



- (51) **International Patent Classification:**
H04L 29/10 (2006.01) *G06F 17/00* (2006.01)
- (21) **International Application Number:**
PCT/CN2013/088567
- (22) **International Filing Date:**
5 December 2013 (05.12.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
201310013857.2 15 January 2013 (15.01.2013) CN
- (71) **Applicant:** **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).
- (72) **Inventors:** **TAN, Wen**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN). **LI, Rongjun**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (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 TROJAN HORSE INTERCEPTION

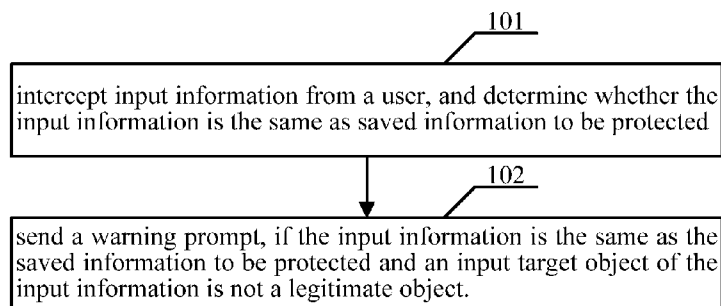


Fig. 1

(57) **Abstract:** In the embodiment of the present invention, a method, a device and a system for Trojan horse interception are provided. The method includes: intercepting input information from a user, and determining whether the input information is the same as saved information to be protected; and sending a warning prompt, if the input information is the same as the saved information to be protected and an input target object of the input information is not a legitimate object. According to the above scheme, all the input information can be intercepted, and a warning is sent if the input information is the same as the saved information to be protected and the input target object of the input information is not legitimate; the above scheme is not limited to monitor a certain input target object, then the scheme has more extensive application.



METHOD, DEVICE AND SYSTEM FOR TROJAN HORSE INTERCEPTION

[0001] This application claims priority to Chinese patent application No. 201310013857.2 titled “Method, device and system for trojan horse interception” and filed with the State Intellectual Property Office on January 15, 2013, which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present disclosure relates to the technical field of communication, and in particular to a method, device and system for trojan horse interception.

BACKGROUND OF THE INVENTION

[0003] In order to prevent usernames and passwords of online bankings, online games, and other network accounts from being stolen, extensive research has been made by technical staff, and various schemes has been used to prevent username and password from being stolen. An example of one of the schemes is as follows.

[0004] A special account and/or password input control is used to prevent an input from being intercepted.

SUMMARY OF THE INVENTION

[0005] In the embodiment of the present disclosure, a method, device and system for Trojan interception is provided, which is adapted to provide a scheme which has extensive application and has lower requirements for the user so as to enhance security.

[0006] A trojan interception method, including:

intercepting input information, and determining whether the input information is the same as saved information to be protected; and

sending a warning prompt, if the input information is the same as the saved information to be protected and an input target object of the input information is not determined as a legitimate object.

—2—

[0007] A device for trojan interception, including:

an inputting unit, adapted to receive input information;

an intercepting unit, adapted to intercept the input information which is inputted by the user through the inputting unit;

5 a comparing unit, adapted to determine whether the input information which is intercepted by the intercepting unit is the same as saved information to be protected;

a legitimacy determining unit, adapted to determine whether an input target object of the input information is a legitimate object if it is determined by the comparing unit that the input information which is intercepted by the intercepting unit is the same as the saved information

10 to be protected; and

a warning unit, adapted to send a warning prompt when it is determined by the legitimacy determining unit that the input target object of the input information is not a legitimate object.

[0008] A system for trojan interception, including a terminal and a cloud server,

15 the terminal is adapted to intercept input information from a user and determine whether the input information is the same as saved information to be protected; and send a warning prompt, if the input information is the same as the saved information to be protected and the query by the terminal to the cloud server shows that an input target object of the input information is not a legitimate object.

[0009] It can be seen from the above technical scheme that the embodiment of the present disclosure has the following advantages: according to the above scheme, all the input information
20 can be intercepted, and a warning is sent if the input information is the same as the saved information to be protected and an input target object of the input information is not legitimate; the above scheme is not limited to monitor a certain input target object, thereby the application range is more extensive; and it is unnecessary for the user to enter the correct web address or
25 operate the correct program, so the requirement for the user is lowered, and thereby the above scheme has better security.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] In order to illustrate the technical solutions of the embodiments of the present disclosure

—3—

more clearly, drawings to be used in the description of the embodiments will be described briefly hereinafter. Apparently, the drawings described hereinafter are only some embodiments of the present disclosure, and other drawings may be obtained by those skilled in the art according to these drawings without creative labor.

5 [0011] Figure 1 is a schematic flow chart of a method according to an embodiment of the present disclosure;

[0012] Figure 2 is a schematic flow chart of another method according to an embodiment of the present disclosure;

10 [0013] Figure 3 is a schematic diagram of a data flow according to an embodiment of the present disclosure;

[0014] Figure 4 is a schematic structural diagram of a device according to an embodiment of the present disclosure;

[0015] Figure 5 is a schematic structural diagram of another device according to an embodiment of the present disclosure;

15 [0016] Figure 6 is a schematic structural diagram of still another device according to an embodiment of the present disclosure; and

[0017] Figure 7 is a schematic structural diagram of a system according to an embodiment of the present disclosure.

