

METHOD AND APPARATUS FOR PROCESSING WEBSITE ADDRESS RISK DETECTION

PRIORITY STATEMENT

5

The present disclosure claims the priority of a Chinese patent application No. 201110331356.X, titled “Method and Apparatus for Processing Website Address Risk Detection” filed with the State Intellectual Property Office of China by the same applicant on October 27, 2011.

10

TECHNICAL FIELD

15 The present disclosure relates to the field of computer technologies, and in particular, relates to a method and a device for processing URL risk detection.

BACKGROUND

20 In recent years, the computer industry has been growing rapidly. With the performance improvement and cost decrease of the products such as smart phones and pad computer, the smart mobile terminals occupy more and more of the market. The smart phone and pad computer can install third-party-provided programs such as application software and games that are selected by the user himself. Among those programs, the browser is one of the programs
25 that are installed most. The user can surf the internet freely anytime and anywhere by using a smart phone or a pad computer, attributing to the browser and the mobile communication network. In order to ensure the network security for the user, the browser on the mobile terminal needs to perform risk detection on the URL of the webpage requested by the user to browse.

In the existing technologies of URL risk detection, when a user accesses a Uniform Resource Locator (URL), the browser firstly detects whether there is a risk in the target webpage pointed to by the URL by a bound risk monitoring component. If there is no risk, the user's browsing operation is not disturbed, and the content of the webpage is shown to the user. If there is a risk, an interception webpage is popped up to warn the user that there is a risk in the target webpage to be browsed, and the browser shows the content of the webpage to be browsed to the user only if the user confirms that he is going to browse it.

The inventor of the present disclosure observes that there exist at least the following deficiencies in the prior art when making the present disclosure:

There is only one processing manner of intercepting loading of the URL with risks so the processing manner is simplex. When the URL is risky, the interception webpage will pop up at any case which needs to be confirmed by the user, so that the number of user's operations is increased, and prevent the user from further accessing. The risk detection for the URL is performed by the browser. That is, the browser in the mobile terminal is bound with a risk detection component, resulting in the corresponding program codes to be long and lack of expansibility.

SUMMARY OF THE DISCLOSURE

At least in order to diversify the interception manner, to reduce the number of user's operations, and to avoid too much harassment to the user, the present disclosure provides a method and a device for processing URL risk detection. The technical solutions include at least as follows.

In one aspect, there is provided a method for processing URL risk detection, comprising processes of: querying a risk type of a URL to be detected; querying a configuration file according to the risk type of the URL to obtain a risk level and a processing policy, the configuration file containing a correspondence relation among the risk type, the risk level and the processing policy; and processing the URL to be detected according to the risk level and the

processing policy.

In another aspect, there is also provided a device for processing URL risk detection, comprising: a query module which is configured to query a risk type of a URL to be detected; a configuration module which is configured to query a configuration file according to the risk type of the URL queried by the query module to obtain a risk level and a processing policy, the configuration file containing a correspondence relation among the risk type, the risk level and the processing policy; and a processing module which is configured to process the URL to be detected according to the risk level and the processing policy obtained by the configuration module.

The solutions provided by the embodiments of the present disclosure bring at least the following benefits.

The risk level is determined according to the risk type of the URL to be detected to obtain a processing policy, and different types of URLs are processed according to different processing policies, so that the processing manners are diversified when the URLs with risks are intercepted. In addition, when the risk type is determined, by matching with data in a pre-created risk database, the risk type of the URL to be detected is obtained without binding with a URL risk monitoring component, resulting in that the codes are concise and robust. Moreover, the URL and its corresponding processing policy are recorded locally, so that when said URL is processed again, it is not necessary to determine its risk type and risk level again, but it is directly processed according to a local query result, facilitating reducing CPU load and power consumption.

