAGE

(54) 发明名称: 一种访问互联网网页的装置、系统及方法

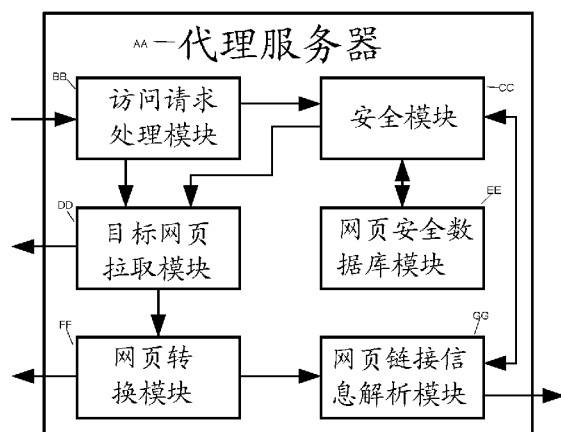


图 2 / Fig. 2

AA PROXY SERVER
BB ACCESS REQUEST PROCESSING MODULE
CC SECURITY MODULE
DD TARGET WEB PAGE PULLING MODULE
EE WEB PAGE SECURITY DATABASE MODULE
FF WEB PAGE CONVERSION MODULE
GG WEB PAGE LINK INFORMATION RESOLUTION MODULE

(57) Abstract: Disclosed are a device, system and method for accessing an Internet web page. The system comprises: a user terminal and a proxy server. The user terminal initiates to the proxy server an access request carrying uniform resource locator (URL) information identifying a target web page requiring security authentication, and receives and presents target web page information output by the proxy server. The proxy server receives the access request, performs security authentication, according to pre-stored web page security database information, on the carried URL information identifying the target web page requiring the security authentication, and if the security authentication succeeds, obtains the target web page information and outputs same to the user terminal. By applying the present invention, network delay overhead in accessing Internet web pages can be reduced, and user experience can be improved.

[见续页]



RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, **本国际公布:**
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

(57) 摘要:

本发明公开了一种访问互联网网页的装置、系统及方法。该系统包括: 用户终端以及代理服务器, 其中, 用户终端向代理服务器发起访问请求, 携带标识需进行安全认证的目标网页的统一资源定位器 URL 信息; 接收代理服务器输出的目标网页信息, 进行展示; 代理服务器接收访问请求, 根据预先存储的网页安全数据库信息, 对携带标识需进行安全认证的目标网页的 URL 信息进行安全认证, 如果安全认证通过, 获取目标网页信息并输出至用户终端。应用本发明, 可以降低访问互联网网页的网络延迟开销、提高用户体验。

一种访问互联网网页的装置、系统及方法

技术领域

本发明涉及安全访问技术，特别涉及一种访问互联网网页的装置、系统及方法。

5 发明背景

近年来，随着智能用户终端的迅速发展，用户使用用户终端浏览器访问互联网网页日趋频繁，用户通过用户终端浏览器访问互联网网页（以下简称为网页），主要包括直连型访问以及代理服务器访问两种方式。其中，

- 10 直连型访问方式就是用户通过用户终端浏览器访问目标网页时，直接向目标网页发起访问请求；而代理服务器访问方式则是用户通过用户终端浏览器访问所有互联网网页时，均通过预设的代理服务器来完成，也就是说，代理服务器负责代理用户向目标网页发起访问请求，获取网页，以及根据需要进行网页转换，并将转换的网页输出至用户终端浏览
- 15 器进行展示。相比直连型访问而言，通过代理服务器访问，一方面，可以帮助用户终端完成网页转换，从而返回适合用户终端浏览器布局显示的网页，不仅可以节约用户终端解释脚本语言的计算量，而且能够有效降低用户终端流量；另一方面，代理服务器自身具备缓存作用，也有利于提高用户访问网页的速度体验。基于这些因素，在实际应用中，用户
- 20 终端浏览器应用代理服务器进行访问较为广泛，例如 QQ 用户终端浏览器、UCWeb 与 Opera Mini 等主流用户终端浏览器，均有提供代理服务器访问的机制。

互联网技术在带给用户极大便利的同时，也给用户带来了安全问题，尤其在用户终端浏览器访问网页的过程中，相关的安全问题也逐渐凸

显。例如，一些恶意钓鱼网站或网页诱骗用户在访问网页时，要求输入账号以及密码信息，从而盗取用户账号及密码；另外一些恶意网站，如果用户一旦连接访问，就会自动收取高昂的信息服务费，或故意设置扣费陷阱；此外，还有一些网站，通过发布病毒木马安装包的链接，影响用户终端的正常使用，危害用户终端。因而，通过用户终端浏览器访问网页引起的安全风险，已成为当前移动互联网广为关注的问题。

为了增强用户终端浏览器访问网页的安全性，当前，在用户终端浏览器访问互联网网页时，基于联网扫描来保障浏览器的安全访问，也就是说，用户通过用户终端浏览器在下载展示页面之前，即在请求访问目标网页时，将该目标网页的统一资源定位器（URL，Uniform Resource Locator）信息向联网的安全服务器发送，请求安全服务器认证该 URL 的安全性，安全服务器根据存储的网页安全数据库信息进行安全认证，并将对该 URL 的安全认证响应结果返回给用户终端，用户终端根据安全认证响应结果执行相应操作：如果安全认证响应结果为安全，则向代理服务器发起访问请求，如果安全服务器判定该 URL 存在安全风险，可以由安全服务器设置禁止用户终端浏览器访问该目标网页，用户终端不能向代理服务器发起对该网页的访问请求，或用户根据安全认证响应结果中包含的安全风险提示信息，决定是否向代理服务器发起访问请求。

