



(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/CN2014/080304

(22) International Filing Date:
19 June 2014 (19.06.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310330142.X 31 July 2013 (31.07.2013) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 815000 (CN).

(72) Inventors: **YAN, Shuaishuai**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 815000 (CN). **LUO, Xijun**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 815000 (CN).

(74) Agent: **SHENPAT INTELLECTUAL PROPERTY AGENCY**; Room 1521, West Block, Guomao Building, Shenzhen, Guangdong 518014 (CN).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): 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, LT, 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.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD, DEVICE, AND SYSTEM FOR DETECTING LINK LAYER HIJACKING, USER EQUIPMENT, AND ANALYZING SERVER

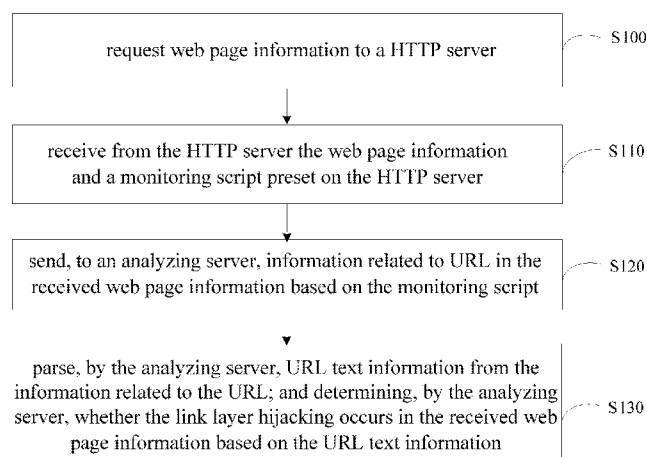


Fig. 2

(57) Abstract: A method for detecting a link layer hijacking includes: requesting web page information to a HTTP server; receiving from the HTTP server the web page information and a monitoring script preset on the HTTP server; sending information related to URL in the received web page information to an analyzing server based on the monitoring script; and parsing, by the analyzing server, URL text information from the information related to the URL and determining, by the analyzing server, whether the link layer hijacking occurs in the received web page information based on the URL text information. Thus, the precision of analysis of the link layer hijacking is improved, the number of missed link layer hijackings is reduced, and the effect for detecting the link layer hijacking is improved.

METHOD, DEVICE, AND SYSTEM FOR DETECTING LINK LAYER HIJACKING, USER EQUIPMENT, AND ANALYZING SERVER

[0001] This application claims priority to Chinese Patent Application No.201310330142.X, entitled "METHOD, DEVICE, AND SYSTEM FOR DETECTING LINK LAYER HIJACKING, USER EQUIPMENT, AND ANALYZING SERVER", filed with the Chinese Patent Office on July 31, 2013, which is incorporated by reference in its entirety herein.

FIELD

[0002] The invention relates to the field of information security technology, and in particular to a method, a device and a system for detecting a link layer hijacking, a user equipment, and an analyzing server.

BACKGROUND

[0003] Link layer hijacking refers to a means for inserting malicious codes or Uniform Resource Locators (URL) into a web page on a network transmission physical link, to steal user information. Because of a security danger of leaking user information due to the link layer hijacking, it is necessary to detect the link layer hijacking, thereby to judge whether there are malicious codes or URLs in a web page requested by a user.

[0004] An existing method for detecting a link layer hijacking in a web page includes: providing a detecting device at a bypass in the link to detect the link layer hijacking for a web page, where the detecting device is adapted to determine whether the link layer hijacking occurs in a returned page based on page information obtained and returned to a user. Fig. 1 is a diagram showing a network topology of a system for detecting a link layer hijacking in the conventional technology. Referring to Fig. 1, the procedure for detecting a link layer hijacking in the conventional technology includes: sending, by user equipment, a GET/POST request (which is a request in http protocol, where GET is configured to obtain data from a server, and POST is configured to send data to a server) to a sever; replying, by the server, response information to the user based on a type of the request; mirroring the response information by a detecting device to obtain a copy of the information replied by the server, parsing a URL from the copy, compares the parsed URL with a preset white list of URLs, and identifies a

malicious URL and a page with the link layer hijacking.

[0005] In the conventional technology, there are at least the following technique problems. The detecting device provided at the bypass additionally has a detecting effect limited by a location thereof. The closer the detecting device to the user equipment, the better the effect for detecting the link layer hijacking. However, the detecting device is generally close to a server, and it is difficult to provide the detecting device close to the user equipment. Thus, the possibility for the link layer hijacking on the transmission link between the detecting device and the user equipment is increased. Therefore, the precision for detecting the link layer hijacking is lowered. In addition, the link layer hijacking may be missed, so that the effect for detecting the link layer hijacking is lowered.

SUMMARY

[0006] In view of the above, a method for detecting a link layer hijacking, a device for detecting a link layer hijacking, a user equipment, an analyzing server and a system for detecting a link layer hijacking are provided according to embodiments of the invention, to resolve the problems in the conventional technology that the effect for detecting the link layer hijacking is affected by the location of the detecting device provided additionally, and thus the precision of an analysis of the link layer hijacking is lowered; and the effect for detecting the link layer hijacking is lowered because the link layer hijacking may be missed.

[0007] In order to achieve the above objects, a technique solution is provided as follows according to the embodiments of the invention.

[0008] A method for detecting a link layer hijacking is provided, which is applied to user equipment and includes:

requesting web page information to a Hypertext Transfer Protocol (HTTP) server;

receiving from the HTTP server the web page information and a monitoring script preset on the HTTP server;

sending, to an analyzing server, information related to Uniform Resource Locator (URL) in the received web page information based on the monitoring script; and

parsing, by the analyzing server, URL text information from the information related

to the URL; and determining, by the analyzing server, whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0009] The information related to the URL may include text information in the received web page information, and/or Java script information obtained from the received web page information.

[0010] The parsing, by the analyzing server, URL text information from the information related to the URL may include:

extracting, by the analyzing server, the URL text information from the text information based on a URL key word, in the case that the information related to the URL includes the text information in the received web page information; and

extracting, by the analyzing server, the URL text information nested in the Java script information by using a preset Java script monitoring engine, in the case that the information related to the URL includes the Java script information obtained from the received web page information.

[0011] According to an embodiment of the invention, a method for detecting a link layer hijacking is further provided, which is applied to an analyzing server and includes:

receiving information related to Uniform Resource Locator (URL) in web page information after user equipment receives from a Hypertext Transfer Protocol (HTTP) server the web page information and the monitoring script preset on the HTTP server, where the information related to the URL is sent by the user equipment based on a monitoring script;

parsing URL text information from the information related to the URL; and

determining whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0012] The information related to the URL may include text information in the received web page information, and/or Java script information obtained from the received web page information.

[0013] The parsing URL text information from the information related to the URL may include:

extracting the URL text information from the text information based on a URL key

word, in the case that the information related to the URL includes the text information in the received web page information; and

extracting the URL text information nested in the Java script information by a preset Java script monitoring engine, in the case that the information related to the URL includes the Java script information obtained from the received web page information.

[0014] The determining whether the link layer hijacking occurs in the received web page information based on the URL text information includes:

judging whether a URL corresponding to the URL text information matches a URL in a URL white list; and

determining that the link layer hijacking occurs in the received web page information, in the case that the URL corresponding to the URL text information does not match any URL in the URL white list.

[0015] The method further includes: judging whether the URL corresponding to the URL text information matches a URL in a malicious URL database after determining that the link layer hijacking occurs in the received web page information;

determining that the link layer hijacking in the received web page information is a malicious hijacking, in the case that the URL corresponding to the URL text information matches a URL in the malicious URL database; and

determining that the link layer hijacking in the received web page information is a non-malicious hijacking, in the case that the URL corresponding to the URL text information does not match any URL in the malicious URL database.

[0016] The method further includes: after determining that the link layer hijacking occurs in the received web page information, determining a source of the link layer hijacking based on a user's IP and a service identifier.

[0017] The method further includes:

outputting first warning information to the user equipment based on region information of the user's IP and region information of Internet Server Provider (ISP), after determining that the link layer hijacking occurs in the received web page information; or

outputting second warning information to the HTTP server corresponding to a web

page, in the case that times the web page is hijacked exceeds a threshold.

[0018] According to an embodiment of the invention, a device for detecting a link layer hijacking is further provided, which is applied to user equipment and includes:

5 a requesting module configured to request web page information to a Hypertext Transfer Protocol (HTTP) server;

a first receiving module configured to receive from the HTTP server the web page information and a monitoring script preset on the HTTP server that are returned; and

10 a sending module configured to send to an analyzing server information related to Uniform Resource Locator (URL) in the received web page information based on the monitoring script, wherein the analyzing server parses URL text information from the information related to the URL and determines whether the link layer hijacking occurs in the received web page information based on the URL text information.

