(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2008 (24.07.2008)

PCT

(10) International Publication Number
WO 2008/086924 A1

(51) International Patent Classification:
G06F 21/20 (2006.01) *G06F 17/30* (2006.01)
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2007/063845

(22) International Filing Date:
12 December 2007 (12.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/623,516 16 January 2007 (16.01.2007) US

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; P.O. Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **REUMANN, John** [DE/US]; 19 Cleveland Drive, Croton-on-Hudson, New York 10520 (US). **VERMA, Dinesh** [US/US]; 56 Kisco Park Drive, Mount Kisco, New York 10549 (US).

(74) Agent: **WILLIAMS, Julian, David**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester Hampshire SO21 2JN (GB).

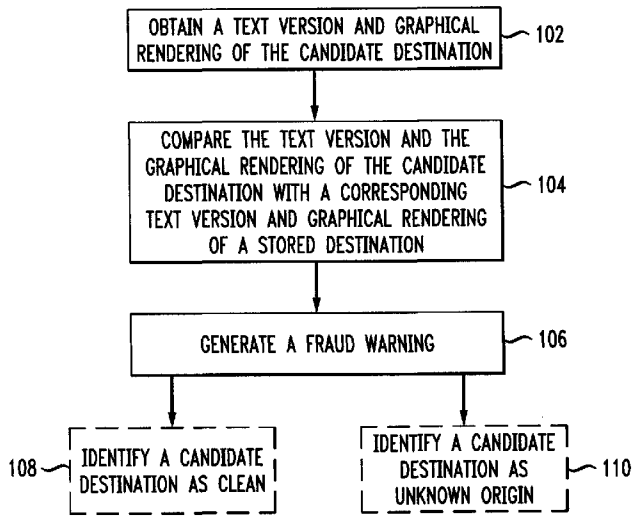
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR DETECTING COMPUTER FRAUD

FIG. 1



(57) Abstract: Techniques are provided for detecting computer fraud. The techniques include obtaining a text version of a candidate destination and a graphical rendering of the candidate destination, comparing the text version of the candidate destination and the graphical rendering of the candidate destination with a corresponding text version of a stored destination and a corresponding graphical rendering of the stored destination, and generating a fraud warning if the graphical rendering of the candidate destination is substantially similar to the graphical rendering of the stored destination while the text version of the candidate destination differs substantially from the corresponding text version of the stored destination.

WO 2008/086924 A1

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

METHOD AND APPARATUS FOR DETECTING COMPUTER FRAUD

Field of the Invention

The present invention generally relates to information technology, and, more particularly, to a method and apparatus for detecting computer fraud.

Background of the Invention

When a user receives an e-mail or other communication which appears to contain a link to web site "A," but is redirected to an impersonated version of web site "A," the user is said to be the subject of a web site "phishing" attack. Users would like to know whether a site that they are visiting is a well-known, legitimate site, or a site that looks like a legitimate site but is not located at the same location as the expected legitimate version of the web site.

A user may initiate a transfer of a web page into a browser by typing the URL, following a link, following a link embedded in an email or an instant messaging session, or via a redirect from another page. As a result, the browser will resolve the protocol to be used to look up the destination page, contact the domain name system (DNS) to resolve the destination host, connect to the internet protocol (IP) address named by the DNS look-up, download the page content, render the page and simultaneously execute any embedded scripts where appropriate. The content of this page can be forged in many ways.

There are known browser tool bars that merely extract the uniform resource locator (URL) from the web browser and normalize it to present to the user the effective site to which he or she is connected. While this may eliminate attacks in which a URL overfills the browser location window by reducing the site name, it does not solve the problem in which two very similar-looking domain names are being used. Since the information about effective sites is fairly coarse, it is possible for an attacker to get a closely looking domain name in the same geography (e.g. United States) and then try to confuse such phishing detectors. Furthermore, with increasing globalization, it is quite likely, for example, that a legitimate site for a U.S.-based bank is located in another country such as, for example, India or Brazil, which makes for several false alarms. Using the known techniques, the user would still be lead to believe that he or she is contacting the correct web site. The known techniques rely on the user to check the domain name for every visited web site. Furthermore, the known techniques only extract the information delivered in the actual URL,

and therefore, these techniques are not safe in the case of DNS poisoning attacks, in which the actual domain names are forced to resolve to a subverted site IP address that is different from the target that the user intended when he or she typed the name into the browser location bar.