由上述可见，现有访问互联网网页的方法，利用后台（安全服务器）预先收集的各网页安全数据信息，对用户请求访问的网页进行安全认证，并将安全认证响应结果输出至用户终端，用户终端再根据安全认证响应结果确定是否向代理服务器发起访问请求，从而达到安全访问的作用，但由于在安全认证后，安全服务器也需要将安全认证的信息发送至用户终端，再由用户终端发起访问请求，使得用户访问网页所需的时间较长，从而带来一定的网络延迟开销；进一步地，即使是通过安全认证

的网页，在其网页中，还存在较多的链接跳转，如果用户需要访问该链接跳转对应的网页，还需要重新将该链接跳转信息向安全服务器发送，进行安全认证，使得访问该链接跳转对应的网页导致的网络延迟更大，降低了用户体验；而且，如果链接跳转信息较多，需要不断与安全服务器进行交互，也增加了流量开销，增加了用户成本。

发明内容

有鉴于此，本发明的主要目的在于提出一种访问互联网网页的装置，降低访问互联网网页的网络延迟开销、提高用户体验。

本发明的另一目的在于提出一种访问互联网网页的系统，降低访问互联网网页的网络延迟开销、提高用户体验。

本发明的再一目的在于提出一种访问互联网网页的方法，降低访问互联网网页的网络延迟开销、提高用户体验。

为达到上述目的，本发明提供了一种访问互联网网页的装置，该装置包括：访问请求处理模块、安全模块、目标网页拉取模块以及网页安全数据库模块，其中，

所述访问请求处理模块用于接收访问请求，如果访问请求中包含的目标网页的统一资源定位器URL信息携带有需进行安全认证的标识，将目标网页的URL信息输出至安全模块；

所述安全模块用于根据网页安全数据库模块存储的网页安全数据库信息，对接收的目标网页的URL信息进行安全认证，如果认证通过，将该目标网页的URL信息输出至目标网页拉取模块；

所述目标网页拉取模块用于根据接收的目标网页的URL信息，从目标网页拉取网页信息，并输出至用户终端；

所述网页安全数据库模块用于存储网页安全数据库信息。

一种访问互联网网页的系统，该系统包括：用户终端以及代理服务器，其中，

所述用户终端用于向代理服务器发起访问请求，携带标识需进行安全认证的目标网页的URL信息；接收代理服务器输出的目标网页信息，
5 进行展示；

所述代理服务器用于接收访问请求，根据预先存储的网页安全数据库信息，对携带标识需进行安全认证的目标网页的URL信息进行安全认证，如果安全认证通过，获取目标网页信息并输出至用户终端。

一种访问互联网网页的方法，该方法包括：

10 用户终端发起访问请求，携带标识需进行安全认证的目标网页的统一资源定位器URL信息；

代理服务器根据预先存储的网页安全数据库信息，对接收的携带标识需进行安全认证的目标网页的URL信息进行安全认证，确定安全认证通过，获取目标网页信息并输出至用户终端；

15 用户终端接收代理服务器输出的目标网页信息，进行展示。

由上述的技术方案可见，本发明提供一种访问互联网网页的装置、系统及方法，该系统包括：用户终端以及代理服务器，其中，用户终端向代理服务器发起访问请求，携带标识需进行安全认证的目标网页的统一资源定位器URL信息；接收代理服务器输出的目标网页信息，进行展示；代理服务器接收访问请求，根据预先存储的网页安全数据库信息，对携带标识需进行安全认证的目标网页的URL信息进行安全认证，如果安全认证通过，获取目标网页信息并输出至用户终端。这样，利用代理服务器扩展用户终端浏览器的安全访问的功能，通过移动终端浏览器与代理服务器的配置，对网页进行安全认证，并在安全认证通过后，
20 直接拉取该网页信息，降低了访问互联网网页的网络延迟开销，从而在
25

不增加额外网络延迟的情况下为用户提供安全浏览的服务，提高了用户体验。

附图简要说明

图1为本发明实施例访问互联网网页的系统结构示意图。

5 图2为本发明实施例代理服务器结构示意图。

图3为本发明实施例访问互联网网页的方法流程示意图。

图4为本发明实施例直接请求网页访问的方法流程示意图。

图5为本发明实施例链接跳转访问的方法流程示意图。

实施本发明的方式

10 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图及具体实施例对本发明作进一步地详细描述。

现有技术中，为了提高访问互联网网页的安全性，用户终端需要将目标网页的 URL 信息向安全服务器发送进行安全认证，并根据安全服务器返回的安全认证响应信息，决定是否通过代理服务器发起对目标网页的访问，增加了用户终端与安全服务器交互引起的网络延迟开销，降低了用户体验。本发明实施例中，考虑由代理服务器代替安全服务器认证用户提交请求访问的网页的安全性，如果请求访问的网页的安全认证通过，则直接访问该请求访问的网页，而对于安全认证未通过的网页，用户终端根据代理服务器返回的安全认证响应结果，确定是否访问该网页，从而在不增加额外网络延迟的情况下为用户提供安全浏览的服务。