20 DETAILED DESCRIPTION OF THE INVENTION

[0018] The technical solutions in the embodiments of the present invention will be further described in detail hereinafter in conjunction with the drawings in the embodiments of the present invention, so that the objects, technical solutions and advantages of the present invention will be clear. Apparently, the described embodiments are only a part but not all of the embodiments of the present invention. All the other embodiments can be obtained by those skilled in the art without creative effort on the basis of the embodiments of the present invention, which fall within the scope of protection of the present invention.

25

[0019] According to an embodiment of the present invention, a method for torjan interception is provided as shown in figure 1, which includes step 101 and step 102.

—4—

[0020] 101: Intercepting input information from a user, and determining whether the input information is the same as saved information to be protected.

[0021] The information may be an important account and password, and may also be other information to be protected. The specific form of the information is not defined in the embodiment of the present invention.

[0022] Preferably, in order to further improve security, it is possible that not the information but the non-reversible information derived from the information is saved on the terminal side. In particular, before the determining whether the input information is the same as the saved information to be protected, the method further includes: receiving the information to be protected, converting the information to be protected into non-reversible information, and saving the non-reversible information. The non-reversible information refers to any information that can't be adapted to recover the information by conversion, for example, the common MD5 (Message Digest Algorithm 5) value.

[0023] 102: Sending a warning prompt, if the input information is the same as the saved information to be protected and an input target object of the input information is not a legitimate object.

[0024] The manner of the warning prompt can be presenting the warning prompt dialog box, or sending a warning audio meanwhile. The specific form of the warning prompt is not defined in the embodiment of the present invention.

[0025] According to the above scheme, all the input information can be intercepted, and a warning is sent if the input information is the same as the saved information to be protected and an input target object of the input information is not illegitimate; the above scheme is not limited to monitor a certain input target object, then the application range is more extensive; and it is unnecessary for the user to enter the correct web address or operate the correct program, so the requirement for the user is lowered, and therefore the above scheme has enhanced security.

[0026] Corresponding to the saving the non-reversible information, in step 102 described above, the determining whether the input information is the same as saved information to be protected includes: converting the input information into the non-reversible information corresponding to the input information, and determining whether the non-reversible information corresponding to the input information is the same as the saved non-reversible information.

—5—

[0027] Alternatively, an example of the non-reversible information is provided according to an embodiment of the present invention, and the non-reversible information described above is a hash algorithm value. The MD5 value described above is one of the values obtained by the hash algorithm.

5 [0028] More particularly, the scheme which is implemented by using a cloud server is provided according to an embodiment of the present invention. The method for determining whether the input target object of the input information is not a legitimate object includes: comparing characteristic information of the input target object of the input information with legitimate characteristic information of the input target object saved in a cloud server, and determining that
10 the input target object of the input information is not a legitimate object if the characteristic information of the input target object of the input information has illegitimate information or unknown information.

[0029] Further, according to an embodiment of the present invention, a scheme through which illegitimate object at cloud end can be counted and the ability of identifying the trojan can be
15 enhanced is provided. In particular, after the determining that the input target object of input information is not a legitimate object, the method further includes: gathering the character information of the input target object of the input information, and sending the input target object of the input information to the cloud server as an illegitimate object if it is determined in
20 accordance with the character information that the input target object of the input information is a malicious program.

[0030] The essential idea of the above scheme is, firstly, setting the information to be protected, such as an important account and a password of the user at the local terminal. It is noted that these important accounts does not mean that the passwords of the accounts are needed to be saved at the local terminal, and it is only required to store a certain character (such as MD5 value) of the
25 password. Once the information to be protected is set, these accounts and passwords can be protected by the scheme according to an embodiment of the present invention. The specific protection scheme is as follows.

[0031] After the starting of the terminal, the input from a user is intercepted to obtain the input information from the user. The interception can be implemented by a kernel driving program.
30 Through this step, no matter in which window the user inputs the information, the input from the user can be detected through the kernel driving program according to the scheme, as long as the

—6—

user inputs the account and password which are set to be protected.

[0032] After it is detected that the user has inputted the information to be protected, the security check is made. The security check may be to verify whether the object window in which the user inputs or the URL of the accessed web page is legitimate. If the object window in which the user
5 inputs or the URL of the accessed web page is confirmed as legitimate, the operation of the user is permitted to proceed. If the object window in which the user inputs or the URL of the accessed web page is confirmed as illegitimate, a different measure can be adopted, for example, prompting the user to pay attention to security risks, or gathering enough information and sending the information to backstage so as to analysis the possible trojan horse and the URL of the
10 illegitimate fishing site manually. Further, if new information of trojan horse and the URL of the fishing site are found, the information can be stored in the cloud server to continually improve the accuracy of cloud query.

