



(51) International Patent Classification:
G06F 17/30 (2006.01)

(21) International Application Number:
PCT/CN2014/083219

(22) International Filing Date:
29 July 2014 (29.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310326542.3 30 July 2013 (30.07.2013) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(72) Inventor: **LUO, Yan**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(74) Agent: **ADVANCE CHINA IP LAW OFFICE**; Room 3901, No. 85 Huacheng Avenue, Tianhe District, Guangzhou, Guangdong 510623 (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 AND DEVICE FOR DETECTING JUMP ACTD/ITIES OF PHISHING WEBPAGES

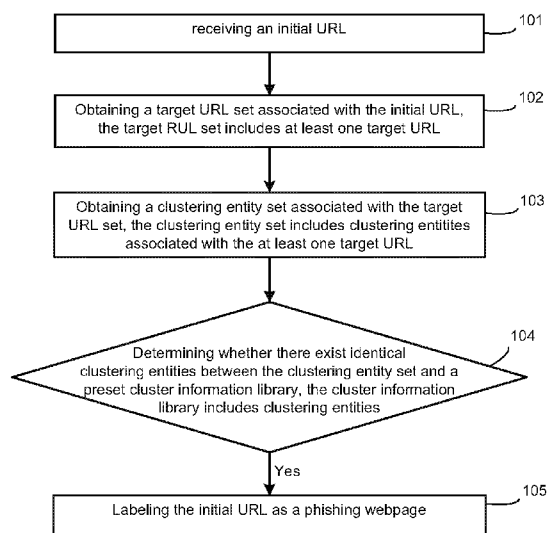


Figure 1

(57) Abstract: A method and a device for detecting jump activities of phishing webpages are disclosed. The method includes the following operations: receiving an initial URL; obtaining a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL; obtaining a clustering entity set associated with the target URL set, wherein the clustering entity set comprises clustering entities associated with the at least one target URL; determining whether there exists any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the clustering information library comprises clustering entities, and if exists, labeling the initial URL as a phishing webpage.

METHOD AND DEVICE FOR DETECTING JUMP ACTD/ITIES OF PHISHING WEBPAGES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The application claims priority to Chinese Patent Application No. 2013103265423, filed on July 30, 2013, which is incorporated by reference in its entirety.

FIELD OF THE TECHNOLOGY

[0002] The present disclosure relates to a method and a device for detecting jump activities of phishing webpages in the field of information security.

BACKGROUND

[0003] A phishing webpage is a disguised bank webpage or e-commerce webpage that intends to infiltrate and steal private information such as bank accounts and passwords submitted by users. Phishing webpage activities are online fraud activities, which phishers counterfeit the URLs and the page content of legitimate websites using different means such as by inserting dangerous HTML codes into certain webpages of legitimate websites by taking advantage of any loopholes in the server programs of such websites, and with the purpose of tricking people into divulging their private information, such as their accounts and passwords of bank/credit cards.

[0004] Phishing webpages pose great security, privacy and identity threats to users, so more and more phishing webpage detection methods have emerged. However, existing methods typically merely detect the initial URL of a phishing webpage. This method is deficient, because the initial URL is being utilized by the phishers as a URL jump to another URL to elude the final URL detection. For example, t.cn/123456 may be the initial URL of a phishing webpage, which a phisher may use the initial URL to jump to a different URL: a.com/1.asp of another phishing webpage. Suppose the later URL: a.com/1.asp being the real URL (i.e., the phisher as an evil-doer), the prior art initial detection method would have missed the real phishing webpage. In other words, the prior art method of detecting initial URLs of phishing webpages would be ineffective to detect the URL jump activities of the phishing webpages.

SUMMARY

[0005] In view of this, the various embodiments of the disclosure provide a method for detecting jump activities of phishing webpages and is capable of detecting all URLs of jump activities of phishing webpages to prevent missing any phishing webpages.

[0006] The embodiments of the present disclosure provide a method for detecting jump activities of phishing webpages, which include at least the following operations: receiving an initial URL;

obtaining a target URL set associated with the initial URL, wherein the target URL set includes at least one target URL; obtaining a clustering entity set associated with the target URL set, wherein the clustering entity set includes clustering entities associated with the at least one target URL; determining whether there exist any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the clustering information library includes clustering entities, and if there exist, labeling the initial URL as a phishing webpage.