15 20

图 1 为本发明实施例访问互联网网页的系统结构示意图。参见图 1，该系统包括：用户终端以及代理服务器，其中，

所述用户终端用于向代理服务器发起访问请求，携带标识需进行安

全认证的目标网页的 URL 信息；接收代理服务器输出的目标网页信息，进行展示；

本发明实施例中，需进行安全认证的标识可由代理服务器与用户终端预先协商确定。

- 5 进一步地，用户终端还用于接收代理服务器返回的安全认证响应结果，确定访问该目标网页，向代理服务器发起访问请求，携带标识强制访问的目标网页的 URL 信息。

所述代理服务器用于接收访问请求，根据预先存储的网页安全数据库信息，对携带标识需进行安全认证的目标网页的 URL 信息进行安全
10 认证，如果安全认证通过，获取目标网页信息并输出至用户终端。

本发明实施例中，代理服务器进一步用于在安全认证未通过时，向用户终端返回安全认证响应结果；接收携带标识强制访问的目标网页的 URL 信息，获取目标网页信息并输出至用户终端。

- 安全认证响应结果包括：目标网页安全级别为未知以及目标网页安全
15 全级别为风险。

进一步地，对于安全级别为风险或未知的扣费网站、钓鱼网站、虚假信息网站以及病毒木马链接等恶意网站，可以在安全认证响应结果中，直接携带该信息，以向用户提示访问的目标网页为扣费网站、钓鱼网站、虚假信息网站或病毒木马链接等恶意网站。

- 20 较佳地，代理服务器还用于根据访问请求携带的用户终端浏览器信息，将目标网页转换为适应该用户终端浏览器的网页结构，输出至该访问请求所属的用户终端。

图 2 为本发明实施例代理服务器结构示意图。参见图 2，该代理服务器包括：访问请求处理模块、安全模块、目标网页拉取模块以及网页
25 安全数据库模块，其中，

所述访问请求处理模块用于接收访问请求，如果访问请求中包含的目标网页的 URL 信息携带有需进行安全认证的标识，将目标网页的 URL 信息输出至安全模块；

5 本发明实施例中，访问请求处理模块还进一步用于判断如果访问请求中包含的目标网页的 URL 信息携带有强制访问的标识，将目标网页的 URL 信息输出至目标网页拉取模块。

所述安全模块用于根据网页安全数据库模块存储的网页安全数据库信息，对接收的目标网页的 URL 信息进行安全认证，如果认证通过，将该目标网页的 URL 信息输出至目标网页拉取模块；

10 本发明实施例中，安全模块还进一步用于当安全认证未通过时，向用户终端返回安全认证响应结果；而且，可以在目标网页的 URL 信息的安全认证未通过后，进一步根据预先设置的安全策略，确定该目标网页不能访问，在返回的安全认证响应结果中携带禁止访问标识。这样，用户终端即使接收代理服务器返回的安全认证响应结果，确定访问该目标网页，也不向代理服务器发起访问请求，而是向用户展示该目标网页被禁止访问的信息，以有效保护用户的利益。当然，为了尊重用户的选择，即使对于存在安全风险的网页，也会在风险提示的页面中给用户提
15 供强制继续访问的入口。这种情况下，用户终端浏览器在再次请求该网页时，在超文本传输协议（HTTP，Hypertext Transfer Protocol）的 GET
20 方法（访问请求）中增加相关安全参数，以指示代理服务器该 URL 请求是用户强制要求的，代理服务器在收到之后，不再主动查询网页安全数据库，而直接代理用户请求以及返回网页。

预先设置的安全策略可以是根据用户访问请求中的用户信息，查询得到该用户为未成年人，或，该目标网页涉及色情、暴力等污秽内容等。

25 所述目标网页拉取模块用于根据接收的目标网页的 URL 信息，从

目标网页拉取网页信息，并输出至用户终端；

所述网页安全数据库模块用于存储网页安全数据库信息。

本发明实施例中，存储的网页安全数据库信息包括网页 URL 信息及其映射的安全级别信息。例如，可以预先设置 1 表示安全级别为安全，
5 2 表示安全级别为未知，3 表示安全级别为风险。这样，如果网页 URL 映射的安全级别值为 1，则表示该网页是安全的。

较佳地，该代理服务器还包括：

网页转换模块，用于根据访问请求携带的用户终端浏览器信息，将目标网页拉取模块拉取到的网页信息转换为适应该用户终端浏览器的
10 网页结构，输出至该访问请求所属的用户终端。

实际应用中，即使是通过安全认证的网页，在其网页中，还存在较多的链接跳转，本发明实施例中，针对拉取的网页存在的链接跳转情况，进一步设置网页链接信息解析模块，用于解析目标网页拉取模块拉取到的网页信息，获取包含的链接跳转信息，输出至安全模块；接收安全模
15 块输出的安全级别信息，嵌入至网页信息的该链接跳转信息中，并将网页信息输出至用户终端；相应地，所述安全模块进一步用于接收网页链接信息解析模块输出的链接跳转信息，进行安全认证，将认证的安全级别信息输出至网页链接信息解析模块；所述用户终端进一步在浏览网页信息，触发对网页信息中的链接跳转进行访问时，向用户展示该链接跳
20 转对应的安全级别信息；并在用户确定访问该链接跳转对应的网页时，向访问请求处理模块发起访问请求，携带强制访问的标识。

这样，如前所述，即使对于存在安全风险的网页，也会在风险提示的页面中给用户提供强制继续访问的入口，如果用户需要访问该链接跳转对应的网页，不需要重新将该链接跳转信息向安全服务器发送以进行
25 安全认证，有效降低了访问该链接跳转对应的网页的网络延迟以及网络