[0033] Because this technology is likely to be performed on all interfaces in user terminals (initial screening of the interfaces should be done before this technology is used), therefore, in
15 theory, there could be a high finding probability no matter in a known or in an unknown ID theft interface (including various fishing sites, ID theft trojan horse, or the like).

[0034] To describe in detail, the following embodiment will be taken as an example of trojan horse interception for instant messaging software with reference to FIG. 2 together with FIG. 3.

[0035] 201: Saving the information to be protected by a user in a suitable manner.

[0036] The information may be an account of instant message software, an account of various games, an account and its password of online banking, or the like. The scheme for saving the information can be that the user inputs these accounts actively and then saves the accounts. Since the account is used in conjunction with the software in the practical application of instant message software, it is not necessary for the user to input the accounts actively. For example,
25 when the user logs in an instant messaging software at a local terminal, the account and password of the instant information software can be automatically set in the protection program which is implemented according to an embodiment of present invention.

[0037] In addition, information needed to be saved as the information generally can be divided into two types, one type is the public information (such as, username), and the other type is the
30 confidential information (such as, password). Even though the protection program has security of

—7—

self protection, the risk for leakage of the confidential information can be increased with no doubt if the confidential information such as password is stored in medium such as a memory or configuration file. Accordingly, the public information can be saved directly. The confidential information can be saved by saving a certain characteristic value (such as, MD5 value) of the confidential information. Since the data itself can't be calculated according to the MD5 value of the data, the possibility of increasing the risk for leakage of confidential information is avoided.

[0038] 202: Intercepting the input (including input operation of mouse and keyboard) from the user.

[0039] Referring to FIG.3, the user inputs input information through input apparatus, the input information inputted by the user is intercepted, the intercepted information is sent to a protection program, and the input information can also be driven by the inputting apparatus to be submitted to an inputting object such as a webpage, software, or login interface along the original path.

[0040] There are many alternative implementation schemes to intercept the input from the user, for example:

[0041] A: installing a hook in an application layer by using a hook interface provided by Windows, wherein the hook can record the information of all the keys and mouse; and

[0042] B: Developing a Windows kernel driver program to attach the keyboard and mouse apparatus in the Windows, wherein the message sent by the hardware is firstly sent to this driver program.

[0043] 203: After intercepting the input information inputted by the user through keys, mouse or the like, comparing the input information with the saved information or characteristic value of the information so as to find whether the information (account and password) to be protected is inputted by the user.

[0044] Because all the input information of the user is monitored in this scheme, the input information from the user can be captured with high probability for each environment which the user is in, for example, accessing webpage, logging game, logging other type software, or being cheated by ID theft Trojan horse.

[0045] 204: Detecting the security of the input object.

[0046] Generally speaking, the input object is likely to be software, for example, instant

—8—

messaging software, game or other software, or a Web with an URL which is being visited by a browser. Legitimacy detection often can be done in conjunction with backstage cloud query. As shown in FIG. 3, the process information of software or URL being accessed is gathered by the protection program, and sent to the background cloud server for querying. The cloud server returns a result about whether the information is legitimate. The protection program can also gather the information (such as, the sample of executable file and URL link) of the illegitimate process and send the information to the cloud serve, if the result is illegitimate. These illegitimate samples can be analyzed by a security staff.

[0047] According to the above scheme, all the input information can be intercepted, and a warning is sent if the input information is the same as the saved information to be protected and an input target object of the input information is not illegitimate; the above scheme is not limited to monitor a certain input target object, then the application range is more extensive; and it is unnecessary for the user to enter the correct web address or operate the correct program, so the requirement for the user is lowered, and thereby the above scheme has better security. It is beneficial to find an illegitimate object when the various possible illegitimate characteristic information are sent to the cloud, thereby it is more beneficial to find unknown trojan horse.

[0048] According to an embodiment of the present invention, a device for torjan interception is provided, as shown in figure 4, which includes:

[0049] an inputting unit 401, adapted to receive input information from a user;

[0050] an intercepting unit 402, adapted to intercept the input information which is inputted by the user through the inputting unit 401;

[0051] a comparing unit 403, adapted to determine whether the input information which is intercepted by the intercepting unit 402 is the same as saved information to be protected;

[0052] a legitimacy determining unit 404, adapted to determine whether an input target object of the input information is a legitimate object if it is determined by the comparing unit 403 that the input information which is intercepted by the intercepting unit is the same as the saved information to be protected; and

[0053] a warning unit 405, adapted to send a warning prompt when it is determined by the legitimacy determining unit 404 that the input target object of the input information is not a legitimate object.

[0054] According to the above scheme, all the input information can be intercepted, and a warning is sent if the input information is the same as the saved information to be protected and an input target object of the input information is not illegitimate; the above scheme is not limited to monitor a certain input target object, then the application range is more extensive; and it is unnecessary for the user to enter the correct web address or operate the correct program, so the requirement for the user is lowered, and thereby the above scheme has enhanced security.