[0007] Preferably, the method further includes: wherein when there exist identical clustering entities between the clustering entity set and a preset cluster information library: obtaining the clustering entities: obtaining the at least one target URL associated with the clustering entities; and labeling the at least one target URL and excluding at least one target URL contained in the target URL set as phishing webpages.

[0008] The embodiments of the present disclosure also provide a device for detecting jump activities of phishing webpages, wherein the device includes at least a processor with circuitry operating in conjunction with at least a memory storing codes to be executed to perform functions as a plurality of modules, wherein the plurality of modules include: a receiving module, which is used to receive an initial URL; a first acquisition module, which is used to obtain a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL; a second acquisition module, which is used to obtain a clustering entity set associated with the target URL set, wherein the clustering entity set comprises clustering entities associated with the target URLs; a determining module, which is used to determine whether there exist any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the cluster information library comprises clustering entities; and a first labeling module, which is used to label the initial URL as a phishing webpage when the determining module determines that there exist identical clustering entities between the clustering entity set and a preset cluster information library.

[0009] Preferably, the device includes: a third acquisition module, which is used to obtain the clustering entities when there exist identical clustering entities between the clustering entity set and a preset cluster information library; a fourth acquisition module, which is used to obtain the target URL associated with the clustering entity; and a second labeling module, which is used to label the target URLs excluding the target URL contained in the target URL set as phishing webpages.

[0010] Yet in another embodiment, the present disclosure discloses a non-transitory computer-readable storage medium, wherein the computer readable storage medium stores a program which comprises codes or instructions to cause a processor circuitry to execute operations for detecting jump activities of phishing webpages, the operations include: receiving an initial URL; obtaining a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL; obtaining a clustering entity set associated with the target URL set, wherein the

WO_2015/014271 comprises clustering entities associated with the at PCT/CN2014/083219L; and determining whether there exist any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the clustering information library comprises clustering entities, and if there exist, labeling the initial URL as a phishing webpage.

[0011] By obtaining the target URL set of the initial URL and determining whether the clustering entity associated with the target URL in the target URL set is available in the preset clustering information library, the initial URL may finally be determined as a phishing webpage or not. Accordingly, the detect jump activities of phishing webpages that are undetectable with the prior art may be detected without missing any.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The accompanying drawings may be included to provide further understanding of the claims and disclosure which may be incorporated in, and constitute a part of this specification. The detailed description and illustrated embodiments described may serve to explain the principles defined by the claims.

[0013] Figure 1 shows a flowchart of a method for detecting jump activities of phishing webpages, according to an embodiment of the disclosure;

[0014] Figure 2 shows an exemplary structural diagram of a device for detecting jump activities of phishing webpages, according to an embodiment of the disclosure;

[0015] Figure 3 shows an exemplary structural diagram of a server, according to an embodiment of the disclosure.

DETAILED DESCRIPTION

[0016] The various embodiments of the disclosure may be further described in details in combination with attached drawings and embodiments below. It should be understood that the specific embodiments described here may be used only to explain the disclosure, and may not be used to limit the disclosure. In addition, for the sake of keeping description brief and concise, the newly added features, or features which may be different from those previously described in each new embodiment will be described in details. Similar features may be referenced back to the prior descriptions in a prior numbered drawing or referenced ahead to a higher numbered drawing. Unless otherwise specified, all technical and scientific terms herein may have the same meanings as understood by a person skilled in the art.

[0017] Embodiment 1

[0018] A jump phishing webpage is a phishing webpage, which may have a URL different from an intended webpage address input by a user into an address bar of the browser. The methods in the prior art for detecting phishing webpages may only detect the URL in the address bar of the browser

inputWO 2015/014271A, yet may not detect jump activities of phishingPCT/CN2014/083219 present embodiment may obtain the URL of the final webpage accessed by the user and a clustering entity set associated with the URL, and compares the clustering entity set with a preset clustering information library to finally determine that it may be a phishing webpage.