流量，从而提高了用户体验。

由上述可见，本发明实施例的访问互联网网页的系统，用户终端向代理服务器发起访问请求，携带标识需进行安全认证的目标网页的 URL 信息；接收代理服务器输出的目标网页信息，进行展示；代理服务器接收访问请求，根据预先存储的网页安全数据库信息，对携带标识需进行安全认证的目标网页的 URL 信息进行安全认证，如果安全认证通过，获取目标网页信息并输出至用户终端。这样，利用代理服务器扩展用户终端浏览器的安全浏览的功能，通过移动终端浏览器与代理服务器的配置，对网页进行安全认证，并在安全认证通过后，直接拉取该网页信息，降低了访问互联网网页的网络延迟开销，从而在不增加额外网络延迟的情况下为用户提供安全浏览的服务，提高了用户体验。进一步地，通过在网页信息的链接跳转信息中嵌入相关安全级别信息，通过增加少量的额外网络流量，能够有效且快速向用户提示扣费网站、钓鱼网站、虚假信息网站以及病毒木马链接等恶意网站，能够给予用户必要的风险提示，并且不延长用户的网页等待时间。

图 3 为本发明实施例访问互联网网页的方法流程示意图。参见图 3，该流程包括：

步骤 301，用户终端发起访问请求，携带标识需进行安全认证的目标网页的 URL 信息；

本步骤中，用户终端需要访问互联网网页时，获取需要访问的目标网页的 URL 信息，并携带需进行安全认证的标识，封装在访问请求中，向代理服务器发送。

步骤 302，代理服务器根据预先存储的网页安全数据库信息，对接收的携带标识需进行安全认证的目标网页的 URL 信息进行安全认证，确定安全认证通过，获取目标网页信息并输出至用户终端；

本步骤中，如果代理服务器对目标网页的 URL 信息的安全认证通过，则直接根据该目标网页的 URL 信息拉取该目标网页信息，不需将认证信息向用户终端返回，从而降低了访问互联网网页的网络延迟开销。

- 5 步骤 303，用户终端接收代理服务器输出的目标网页信息，进行展示。

较佳地，对接收的携带标识需进行安全认证的目标网页的 URL 信息进行安全认证还包括：

- 代理服务器确定安全认证未通过，向用户终端返回安全认证响应结果；
10 果；

用户终端接收代理服务器返回的安全认证响应结果，确定访问该目标网页，向代理服务器发起访问请求，携带标识强制访问的目标网页的 URL 信息；

- 接收携带标识强制访问的目标网页的 URL 信息，执行所述获取目标网页信息并输出至用户终端的步骤。
15 标网页信息并输出至用户终端的步骤。

- 实际应用中，用户终端浏览器访问互联网网页时，根据用户的网页打开方式，可以分为“直接请求网页”与“链接跳转”两种情况，对于直接请求网页的情况，即打开的目标网页中，不包含嵌入的链接网页 URL 信息，而对于链接跳转的情况，即打开的目标网页中，包含嵌入的链接网页 URL 信息，用户可以通过在打开的网页中，点击链接网页 URL 信息，从而触发访问另一网页，本发明实施例中，为了保障用户的访问安全，还需要对链接网页 URL 信息进行安全认证，下面分别进行描述。
20 链接网页 URL 信息，用户可以通过在打开的网页中，点击链接网页 URL 信息，从而触发访问另一网页，本发明实施例中，为了保障用户的访问安全，还需要对链接网页 URL 信息进行安全认证，下面分别进行描述。

图 4 为本发明实施例直接请求网页访问的方法流程示意图。参见图 4，该流程包括：

- 25 步骤 401，用户终端浏览器向代理服务器请求认证 URL；

步骤 402, 代理服务器查询网页安全数据库, 得到该 URL 的安全属性;

步骤 403, 判断该 URL 的安全属性是否存在安全风险, 如果是, 执行步骤 404, 否则, 执行步骤 405;

5 步骤 404, 代理服务器根据风险类型生成提示网页信息, 返回给用户终端浏览器;

本步骤中, 代理服务器可以直接返回一个特定的网页页面, 告知用户其安全风险。

步骤 405, 访问该 URL 对应的网页。

10 本步骤中, 如果 URL 的安全属性不存在安全风险, 则直接访问该 URL 对应的网页, 为用户提供服务。

图 5 为本发明实施例链接跳转访问的方法流程示意图。是否发生链接跳转, 可以通过代理服务器解析拉取的目标网页信息, 判断该目标网页信息中是否存在链接跳转信息, 如果存在, 参见图 5, 该流程包括:

15 步骤 501, 代理服务器对网页页面中出现的每个 URL 的安全属性进行判断;

本步骤中, 代理服务器接收目标网页 (web 服务器) 返回的页面内容, 其安全模块针对页面中包含的每个 URL, 连接网页安全数据库进行安全属性的查询。

20 步骤 502, 代理服务器根据预先设置的安全属性标记策略在部分或全部 URL 对应的标签中增加相应安全属性值描述;

实际应用中, 为了减少代理服务器与用户终端浏览器对新追加属性的处理复杂度, 代理服务器的安全模块在追加安全属性的时候, 可以根据预先设置的安全属性标记策略, 对需要标记的 URL 进行标记, 本发明
25 明实施例中, 安全属性标记策略包括: 黑名单机制标记策略、白名单机

制标记策略以及混合名单机制标记策略，其中，

一、黑名单机制：即只在存在安全风险的 URL 标签中增加安全属性值，这样，对于大部分正常的网页都不用再额外处理。对应地，在用户试图打开存在安全属性值且指示为风险的 URL 时，用户终端浏览器会以合适的方式阻塞并弹出提示信息以提醒用户。