15 **[0019]** The information related to the URL may include text information in the received web page information, and/or Java script information obtained from the received web page information.

[0020] According to an embodiment of the invention, a user equipment is further provided, which includes the above device for detecting the link layer hijacking.

[0021] According to an embodiment of the invention, a device for detecting a link layer hijacking is further provided, which is applied to an analyzing server and includes:

20 a second receiving module configured to receive information related to Uniform Resource Locator (URL) in web page information, after user equipment receives from a Hypertext Transfer Protocol (HTTP) server the web page information and the monitoring script preset on the HTTP server, wherein the information related to the URL is sent by the user equipment based on a monitoring script;

25 a parsing module configured to parse URL text information from the information related to the URL; and

an identifying module configured to determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0022] The information related to the URL may include text information in the received

web page information, and/or Java script information obtained from the received web page information.

[0023] The parsing module may include:

5 a first parsing unit configured to extract the URL text information from the text information based on a URL key word, in the case that the information related to the URL includes the text information in the received web page information; and

10 a second parsing unit configured to extract the URL text information nested in the Java script information by a preset Java script monitoring engine, in the case that the information related to the URL includes the Java script information obtained from the received web page information.

[0024] According to an embodiment of the invention, an analyzing server is further provided, which includes the above device for detecting the link layer hijacking.

15 **[0025]** According to an embodiment of the invention, a system for detecting a link layer hijacking is further provided, which includes a Hypertext Transfer Protocol (HTTP) server, user equipment and an analyzing server,

the HTTP server is configured to preset a monitoring script, and reply web page information and the monitoring script to the user equipment in response to the request of the user equipment for the web page information;

20 the user equipment is configured to request the web page information to the HTTP server, receive from the HTTP server the web page information and the monitoring script, and send to the analyzing server information related to Uniform Resource Locator (URL) in the received web page information based on the monitoring script; and

25 the analyzing server is configured to parse URL text information from the information related to the URL and determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0026] In the method for detecting the link layer hijacking according to the embodiments of the invention, user equipment requests web page information to an HTTP server, receives from the HTTP server the web page information and a monitoring script preset on the HTTP server, and sends to an analyzing server information related to URL in the received web page information based on the monitoring script; the analyzing server parses URL text information

30

from the information related to the URL, and determines whether the link layer hijacking occurs in the received web page information based on the URL text information. Thus, in the embodiment, the detection of the link layer hijacking does not depend on a detecting device provided at a bypass additionally, thus the detection effect is not affected by the location of the detecting device provided at the bypass additionally. In the embodiments, the analyzing server is configured to determine a state of the link layer hijacking by analyzing the URL text information, i.e., the URL text information in the web page information received by the user equipment. In this way, the precision of the analysis of the link layer hijacking is improved, the number of missed link layer hijackings is reduced, and the effect for detecting the link layer hijacking is improved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] The accompanying drawings applied to the description of the embodiments or the existing technologies will be described briefly as follows, to clarify the technical solutions according to the embodiments of the invention or the existing technologies. It is obvious that the accompanying drawings in the following description are only some embodiments of the invention. For those skilled in the art, other accompanying drawings may be obtained according to these accompanying drawings without any creative work.

[0028] Fig. 1 is a diagram showing a network topology of a system for detecting a link layer hijacking in the conventional technology;

[0029] Fig. 2 is a flowchart of a method for detecting a link layer hijacking according to an embodiment of the invention;

[0030] Fig. 3 is another flowchart of a method for detecting a link layer hijacking according to an embodiment of the invention;

[0031] Fig. 4 is a flowchart of a method for determining a link layer hijacking in received web page information according to an embodiment of the invention;

[0032] Fig. 5 is a flowchart of a method for determining a malicious hijacking according to an embodiment of the invention;

[0033] Fig. 6 is yet another flowchart of a method for detecting a link layer hijacking according to an embodiment of the invention;

[0034] Fig. 7 is a block diagram showing a structure of a device for detecting a link layer hijacking according to an embodiment of the invention;

[0035] Fig. 8 is a block diagram showing another structure of a device for detecting a link layer hijacking according to an embodiment of the invention;

5 [0036] Fig. 9 is a block diagram showing a structure of a parsing module according to an embodiment of the invention;

[0037] Fig. 10 is a block diagram showing a structure of an identifying module according to an embodiment of the invention;

10 [0038] Fig. 11 is a block diagram showing another structure of a device for detecting a link layer hijacking according to an embodiment of the invention;

[0039] Fig. 12 is a block diagram of yet another structure of a device for detecting a link layer hijacking according to an embodiment of the invention;

[0040] Fig. 13 is a block diagram showing a structure of a system for detecting a link layer hijacking according to an embodiment of the invention;

15 [0041] Fig. 14 is a diagram showing a hardware structure of user equipment according to an embodiment of the invention; and

[0042] Fig. 15 is a diagram showing a hardware structure of an analyzing server according to an embodiment of the invention.

20 DETAILED DESCRIPTION OF EMBODIMENTS

[0043] In order to make the object, technical solution and advantage according to the embodiments of the invention more clear, the technical solution according to the embodiments of the invention will be described clearly and completely as follows in conjunction with the accompanying drawings in the embodiments of the invention. It is
25 obvious that the described embodiments are only a part of the embodiments according to the invention. All the other embodiments obtained by those skilled in the art based on the embodiments in the invention without any creative work belong to the scope of the invention.

[0044] Fig. 2 is a flowchart of a method for detecting a link layer hijacking according to an embodiment of the invention. The method is applied to user equipment, which is performed at

a user side. Referring to Fig. 2, the method may include steps S100 to S130 as follows.

[0045] Step S100 includes: requesting web page information to a Hypertext Transfer Protocol (HTTP) server.

[0046] The user equipment may send a GET/POST request to the HTTP server, to obtain
5 the requested web page information from the HTTP server.

[0047] Step S110 includes: receiving from the HTTP server the web page information and a monitoring script preset on the HTTP server.

[0048] The monitoring script may be a monitoring script in JavaScript (JS). JavaScript is a
10 prototype-based and object-oriented case sensitive client-side script language with dynamic
typing and developed from LiveScript of Netscape.

[0049] In an embodiment, the JS monitoring script may be preset on an HTTP server to be
monitored. The JS monitoring script may be downloaded to the user equipment when the
HTTP server replies the web page information to the user equipment. For example, if a web
site www.qq.com needs to be monitored to detect a link layer hijacking in an embodiment, an
15 HTTP server corresponding to the web set www.qq.com is preset with a JS script. When the
user equipment requests a web page information of the web site www.qq.com to the HTTP
server corresponding to the web set www.qq.com, the HTTP server replies the web page
information of the web site www.qq.com as well as the JS preset script to the user equipment.

[0050] Step S120 includes: sending, to an analyzing server, information related to Uniform
20 Resource Locator (URL) in the received web page information to an analyzing server based
on the monitoring script.

[0051] Step S130 includes: parsing, by the analyzing server, URL text information from the
information related to the URL; and determining, by the analyzing server, whether the link
layer hijacking occurs in the received web page information based on the URL text
25 information.

[0052] After receiving the web page information and the JS monitoring script, the user
equipment is not able to determine whether the link layer hijacking occurs in the received web
page information or whether malicious codes and URLs are inserted in the received web page
information. The user equipment sends, to the analyzing server at a network side, information
30 related to the URL in the received web page information based on the received monitoring

script. The analyzing server parses URL text information from the information related to the URL after receiving the information related to the URL; and identifies a state of the link layer hijacking of the received web page information based on the URL text information. Here, the state of the link layer hijacking means that the link layer hijacking does or does not occur in the received web page information.

[0053] It needs to be noted that the monitoring script is set on the HTTP server corresponding to the site to be monitored in the embodiment. Thus, the monitoring script will be provided to the user equipment together with the web page information, only when the user equipment requests the web page information to the HTTP server. After receiving the monitoring script, the user equipment may know that the web site corresponding to the requested web page information needs to be monitored, and may send information related to the URL in the received web page information to the analyzing server based on the monitoring script. The analyzing server determines whether the link layer hijacking occurs in the received web page information. In the embodiment, the monitoring script is mainly configured to trigger the user equipment to report to the analyzing server the information related to the URL in the received web page information.