It would thus be desirable to overcome the limitations in previous approaches.

Summary of the Invention

Principles of the present invention provide techniques for detecting computer fraud. An exemplary method (which can be computer-implemented) for detecting computer fraud, according to one aspect of the invention, can include steps of obtaining a text version of a candidate destination and a graphical rendering of the candidate destination, comparing the text version and graphical rendering of the candidate destination with a corresponding text version and a corresponding graphical rendering of a stored destination, and generating a fraud warning if the graphical rendering of the candidate destination is substantially similar to the graphical rendering of the stored destination while the text version of the candidate destination differs substantially from the corresponding text version of the stored destination.

In one aspect of the invention, the candidate destination and stored destination are represented as URLs. Also, in another aspect of the invention, the techniques for detecting computer fraud are automatically executed upon loading a web page associated with a candidate destination. The techniques may also be executed by using a button that is shown to a user in at least one of a window and a status bar external to a browser window associated with the candidate destination. Furthermore, in another aspect of the invention, a fraud warning may be generated via a visual prompt displayed to a user in at least one of a window and a status bar external to a browser window associated with the candidate destination. In yet another aspect of the invention, the candidate destination is identified as clean if all determined organizations match to a corresponding stored organization and if the stored organization is not substantially similar to another organization ranked as more popular in a database. The candidate destination is identified as unknown if visual cues can not be matched to an organization, but for which the candidate destination coincides with a visual URL and destination unlikely to be a phishing destination.

In an embodiment of the invention, an exemplary method of generating a database, or white-list, of destinations to be protected against computer fraud can include the steps of

generating at least one category of destinations to be protected, and retrieving at least one list of destinations belonging to the at least one category. In one aspect of the invention, the step of retrieving at least one list of destinations belonging to the at least one category comprises obtaining a first list of destinations and a second list of destinations, and merging the first and second lists of destinations. Also, in another aspect of the invention, the retrieving step comprises accessing an Internet search engine and/or accessing an Internet indexing service.

At least one embodiment of the invention can be implemented in the form of a computer product including a computer usable medium with computer usable program code for performing the method steps indicated. Furthermore, at least one embodiment of the invention can be implemented in the form of an apparatus including a memory and at least one processor that is coupled to the memory and operative to perform exemplary method steps.

At least one embodiment of the invention may provide one or more beneficial technical effects, such as, for example, detecting computer fraud when the candidate or phishing entity comprises a domain name that is very similar-looking to that of an intended or stored entity. Also, at least one embodiment of the invention may provide the beneficial effect of detecting computer fraud in situations in which an intended domain name is forced to resolve to a candidate or phishing destination that is different from the target that a user intended when the user typed the name into the browser location bar.

These and other objects, features and advantages of the present invention will become apparent from the following detailed description of illustrative embodiments thereof, which is to be read in connection with the accompanying drawings.

Brief Description of Drawings

FIG. 1 is a flow diagram illustrating an exemplary method for detecting computer fraud, according to one aspect of the invention;

FIG. 2 is a block diagram illustrating an exemplary system that can execute an exemplary method for detecting computer fraud, according to another aspect of the invention;

FIG. 3 is a flow diagram illustrating an exemplary method for generating a database of destinations to be protected against computer fraud, according to yet another aspect of the invention; and

FIG. 4 is a system diagram of an exemplary computer system on which at least one embodiment of the present invention can be implemented.

Detailed Description of Preferred Embodiments

An embodiment of the invention constructs at least one site signature based on what the user can view in his or her browser window. A software agent that computes these signatures also maintains a database, or a white-list, of well-known graphical and other signatures for websites. Whenever signatures are computed for a site, they are compared against the signatures in the database. If some signatures match those of well-known websites while other signatures are either not registered or match sources of phishing attacks (e.g., certain domain names, IP address ownership), the site phishing score will increase and the browser status bar will present a symbol to indicate the risk of phishing (e.g., <><).

A common form of phishing attacks comprises including a link to a site that appears to be from the web site "A", but in reality points to some other web-site. With rich text and Hypertext Markup Language (HTML) encoding of e-mail, a link may typically be represented using the following syntax or equivalent:

 Text Displayed to User

In most readers, a user is shown only the string marked "Text Displayed to User", and the "target link" is not shown. While some users may actually examine the link, some effort is made to disguise the link so that the "target link" appears to be somewhat similar to the link to the real site that would be indicated as "Text Displayed to the User". Some examples of this type of masquerading are provided below.