当然，如前所述，在用户试图打开存在安全属性值且指示为风险的 URL 时，也可以弹出禁止访问该网页的提示，禁止用户访问。

黑名单机制适用于对用户终端浏览安全要求相对宽松的上网环境，这样，通过维护只存在风险的网页信息，可以减少数据库大小，当然，如果网页安全数据库不够完善，也会引入一些安全风险的漏判。

二、白名单机制：即只对不存在任何安全风险的 URL 标签中增加安全属性值，对应地，在用户试图打开存在安全属性值且指示为安全的 URL 时，用户终端浏览器会以合适的方式显式指示用户当前的访问是安全的，对于安全属性值未给出的 URL，即其他不确定风险级别以及有风险的 URL，在试图打开时用户终端浏览器不会给出安全浏览的指示，当然，实际应用中，也可以弹出风险提示。

这种机制适用于对访问安全要求相对严格的上网环境，通过只维护安全网页的信息，也可以有效减少数据库的大小，当然，实际应用中，如果网页安全数据库不够完善，也会引入一些原本安全的 URL 未被浏览器显式指示的情况。

三、混合名单机制：即对于不存在安全风险的 URL、增加 URL 安全标签属性值，指示该 URL 安全；对于不确定的 URL，例如，网页安全数据库查询未命中的 URL 或存在安全风险的 URL，不进行额外处理或增加含义为未知安全或风险的标签属性值。

该种机制下，网页安全数据库需要维护全量的 URL 信息，因而，

浏览器能够给出更明确的安全指示。

上述示例中，安全属性值的取值范围依赖于网站的安全状态描述，包括安全、未知与风险三大类，风险可以进一步细分为扣费网站、病毒网站、木马网站、虚假信息网站、钓鱼网站等。这些信息用特定的 ID 表示，并在代理服务器与浏览器之间建立约定统一，这样，便于浏览器向用户展现详细的风险类型提示。

本步骤中，安全模块将查询结果以属性值的方式追加到网页脚本中，举例来说，对于常规的链接跳转表示：`<a href="http://www.qq.com">QQ</a>`，代理服务器的安全模块追加 security_level 的属性值，新的链接跳转表示为`<a href="http://www.qq.com" security_level="1">QQ</a>`，这里值为 1 表示为安全的 URL。

此外，为了降低浏览器处理复杂度，对于所有的机制，代理服务器在标识安全属性值的时候采取去重的方法。这样，同样的 URL 不会被多次添加安全属性值，减少浏览器解析的计算开销。

步骤 503，用户终端浏览器解析网页中每个 URL 标签，并记录其安全属性值，基于 URL 的安全属性值，在展示页面时采用适当的提示。

本步骤中，用户可以根据提示的信息决定是否访问该 URL 对应的链接跳转，如果确定访问，向代理服务器发起访问请求，携带标识强制访问的目标网页的 URL 信息。

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原则之内，所作的任何修改、等同替换以及改进等，均应包含在本发明的保护范围之内。

权利要求书

1、一种访问互联网网页的装置，其特征在于，该装置包括：访问请求处理模块、安全模块、目标网页拉取模块以及网页安全数据库模块，其中，

5 所述访问请求处理模块用于接收访问请求，如果访问请求中包含的目标网页的统一资源定位器 URL 信息携带有需进行安全认证的标识，将目标网页的 URL 信息输出至安全模块；

 所述安全模块用于根据网页安全数据库模块存储的网页安全数据库信息，对接收的目标网页的 URL 信息进行安全认证，如果认证通过，
10 将该目标网页的 URL 信息输出至目标网页拉取模块；

 所述目标网页拉取模块用于根据接收的目标网页的 URL 信息，从目标网页拉取网页信息，并输出至用户终端；

 所述网页安全数据库模块用于存储网页安全数据库信息。

2、如权利要求 1 所述的装置，其特征在于，所述安全模块进一步用于当安全认证未通过时，向用户终端返回安全认证响应结果；相应地，
15 所述访问请求处理模块进一步用于确定访问请求中包含的目标网页的 URL 信息携带有强制访问的标识，将目标网页的 URL 信息输出至目标网页拉取模块。

 所述访问请求处理模块进一步用于确定访问请求中包含的目标网页的 URL 信息携带有强制访问的标识，将目标网页的 URL 信息输出至目标网页拉取模块。

3、如权利要求 2 所述的装置，其特征在于，所述安全模块进一步用于当安全认证未通过时，根据预先设置的安全策略，确定该目标网页不能访问，在返回的安全认证响应结果中携带禁止访问标识。
20 于当安全认证未通过时，根据预先设置的安全策略，确定该目标网页不能访问，在返回的安全认证响应结果中携带禁止访问标识。

4、如权利要求 3 所述的装置，其特征在于，所述安全认证响应结果包括：目标网页安全级别为未知以及目标网页安全级别为风险。

5、如权利要求 1 至 4 任一项所述的装置，其特征在于，该装置进一

步包括:

网页转换模块, 用于根据访问请求携带的用户终端浏览器信息, 将目标网页拉取模块拉取到的网页信息转换为适应该用户终端浏览器的网页结构, 输出至该访问请求所属的用户终端。

- 5 6、如权利要求 5 所述的装置, 其特征在于, 该装置进一步包括: 网页链接信息解析模块, 用于解析目标网页拉取模块拉取到的网页信息, 获取包含的链接跳转信息, 输出至安全模块; 接收安全模块输出的安全级别信息, 嵌入至网页信息的该链接跳转信息中, 并将网页信息输出至用户终端; 相应地,