[0054] In the method for detecting the link layer hijacking according to the embodiment, the user equipment requests the web page information to an HTTP server, receives from the HTTP server the web page information and the monitoring script preset on the HTTP server, and sends the information related to the URL in the received web page information to an analyzing server based on the monitoring script. The analyzing server parses URL text information from the information related to the URL, and determines whether the link layer hijacking occurs in the received web page information based on the URL text information. In the embodiment, the detection of the link layer hijacking does not depend on a detecting device provided at a bypass additionally, thus the detection effect is not affected by the location of the detecting device provided at the bypass additionally. In the embodiments, the analyzing server is configured to determine a state of the link layer hijacking by analyzing the URL text information, i.e., is the URL text information in the web page information received by the user equipment. In this way, the precision of the analysis of the link layer hijacking is improved, the number of missed link layer hijacks is reduced, and the effect for detecting the link layer hijacking is improved.

[0055] Optionally, the information related to the URL may include text information in the received web page information, and/or JS information obtained from the received web page information.

[0056] The URL text information refers to a file for indicating URL carried in the web page information. Thus, the state of the link layer hijacking of the received web page information may be identified based on the URL text information. The URL mainly includes: URL in text-type (mainly for static web page) and URL packed by JS arithmetic, i.e., URL nested by a dynamic JS arithmetic (mainly for dynamic web page). The user equipment may send the information related to the URL to the analyzing server by three ways. In the first way, the user equipment may send text information in the received web page information to the analyzing server. In the second way, the user equipment may send JS information obtained from the received web page information to the analyzing server. In the third way, the user equipment may send to the analyzing server both the text information in the received web page information and the JS information obtained from the received web page information.

[0057] In the case that the user equipment send the text information in the received web page information to the analyzing server, the analyzing server may extract URL text information from the text information based on a URL key word. The URL key word mainly includes some key words related to the URL, such as frame, iframe, script, and form.

[0058] In the case that the user equipment sends the JS information obtained from the received web page information to the analyzing server, the analyzing server may extract the nested URL text information from the JS information by a preset JS monitoring engine. The preset JS monitoring engine may be spidermonkey engine.

[0059] A method for detecting a link layer hijacking according to an embodiment will be described below with respect to an analyzing server. The method to be described below corresponds to the method described with respect to the user equipment, which may be referred to the method with respect to the user equipment.

[0060] Fig. 3 is another flowchart of a method for detecting a link layer hijacking according to an embodiment of the invention. The method is applied to an analyzing server. The analyzing server is a server provided at the network side and configured to process data and logic operations. A data communication is provided between the analyzing server and the user equipment. Referring to Fig. 3, the method may include steps S200 to S220.

[0061] Step S200 may include: receiving information related to URL in web page information, where the information related to the URL is sent by user equipment based on a monitoring script, after the user equipment receives from a HTTP server the web page information and the monitoring script preset on the HTTP server.

5 **[0062]** Step S210 may include: parsing URL text information from the information related to the URL.

[0063] Step S220 may include: determining whether the link layer hijacking occurs in the received web page information based on the URL text information.

10 **[0064]** In the method for detecting the link layer hijacking according to the embodiment, the detection of a link layer hijacking does not depend on a detecting device provided at a bypass additionally, thus the detection effect is not affected by the location of the detecting device provided at the bypass additionally. In the embodiments, the analyzing server is configured to determine a state of the link layer hijacking by analyzing the URL text information, i.e., the URL text information in the web page information received by the user
15 equipment. In this way, the precision of the analysis of the link layer hijacking is improved, the number of missed link layer hijackings is reduced, and the effect for detecting the link layer hijacking is improved.

[0065] Optionally, the information related to the URL may include text information in the received web page information, and/or JS information obtained from the received web page
20 information.

[0066] In the case that the information related to the URL includes the text information, the analyzing server may extract the URL text information from the text information based on a URL key word. The URL key word may includes some key words related to the URL, such as frame, iframe, script, and form.

25 **[0067]** In the case that the information related to the URL includes the JS information, the analyzing server may extract the URL text information nested into the JS information by a preset JS monitoring engine. The preset JS monitoring engine may be spidermonkey engine.

[0068] In the embodiment, the URL text information of both static web page and dynamic web page may be extracted. Therefore, the method for detecting the link layer hijacking may
30 be applied to more types of web page, the number of missed link layer hijackings is reduced,

and the effect for detecting the link layer hijacking is improved.

[0069] Fig. 4 is a flowchart of a method for determining a link layer hijacking in received web page information. The method may include steps S221 to S223.

[0070] Step S221 may include: judging whether a URL corresponding to the URL text
5 information matches a URL in a URL white list; if the URL corresponding to the URL text information matches the URL in the URL white list, performing step S222; otherwise, performing step S223.

[0071] Step S222 may include: determining that no link layer hijacking occurs in the received web page information.

10 **[0072]** Step S223 may include: determining that a link layer hijacking occurs in the received web page information.

[0073] The method shown in Fig. 4 may be considered as an optional implementation for the step S220 in Fig. 3.

[0074] The link layer hijacking includes non-malicious hijacking and malicious hijacking.
15 The non-malicious hijacking refers to some action with a low risk, such as an insertion of an advertisement page. The malicious hijacking includes some action such as an insertion of a code or a URL for stealing user's identity information. Therefore, in the embodiment, after determining the link layer hijacking in the web page information received by the user equipment, the method further includes: judging whether the link layer hijacking is a
20 malicious hijacking. Referring to Fig. 5, the method for determining the malicious hijacking according to an embodiment includes steps S300 to S320.

[0075] Step S300 may include: judging whether the URL corresponding to the URL text information matches a URL in a malicious URL database; if the URL corresponding to the URL text information matches the URL in the malicious URL database, performing step S310;
25 otherwise, performing step S320.

[0076] Step S310 may include: determining that the link layer hijacking in the received web page information is a malicious hijacking.

[0077] Step S223 may include: determining that the link layer hijacking in the received web page information is a non-malicious hijacking.

[0078] Optionally, after determining the link layer hijacking in the received web page information, the method includes: determining a source of the link layer hijacking, to make a statistic of the sources of link layer hijackings. In a particular implementation, the source of a link layer hijacking may be determined based on a user's Internet Protocol (IP) and a service identifier.

[0079] Optionally, the analyzing server may further output warning information after determining that the link layer hijacking in the web page information received by the user equipment. The warning information may be output to either the user equipment or the HTTP server corresponding to the site expected to be monitored. The step of outputting the warning to the user equipment may include: outputting first warning information to the user equipment based on region information of the user's IP and region information of Internet Server Provider (ISP). In an embodiment, the first warning information may be grouped based on the region information of IP region and the region information of ISP for output. The step of outputting the warning to the http server may include: outputting second warning information to the HTTP server corresponding to the web page, in the case that times the web page suffers from the link layer hijacking exceeds a threshold. For example, if the analyzing server finds that the times the web page www.qq.com suffers from the link layer hijacking exceeds a threshold, the analyzing server sends the second warning information to the HTTP server corresponding to www.qq.com, to alter web site operators.

[0080] A method for detecting a link layer hijacking is provided below. Fig. 6 is yet another flowchart of a method for detecting a link layer hijacking according to an embodiment of the invention. Referring to Fig. 6, the method may include steps S400 to S500.

[0081] Step S400 may include: receiving information related to URL in web page information, where the information related to the URL is sent by user equipment based on a monitoring script, after the user equipment receives from a HTTP server the web page information and the monitoring script preset on the HTTP server.

[0082] Step S410 may include: determining a type of the information related to the URL.

[0083] Step S420 may include: extracting URL text information from text information based on a URL key word, in the case that the information related to the URL includes the text information in the received web page information.

[0084] Step S430 may include: extracting URL text information nested in JS information by a preset JS monitoring engine, in the case that the information related to the URL includes the JS information obtained from the received web page information.

[0085] It should be noted that steps S420 and S430 are different processes for different types of information related to the URL after step S410.

[0086] Step S440 may include: judging whether the URL corresponding to the URL text information matches a URL in a URL white list; if the URL corresponding to the URL text information matches the URL in the URL white list, performing step S450; otherwise, performing step S465.

[0087] Step S450 may include: determining that no link layer hijacking occurs in the received web page information, and ending the process.

[0088] Step S460 may include: determining that the link layer hijacking occurs in the received web page information; judging whether the URL corresponding to the URL text information matches a URL in a malicious URL database, if the URL corresponding to the URL text information does not match any URLs in the malicious URL database, performing step S470; otherwise, performing step S480.

[0089] Step S470 may include: determining that the link layer hijacking in the received web page information is a non-malicious hijack.

[0090] Step S480 may include: determining that the link layer hijacking in the received web page information is a malicious hijack.

[0091] Step S490 may include: determining a source of the link layer hijacking based on a user's IP and a service identifier.

[0092] Step S500 may include: outputting first warning information to the user equipment based on region information of the user's IP and region information of Internet Server Provider (ISP), and/or outputting second warning information to the HTTP server corresponding to a web page when the times the web page is hijacked exceeds a threshold.