The above description is only a summary of the solutions of the present disclosure. In order to better understand the technical measures of the present disclosure to implement it according to the content of the specification, and to make the above and other objects, features and advantages of the present disclosure more easily understood, specific embodiments are described in detail in connection with the accompanying figures as follows.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a flowchart of a method for processing URL risk detection provided by one embodiment of the present disclosure;

Fig. 2 is a flowchart of a method for processing URL risk detection provided by another embodiment of the present disclosure;

Fig. 3 is a schematic diagram of structure of a device for processing URL risk detection provided by yet another embodiment of the present disclosure;

Fig. 4 is a schematic diagram of structure of another device for processing URL risk detection provided by yet another embodiment of the present disclosure.

DESCRIPTION OF THE EMBODIMENTS

In order to further describe the technical measures of the present disclosure employed to obtain the predetermined inventive object and its benefits, some embodiments, structures, features and benefits of the method and device for processing URL risk detection provided by the present disclosure are described in detail as follows.

The above and other objects, features and benefits will be clearly presented by the following detailed description of the preferable embodiments in connection with the figures. While the technical measures of the present disclosure employed to obtain the predetermined inventive object and its benefits can be understood in depth and specifically by the description of the embodiments, the accompanying figures are provided only for reference and illustration, but not to limit the present disclosure.

EMBODIMENT 1

The present embodiment provides a method for processing URL risk detection. Referring to Fig. 1, the method provided by the present embodiment is as follows.

101: querying a risk type of a URL to be detected.

In one embodiment, the present disclosure does not limit the manner for querying a risk

type of a URL to be detected, which includes but not limited to, matching the URL to be detected with data in a pre-created risk database to obtain the risk type of the URL to be detected, where a correspondence relation between the URL and the risk type is stored in the pre-created risk database.

5 102: querying a configuration file according to the risk type of the URL to be detected to obtain a corresponding risk level and processing policy.

Likewise, the present embodiment does not limit the risk level and its corresponding processing policy. The risk level includes but not limited to, four levels which are a safety level, an unknown level, a low-risk level and a high-risk level.

10 Accordingly, the processing policy corresponding to the safety level is to present a safety prompt and permit accessing the original webpage content of the URL to be detected.

The processing policy corresponding to the unknown level is to present an unknown-risk prompt and permit accessing the original webpage content of the URL to be detected.

15 The processing policy corresponding to the low-risk level is to pop up a prompt bar and permit accessing the original webpage content of the URL to be detected.

The processing policy corresponding to the high-risk level is to pop up a conception webpage and prevent from accessing the original webpage content of the URL to be detected.

It is noted that, the process 101 and process 102 can be performed locally, or can be performed on other devices via a network, which is not limited by the present embodiment.

20 103: processing the URL to be detected according to the risk level and the processing policy.

25 In one embodiment, since different risk levels and processing policies are obtained according to different risk types of the URLs in the above process 102, when the URL to be detected is processed, the URL to be detected is processed according to the obtained risk level and processing policy, so that different processing manners are obtained.

In another embodiment, when the processing policy is to present a safety prompt, to present a unknown-risk prompt, or to pop up a prompt bar, and to permit accessing the original webpage content of the URL to be detected, when the URL to be detected is processed according to the risk level and the processing policy. The method provided by the present embodiment also

enables to present the safety prompt in a fixed position, presenting the unknown-risk prompt in a fixed position, or popping up the prompt bar in a fixed position, and permitting accessing the original webpage content of the URL to be detected.

5 In another embodiment, when processing the URL to be detected according to the risk level and the processing policy, the method further includes: displaying corresponding detailed risk information. The detailed risk information includes the risk type, the risk level, and a risk content description.

10 In another embodiment, after processing the URL to be detected according to the risk level and the processing policy, the method provided by the present embodiment further includes:

recording the URL to be detected and its corresponding processing policy locally; and accordingly directly querying the processing policy corresponding to the URL to be detected locally and processing the URL to be detected according to the query result when the URL to be detected is processed next time.