As means of example only, an e-mail may contain an embedded link Acme Investments and it may thus purport to come from the Acme Investments website, http://www.acmeinvestments.com. When the user accesses this link in the browser, he is taken to the site www.acme1nvestments.com. Unless the user is diligent enough to notice that the ninth letter in the URL is a 1 (numeric one) instead of an "i," he or she would mistakenly believe that he/she is at the website of Acme Investments.

A particular insidious case of such impersonation is made possible due to the standards for encoding of characters in multiple languages. This standard, the Internationalized Domain Names allows for representing domain names (the name of the

machine in the URL) using uni-code characters in languages other than English. For example, Unicode character U+0430, Cyrillic small letter a ("a"), can look identical to Unicode character U+0061, Latin small letter a, ("a") which is the lowercase "a" used in English. Thus, a phishing email may refer to a URL www.<a>cmeinvestments.com where <a> refers to the Cyrillic small letter a, but the user of a website would not be able to distinguish it from the URL of www.acmeinvestments.com. Several browsers are vulnerable to such masquerading.

There are other ways of tricking a user to go to a website different than that to which one intended to go, including schemes that compromise the domain name system (e.g. a virus could be used to overwrite the hosts file or the browser cache). However, such an attack requires compromising the security of a machine, and is less likely to be used. Examples of attacks of this nature are described in the paragraphs below for completeness. Most commonly, techniques for phishing rely on tricking the user about accessing a different URL, since that can be done by means of a misleading e-mail without sophisticated attacks on the operating system security.

For example, one way that the page can be forged is via an attack on the above-noted step to resolve the protocol to be used to look up the destination page. It is possible to redirect the user to a page on the user's own hard disk by pointing the browser to a "file:/" reference. This kind of redirection can be especially dangerous because it circumvents most browser security mechanisms. The attacker must be able to plant code in the user's file system at a known location (e.g., in the browser cache).

Another way, for example, that the page can be forged is via an attack on the above-noted step to contact the DNS to resolve the destination host. The attacker may "poison" a DNS server to redirect the user to an IP address that is controlled by the attacker instead of forwarding the browser to the requested location. For example, a user could be directed to IP address 10.1.1.1 if the IP address mapping for www.acmeinvestments.com were undermined.

As another example, one way that the page can be forged is via an attack on the above-noted step to connect to the IP address named by the DNS look-up. An IP address take-over can be initiated by redirecting routes or man-in-the-middle attacks where the attacker owns a machine on the path to the actual target of the web page download. In these

cases, the attacker can act as a proxy and control and intercept the input and/or output (I/O) from a user's browser.

Yet another way, for example, that the page can be forged is via an attack on the above-noted step to render the page and simultaneously execute any embedded scripts where appropriate. The attacker may not be able to execute any of the attacks noted above and therefore may be forced to conceal the fact that it (the attacker) has redirected the user to the attacker's own forged website by impersonating the look of the forged website and by hiding the evidence that shows the user that he or she is not currently browsing the website that he or she expects to be browsing based on the content viewed in the browser window.

FIG. 1 shows a flow diagram illustrating a method for detecting computer fraud, according to one embodiment of the invention. Step **102** includes obtaining a text version of a candidate destination and a graphical rendering of the candidate destination. A candidate destination is a network address or a Universal Resource Identifier (URI) or a Uniform Resource Locator (URL) to which a portion of a message is directed. A text version of the candidate destination is the rendering of the destination using a textual representation standard such as, for example, ASCII or Unicode. A graphical rendering is the representation of the candidate destination in an image format, e.g. as a gif, jpeg or tiff format. Step **104** includes comparing the text version of the candidate destination and the graphical rendering of the candidate destination with, respectively, a corresponding text version of a stored destination and a corresponding graphical rendering of the stored destination. A stored destination can be a network address, URI or URL which is intended to be protected against fraud and is maintained in a repository at the computer. Such a repository may be a text file, a local database, an XML file, etc. Step **106** includes generating a fraud warning if the graphical rendering of the candidate destination is substantially similar to the graphical rendering of the stored destination while the text version of the candidate destination differs substantially from the corresponding text version of the stored destination. Optionally, the method illustrated in **FIG. 1** can also include step **108**, identifying a candidate destination page as clean if all of the determined organizations match to a corresponding stored organization identity and/or identification (ID) in the repository and if the stored organization is not too similar to another organization that is ranked as more popular in the repository database. The method illustrated in **FIG. 1** can also optionally include step **110**, identifying the candidate destination page as "unknown origin"

if the visual cues could not be matched to an organization, but for which the candidate destination coincides with the visual URL and whose destination is not a likely phishing destination.