[0093] A device for detecting a link layer hijacking according to an embodiment of the invention is described below with respect to user equipment. The device for detecting the link layer hijacking described below corresponds to the method for detecting the link layer hijacking described above with respect to user equipment, which may be referred to the

method for detecting the link layer hijacking with respect to user equipment.

[0094] Fig. 7 is a block diagram showing a structure of a device for detecting a link layer hijacking according to the embodiment. Referring to Fig. 7, the device may include: a requesting module 100, a first receiving module 110 and a sending module 120.

5 **[0095]** The requesting module 100 is configured to request web page information to an HTTP server.

[0096] The first receiving module 110 is configured to receive from the HTTP server the web page information and a monitoring script preset on the HTTP server.

10 **[0097]** The sending module 120 is configured to send to an analyzing server information related to URL in the received web page information based on the monitoring script, where the analyzing server parses URL text information from the information related to the URL and determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

15 **[0098]** With the device for detecting the link layer hijacking according to the embodiment, the detection of the link layer hijacking does not depend on a detecting device provided at a bypass additionally, thus the detection effect is not affected by the location of the detecting device provided at the bypass additionally. In the embodiments, the analyzing server is configured to determine a state of the link layer hijacking by analyzing the URL text information, i.e., the URL text information in the web page information received by the user
20 equipment. In this way, the precision of the analysis of the link layer hijacking is improved, the number of missed link layer hijackings is reduced, and the effect for detecting the link layer hijacking is improved.

[0099] Optionally, the information related to the URL may include text information in the received web page information, and/or JS information obtained from the received web page
25 information.

[0100] According to an embodiment of the invention, user equipment is further provided, which includes the device for detecting the link layer hijacking described above with respect to the user equipment.

30 **[0101]** A device for detecting a link layer hijacking according to an embodiment of the invention is described below with respect to an analyzing server. The device for detecting the

link layer hijacking described below corresponds to the method for detecting the link layer hijacking described above with respect to the analyzing server, which may be referred to the method for detecting the link layer hijacking with respect to the analyzing server.

[0102] Fig. 8 is a block diagram showing another structure of a device for detecting a link layer hijacking according to the embodiment. The device for detecting the link layer hijacking is applied to an analyzing server. Referring to Fig. 8, the device may include: a second receiving module 200, a parsing module 210, and an identifying module 220.

[0103] The second receiving module 200 is configured to receive information related to URL in web page information, where the information related to the URL is sent by user equipment based on a monitoring script, after the user equipment receives from a HTTP server the web page information and the monitoring script preset on the HTTP server.

[0104] The parsing module 210 is configured to parse URL text information from the information related to the URL.

[0105] The identifying module 220 is configured to determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0106] In the embodiment, the analyzing server is configured to analyze the URL text information, i.e., the URL text information in the web page information received by the user equipment, to determine a state of the link layer hijacking. In this way, the precision of an analysis of the link layer hijacking is improved, the number of missed link layer hijackings is reduced, and the effect for detecting the link layer hijacking is improved.

[0107] Optionally, the information related to the URL may include text information in the received web page information, and/or JS information obtained from the received web page information. Correspondingly, the parsing module 210 may have a structure shown in Fig. 9. Referring to Fig. 9, the parsing module 210 may include: a first parsing unit 211 and a second parsing unit 212.

[0108] The first parsing unit 211 is configured to extract URL text information from the information related to the URL based on a URL key word, in the case that the information related to the URL includes the text information in the received web page information.

[0109] The second parsing unit 212 is configured to extract URL text information nested in JS information by a preset JS monitoring engine, in the case that the information related to the

URL includes the JS information obtained from the received web page information.

[0110] Fig. 10 is a block diagram showing a structure of the identifying module 220 according to an embodiment of the invention. Referring to Fig. 10, the identifying module 220 may include: a match judging unit 221, a first hijacking determining unit 222 and a second hijacking determining unit 223

[0111] The match judging unit 221 is configured to judge whether the URL corresponding to the URL text information matches a URL in a URL white list.

[0112] The first hijacking determining unit 222 is configured to determine that no link layer hijacking occurs in the received web page information, if the URL corresponding to the URL text information matches the URL in the URL white list.

[0113] The second hijacking determining unit 223 is configured to determine that the link layer hijacking occurs in the received web page information, if the URL corresponding to the URL text information does not match any URLs in the URL white list.

[0114] The device for detecting the link layer hijacking may have another structure according to an embodiment of the invention. Fig. 11 is a block diagram showing another structure of a device for detecting a link layer hijacking according to an embodiment of the invention. This device differs the device for detecting the link layer hijacking in Fig. 8 in that this device may further include: a malicious hijacking judging module 230, a first malicious hijacking determining module 240, and a second malicious hijacking determining module 250.

[0115] The malicious hijacking judging module 230 is configured to judge whether the URL corresponding to the URL text information matches a URL in a malicious URL database, after it is determined that the link layer hijacking occurs in the received web page information.

[0116] The first malicious hijacking determining module 240 is configured to determine that the link layer hijacking in the received web page information is a malicious hijack, if the URL corresponding to the URL text information matches the URL in the malicious URL database; and

[0117] The second malicious hijacking determining module 250 is configured to determine that the link layer hijacking in the received web page information is a non-malicious hijack, if the URL corresponding to the URL text information does not match any URLs in the

malicious URL database;

[0118] Fig. 12 is a block diagram showing yet another structure of a device for detecting a link layer hijacking according to an embodiment of the invention. This device differs the device for detecting the link layer hijacking in Fig. 11 in that this device may further include:
5 a hijacking source determining module 260 and a warning information sending module 270.

[0119] The hijacking source determining module 260 is configured to determine a source of the link layer hijacking based on a user's IP and a service identifier, after it is determined that the link layer hijacking occurs in the received web page information.

[0120] The warning information sending module 270 is configured to output first warning
10 information to the user equipment based on region information of the user's IP and region information of Internet Server Provider (ISP), after it is determined that a link layer hijacking occurs in the received web page information; and/or output second warning information to the HTTP server corresponding to the web page in the case that times the web page is hijacked exceeds a threshold.

15 [0121] According to an embodiment of the invention, an analyzing server is further provided, which includes the device for detecting the link layer hijacking described above with respect to an analyzing server.

[0122] A system for detecting a link layer hijacking according to an embodiment of the invention is described below. The system for detecting the link layer hijacking described
20 below corresponds to the method and device for detecting the link layer hijacking described above with respect to user equipment and an analyzing server, which may be referred to them.

[0123] Fig. 13 is a block diagram showing a structure of a system for detecting a link layer hijacking according to an embodiment of the invention. Referring to Fig. 13, the system for detecting the link layer hijacking may include an HTTP server 10, user equipment 20 and an
25 analyzing server 30.

[0124] The HTTP server 10 is configured to preset a monitoring script, and reply web page information and the monitoring script to the user equipment in response to the request of the user equipment 20 for the web page information.

[0125] The user equipment 20 is configured to request the web page information to the
30 HTTP server 10, receive from the HTTP server the web page information and the monitoring

script, and send to the analyzing server 30 information related to URL in the received web page information based on the monitoring script.

[0126] The analyzing server 30 is configured to parse URL text information from the information related to the URL and determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0127] In the system for detecting the link layer hijacking according to the embodiment, a monitoring script is preset at an HTTP server. When the user equipment requests web page information, the user equipment receives from the HTTP server the web page information and the monitoring script preset on the HTTP server, and sends information related to the URL in the received web page information to the analyzing server based on the monitoring script. The analyzing server parses URL text information from the information related to URL, and determines whether the link layer hijacking occurs in the received web page information based on the URL text information. In the embodiment, the detection of the link layer hijacking does not depend on a detecting device provided at a bypass additionally, thus the detection effect is not affected by the location of the detecting device provided at the bypass additionally. In the embodiments, the analyzing server is configured to determine a state of the link layer hijacking by analyzing the URL text information, i.e., the URL text information in the web page information received by the user equipment. In this way, the precision of the analysis of the link layer hijacking is improved, the number of missed link layer hijacks is reduced, and the effect for detecting the link layer hijacking is improved.

[0128] In the following, a hardware structure of user equipment is described according to an embodiment of the invention. Fig. 14 is a diagram showing a hardware structure of user equipment according to an embodiment of the invention. Referring to Fig. 14, the user equipment may include a communication interface 1, a memory 2, a processor 3 and a communication bus 4.

[0129] Components of the user equipment are described in detail in conjunction with Fig. 14.

[0130] A communication interface 1 may be an interface of a communication module, such as an interface of a network card, which is configured to receive and transmit signals between an access server and peripheral equipment.