- 10 所述安全模块进一步用于接收网页链接信息解析模块输出的链接跳转信息, 进行安全认证, 将认证的安全级别信息输出至网页链接信息解析模块。

7、一种访问互联网网页的系统, 其特征在于, 该系统包括: 用户终端以及代理服务器, 其中,

- 15 所述用户终端用于向代理服务器发起访问请求, 携带标识需进行安全认证的目标网页的 URL 信息; 接收代理服务器输出的目标网页信息, 进行展示;

- 所述代理服务器用于接收访问请求, 根据预先存储的网页安全数据库信息, 对携带标识需进行安全认证的目标网页的 URL 信息进行安全
20 认证, 如果安全认证通过, 获取目标网页信息并输出至用户终端。

8、如权利要求 7 所述的系统, 其特征在于, 所述代理服务器包括: 访问请求处理模块、安全模块、目标网页拉取模块以及网页安全数据库模块, 其中,

- 所述访问请求处理模块用于接收访问请求, 如果访问请求中包含的
25 目标网页的统一资源定位器 URL 信息携带有需进行安全认证的标识,

将目标网页的 URL 信息输出至安全模块;

所述安全模块用于根据网页安全数据库模块存储的网页安全数据库信息,对接收的目标网页的 URL 信息进行安全认证,如果认证通过,将该目标网页的 URL 信息输出至目标网页拉取模块;

- 5 所述目标网页拉取模块用于根据接收的目标网页的 URL 信息,从目标网页拉取网页信息,并输出至用户终端;

所述网页安全数据库模块用于存储网页安全数据库信息。

9、如权利要求 8 所述的系统,其特征在于,所述代理服务器进一步包括:

- 10 网页转换模块,用于根据访问请求携带的用户终端浏览器信息,将目标网页拉取模块拉取到的网页信息转换为适应该用户终端浏览器的网页结构,输出至该访问请求所属的用户终端。

- 10、如权利要求 8 所述的系统,其特征在于,所述代理服务器进一步用于在安全认证未通过时,向用户终端返回安全认证响应结果;接收
15 携带标识强制访问的目标网页的 URL 信息,获取目标网页信息并输出至用户终端;相应地,

所述用户终端进一步用于接收代理服务器返回的安全认证响应结果,确定访问该目标网页,向代理服务器发起访问请求,携带标识强制访问的目标网页的 URL 信息。

- 20 11、如权利要求 8 至 10 任一项所述的系统,其特征在于,所述代理服务器进一步包括:

- 网页链接信息解析模块,用于解析目标网页拉取模块拉取到的网页信息,获取包含的链接跳转信息,输出至安全模块;接收安全模块输出的安全级别信息,嵌入至网页信息的该链接跳转信息中,并将网页信息
25 输出至用户终端;相应地,

所述安全模块进一步用于接收网页链接信息解析模块输出的链接跳转信息，进行安全认证，将认证的安全级别信息输出至网页链接信息解析模块；

5 所述用户终端进一步在浏览网页信息，触发对网页信息中的链接跳转进行访问时，向用户展示该链接跳转对应的安全级别信息；并在用户确定访问该链接跳转对应的网页时，向访问请求处理模块发起访问请求，携带强制访问的标识。

12、一种访问互联网网页的方法，其特征在于，该方法包括：

10 用户终端发起访问请求，携带标识需进行安全认证的目标网页的统一资源定位器 URL 信息；

代理服务器根据预先存储的网页安全数据库信息，对接收的携带标识需进行安全认证的目标网页的 URL 信息进行安全认证，确定安全认证通过，获取目标网页信息并输出至用户终端；

用户终端接收代理服务器输出的目标网页信息，进行展示。

15 13、如权利要求 12 所述的方法，其特征在于，所述对接收的携带标识需进行安全认证的目标网页的 URL 信息进行安全认证进一步包括：

代理服务器确定安全认证未通过，向用户终端返回安全认证响应结果；

20 用户终端接收代理服务器返回的安全认证响应结果，确定访问该目标网页，向代理服务器发起访问请求，携带标识强制访问的目标网页的 URL 信息；

接收携带标识强制访问的目标网页的 URL 信息，执行所述获取目标网页信息并输出至用户终端的步骤。

25 14、如权利要求 12 或 13 所述的方法，其特征在于，在所述获取目标网页信息之后，输出至用户终端之前，进一步包括：

解析获取的目标网页信息，获取包含的链接跳转信息，进行安全认证，根据预先设置的安全属性标记策略，将安全认证的安全级别信息嵌入至目标网页信息包含的该链接跳转信息中。

- 15、如权利要求 14 所述的方法，其特征在于，所述安全属性标记策略包括：只在存在安全风险的 URL 标签中增加安全属性值的黑名单机制标记策略、只对不存在任何安全风险的 URL 标签中增加安全属性值的白名单机制标记策略以及对所有 URL 标签中增加安全属性值的混合名单机制标记策略。