FIG. 2 shows a block diagram illustrating an exemplary system that can execute an exemplary method for detecting computer fraud, according to one embodiment of the invention. The system **200** comprises components including a database, or repository, **202**, which may comprise at least one well-known destination, IP addresses, URL prefixes or patterns, content landmarks (e.g., logos), and IP address ownership records. The system **200** also comprises an anti-phishing plug-in **224**, and a browser **226**. The system **200** also comprises appropriate software, hardware, or mixed hardware-software modules to execute method steps as described below.

Step **228** comprises a visual analysis phase. Step **228** may include the steps of URL rendering **204**, URL destination estimation **206**, content landmark extraction **208**, and content origin estimation **210**. Step **230** comprises a physical analysis. Step **230** may include the steps of an IP address origin test **212**, and DNS name similarity scoring **214**. Step **216** includes producing a visual-to-physical discrepancy score. Step **218** includes producing score visualization. Step **220** comprises a phishing alerter process, which may include producing a phishing alert pop-up **222** at a randomized location. A randomized location may comprise generating a fraud warning or phishing alert pop-up **222** via a visual prompt displayed to the user in at least one of a window and a status bar external to the browser window associated with the candidate destination, wherein the window is opened in a randomly placed window separate from the browser to prevent overlay attacks by the phishers.

When a website is completely rendered in the browser, a software agent takes a snapshot of the information displayed in the browser window. This snapshot includes the source content comprising, for example, images, location URL, and displayed text. The software agent also takes a screen-shot of the image rendered inside the browser.

One aspect of the invention is to maintain a database of existing known URLs targeted for phishing attacks, and the graphical rendering of those URLs, using a predefined convention. The inventive techniques execute the following steps on each web page that is downloaded or for which the user initiates a check. The techniques include obtaining a text version of a candidate destination and a graphical rendering of the candidate destination,

comparing the text version of the candidate destination and the graphical rendering of the candidate destination with, respectively, a corresponding text version of a stored destination and a corresponding graphical rendering of the stored destination, and generating a fraud warning if the graphical rendering of the candidate destination is substantially similar to the graphical rendering of the stored destination while the text version of the candidate destination differs substantially from the corresponding text version of the stored destination.

In one embodiment of the invention, the candidate destination and the stored destination are represented as URLs. The inventive techniques may be automatically executed upon loading a web page associated with the candidate destination. Also, the inventive techniques may be executed by using a test phishing button that is shown to the user in a window or status bar external to the browser window associated with the candidate destination in order to prevent overlaying attacks by phishers. In another aspect of the invention, the step of comparing the text version and the graphical rendering of the candidate destination with the corresponding text version and graphical rendering of the stored destination is performed on a subset of the candidate destination and the stored destination, wherein a subset may comprise, for example, the prefix and/or suffix of a URL.

In one aspect of the invention, the inventive techniques allow for a web page to be downloaded through a browser. Upon successfully downloading a page, but before the page's onLoad() Java and other scripts execute, the anti-phishing plug-in **224** will extract the URL that is stored in the browser location field. The plug-in **224** allows the page to be fully rendered and extracts the visible browser location by taking a snapshot image of the browser window. The snapshot function is used, preferably, because there are known attacks in which a phishing web site disables the browser toolbar and present its own (e.g. JavaScript version) of the location field to the user.

The plug-in **224** will read the image map of the browser toolbar associated with the candidate destination and determine a character representation of the image map by using an optical character recognition (OCR) algorithm for character recognition. In one aspect of the invention, the inventive techniques include parsing the character representation, and also normalizing the character representation by lowercasing all characters. The inventive techniques can also include generating various derivative versions of the candidate destination through character permutation and substitution based on known optical similarity and identification in a repository **202** containing well-known destination URLs via a search

of the repository **202** or database. The inventive techniques record any matches between the well-known destinations and versions of the candidate destinations.

The plug-in **224** will take a snapshot of the web page window associated with the candidate destination, execute OCR on the entire rendered image and store the recognized words into an array. The plug-in **224** performs these actions because phishers can substitute graphical elements for plain text to evade recognition by automated tests.