[0131] A memory 2 may be configured to store software programs and modules. A processor 3 performs various function applications and data processes in the access server by running the software programs and modules stored in the memory 2. The memory 2 may mainly include a storage region for program and a storage region for data. The storage region for program may store operating system, application needed by at least one function (such as an audio playing function, a video playing function) and the like. The storage region for data may store data (such as video data, an address book) generated by using the access server and the like. Furthermore, the memory 2 may include a high speed random access memory and may further include a non-volatile storage, such as at least one of a disk storage device, a flash memory or other non-volatile solid-state storage device.

[0132] The processor 3 is a control center of the access server, which is connected to various components of the access server through various interfaces and lines. The processor 3 performs various functions and data processes by executing or running the software programs and modules stored in the memory 2 and calling the data stored in the memory 2, thereby monitoring the access server. Optionally, the process 3 may include one or more processing unit. Preferably, an application processor and a modem may be integrated into the processor 3, in which the application processor is applied to the operating system and applications, and the modem is applied to a wireless communication. It can be understood that the above modem may further not be integrated into the process 3.

[0133] The communication 1, the memory 2 and the processor 3 communicate with each other through a communication bus 4.

[0134] In an embodiment of the invention, the processor 3 may further have the following functions:

requesting web page information to a HTTP server;

receiving from the HTTP server the web page information and a monitoring script preset on the HTTP server; and

sending information related to URL in the received web page information to an analyzing server based on the monitoring script, where the analyzing server parses URL text information from the information related to the URL and determines whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0135] A hardware structure of an analyzing server will be described below according to an embodiment of the invention. Fig. 15 is a diagram showing a hardware structure of an analyzing server according to an embodiment of the invention. Referring to Fig. 15, the analyzing server may include a communication interface 1', a memory 2', a processor 3' and a communication bus 4'.

[0136] The components of the analyzing server are described in detail by referring to Fig. 15.

[0137] A communication interface 1' may be an interface of a communication module, such as an interface of a network card, which is configured to receive and transmit signals between an access server and peripheral equipment.

[0138] A memory 2' may be configured to store software programs and modules. A processor 3' performs various function applications and data processes in the access server by running the software programs and modules stored in the memory 2'. The memory 2' may mainly include a storage region for program and a storage region for data. The storage region for program may store operating system, applications needed by at least one function (such as an audio playing function, a video playing function), and the like. The storage region for data may store data (such as video data, an address book) generated by using the access server, and the like. Furthermore, the memory 2' may include a high speed random access memory and may further include a non-volatile storage, such as at least one of a disk storage device, a flash memory or other non-volatile solid-state storage device.

[0139] The processor 3' is a control center of the access server, which is connected to various components of the access server through various interfaces and lines. The processor 3' performs various functions and data processes by executing or running the software programs and modules stored in the memory 2' and calling the data stored in the memory 2', thereby monitoring the access server. Optionally, the process 3' may include one or more processing unit. Preferably, an application processor and a modem may be integrated into the processor 3, in which the application processor is applied to the operating system and applications, and the modem is applied to a wireless communication. It can be understood that the above modem may further not be integrated into the process 3'.

[0140] The communication 1', the memory 2' and the processor 3' communicate with each other through a communication bus 4'.

[0141] In an embodiment of the invention, the processor 3 may further have the following functions:

receiving information related to URL in web page information, where the information related to the URL is sent by user equipment based on a monitoring script, after the user equipment receives from a HTTP server the web page information and the monitoring script preset on the HTTP server;

parsing URL text information from the information related to the URL; and

determining whether the link layer hijacking occurs in the received web page information based on the URL text information.

[0142] The embodiments of the invention are described herein in a progressive manner, with an emphasis placed on explaining the difference between each embodiment and the other embodiments; hence, for the same or similar parts among the embodiments, they can be referred to from one another. For the device and system disclosed in the embodiments, the corresponding descriptions are relatively simple because the device and system correspond to the methods disclosed in the embodiments. The relevant portions may be referred to the description for the method parts.

[0143] Those skilled in the art can further understand that the individual exemplary units and steps that are described in conjunction with the embodiment disclosed herein are able to be implemented in the electronic hardware, the computer software or a combination of both the electronic hardware and the computer software, and the components and the steps of the individual examples have been described according to the function generally in the above description, for describing the interchangeability between the hardware and the software clearly. Whether these functions are implemented in hardware or software is determined by the technical solution-specific application and the design constraint condition. For each specific application, the described function can be implemented by those skilled in the art using different method, but this implementation should not be considered as beyond the scope of the invention.

[0144] The steps of the method or the algorithm that are described in conjunction with the embodiment disclosed herein can be implemented by the hardware, the software module performed by the processor or the combination of both the hardware and the software module

performed by the processor. The software module can be built in the Random Access Memory (RAM), the memory, the Read-Only Memory (ROM), the electrically programmable ROM, the electrically erasable programmable ROM, the register, the hardware, the movable disc, the CD-ROM, or any other forms of storing medium that is well-known in the technical field.

- 5 **[0145]** The description of the embodiments herein enables those skilled in the art to implement or use the present invention. Numerous modifications to the embodiments will be apparent to those skilled in the art, and the general principle herein can be implemented in other embodiments without deviation from the spirit or scope of the invention. Therefore, the invention will not be limited to the embodiments described herein, but in accordance with the
- 10 widest scope consistent with the principle and novel features disclosed herein.

CLAIMS

1. A method for detecting a link layer hijacking, applied to user equipment, wherein the method comprises:

5 requesting web page information to a Hypertext Transfer Protocol (HTTP) server;

 receiving from the HTTP server the web page information and a monitoring script preset on the HTTP server;

 sending, to an analyzing server, information related to Uniform Resource Locator (URL) in the received web page information based on the monitoring script; and

10 parsing, by the analyzing server, URL text information from the information related to the URL, and determining, by the analyzing server, whether the link layer hijacking occurs in the received web page information based on the URL text information.

 2. The method according to claim 1, wherein the information related to the URL comprises text information in the received web page information, and/or Java script
15 information obtained from the received web page information.

 3. The method according to claim 2, wherein the step of parsing, by the analyzing server, URL text information from the information related to the URL comprises:

 extracting, by the analyzing server, the URL text information from the text information based on a URL key word, in the case that the information related to the URL comprises the
20 text information in the received web page information; and

 extracting, by the analyzing server, the URL text information nested in the Java script information by using a preset Java script monitoring engine, in the case that the information related to the URL comprises the Java script information obtained from the received web page information.

25 4. A method for detecting a link layer hijacking, applied to an analyzing server, wherein the method comprises:

 receiving information related to Uniform Resource Locator (URL) in web page information after user equipment receives the web page information and the monitoring script preset on a Hypertext Transfer Protocol (HTTP) server, wherein the information related to the

URL is sent by the user equipment based on a monitoring script;

parsing URL text information from the information related to the URL; and

determining whether the link layer hijacking occurs in the received web page information based on the URL text information.

5 5. The method according to claim 4, wherein the information related to the URL comprises text information in the received web page information, and/or Java script information obtained from the received web page information.

6. The method according to claim 5, wherein the parsing URL text information from the information related to the URL comprises:

10 extracting the URL text information from the text information based on a URL key word, in the case that the information related to the URL comprises the text information in the received web page information; and

extracting the URL text information nested in the Java script information by a preset Java script monitoring engine, in the case that the information related to the URL comprises the
15 Java script information obtained from the received web page information.

7. The method according to claim 6, wherein the determining whether the link layer hijacking occurs in the received web page information based on the URL text information comprises:

judging whether a URL corresponding to the URL text information matches a URL in a
20 URL white list; and

determining that the link layer hijacking occurs in the received web page information, in the case that the URL corresponding to the URL text information does not match any URLs in the URL white list.

8. The method according to claim 7, further comprising:

25 judging whether the URL corresponding to the URL text information matches a URL in a malicious URL database after determining that the link layer hijacking occurs in the received web page information;

determining that the link layer hijacking in the received web page information is a malicious hijack, in the case that the URL corresponding to the URL text information matches

a URL in the malicious URL database; and

determining that the link layer hijacking in the received web page information is a non-malicious hijack, in the case that the URL corresponding to the URL text information does not match any URLs in the malicious URL database.

5 9. The method according to claim 7, further comprising:

determining a source of the link layer hijacking based on a user's IP and a service identifier, after determining that the link layer hijacking occurs in the received web page information.

10. The method according to any one of claims 7 to 9, further comprising:

10 outputting first warning information to the user equipment based on region information of the user's IP and region information of Internet Server Provider (ISP) after determining that the link layer hijacking occurs in the received web page information; or

outputting second warning information to the HTTP server corresponding to the web page, in the case that times the web page is hijacked exceeds a threshold.