15 The method provided by the present embodiment has the following benefits.

The risk level is determined according to the risk type of the URL to be detected to obtain a corresponding processing policy, and different types of URLs are processed according to different processing policies, so that the processing manners are diversified when the URLs with a risk is intercepted. In addition, when the risk type is determined, by matching with data in a pre-created risk database, the risk type of the URL to be detected is obtained without the need of binding a URL risk monitoring component, resulting in that the codes are concise, forceful, and robust. Moreover, the URL to be detected and its corresponding processing policy are recorded locally, so that when said URL is processed again, it is not necessary to determine its risk type and risk level again, but it is directly processed according to a local query result, facilitating
25 reducing CPU load and power consumption.

EMBODIMENT 2

The present embodiment provides a method for processing URL risk detection, referring to Fig. 2. The method provided by the present embodiment is as follows.

201: querying a risk type of a URL to be detected.

The URL to be detected is a URL determined according to a request made by a user for browsing a webpage after the request is received. When querying the risk type of the URL to be detected, the present embodiment does not limit the manner for querying the risk type of the URL, which includes but not limited to: by matching the URL to be detected with a data in a pre-created risk database, the URL is detected to obtain the risk type of the URL, wherein a correspondence relation between the URL and the risk type is stored in the pre-created risk database. If no matched risk type is obtained from the risk database, that is, said URL is not recorded in the risk database, and the correspondence relation between the URL and the risk type is not found in the risk database, then the risk type of such a URL is set as an unknown risk type by default.

The risk type may include a type of malicious advertisement, a type of counterfeiting, a type of fraudulency by stealing an account, and a type of threatening the account security, etc. Other risk types may also be included. The present embodiment does not limit the risk type particularly.

In addition, the data in the risk database may be updated automatically and periodically, or updated through manual aid or the like. The present embodiment does not limit the time of the update, for example, the data in the database may be updated automatically every 30 minutes, or the data is added manually, and so on. The present embodiment does not make limit to data processing including updating.

202: querying a configuration file according to the risk type of the URL to be detected to obtain a risk level and a processing policy.

For this process, the configuration file may be created in advance, which includes a correspondence relation among the risk type, the risk level and the processing policy. Therefore, after the risk type of the URL to be detected is determined, when the configuration file is queried according to the risk type of the URL, the risk level and the processing policy are obtained. The present embodiment does not limit the specific form of the configuration file, and does not limit the manner of querying the configuration file, either. In the case that the risk type is unknown, when the configuration file is queried according to the risk type of the URL, the

unknown risk type is set as an unknown-risk level by default.

The risk level includes but not limited to: the four levels which can be a safety level, an unknown level, a low-risk level and a high-risk level. Each risk type corresponds to a risk level, for example, the malicious advertisement corresponds to the low-risk level, and the counterfeiting, the fraudulency by stealing an account, and the threatening account security corresponds to the high-risk level. In practical application, the risk level may be further fractionized. The present embodiment does not limit specifically the types of the risk level, and the correspondence between each risk type and the risk level to which it belongs, and does not limit its corresponding processing policy.

Taking the risk level including but not limited to the four levels which are the safety level, the unknown level, the low-risk level and the high-risk level as an example, the processing policies corresponding to the respective risk levels include the followings:

The processing policy corresponding to the safety level is to present a safety prompt and permit accessing the original webpage content of the URL to be detected.

The processing policy corresponding to the unknown level is to present an unknown-risk prompt and permit accessing the original webpage content of the URL to be detected.

The processing policy corresponding to the low-risk level is to pop up a prompt bar and permit accessing the original webpage content of the URL to be detected.

The processing policy corresponding to the high-risk level is to pop up an interception webpage and prevent from accessing the original webpage content of the URL to be detected.