[0055] Further, in order to further improve security, it is possible that not directly the information but the non-reversible information derived from the information is saved at the terminal side. As shown in FIG. 5, the device further includes:

[0056] a protection information receiving unit 501, adapted to receive the information to be protected before it is determined whether the input information is the same as the stored information to be protected; and

[0057] a converting unit 502, adapted to convert the information to be protected which is received by the protection information receiving unit 501 into non-reversible information for saving, and convert the input information which is intercepted by the intercepting unit 501 into the non-reversible information corresponding to the input information,

[0058] wherein the comparing unit 403 is adapted to determine whether the non-reversible information corresponding to the input information is the same as the saved non-reversible information.

[0059] Alternatively, the converting unit 502 is adapted to convert the information to be protected which is received by the protection information receiving unit 501 into a hash algorithm value, and convert the input information which is intercepted by the intercepting unit 402 into a hash algorithm value corresponding to the input information.

[0060] Alternatively, the comparing unit 403 is adapted to: compare characteristic information of the input target object of the input information with legitimate characteristic information of the input target object saved in a cloud server, and determine that the input target object of input information is not a legitimate object if the characteristic information of the input target object of the input information has illegitimate information or unknown information.

[0061] Further, the scheme which is implemented using the cloud server is provided according to an embodiment of the present invention, as shown in FIG. 6, and the device further includes:

— 10 —

[0062] an information gathering unit 601, adapted to gather the character information of the input target object of the input information after it is determined by the legitimacy determining unit 404 that the input target object of the input information is not a legitimate object; and

[0063] a sending unit 602, adapted to send the input target object of the input information to a cloud server as an illegitimate object after it is determined in accordance with the character information gathered by the information gathering unit 601 that the input target object of the input information is a malicious program.

[0064] A system for trojan horse interception is further provided according to an embodiment of the present invention, as shown in FIG. 7, which includes, a terminal 701 and a cloud server 702, wherein the terminal 701 is adapted to intercept input information from a user and determine whether the input information is the same as saved information to be protected; and send a warning prompt, if the input information is the same as the saved information to be protected and the query by the terminal 701 to the cloud server 702 shows that an input target object of the input information is not a legitimate object.

[0065] According to the above scheme, all the input information can be intercepted, and a warning is sent if the input information is the same as the saved information to be protected and an input target object of the input information is not illegitimate; the above scheme is not limited to monitor a certain input target object, then the application range is more extensive; and it is unnecessary for the user to enter the correct web address or operate the correct program, so the requirement for the user is lowered, and thereby the above scheme has better security.

[0066] Further, in order to further improve security, it is possible to that not directly the information but the non-reversible information derived from the information is saved at the terminal side. In particular, the terminal 701 is further adapted to receive the information to be protected, convert the information to be protected into non-reversible information, and save the non-reversible information before it is determined whether the input information is the same as the saved information to be protected, and

[0067] the determining by the terminal 701 whether the input information is the same as the saved information to be protected includes: converting the input information into the non-reversible information corresponding to the input information, and determining whether the non-reversible information which corresponding to the input information is the same as the saved non-reversible information.

[0068] Alternatively, an example of non-reversible information is provided according to an embodiment of the present invention, the terminal 701 is adapted to convert the information to be protected into a hash algorithm value, and convert the intercepted input information into a hash algorithm value corresponding to the input information.

5 [0069] Alternatively, a scheme through which the illegitimate object in cloud can be counted and the ability of recognizing trojan horse can be enhanced is further provided according to an embodiment of the present invention, the terminal 701 is further adapted to gather the character information of the input target object of the input information after it is determined that the input target object of the input information is not a legitimate object, and send the input target object of
10 the input information to a cloud server 702 as an illegitimate object after it is determined in accordance with the character information that the input target object of the input information is a malicious program.

[0070] It should be noted that in the embodiment of terminal described above, the various units therein are only divided by functional logic, but are not limited by the division described above,
15 as long as the related function can be implemented; in addition, the special name of every function unit is only used to distinguish it easily, and is not used to limit the scope of protection of the present invention.

[0071] In addition, it can be understood by those skilled in the art that the all or some of the procedures can be achieved by instructing the related hardware through a program. The
20 corresponding program can be stored in a computer readable storage medium, which can be a ROM, a magnetic disk or an optical disk.

[0072] The above descriptions are only the better specific embodiments of the present invention, and the scope of protection of the present invention is not limited thereto. Any variation or replacement which can be easily thought by those skilled in the art in the technical
25 scope disclosed in the present invention should be covered within the scope of protection of the present invention. Therefore, the scope of protection of the present invention should be in accordance with the scope of the claims.

CLAIMS

1. A method for trojan horse interception, comprising:

intercepting input information, and determining whether the input information is the same as
5 saved information to be protected; and

sending a warning prompt, if the input information is the same as the saved information to
be protected and an input target object of the input information is not determined as a legitimate
object.

10 2. The method according to claim 1, further comprising, before the determining whether the input
information is the same as saved information to be protected,

receiving the saved information to be protected, converting the saved information to be
protected into non-reversible information, and saving the non-reversible information, and

15 the determining whether the input information is the same as saved information to be
protected comprises:

converting the input information into the non-reversible information corresponding to the
input information, and determining whether the non-reversible information corresponding to the
input information is the same as the saved non-reversible information.