[0019] Figure 1 shows a flowchart of the method for detecting jump activities of phishing webpages provided in this embodiment. The method includes at least the following operations:

[0020] Step 101: Receiving an initial URL. In this embodiment, a terminal or device (such as in Fig. 3) may obtain an initial URL inputted by a user, wherein the initial URL may be a URL that the user inputs in an address bar of a browser of the terminal or the device.

[0021] Step 102: Obtaining a target URL set associated with the initial URL, wherein the target URL set may include at least one target URL. A jump phishing webpage may be characterized by that the URL in the address bar of the browser inputted by a user being different from the URL of the webpage eventually accessed by the user. To detect a jump phishing webpage activity, the disclosed embodiment may receive an initial URL and then obtains a target URL set associated with the initial URL. The target URL set may include at least one target URL.

[0022] In actual practice, the target URL set may include only one target URL. In other words, the jump phishing webpage may be a 1-level phishing webpage. For example, the initial URL may be A, the target URL may be B, that is, the target URL set may be {B}. In this case, jumping from A to B is a 1-level jump. Likewise, the target URL set may include more than one target URL. For example, the target URL set may include two target URLs, that is to say, when the initial URL may be A, A may first jump to B and then from B jump to C. In this case, the target URLs may be B and C, and the target URL set may be {B, C}. Accordingly, the jump from A to B and then from B to C is a 2-level jump.

[0023] More specifically, jump activities of phishing webpages may use a variety of URL jump technologies including a 301 jump, or a 302 jump, js (javascript) jump, and iframe jump. The disclosure in this illustrated embodiment does not restrict the jump method used by jump activities of phishing webpages, and the method is capable of obtaining the target URL set associated with the initial URL.

[0024] Step 103: Obtaining a clustering entity set associated with the target URL set, wherein the clustering entity set may include clustering entities associated with the at least one target URLs. In this embodiment, upon obtaining the target URL set associated with the initial URL, the clustering entity set associated with the target URL set may be obtained, wherein the clustering entity set may include the clustering entities associated with the at least one target URL.

[0025] In this embodiment, the clustering entity may include domains, sites, and domains and

pathsWO 2015/014271nd-level domains. Taking the target URL PCT/CN2014/083219/path1, d.c.com/path1/path2/1.asp} as an example, the following section describes the process of obtaining a clustering entity set. Obtain the clustering entities associated with b.a.com/path1 first; the domain associated with b.a.com/path1 is a.com, the site associated with b.a.com/path1 is b.a.com, and the path associated with b.a.com/path1 is b.a.com/path1. Therefore, a.com, b.a.com, and b.a.com/path1 are the clustering entities associated with b.a.com/path1.

[0026] Likewise, determining that the clustering entities associated with d.c.com/path1/path2/1.asp may include: c.com, d.c.com, d.c.com/path1, and d.c.com/path1/path2 respectively. To sum up, {a.com, b.a.com, b.a.com/path1, c.com, d.c.com, d.c.com/path1, and d.c.com/path1/path2} is the clustering entity set associated with the target URL set of {b.a.com/path1, d.c.com/path1/path2/1.asp}.

[0027] Step 104: Determining whether there exist identical clustering entities between the clustering entity set and a preset cluster information library, wherein the cluster information library may include clustering entities, and if yes, proceeding to Step 105.

[0028] In this embodiment, upon obtaining the clustering entity set, the present disclosure compares the clustering entity set with a preset cluster information library, determines whether there exist identical clustering entities between the clustering entity set and the preset cluster information library, and if yes, proceeds to Step 105, wherein, the cluster information library comprises a clustering entity determined as the entity of a phishing webpage.

[0029] In practice, the present disclosure determines whether the clustering entity set and the preset cluster information library have any identical clustering entities, wherein the number of identical clustering entities is not restricted (the number of identical clustering entities may be one or more), and if yes, proceed to Step 105. Likewise, the different ways of obtaining a cluster information library may fall within the same scope of this embodiment.

[0030] Step 105: Labeling the initial URL as a phishing webpage. In this embodiment of the present disclosure, the initial URL as a phishing webpage may be labeled when there exist identical clustering entities between clustering entity set and the preset cluster information library. Likewise, it is not necessary to label any URL when there exists no identical clustering entities between the clustering entity set and the preset cluster information library.