It is noted that, the process 201 and process 202 may be performed locally, or may be performed on other devices via a network. For example, if the above risk database and configuration file are stored locally, then the risk type, the risk level and the processing policy of the URL may be queried locally. As another example, in order to reduce the local storage space, the above risk database and the configuration file may be stored in other devices over a network. The risk type, the risk level and the processing policy of the URL to be detected may be queried by coupling to the other devices through the network. The present embodiment does not limit the implementation to be specifically employed.

203: processing the URL according to the risk level and the processing policy.

For this process, when the URL to be detected is processed according to the risk level and the processing policy, an exemplary process is as follows:

a) for the safety level, presenting a safety prompt to the user, and permitting accessing the original webpage content of the URL to be detected;

5 b) for the unknown level, presenting an unknown-risk prompt to the user, and permitting accessing the original webpage content of the URL to be detected;

c) for the low-risk level, displaying the original webpage content to the user, and popping up a prompt bar simultaneously;

10 d) for the high-risk level, popping up an interception webpage, and preventing the user from accessing the original webpage content.

As a solution of the above processes for the URL, for the processing manners of presenting the safety prompt, presenting the unknown-risk prompt, and popping up the prompt bar, the method provided by the present embodiment also supports presenting the safety prompt in a fixed position, presenting the unknown-risk prompt in a fixed position, or popping up the prompt bar in a fixed position. That is, the safety prompt, the unknown-risk prompt, and the prompt bar do not change their positions as the display of webpage slides, so that the risk of being counterfeited by a malicious URL is reduced. In addition, a manner of manually screening the safety prompt, the unknown-risk prompt, or the prompt bar by the user is also supported. After the safety prompt, the unknown-risk prompt, or the prompt bar is screened, 15 the safety prompt, the unknown-risk prompt, or the prompt bar is not displayed any more during the processing of the URL to be detected, so the harassment to the user is reduced.

In addition, when the URL to be detected is processed according to the risk level and the processing policy, detailed risk information may be displayed. The present embodiment does not limit the specific content of the detailed risk information, which includes but not limited to 25 the risk type, the risk level, and a risk content description.

For example, when a URL “A” to be detected is processed, if the risk type of the URL “A” to be detected is a risk URL with the malicious advertisement of which the risk level is “low risk”, the processing policy corresponding to the low-risk level is to display the original webpage content, and pop up a prompt bar simultaneously, and the risk content description may be “the

website has malicious advertisement or illegal link to seduce a risky operation”, then when the URL “A” to be detected is processed according to the risk level and the processing policy of the URL “A” to be detected, in addition to displaying the original webpage content corresponding to the URL “A” to be detected and popping up the prompt bar, its risk type, risk level, and risk content description are also presented on the webpage. The specific presentation manner may be: displaying on the prompt bar, or on a separate window. The present embodiment does not limit the specific presentation manner.

204: recording the URL to be detected and its corresponding processing policy locally; and directly querying the processing policy corresponding to the URL to be detected locally and processing the URL to be detected according to the query result when processing the URL to be detected next time.

In one embodiment, when the URL to be detected and its corresponding processing policy are recorded locally, a black list and/or a white list may be employed. The white list stores the URLs with no risk and their corresponding processing policies, and the black list stores the URLs with risks and their corresponding processing policies, such that when the URL to be detected is processed next time, the processing policy corresponding to the URL may be queried in the black list or the white list, and the URL is processed according to the query result.

For example, when the user opens a window to visit some webpage again, the URL of the webpage is compared with the URLs recorded in the black/white list. If the URL of the webpage is recorded in the black/white list, the webpage is processed directly according to the processing policy recorded in the black/white list. If the URL is not recorded in the black/white list, a request for the risk detection of the URL is initiated again, that is, the procedures of the process 201 to 203 are performed.

The method provided by the present embodiment has the following benefits.

The risk level is determined according to the risk type of the URL to be detected to obtain a processing policy, and different types of URLs are processed according to different processing policies, so that the processing manners are diversified when the URLs with risks are intercepted. In addition, when the risk type is determined, by matching with data in a pre-created risk database, the risk type of the URL is obtained without the need of binding a URL risk monitoring

component, resulting in that the codes are concise and robust. Moreover, the URL and its corresponding processing policy are recorded locally, so that when said URL is processed again, it is not necessary to determine its risk type and risk level again, but it is directly processed according to a local query result, facilitating reducing CPU load and power consumption.