15 11. A device for detecting a link layer hijacking, applied to user equipment, wherein the device comprises:

a requesting module configured to request web page information to a Hypertext Transfer Protocol (HTTP) server;

20 a first receiving module configured to receive from the HTTP server the web page information and a monitoring script preset on the HTTP server; and

a sending module configured to send to an analyzing server information related to Uniform Resource Locator (URL) in the received web page information based on the monitoring script, wherein the analyzing server parses URL text information from the information related to the URL and determines whether the link layer hijacking occurs in the
25 received web page information based on the URL text information.

12. The device according to claim 11, wherein the information related to the URL comprises text information in the received web page information, and/or Java script information obtained from the received web page information.

13. A user equipment, comprising the device for detecting the link layer hijacking

according to claim 11 or 12.

14. A device for detecting a link layer hijack, applied to an analyzing server, wherein the device comprises:

5 a second receiving module configured to receive information related to Uniform Resource Locator (URL) in web page information, after user equipment receives from a Hypertext Transfer Protocol (HTTP) server the web page information and the monitoring script preset on the HTTP server, wherein the information related to the URL is sent by the user equipment based on a monitoring script;

10 a parsing module configured to parse URL text information from the information related to the URL; and

an identifying module configured to determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

15 15. The device according to claim 14, wherein the information related to the URL comprises text information in the received web page information, and/or Java script information obtained from the received web page information.

16. The device according to claim 15, wherein the parsing module comprises:

a first parsing unit configured to extract the URL text information from the text information based on a URL key word, in the case that the information related to the URL comprises the text information in the received web page information; and

20 a second parsing unit configured to extract the URL text information nested in the Java script information by a preset Java script monitoring engine, in the case that the information related to the URL comprises the Java script information obtained from the received web page information.

25 17. An analyzing server, comprising the device for detecting the link layer hijacking according to any one of claims 14 to 16.

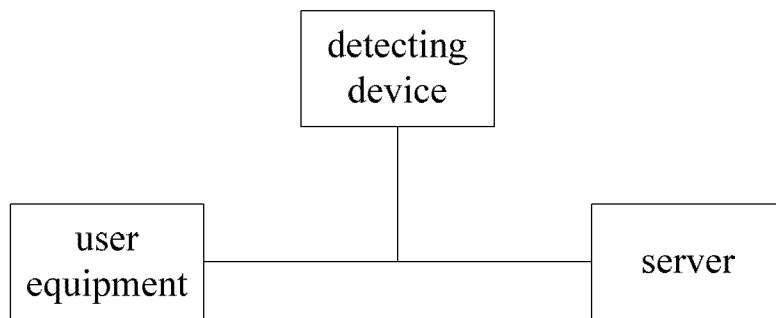
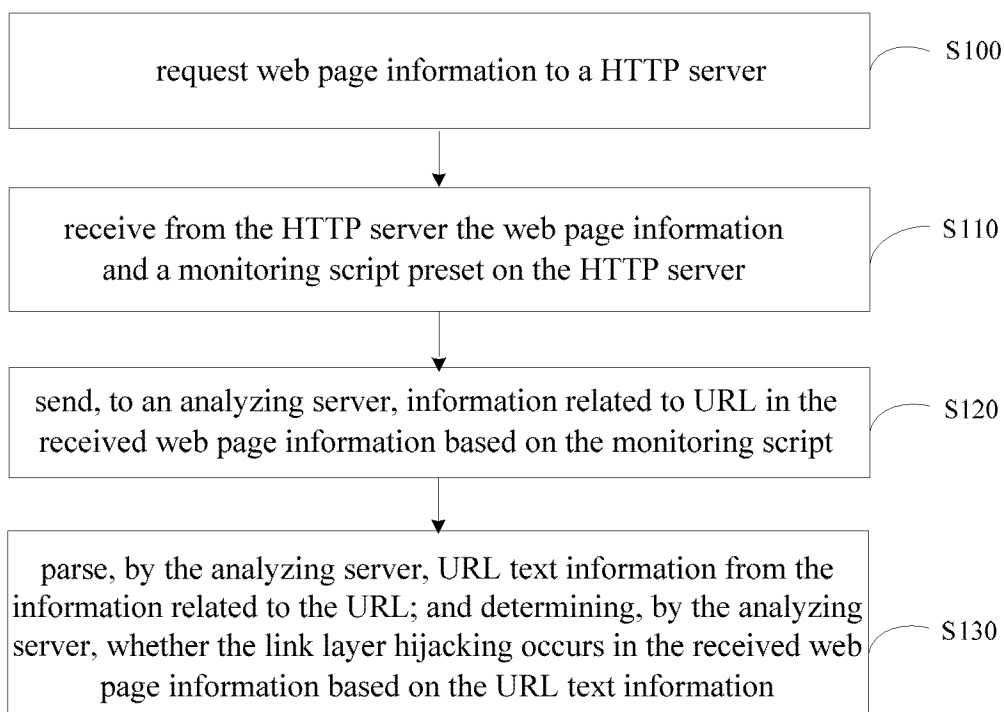
18. A system for detecting a link layer hijacking, comprising a Hypertext Transfer Protocol (HTTP) server, user equipment and an analyzing server, wherein

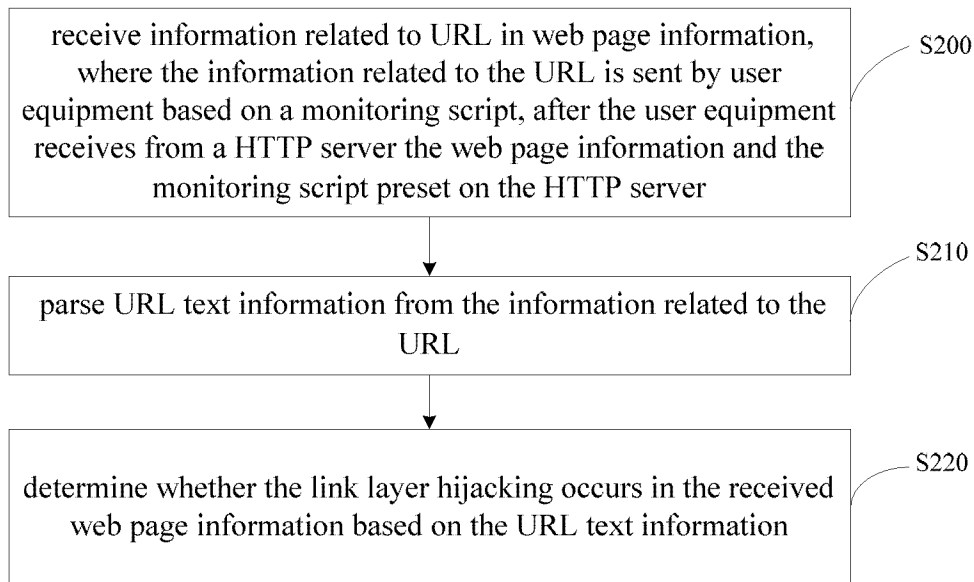
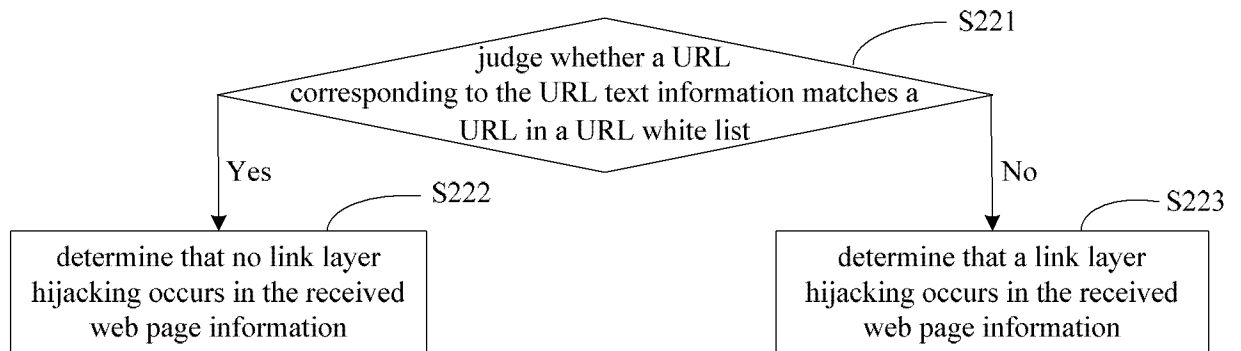
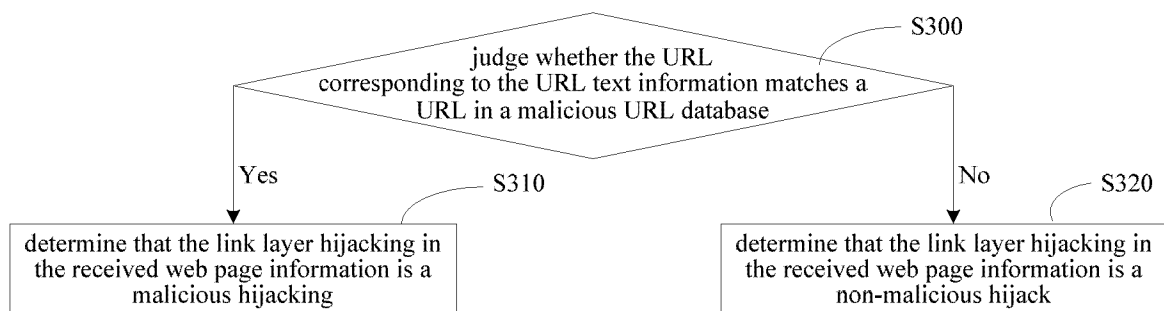
the HTTP server is configured to preset a monitoring script, and reply web page information and the monitoring script to the user equipment in response to the request of the