In another aspect of the invention, the inventive techniques read only the text of the web page associated with the candidate destination into the array. Also, an algorithm computes the word-distribution signature of the web page by extracting a word histogram. Such inventive techniques compare the extracted word histogram to the histograms of well-known destination web pages that are recorded in the database or repository, record any matches between the extracted word histogram and histograms of well-known destination web pages, and sort the matches by percentage overlap in the word histogram. In another aspect of the invention, the inventive techniques extract the estimated sources based on the closest matches in content overlap on the basis of text analysis, and record the sources as potential origins for the candidate destination.

If the candidate web page contains images, the inventive techniques can convert the images to a common graphics format (e.g. graphic interchange format (GIF)), generate image fingerprints for the images, compare the image fingerprints against signatures of well-known logos, and record any matches between the image fingerprints and the signatures of well-known logos. Preferably, logo fingerprints in the database or repository contain fingerprints of the same corporate logo rendered at a variety of different resolutions to prevent pixelization effects from hampering logo identification.

The plug-in **224** determines the effective IP address that is mapped by the candidate destination. The inventive techniques determine the effecting owning organization for the effective IP address from its repository **202** or by using secondary databases such as, for example, "whois." The whois service is described in Internet Request for Comments 954, authored by Harrenstein et al in 1985, and available at URL http://www.rfc-archive.org/getrfc.php?rfc=954, and is widely deployed in the Internet. In another aspect of the invention, the inventive techniques check the candidate destination for typical phishing attack signs, e.g., long strings that overflow the location window, locations that have a high likelihood of phishing, or only subtle differences to well-known URL names. Also, the

inventive techniques determine the ownership of the DNS domain that is identified in the candidate destination.

In another aspect of the invention, the inventive techniques compute a phishing score for the candidate destination. The techniques identify a candidate destination page as clean if all of the determined organizations match to a corresponding stored organization identity and/or identification (ID) in the repository **202** and if the stored organization is not too similar to another organization that is ranked as more popular in the repository database **202**.

In another aspect of the invention, if a candidate destination page has conflicting visual cues (e.g. organization ID = X) and physical organization (ID = Y), the inventive techniques produce a window **222** that alerts the user to the potential of phishing and shows the results of visual cue checking and those of the physical trace back. The techniques generate a fraud warning **222** via a visual prompt displayed to the user in at least one of a window and a status bar external to the browser window associated with the candidate destination. The window **222** is opened in a randomly placed window separate from the browser to prevent overlay attacks by the phishers.

In yet another aspect of the invention, the inventive techniques identify the candidate destination page as "unknown origin" if the visual cues could not be matched to an organization, but for which the candidate destination coincides with the visual URL and whose destination is not a likely phishing destination. Also, the techniques identify the candidate destination page as "safe" if the visual cues of the pages map to a well-known target, and the physical organization determination obtained the same organization ID.

The inventive techniques, in another aspect of the invention, determine the location of the candidate destination URL in the browser toolbar. The user may collaborate with the software agent in order to establish the location to the URL display relative to the browser window. The software agent may include OCR software to locate the location of the ADDRESS bar. Also, the software agent may include a test suite that redirects the browser to a list of distinct URLs which fill out the entire location window in the browser toolbar. The content to be displayed at those distinct URLs is identical so that only the URL will change in the entire browser window. By using a combination of all letters and regional character codes in the set of tested URLs, it is possible to determine the exact height of the text. This test can be automated on every restart of the browser. An agent can be installed

as a browser plug-in that captures the current browser location, runs the URL location test, and restores the original browser location on every resizing for the browser window.

In other aspects of the invention, the inventive techniques may be performed by a software agent, in a web browser, or in an e-mail client.

FIG. 3 shows a flow diagram illustrating a method for generating a database of destinations to be protected against computer fraud, according to one embodiment of the invention. Step **302** includes generating at least one category of destinations to be protected. Step **304** includes retrieving at least one list of destinations belonging to the at least one category. In an aspect of the invention, the step of retrieving at least one list of destinations belonging to the at least one category may include obtaining a first list of destinations and a second list of destinations, and merging the first list of destinations and the second list of destinations. In another aspect of the invention, the step of retrieving at least one list of destinations belonging to the at least one category may include accessing at least one of an Internet search engine and an Internet indexing service.