20 3. The method according to claim 2, wherein the non-reversible information is a hash algorithm
value.

4. The method according to any one of claims 1 to 3, wherein a method for determining whether
the input target object of the input information is not a legitimate object comprises:

25 comparing characteristic information of the input target object of the input information with
legitimate characteristic information of the input target object saved in a cloud server, and
determining that the input target object of the input information is not a legitimate object if the
characteristic information of the input target object of the input information has illegitimate
information or unknown information.

5. The method according to claim 4, further comprising, after the determining that the input target object of input information is not a legitimate object,

5 gathering the character information of the input target object of the input information, and sending the input target object of the input information to a cloud server as an illegitimate object if it is determined in accordance with the characteristic information that the input target object of the input information is a malicious program.

6. A device for trojan horse interception, comprising:

10 an inputting unit, adapted to receive input information;

an intercepting unit, adapted to intercept the input information which is inputted by the user through the inputting unit;

a comparing unit, adapted to determine whether the input information which is intercepted by the intercepting unit is the same as saved information to be protected;

15 a legitimacy determining unit, adapted to determine whether an input target object of the input information is a legitimate object if it is determined by the comparing unit that the input information which is intercepted by the intercepting unit is the same as the saved information to be protected,; and

20 a warning unit, adapted to send a warning prompt when it is determined by the legitimacy determining unit that the input target object of the input information is not a legitimate object.

7. The device according to claim 6, further comprising:

25 a protection information receiving unit, adapted to receive the saved information to be protected before it is determined whether the input information is the same as the saved information to be protected; and

a converting unit, adapted to convert the saved information to be protected which is received by the protection information receiving unit into non-reversible information for saving, and convert the input information which is intercepted by the intercepting unit into the

— 14 —

non-reversible information corresponding to the input information,

wherein the comparing unit is adapted to determine whether the non-reversible information corresponding to the input information is the same as the saved non-reversible information.

5 8. The device according to claim 7, wherein

the converting unit is adapted to convert the saved information to be protected which is received by the protection information receiving unit into a hash algorithm value, and convert the input information which is intercepted by the intercepting unit into a hash algorithm value corresponding to the input information.

10

9. The device according to any one of claims 6 to 8, wherein

the comparing unit is adapted to: compare characteristic information of the input target object of the input information with legitimate characteristic information of the input target object saved in a cloud server, and determine that the input target object of input information is not a legitimate object if the characteristic information of the input target object of the input information has illegitimate information or unknown information.

15

10. The device according to claim 9, further comprising:

an information gathering unit, adapted to gather the character information of the input target object of the input information after it is determined by the legitimacy determining unit that the input target object of the input information is not a legitimate object; and

20

a sending unit, adapted to send the input target object of the input information to a cloud server as an illegitimate object after it is determined in accordance with the character information gathered by the information gathering unit that the input target object of the input information is a malicious program.

25

11. A system for trojan horse intercept, comprising a terminal and a cloud server communicated with the terminal, wherein

— 15 —

the terminal is adapted to intercept input information from a user and determine whether the input information is the same as saved information to be protected; and send a warning prompt, if the input information is the same as the saved information to be protected and a query sent by the terminal to the cloud server shows that an input target object of the input information is not a
5 legitimate object.

12. The system according to claim 11, wherein

the terminal is further adapted to receive the saved information to be protected, convert the saved information to be protected into non-reversible information, and save the non-reversible
10 information before it is determined by the terminal whether the input information is the same as the saved information to be protected;

the determining by the terminal whether the input information is the same as the saved information to be protected comprises: converting the input information into the non-reversible information corresponding to the input information, and determining whether the non-reversible
15 information which corresponding to the input information is the same as the saved non-reversible information.

13. The system according to claim 12, wherein

the terminal is adapted to convert the saved information to be protected into a hash
20 algorithm value, and convert the intercepted input information into a hash algorithm value corresponding to the input information.

14. The system according to any one of claims 11 to 13, wherein

the terminal is further adapted to gather the character information of the input target object
25 of the input information after it is determined that the input target object of input information is not a legitimate object, and send the input target object of the input information to a cloud server as an illegitimate object after it is determined in accordance with the character information that the input target object of the input information is a malicious program.