5

EMBODIMENT 3

Referring to Fig. 3, the present embodiment provides a device for processing URL risk detection. The device comprises the following modules: a query module 301 which is configured to query a risk type of a URL to be detected; a configuration module 302 which is configured to
10 determine a risk level according to the risk type of the URL queried by the query module 301, and query a corresponding configuration file to obtain a processing policy, the configuration file includes a correspondence relation among the risk type, the risk level and the processing policy; and a processing module 303 which is configured to process the URL to be detected according to the risk level and the processing policy obtained in the configuration module 302.

15 The query module is used for matching the URL to be detected with data in a pre-created risk database, to obtain the risk type of the URL to be detected. A correspondence between the URL and the risk type is stored in the risk database built in advance.

The processing module 303 is used for presenting the safety prompt in a fixed position, presenting the unknown-risk prompt in a fixed position, or popping up the prompt bar in a fixed
20 position, and permitting accessing the original webpage content of the URL to be detected.

In one embodiment, the processing module 303 is further used for displaying detailed risk information including the risk type, the risk level, and a risk content description.

Referring to Fig. 4, the device also comprises: a recording module 304 which is configured to record the URL to be detected and its corresponding processing policy locally.

25 The processing module 303 is further used for directly querying the processing policy corresponding to the URL to be detected locally and processing the URL according to the query result when the URL is processed next time.

The present embodiment has the following benefits.

The risk level is determined according to the risk type of the URL to be detected to obtain

a processing policy, and different types of URLs are processed according to different processing policies, so that the processing manners are diversified when the URLs with risks are intercepted. In addition, when a risk type is determined, by matching with data in a pre-created risk database, the risk type of the URL to be detected is obtained without binding with a URL risk monitoring component, resulting in that the codes are concise, and robust. Moreover, the URL and its corresponding processing policy are recorded locally, so that when said URL is processed again, it is not necessary to determine its risk type and risk level again, but it is directly processed according to a local query result, facilitating reducing CPU load and power consumption.

It is noted that, when the method for processing URL risk detection provided by the above embodiment performs the process for the URL risk detection, the above individual functional modules are illustrated only for example. In a practical application, the above functions may be allocated to be implemented by different function modules as required. That is, the internal structures of the above functional modules may be fractionized into different functional modules to implement the above-described functions or a part thereof, or the above functional modules may be combined into one module to implement the above functions or a part thereof while saving system resources. Further, the device for processing URL risk detection and the method for processing URL risk detection provided by the above embodiments have the same technical concept. The detailed implementation of the device refers to the method embodiments, and is not described in detail herein.

It is understood by those ordinarily skilled in the art that the processes or a part thereof of the above embodiments may be implemented by hardware, or by a program instructing related hardware. The program may be stored in a computer readable storage medium, which may be read-only memory, magnetic disk, optical disk, or the like.

The above description is only embodiments of the present disclosure, but not as limitation to the present disclosure in any form. Although the present disclosure has been disclosed in form of embodiments as the above, the embodiments are not used to define the present disclosure. Anyone skilled in the art can make some changes or decorations according to the above disclosed technical content as equivalent embodiments without departing from the technical scope of the present disclosure. Any simple modifications, equivalent changes, and

decorations to the above embodiments substantially according to the techniques of the present disclosure without departing from the technical solution content of the present disclosure fall into the scope of the technical solutions of the present disclosure.