A variety of techniques, utilizing dedicated hardware, general purpose processors, firmware, software, or a combination of the foregoing may be employed to implement the present invention. At least one embodiment of the invention can be implemented in the form of a computer product including a computer usable medium with computer usable program code for performing the method steps indicated. Furthermore, at least one embodiment of the invention can be implemented in the form of an apparatus including a memory and at least one processor that is coupled to the memory and operative to perform exemplary method steps.

At present, it is believed that the preferred implementation will make substantial use of software running on a general purpose computer or workstation. With reference to **FIG. 4**, such an implementation might employ, for example, a processor **402**, a memory **404**, and an input and/or output interface formed, for example, by a display **406** and a keyboard **408**. The term "processor" as used herein is intended to include any processing device, such as, for example, one that includes a CPU (central processing unit) and/or other forms of processing circuitry. Further, the term "processor" may refer to more than one individual processor. The term "memory" is intended to include memory associated with a processor or CPU, such as, for example, RAM (random access memory), ROM (read only memory), a fixed memory device (e.g., hard drive), a removable memory device (e.g., diskette), a flash

memory and the like. In addition, the phrase "input and/or output interface" as used herein, is intended to include, for example, one or more mechanisms for inputting data to the processing unit (e.g., mouse), and one or more mechanisms for providing results associated with the processing unit (e.g., printer). The processor **402**, memory **404**, and input and/or output interface such as display **406** and keyboard **408** can be interconnected, for example, via bus **410** as part of a data processing unit **412**. Suitable interconnections, for example via bus **410**, can also be provided to a network interface **414**, such as a network card, which can be provided to interface with a computer network, and to a media interface **416**, such as a diskette or CD-ROM drive, which can be provided to interface with media **418**.

Accordingly, computer software including instructions or code for performing the methodologies of the invention, as described herein, may be stored in one or more of the associated memory devices (e.g., ROM, fixed or removable memory) and, when ready to be utilized, loaded in part or in whole (e.g., into RAM) and executed by a CPU. Such software could include, but is not limited to, firmware, resident software, microcode, and the like.

Furthermore, the invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium (e.g., media **418**) providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer usable or computer readable medium can be any apparatus for use by or in connection with the instruction execution system, apparatus, or device.

The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid-state memory (e.g. memory **404**), magnetic tape, a removable computer diskette (e.g. media **418**), a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk-read only memory (CD-ROM), compact disk-read and/or write (CD-R/W) and DVD.

A data processing system suitable for storing and/or executing program code will include at least one processor **402** coupled directly or indirectly to memory elements **404** through a system bus **410**. The memory elements can include local memory employed during actual execution of the program code, bulk storage, and cache memories which

provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution.

Input and/or output or I/O devices (including but not limited to keyboards **408**, displays **406**, pointing devices, and the like) can be coupled to the system either directly (such as via bus **410**) or through intervening I/O controllers (omitted for clarity).

Network adapters such as network interface **414** may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks. Modems, cable modem and Ethernet cards are just a few of the currently available types of network adapters.

In any case, it should be understood that the components illustrated herein may be implemented in various forms of hardware, software, or combinations thereof, e.g., application specific integrated circuit(s) (ASICS), functional circuitry, one or more appropriately programmed general purpose digital computers with associated memory, and the like. Given the teachings of the invention provided herein, one of ordinary skill in the related art will be able to contemplate other implementations of the components of the invention.

Although illustrative embodiments of the present invention have been described herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various other changes and modifications may be made by one skilled in the art without departing from the scope or spirit of the invention.

CLAIMS

1. A method of detecting computer fraud, comprising the steps of:

obtaining a text version of a candidate destination and a graphical rendering of said candidate destination;

comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding text version of a stored destination and a corresponding graphical rendering of said stored destination; and

generating a fraud warning if said graphical rendering of said candidate destination is substantially similar to said graphical rendering of said stored destination while said text version of said candidate destination differs substantially from said corresponding text version of said stored destination.

2. The method according to claim 1, wherein said candidate destination and said stored destination are represented as URLs (uniform resource locators).

3. The method according to claim 1, wherein said steps are automatically executed upon loading a web page associated with said candidate destination.

4. The method according to claim 1, wherein said steps are executed by using a button that is shown to a user in at least one of a window and a status bar external to a browser window associated with said candidate destination.

5. The method according to claim 1, wherein said fraud warning is generated via a visual prompt displayed to a user in at least one of a window and a status bar external to a browser window associated with said candidate destination.

6. The method according to claim 1, wherein the comparing step is performed on a subset of said candidate destination and said stored destination.