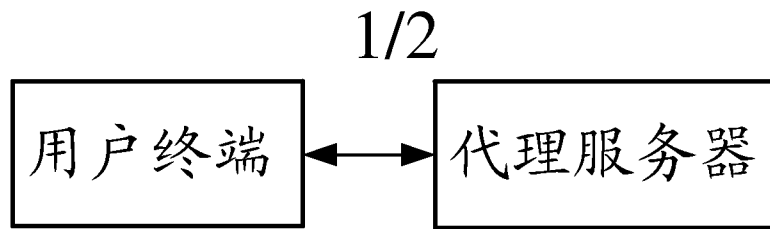


图 1

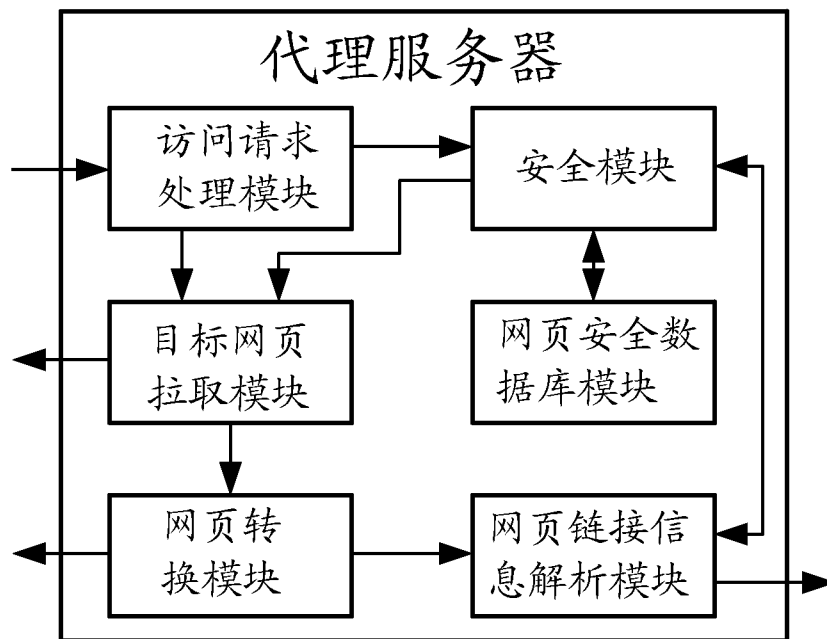


图 2

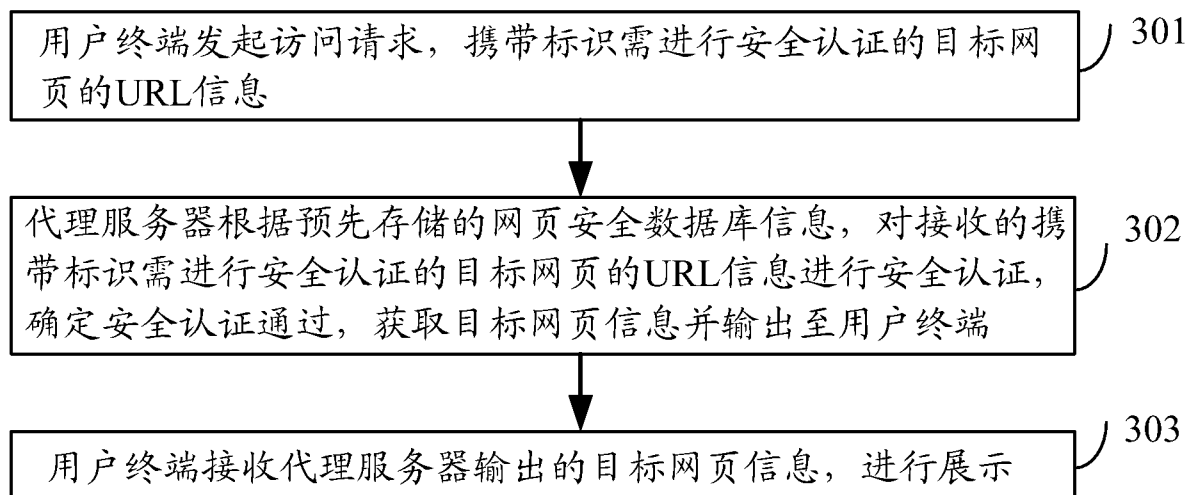


图 3

2/2

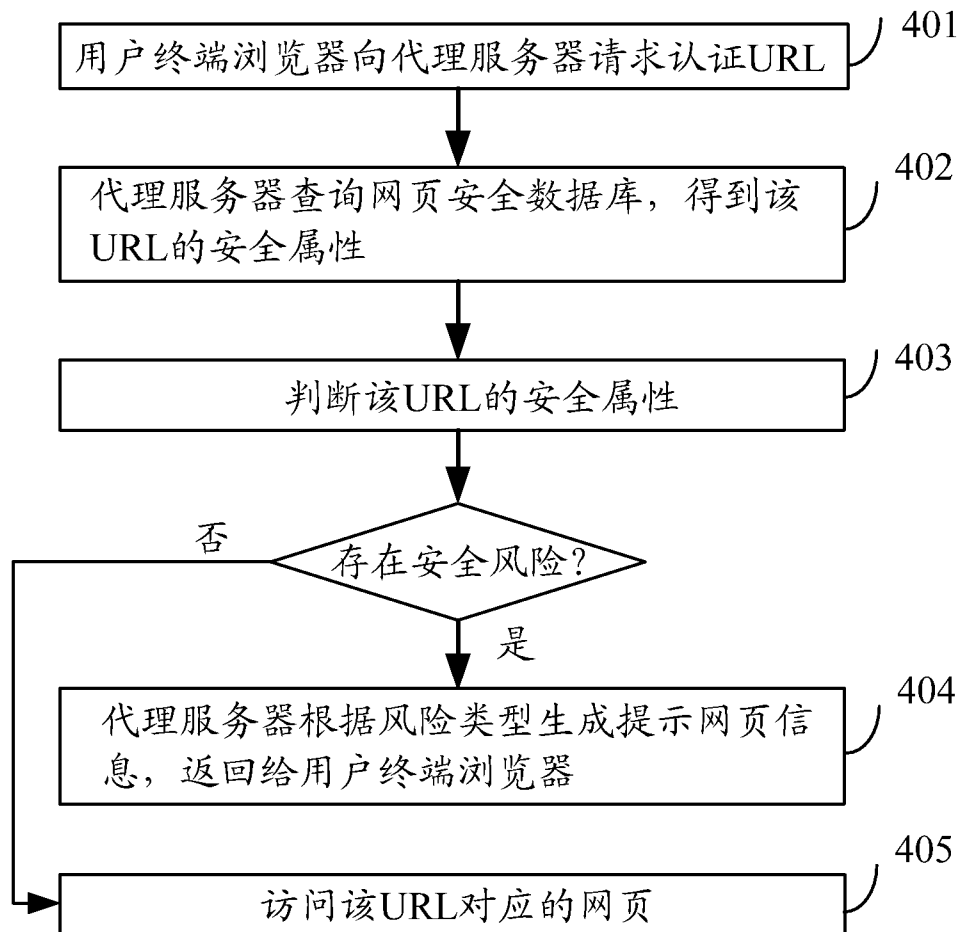


图 4

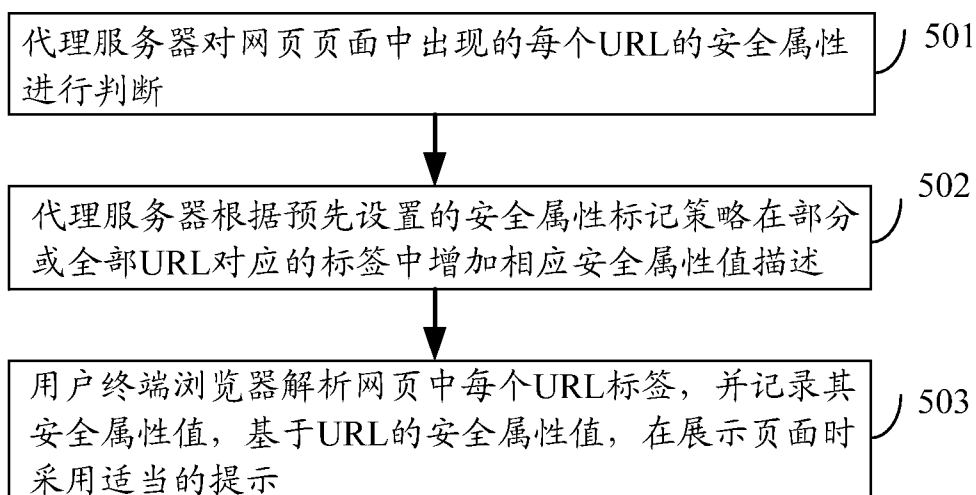


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/083807

A. CLASSIFICATION OF SUBJECT MATTER

H04I 29/06 (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)

IPC: H04L

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)

CPRSABS, CNKI, VEN: URL, united resource location, web page, identifier, safety, security, secure, safe, authenticate, request, database, internet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101729857A (ZTE CORP.) 09 Jun. 2010(09.06.2010) description, paragraphs 0028-0059	1, 7-8, 12
A	CN101977235A (BEIJING BEIXINYUAN SOFTWARE CO., LTD.) 16 Feb. 2011(16.02.2011) the whole document	1-15
A	CN101159000A(SHENZHEN THUNDER NETWORK TECHNOLOGY CO., LTD.) 09 Apr. 2008(09.04.2008) the whole document	1-15
A	CN101132404A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 27 Feb. 2008 (27.02.2008) the whole document	1-15
A	US2008119177A1 (SPEEDUS CORP.) 22 May 2008(22.05.2008) the whole document	1-15

☐ 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 09 Mar. 2012(09.03.2012)	Date of mailing of the international search report 22 Mar. 2012(22.03.2012)
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 MAO, Yunnan Telephone No. (86-10)62412004

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/083807