[0031] To summarize, detecting jump activities of phishing webpages in processing the target URLs in the target URL may be as follows: Firstly, when there exists identical clustering entities between the clustering entity set and a preset cluster information library, the present disclosure obtains the clustering entities. Secondly, the present disclosure may obtain the target URLs associated with the clustering entities. Finally, the present disclosure may label the target URLs excluding the target URLs contained in the target URL set as phishing webpages.

[0032] WO 2015/014271 embodiment, the present disclosure firstly obtains the iPCT/CN2014/083219 entities between the preset cluster information library and the clustering entity set, secondly obtains the target URLs associated with the identical clustering entities, and finally labels other target URLs contained in the target URL set as phishing webpages because the associated target URLs have been determined as phishing webpages.

[0033] Wherein, the clustering entities contained in the clustering entity set may be obtained through at least one target URLs, so the at least one target URLs associated with the clustering entities form the target URLs at the source of the clustering entities. After determining that there exist identical clustering entities between the clustering entity set and a preset cluster information library (which the clustering information library includes clustering entities), the initial URL may be labeled as a phishing webpage.

[0034] This above disclosed embodiment may effectively detect jump activities of phishing webpages that are undetectable with the prior art method and may detect all the phishing webpages that carry out URL jump activities, consequently, no phishing webpage may be missed.

[0035] Embodiment 2

[0036] Figure 2 shows an exemplary structure diagram of a device (200) for detecting jump activities of phishing webpages. The device (200) includes at least a processor with circuitry (270) operating in conjunction with at least a memory (260) storing codes to be executed to perform functions as a plurality of modules, wherein the plurality of modules include at least: a receiving module (201), a first acquisition module (202), a second acquisition module (203), a determining module (204) and a first labeling module (205).

[0037] The receiving module (201) may be used to receive an initial URL. The first acquisition module (202) may be used to obtain a target URL set which is associated with an initial URL, wherein the target URL set may include at least one target URL. The second acquisition module (203) may be used to obtain a clustering entity set associated with the target URL set, wherein the clustering entity set may include clustering entities associated with the target URLs. The determining module (204) may be used to determine whether there exist identical clustering entities between the clustering entity set and a preset cluster information library, wherein the cluster information library comprises clustering entities. The first labeling module (205) may be used to label the initial URL as a phishing webpage when the determining module determines that there exist identical clustering entities between the clustering entity set and a preset cluster information library.

[0038] To detect jump activities of phishing webpages thoroughly, the device (200) provided in this embodiment may further include: a third acquisition module, which is used to obtain the clustering entities when there exist identical clustering entities between the clustering entity set and a

preseWO 2015/014271 nation library; a fourth acquisition module, which isPCT/CN2014/083219 target URLs associated with the clustering entities; a second labeling module, which used to label the target URLs excluding the target URLs contained in the target URL set as phishing webpages.

[0039] Figure 3 shows a server (300) provided in this alternate embodiment, wherein the server (300) may be used to carry out the method provided in the foregoing embodiment as described in the flow chart of Fig. 1. More specifically, the server (300) may include one or more memories (310) made of non-transitory computer readable storage media, an input unit (320), an output unit (330), a processor (340) which include one or more processing cores, and a power supply (350), wherein:

[0040] The memory (310) may be used to store software programs and modules. By running a software program or module stored in the memory (310), the processor (330) may execute various functional applications and data processing operations. The memory (310) may mainly include a storage program area and a storage data area, wherein the storage program area may store an operating system, applications required for at least one function, and the storage data area may store the data based on usage of the computer. In addition, the memory (310) may be such as a high-speed random access memory and a non-volatile memory, for example, at least one disk storage device, a flash memory device, or a volatile solid memory device of another type. Correspondingly, the memory (310) may include a memory controller, which may enable the processor (340) and the input unit (320) to access the memory (310).

[0041] The input unit (320) may be used to receive the inputted numerical or character information, and generate keyboard inputs, mouse inputs, operating rod inputs, optical inputs, or trackball signal inputs which are related to user's setting and functional control.