7. The method according to claim 1, wherein the step of comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding stored text version and a corresponding stored graphical rendering comprises the steps of:

determining an effective IP (internet protocol) address that is mapped by said candidate destination; and

determining an effective owning organization for said effective IP address.

8. The method according to claim 1, wherein the step of obtaining a text version of a candidate destination and a graphical rendering of said candidate destination comprises the steps of:

reading an image map of a browser toolbar of a web page associated with said candidate destination; and

determining a character representation of said image map by using an optical character recognition (OCR) algorithm.

9. The method according to claim 1, wherein the step of obtaining a text version of a candidate destination and a graphical rendering of said candidate destination comprises the steps of:

parsing a character representation;

normalizing said character representation; and

generating appropriate derivative versions of said candidate destination from character permutation and substitution.

10. The method according to claim 1, wherein the step of comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding stored text version and a corresponding stored graphical rendering comprises the step of:

searching a database of well-known destinations; and

recording matches between said well-known destinations and derivative versions of said candidate destination.

11. The method according to claim 1, wherein the step of obtaining a text version of a candidate destination and a graphical rendering of said candidate destination comprises the step of:

reading only text of a web page associated with said candidate destination into an array.

12. The method according to claim 1, wherein the step of obtaining a text version of a candidate destination and a graphical rendering of said candidate destination comprises the steps of:

taking a snapshot of a web page associated with said candidate destination;

executing OCR on an entire rendered image of said web page; and

storing recognized words into an array.

13. The method according to claim 12, further comprising the additional steps of:

computing a word-distribution signature of said web page by extracting a word histogram;

comparing said word histogram to histograms of well-known destination web pages;

recording matches between said word histogram and histograms of well-known destination web pages;

sorting said matches by percentage overlap in said word histogram; and

extracting estimated sources for said web page from said matches with high percentage overlap.

14. The method according to claim 1, wherein the step of obtaining a text version of a candidate destination and a graphical rendering of said candidate destination comprises the steps of:

converting images in a web page associated with said candidate destination to a common graphics format;

generating image fingerprints for said images;

comparing said image fingerprints against signatures of well-known logos; and

recording any matches between said image fingerprints and said signatures of well-known logos.

15. The method according to claim 1, wherein the step of comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding stored text version and a corresponding stored graphical rendering comprises the step of:

checking said candidate destination for typical phishing attack signs.

16. The method according to claim 1, wherein the step of comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding stored text version and a corresponding stored graphical rendering comprises the step of:

determining ownership of a DNS (domain name system) domain identified in said candidate destination.

17. The method according to claim 1, wherein the step of comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding stored text version and a corresponding stored graphical rendering further comprises the additional step of:

computing a phishing score for said candidate destination.

18. The method according to claim 1, further comprising the step of:

identifying said candidate destination as clean if all determined organizations match to a corresponding stored organization and if said stored organization is not substantially similar to another organization ranked as more popular in a database.

19. The method according to claim 1, further comprising the step of:

identifying said candidate destination as unknown origin if visual cues could not be matched to an organization, but for which said candidate destination coincides with a visual URL and said candidate destination is unlikely to be a phishing destination.

20. The method according to claim 1, wherein the steps are performed by a software agent.

21. The method according to claim 1, wherein the steps are performed in a web browser.

22. The method according to claim 1, wherein the steps are performed in an e-mail client.

23. A method for automatically generating a database of destinations to be protected against computer fraud, comprising the steps of:

generating at least one category of destinations to be protected; and

retrieving at least one list of destinations belonging to said at least one category.

24. The method according to claim 23, wherein the step of retrieving at least one list of destinations belonging to said at least one category comprises the steps of:

obtaining a first list of destinations and a second list of destinations; and

merging said first list of destinations and said second list of destinations.

25. The method according to claim 23, wherein the step of retrieving at least one list of destinations belonging to said at least one category comprises the step of:

accessing at least one of an Internet search engine and an Internet indexing service.

26. An apparatus for detecting computer fraud, comprising:

a memory; and

at least one processor coupled to said memory and operative to:

obtain a text version of a candidate destination and a graphical rendering of said candidate destination;

compare said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding text version of a stored destination and a corresponding graphical rendering of said stored destination; and

generate a fraud warning if said graphical rendering of said candidate destination is substantially similar to said graphical rendering of said stored destination while said text version of said candidate destination differs substantially from said corresponding text version of said stored destination.