user equipment for the web page information;

the user equipment is configured to request the web page information to the HTTP server, receive from the HTTP server the web page information and the monitoring script, and send to the analyzing server information related to Uniform Resource Locator (URL) in the
5 received web page information based on the monitoring script; and

the analyzing server is configured to parse URL text information from the information related to the URL and determine whether the link layer hijacking occurs in the received web page information based on the URL text information.

**Fig. 1****Fig. 2**

**Fig. 3****Fig. 4****Fig. 5**

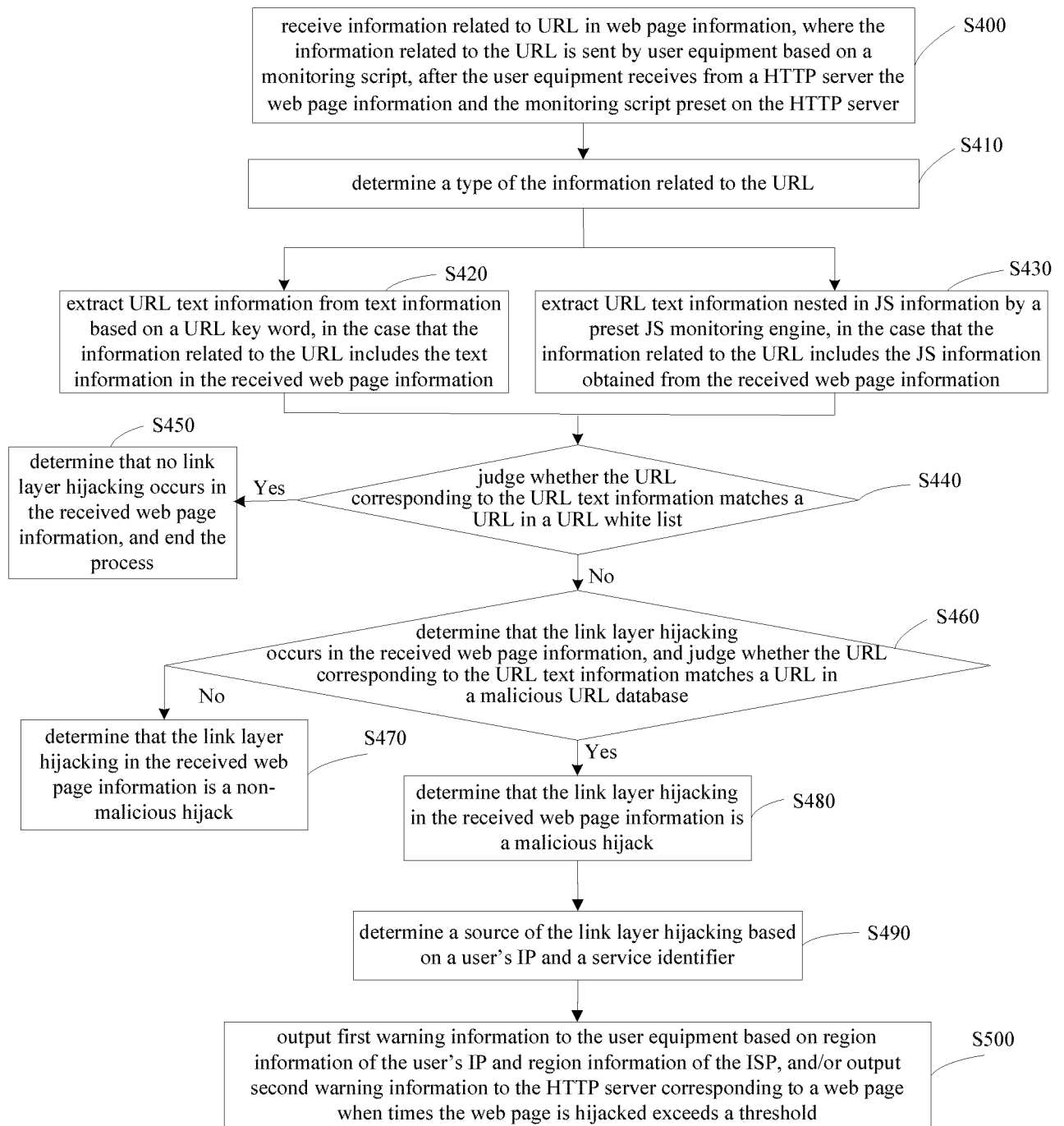
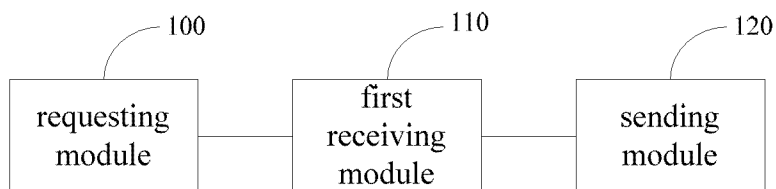
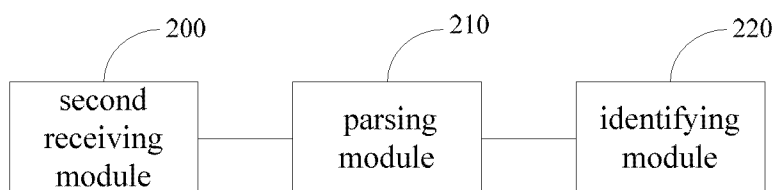
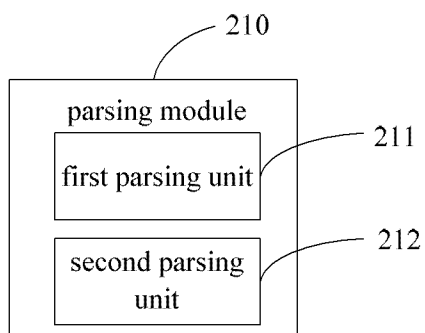
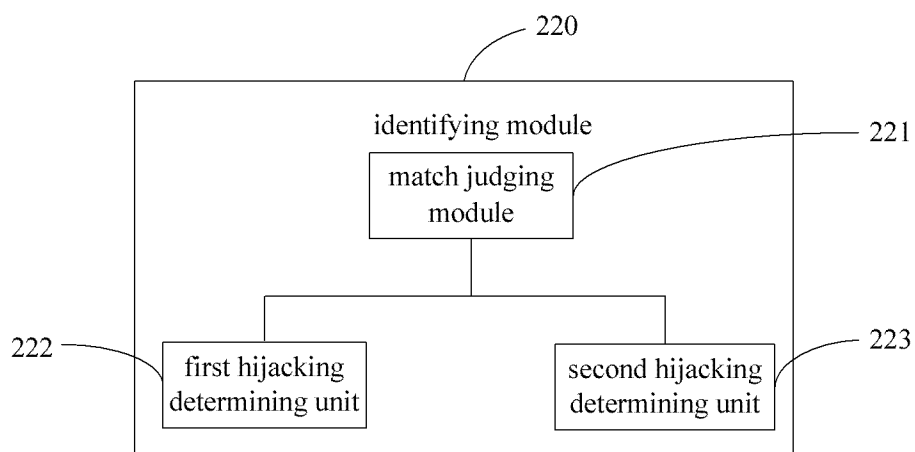
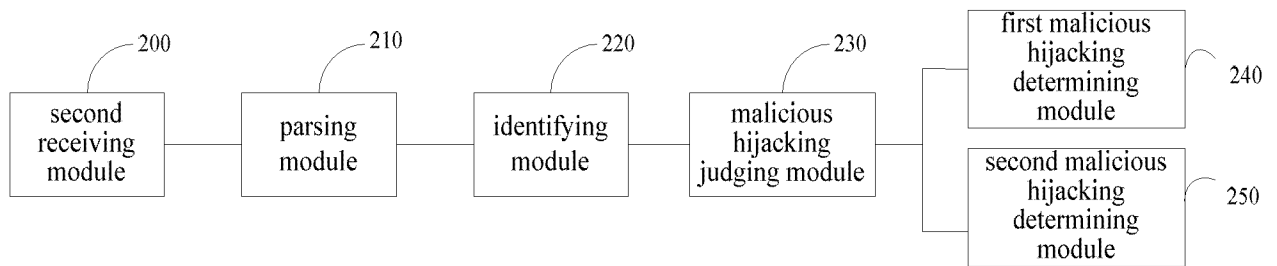
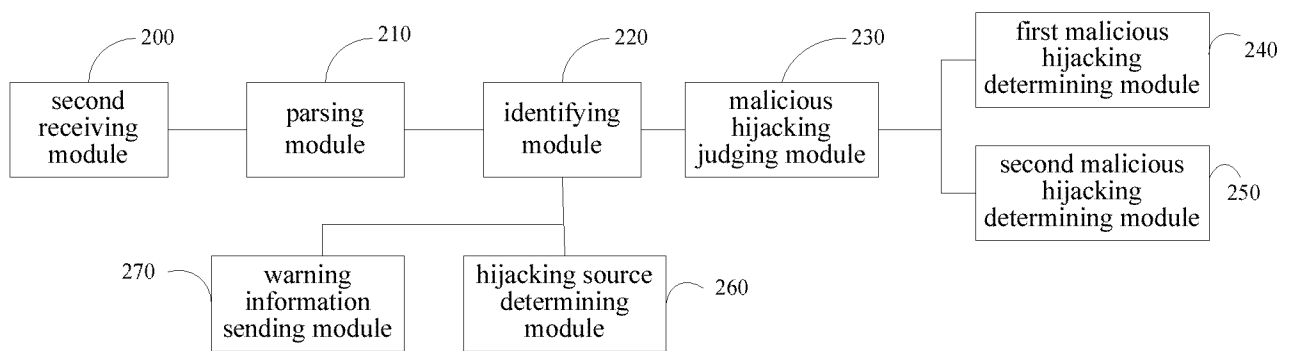
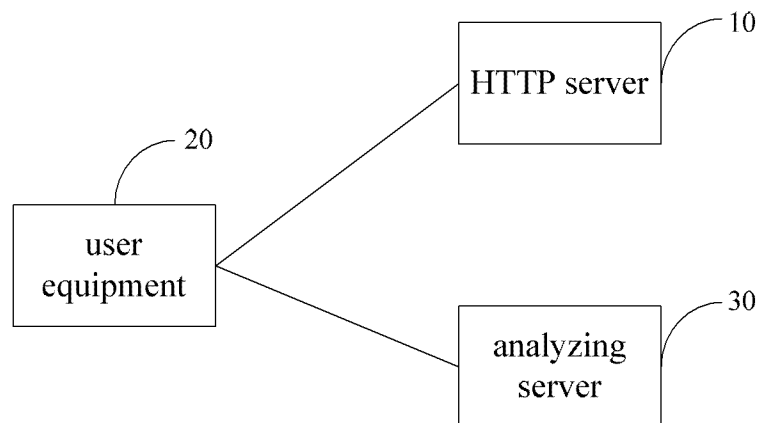
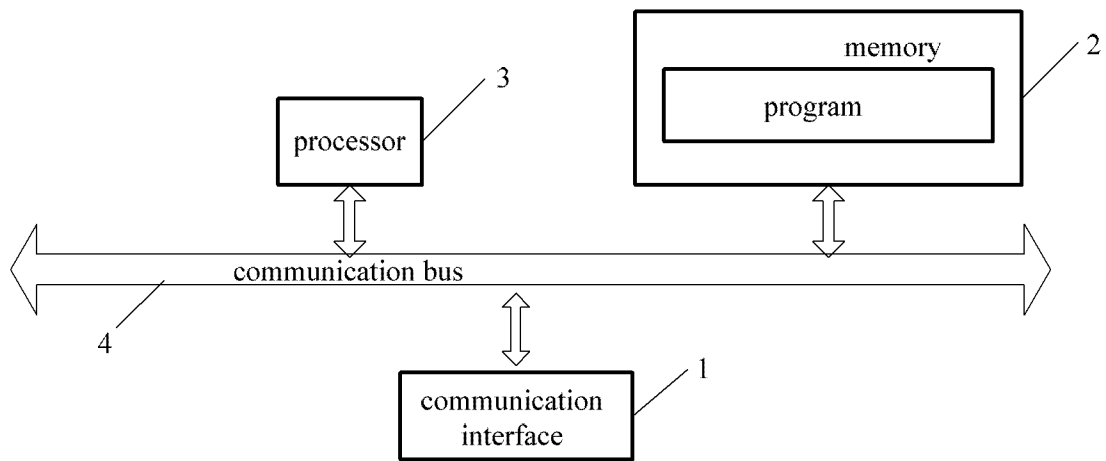
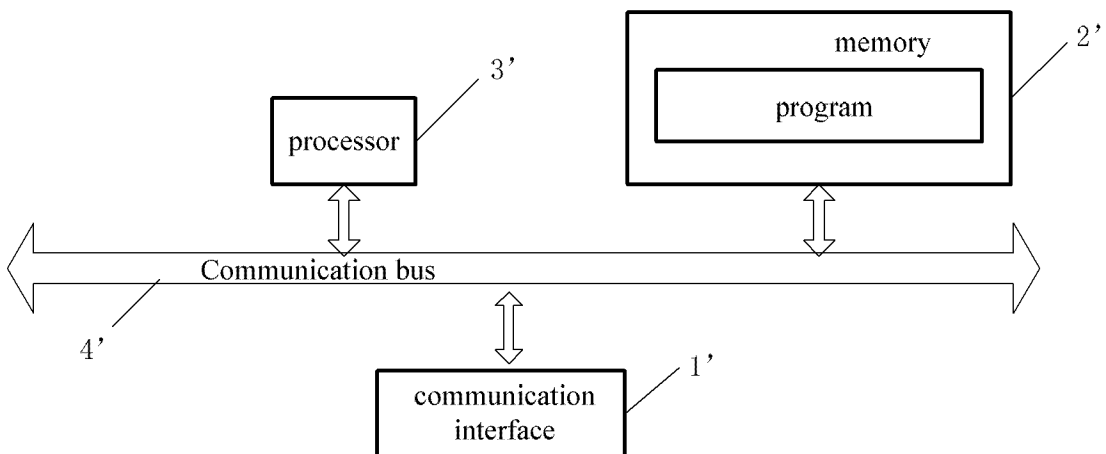