[0042] As the control center of the server (300), the processor (340) may connect different parts of the server by means of various interfaces and lines, and performs various functions of the computer and processes data by running or executing the software program and/or module stored in the memory (310) and invoking the data stored in the memory (310), thereby performing overall monitoring to the device (200) such as a smart mobile phone or to a terminal. Optionally, the processor (340) may include one or more processing cores.

[0043] The server also comprises the power supply (350) (such as a battery) that supplies power to various parts of the server. Preferably, the power supply (350) may be connected to the processor (330) logically through a power management system, so that the power management system may perform such functions as charging management, discharging management, and power consumption management. The power supply (350) may further comprise one or multiple DC/AC power supplies, a recharging system, a power failure detection circuit, a power converter or inverter, and a power status indicator.

[0044] In this embodiment, the processor (330) may specifically load the executable files

WO 2015/014271 processes of one or multiple applications to the memory (310) to the following instructions, and may run the applications stored in the memory (310), thereby implementing the various functions as described in the flow chart of Fig. 1 as follows: receiving an initial URL; obtaining a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL; obtaining a clustering entity set associated with the target URL set, wherein the clustering entity set comprises clustering entities associated with the target URLs; determining whether there exist identical clustering entities between the clustering entity set and a preset cluster information library, wherein the clustering information library comprises clustering entities, and if yes, labeling the initial URL as a phishing webpage.

[0045] Preferably, the method performed by the server may further include that when there exist identical clustering entities between the clustering entity set and a preset cluster information library: obtaining the clustering entities; obtaining the target URLs associated with the clustering entities; and labeling the target URLs by excluding the target URLs contained in the target URL set as phishing webpages.

[0046] The embodiment of both the device (200) and the server (300) for detecting jump activities of phishing webpages basically corresponds to the embodiment of the method for detecting jump activities of phishing webpages. For related details about the embodiment of the device for detecting jump activities of phishing webpages, refer to the related descriptions of the embodiment of the method for detecting jump activities of phishing webpages. The above described embodiment of the device for detecting jump activities of phishing webpages is only for illustrative purposes. The various modules or units described as separate parts may or may not be physically separated, and parts displayed as modules or units may or may not be physical units, that is, they may be located at the same place or be distributed on multiple network units. Some or all of the modules may be selected as needed to attain the objectives of this embodiment. A person with ordinary skills in the art may understand and carry out it without inputting creative effort.

[0047] The sequence numbers of the above-mentioned embodiments may be intended only for description, instead of indicating the relative merits of the embodiments. It should be understood by those with ordinary skill in the art that all or some of the steps of the foregoing embodiments may be implemented by hardware, or software program codes stored on a non-transitory computer-readable storage medium with computer-executable commands stored within. For example, the disclosure may be implemented as an algorithm as codes stored in a program module or a system with multi-program-modules. The computer-readable storage medium may be, for example, nonvolatile memory such as compact disc, hard drive, ROM or flash memory. The computer-executable commands may enable a computer, a server, a smart phone, a tablet or any similar computing device to render detecting of jump activities of phishing webpages operations.

[004] WO 2015/014271 going represents only some preferred embodiments (PCT/CN2014/083219) and their disclosure may not be construed to limit the disclosure in any way. Those of ordinary skill in the art will recognize that equivalent embodiments may be created via slight alterations and modifications using the technical content disclosed above without departing from the scope of the technical solution of the disclosure, and such summary alterations, equivalent has changed and modifications of the foregoing embodiments may be to be viewed as being within the scope of the technical solution of the disclosure.