— 1/4 —

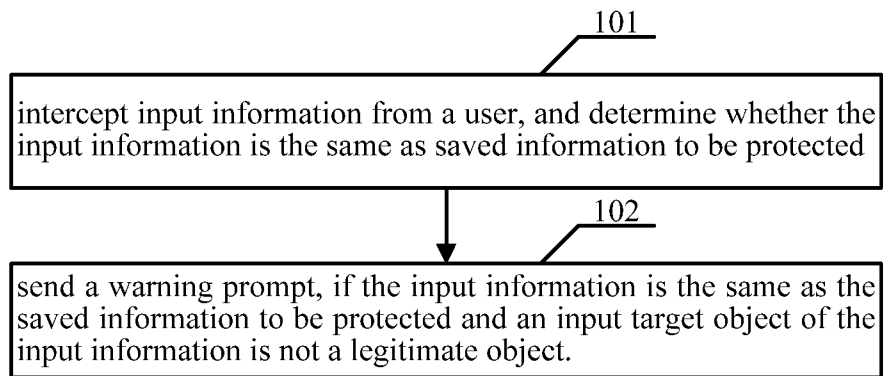


Fig. 1

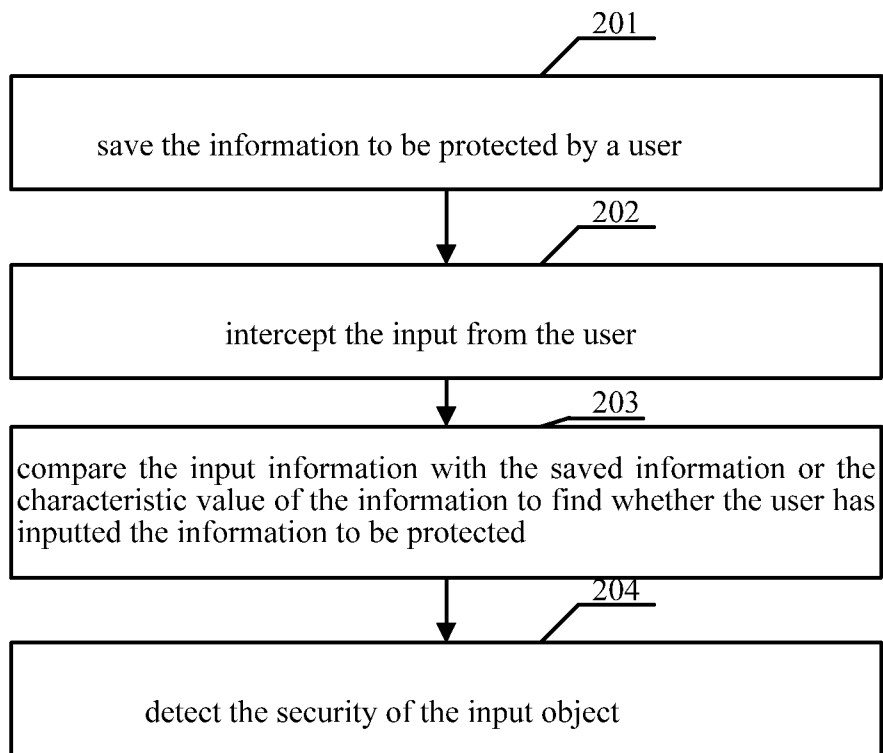


Fig. 2

—2/4—

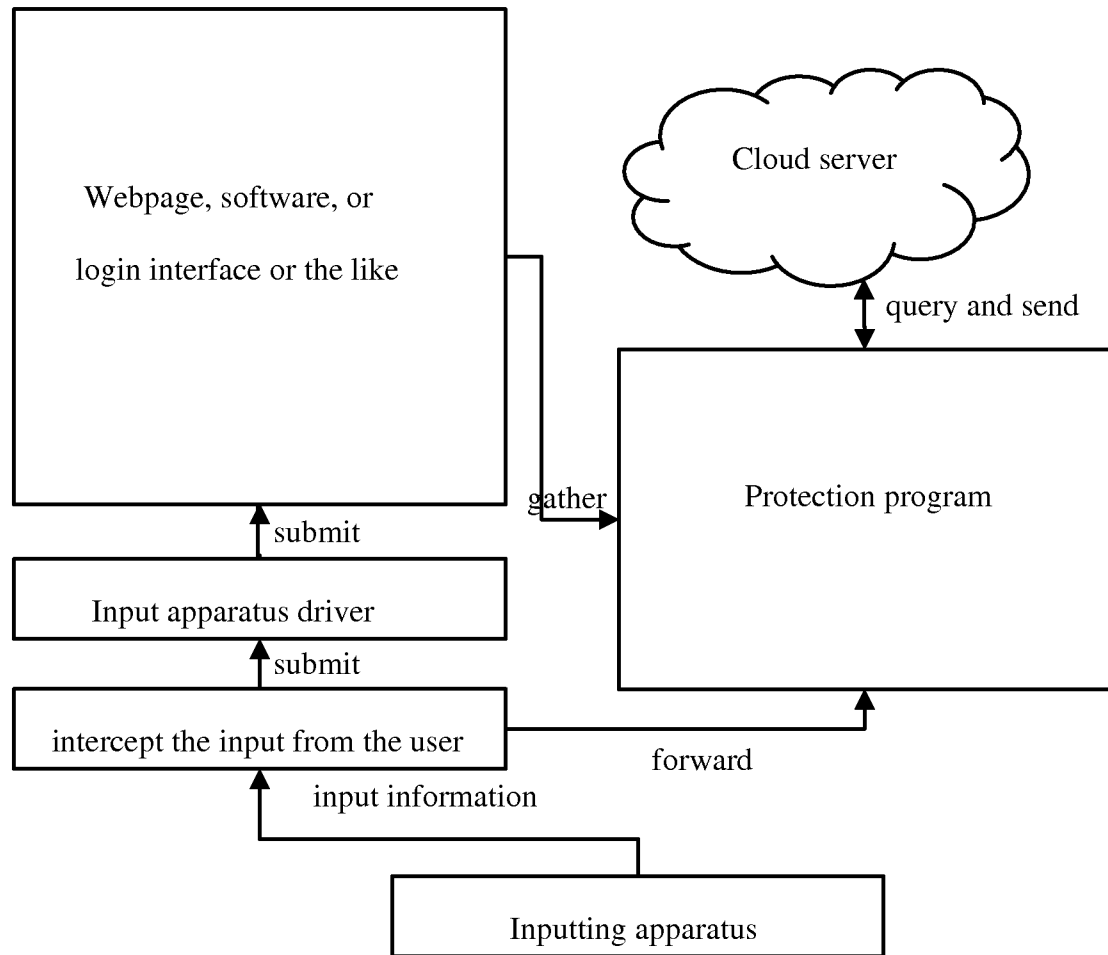


Fig. 3

— 3/4 —

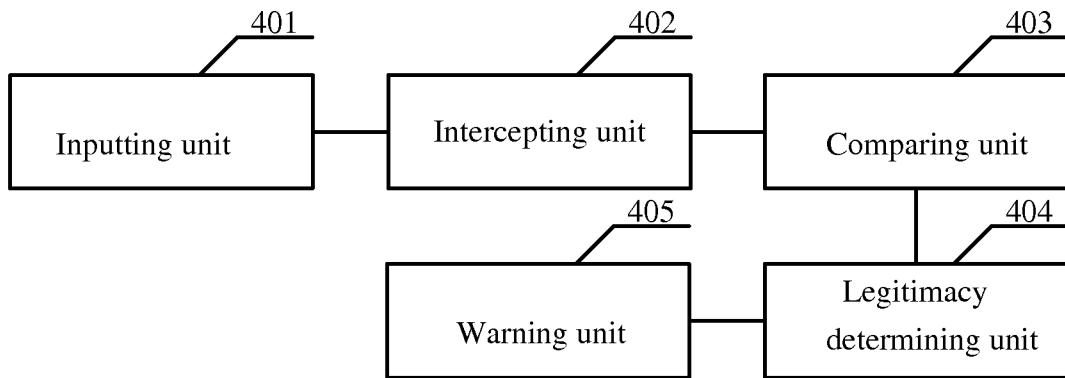


Fig. 4

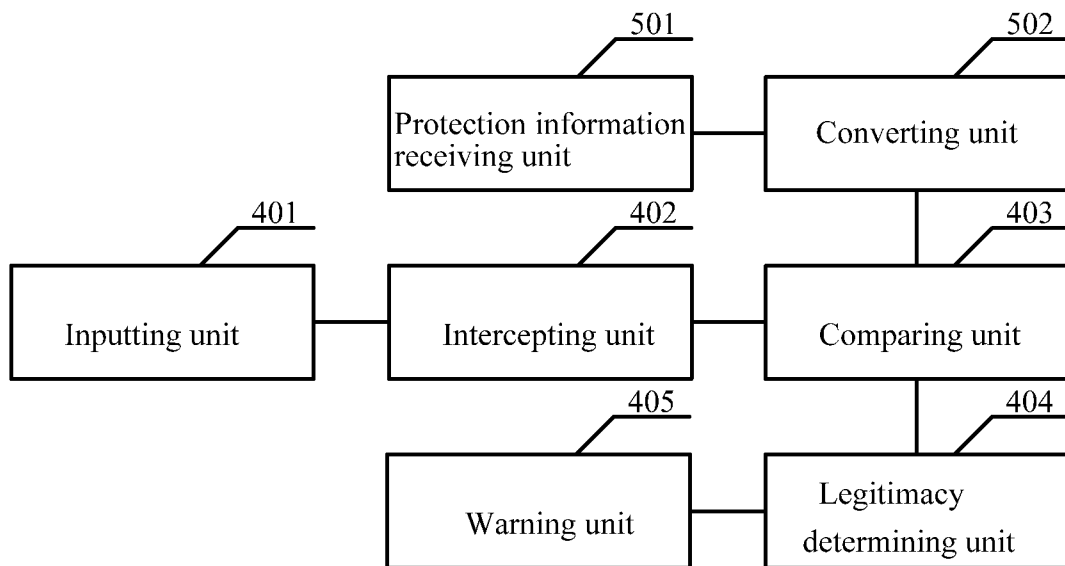


Fig. 5

—4/4—

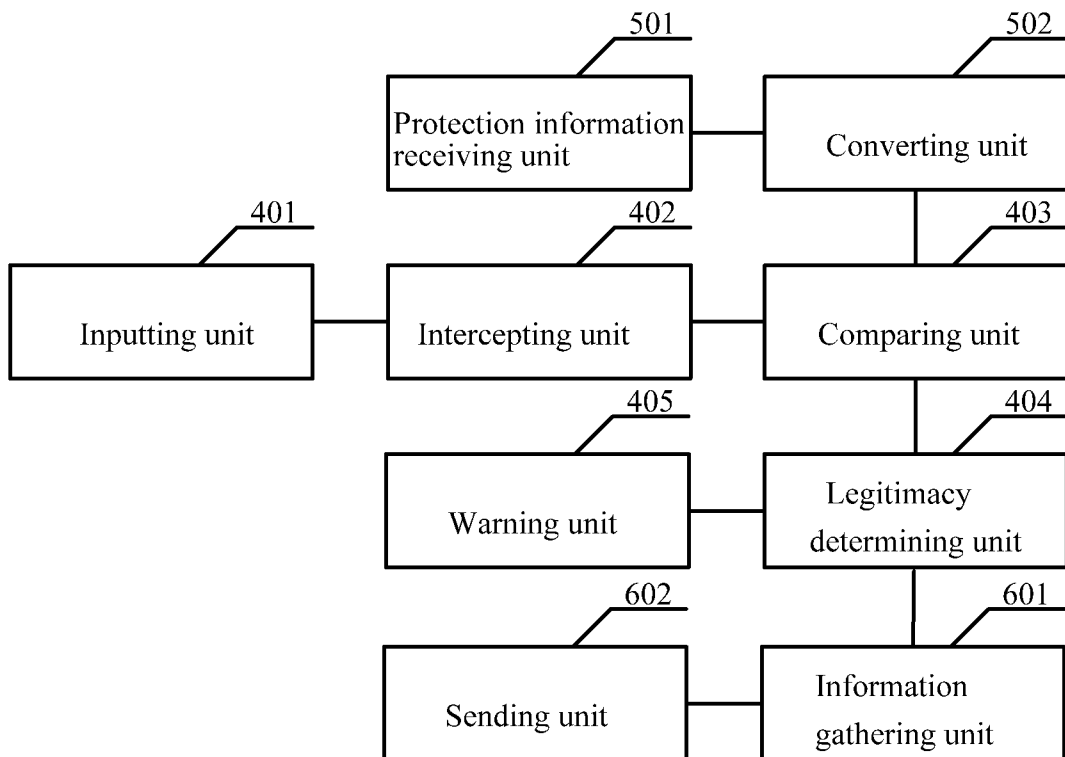


Fig. 6

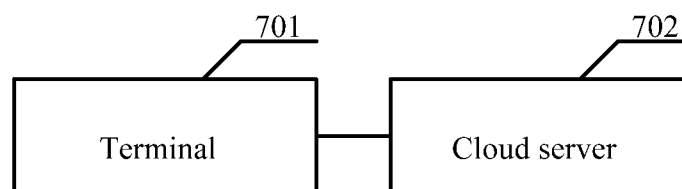


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/088567

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, 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)

CNABS, CNTXT, CNKI, VEN: trojan horse, intercept, web page, compare, match, phishing, virus, URL, input, password, illegitimate, non-reversible, hash, user, detection

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 101147138 A (DUAXES CORPORATION) 19 March 2008 (19.03.2008) Description, page 23, line 10- page 24, line 20	1-14