5 INDUSTRIAL APPLICABILITY

According to the present disclosure, the risk level is determined according to the risk type of the URL to be detected to obtain a corresponding processing policy, and different types of URLs are processed according to different processing policies, so that the processing manners are diversified when the URLs with risks are intercepted. In addition, when a risk type is
10 determined, by matching with data in a pre-created risk database, the risk type of the URL to be detected is obtained without binding with a URL risk monitoring component, resulting in that the codes are concise, and robust. Moreover, the URL and its corresponding processing policy are recorded locally, so that when said URL is processed again, it is not necessary to determine its risk type and risk level again, but it is directly processed according to a local query result,
15 facilitating reducing CPU load and power consumption.

WHAT IS CLAIMED IS:

1. A method for processing URL risk detection, comprising processes of:

5 querying a risk type of a URL to be detected;

querying a configuration file according to the risk type of the URL to be detected to obtain a risk level and a processing policy, the configuration file containing a correspondence relation among the risk type, the risk level and the processing policy; and

processing the URL to be detected according to the risk level and the processing policy.

10 2. The method according to claim 1, wherein said querying a risk type of a URL to be detected comprises a process of:

matching the URL to be detected with data in a pre-created risk database, to obtain the risk type of the URL to be detected, wherein a correspondence between the URL and the risk type is stored in the pre-created risk database.

3. The method according to claim 1, wherein the risk level comprises four levels which are a safety level, an unknown level, a low-risk level and a high-risk level,

the processing policy corresponding to the safety level is to present a safety prompt and permit accessing the original webpage content of the URL to be detected;

20 the processing policy corresponding to the unknown level is to present an unknown-risk prompt and permit accessing the original webpage content of the URL to be detected;

the processing policy corresponding to the low-risk level is to pop up a prompt bar and permit accessing the original webpage content of the URL to be detected;

25 the processing policy corresponding to the high-risk level is to pop up an interception webpage and prevent from accessing the original webpage content of the URL to be detected.

4. The method according to claim 3, wherein when the processing policy is to present a safety prompt, present a unknown-risk prompt, or pop up a prompt bar, and permit accessing the

original webpage content of the URL to be detected, said processing the URL to be detected according to the risk level and the processing policy comprises a process of:

presenting the safety prompt in a fixed position, presenting the unknown-risk prompt in a fixed position, or popping up the prompt bar in a fixed position, and permitting accessing the original webpage content of the URL to be detected.

5. The method according to claim 1, wherein when processing the URL to be detected according to the risk level and the processing policy, further comprising a process of:

displaying a detailed risk information containing the risk type, the risk level, and a risk content description.

6. The method according to claim 1, wherein after processing the URL to be detected according to the risk level and the processing policy, further comprising a process of:

recording the URL to be detected and its processing policy locally;
directly querying the processing policy corresponding to the URL to be detected locally, and processing the URL to be detected according to the query result when the URL to be detected is processed next time.

7. A device for processing URL risk detection, comprising:

a query module configured to query a risk type of a URL to be detected;
a configuration module configured to query a configuration file according to the risk type of the URL queried by the query module to obtain a risk level and processing policy, the configuration file containing a correspondence relation among the risk type, the risk level and the processing policy; and
a processing module configured to process the URL to be detected according to the risk level and the processing policy obtained by the configuration module.

8. The device according to claim 7, wherein the query module is further configured to match the URL to be detected with data in a pre-created risk database, to obtain the risk type of

the URL to be detected, a correspondence between the URL and the risk type is stored in the pre-created risk database.

5 9. The device according to claim 7, wherein the processing module is further configured to present the safety prompt in a fixed position, present the unknown-risk prompt in a fixed position, or pop up the prompt bar in a fixed position, and permit accessing the original webpage content of the URL to be detected.

10 10. The device according to claim 7, wherein the processing module is further configured to display a detailed risk information containing the risk type, the risk level, and a risk content description.

11. The device according to claim 7, further comprising:
a recording module configured to record the URL to be detected and its processing policy
15 locally,
wherein the processing module is further configured to directly query the processing policy corresponding to the URL to be detected locally, and process the URL according to the query result when the URL to be detected is processed next time.

20