1. A method for detecting jump activities of phishing webpages, comprising:
 - receiving an initial URL;
 - obtaining a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL;
 - obtaining a clustering entity set associated with the target URL set, wherein the clustering entity set comprises clustering entities associated with the at least one target URL; and
 - determining whether there exist any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the clustering information library comprises clustering entities, and if there exist, labeling the initial URL as a phishing webpage.
2. The method according to claim 1, wherein when there exists identical clustering entities between the clustering entity set and a preset cluster information library:
 - obtaining the clustering entities;
 - obtaining the at least one target URL associated with the clustering entities; and
 - labeling the at least one target URL and excluding at least one target URL contained in the target URL set as phishing webpages.
3. A device for detecting jump activities of phishing webpages, wherein the device comprises at least a processor with circuitry operating in conjunction with at least a memory storing codes to be executed to perform functions as a plurality of modules, wherein the plurality of modules comprise:
 - a receiving module, which is used to receive an initial URL;
 - a first acquisition module, which is used to obtain a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL;
 - a second acquisition module, which is used to obtain a clustering entity set associated with the target URL set, wherein the clustering entity set comprises clustering entities associated with the target URLs;
 - a determining module, which is used to determine whether there exist any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the cluster information library comprises clustering entities; and
 - a first labeling module, which is used to label the initial URL as a phishing webpage when the determining module determines that there exist identical clustering entities between the clustering entity set and a preset cluster information library.
4. The device according to claim 3, further comprises:

WO 2015/014271 tion module, which is used to obtain the clusteringPCT/CN2014/083219re exist identical clustering entities between the clustering entity set and a preset cluster information library;

a fourth acquisition module, which is used to obtain the target URL associated with the clustering entity; and

a second labeling module, which is used to label the target URLs excluding the target URL contained in the target URL set as phishing webpages.

5. The device according to claim 3, wherein the device is contained within a terminal which communicates to a network, the terminal comprises anyone of: a smart phone, a personal computer, a laptop computer, a notebook computer, a computing tablet, a mobile phone or a server.

6. A non-transitory computer-readable storage medium, wherein the computer readable storage medium stores a program which comprises codes or instructions to cause a processor circuitry to execute operations for detecting jump activities of phishing webpages, the operations comprising:

receiving an initial URL;

obtaining a target URL set associated with the initial URL, wherein the target URL set comprises at least one target URL;

obtaining a clustering entity set associated with the target URL set, wherein the clustering entity set comprises clustering entities associated with the at least one target URL; and

determining whether there exist any identical clustering entities between the clustering entity set and a preset cluster information library, wherein the clustering information library comprises clustering entities, and if there exist, labeling the initial URL as a phishing webpage.

7. The non-transitory computer readable storage medium according to claim 6, wherein when there exist identical clustering entities between the clustering entity set and a preset cluster information library:

obtaining the clustering entities;

obtaining the at least one target URL associated with the clustering entities; and

labeling the at least one target URL and excluding at least one target URL contained in the target URL set as phishing webpages.