Y	CN 101390068 A (MICROSOFT CORPORATION) 18 March 2009 (18.03.2009) Description, page 11, lines 12-18 and figure 1	1-14
A	CN 101291227 A (XUE, Ming) 22 October 2008 (22.10.2008) the whole document	1-14

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

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
03 March 2014 (03.03.2014)

Date of mailing of the international search report
13 Mar. 2014 (13.03.2014)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
YU, Hongrui
Telephone No. (86-10)62411490

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2013/088567

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101147138 A	19.03.2008	CN 101147138 B	12.05.2010
		WO 2006087837 A1	24.08.2006
		EP 1850234 A1	31.10.2007
		JP WO2006087837S X	03.07.2008
		US 2009178116 A1	09.07.2009
		KR 20070103774 A	24.10.2007
		JP 4546998 B2	22.09.2010
CN 101390068 A	18.03.2009	US 8336092 B2	18.12.2012
		JP 5382850 B2	08.01.2014
		EP 1999609 A2	10.12.2008
		IN 200804240 P4	13.03.2009
		US 2007199054 A1	23.08.2007
		MX 2008010711 A1	31.08.2008
		US 8640231 B2	28.01.2014
		BR PI0707987A2	17.05.2011
		NO 20083486 A	24.11.2008
		KR 20080100204 A	14.11.2008
		AU 2007239055 A1	25.10.2007
		CA 2643294 A1	25.10.2007
		WO 2007120383 A2	25.10.2007
		JP 2009527855 A	30.07.2009
		WO 2007120383 A3	21.02.2008
		CN 101390068 B	08.12.2010
		WO 2009146655 A1	10.12.2009
CN 101291227 A	22.10.2008		

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/088567

Continuation of : cover sheet

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/10 (2006.01) i

G06F 17/00 (2006.01) i