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101729857A	09.06.2010	WO2011063731A1	03.06.2011
CN101977235A	16.02.2011	NONE	
CN101159000A	09.04.2008	CN100527147C	12.08.2009
CN101132404A	27.02.2008	NONE	
US2008119177A1	22.05.2008	NONE	

国际检索报告

国际申请号

PCT/CN2011/083807

A. 主题的分类

H04L29/06 (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)

IPC: H04L

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))

CPRSABS,CNKI: URL, 统一资源定位器, 网页, 标识, 安全, 认证, 请求, 数据库, 互联网

VEN: URL, united resource location, web page, identifier, safety, security, secure, safe, authenticate, request, database, internet

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	CN101729857A (中兴通讯股份有限公司) 09.6 月 2010 (09.06.2010) 说明书第 0028-0059 段	1, 7-8, 12
A	CN101977235A (北京北信源软件股份有限公司) 16.2 月 2011 (16.02.2011) 全文	1-15
A	CN101159000A (深圳市迅雷网络技术有限公司) 09.4 月 2008 (09.04.2008) 全文	1-15
A	CN101132404A (腾讯科技(深圳)有限公司) 27.2 月 2008 (27.02.2008) 全文	1-15
A	US2008119177 A1(SPEEDUS CORP.) 22.5 月 2008 (22.05.2008) 全文	1-15

☐ 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
09.3 月 2012 (09.03.2012)

国际检索报告邮寄日期
22.3 月 2012 (22.03.2012)

ISA/CN 的名称和邮寄地址:
中华人民共和国国家知识产权局
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

毛韵楠
电话号码: (86-10) **62412004**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2011/083807

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101729857A	09.06.2010	WO2011063731A1	03.06.2011
CN101977235A	16.02.2011	无	
CN101159000A	09.04.2008	CN100527147C	12.08.2009
CN101132404A	27.02.2008	无	
US2008119177 A1	22.05.2008	无	