Fig. 6

**Fig. 7****Fig. 8****Fig. 9****Fig. 10**

**Fig. 11****Fig. 12****Fig. 13**

**Fig. 14****Fig. 15**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/080304

A. CLASSIFICATION OF SUBJECT MATTER

H04L 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)

H04L; H04W; H04Q; 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)

CPRSABS;CNTXT;VEN;CNKI:detect+, monitor+, inspect+, hijack+, link, URL, uniform w resource w locator, safe, security, java, script, HTTP, hypertext w transfer w protocol, malicious, information, attack+, steal+, web w page, site, text, pars+, extract +, analyz+, analys+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102663319 A (QIZHI SOFTWARE BEIJING CO LTD) 12 September 2012 (2012-09-12) description, paragraphs [0064] to [0105], and figures 1 and 2	1-18
A	CN 102638448 A (ZHUHAI JUNTIAN ELECTRONIC TECH) 15 August 2012 (2012-08-15) the whole document	1-18
A	CN 101820419 A (UNIV BEIJING) 01 September 2010 (2010-09-01) the whole document	1-18
A	EP 1420562 A2 (MICROSOFT CORP) 19 May 2004 (2004-05-19) the whole document	1-18

☐ 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	“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
“E”	earlier application or patent but published on or after the international filing date	“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
“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)	“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
“O”	document referring to an oral disclosure, use, exhibition or other means	“&”	document member of the same patent family
“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

15 September 2014

Date of mailing of the international search report

10 October 2014

Name and mailing address of the ISA/

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA(ISA/CN)
6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088 China

Facsimile No. (86-10)62019451

Authorized officer

GONG,Mei

Telephone No. (86-10)62089571

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/080304

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	102663319	A	12 September 2012	Non e			
CN	102638448	A	15 August 2012	Non e			
CN	101820419	A	01 September 2010	CN	101820419	B	26 December 2012
EP	1420562	A2	19 May 2004	US	7343626	B1	11 March 2008
				EP	1420562	A3	07 June 2006
				JP	2004164617	A	10 June 2004
				JP	4625246	B2	02 February 2011