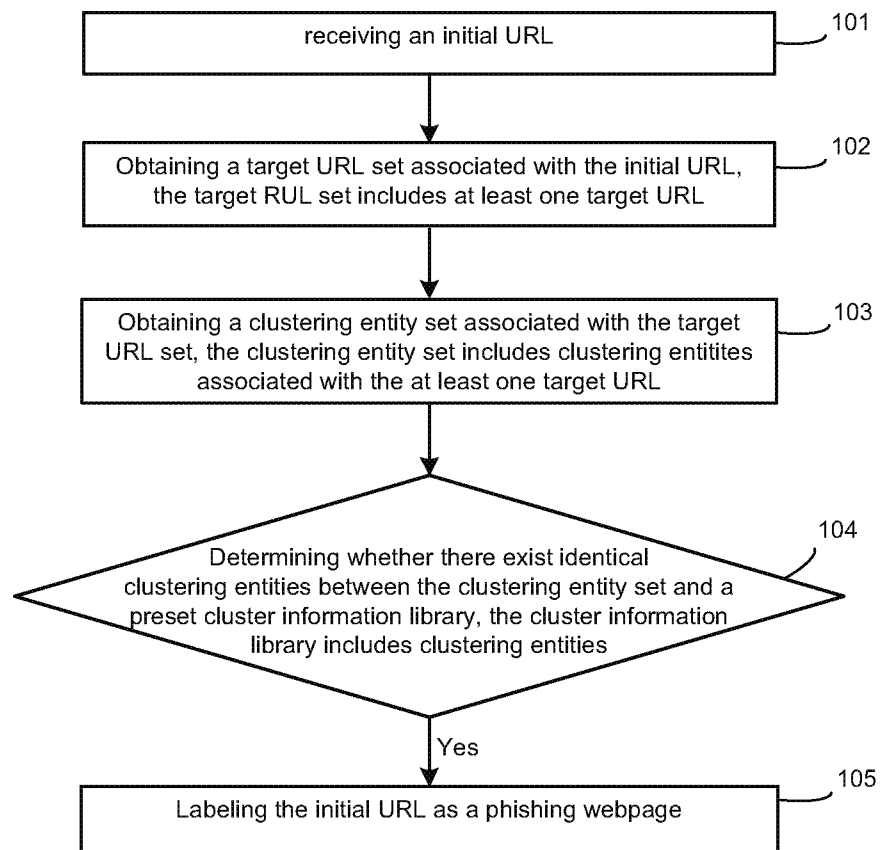


Figure 1

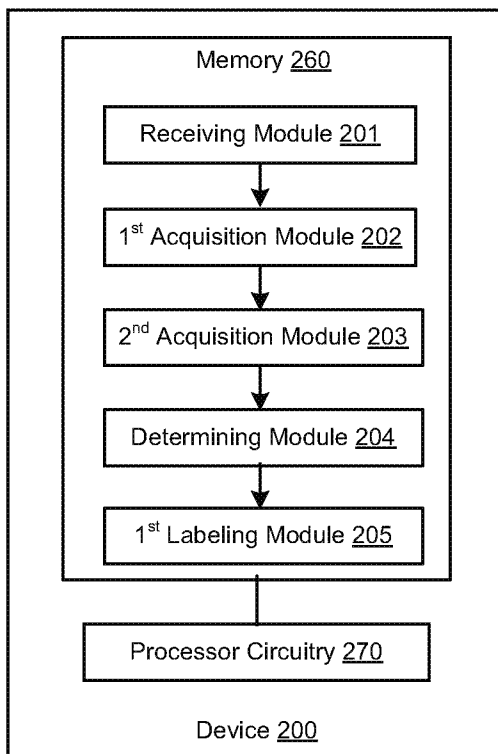


Figure 2

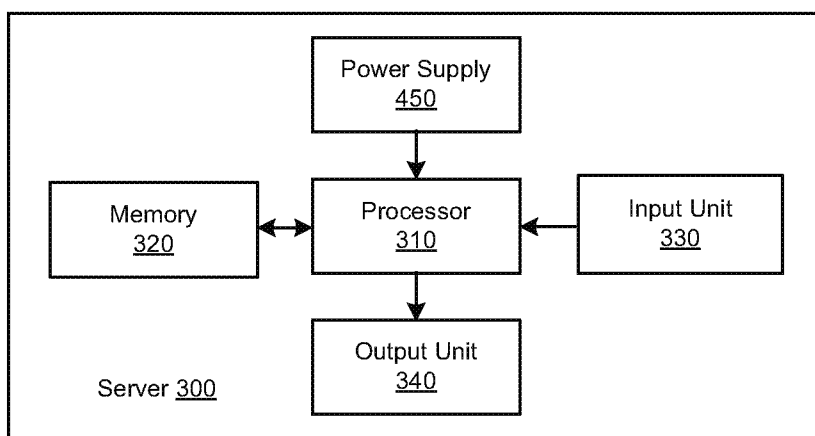


Figure 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/083219

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/30(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

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)

WPI, EPODOC, CNPAT, CNKI: initial, target, url, compare, database, segment

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008034073 A1 (MCCLOY, HARRY MURPHEY ET AL.) 07 February 2008 (2008-02-07) description, paragraphs [0027]-[0049]	1-7
Y	CN 102594934 A (QIZHI SOFTWARE BEIJING COMPANY LIMITED) 18 July 2012 (2012-07-18) claims 1-3	1-7
A	US 2012136764 A1 (INTUIT INC.) 31 May 2012 (2012-05-31) the whole document	1-7

☐ 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

28 September 2014

Date of mailing of the international search report

06 November 2014

Name and mailing address of the ISA/CN

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

Authorized officer

HU,Ping

Facsimile No. (86-10)62019451

Telephone No. (86-10)82245429

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/083219

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2008034073	A1	07 February 2008	None			
CN	102594934	A	18 July 2012	WO	2013097742	A1	04 July 2013
US	2012136764	A1	31 May 2012	WO	2012074569	A1	07 June 2012