27. The apparatus of claim 26, wherein:

said candidate destination and said stored destination are represented as URLs.

28. The apparatus of claim 26, wherein:

said steps are automatically executed upon loading a web page associated with said candidate destination.

29. The apparatus of claim 26, wherein:

said steps are executed by using a button that is shown to the user in at least one of a window and a status bar external to a browser window associated with said candidate destination.

30. A computer program product comprising a computer useable medium having computer useable program code for detecting computer fraud, said computer program product including:

computer useable program code for obtaining a text version of a candidate destination and a graphical rendering of said candidate destination;

computer useable program code for comparing said text version of said candidate destination and said graphical rendering of said candidate destination with, respectively, a corresponding text version of a stored destination and a corresponding graphical rendering of said stored destination; and

computer useable program code for generating a fraud warning if said graphical rendering of said candidate destination is substantially similar to said graphical rendering of said stored destination while said text version of said candidate destination differs substantially from said corresponding text version of said stored destination.

31. The computer program product of claim 30, wherein:

said candidate destination and said stored destination are represented as URLs.

32. The computer program product of claim 30, wherein:

said steps are automatically executed upon loading a web page associated with said candidate destination.

33. The computer program product of claim 30, further comprising:

computer useable program code for enabling execution of said steps via using a button that is shown to the user in at least one of a window and a status bar external to a browser window associated with said candidate destination.

34. A computer program product comprising a computer useable medium having computer useable program code for automatically generating a database of destinations to be protected against computer fraud, said computer program product including:

computer useable program code for generating at least one category of destinations to be protected; and

computer useable program code for retrieving at least one list of destinations belonging to said at least one category.

35. The computer program product of claim 34, wherein:

retrieving at least one list of destinations belonging to said at least one category comprises the steps of:

obtaining a first list of destinations and a second list of destinations; and

merging said first list of destinations and said second list of destinations.

FIG. 1

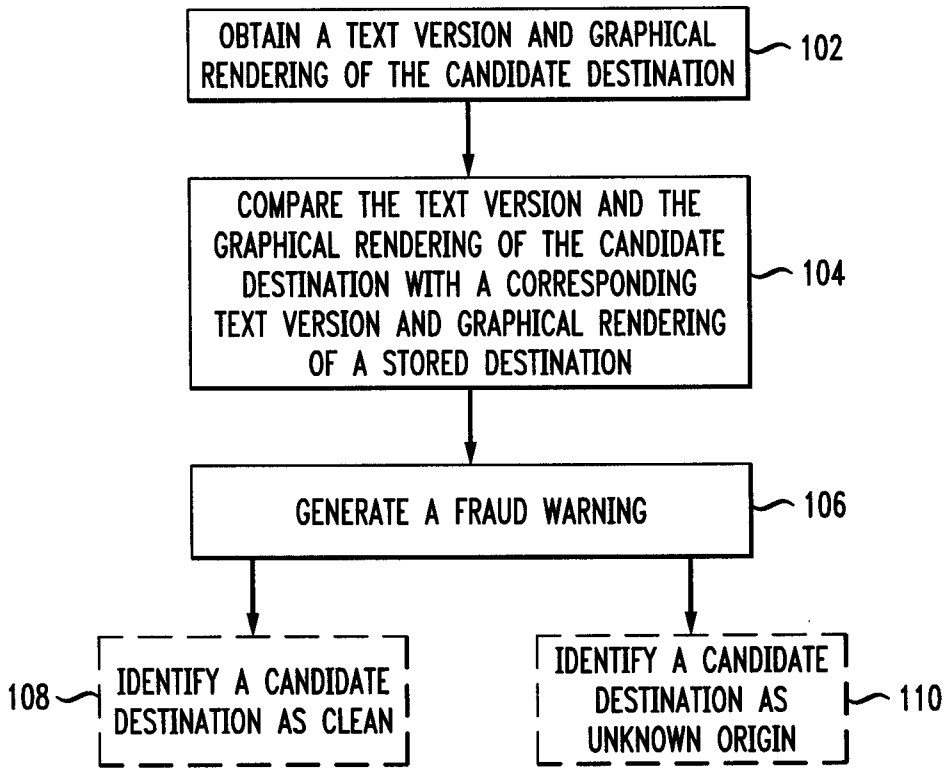

OBTAIN A TEXT VERSION AND GRAPHICAL RENDERING OF THE CANDIDATE DESTINATION
102
COMPARE THE TEXT VERSION AND THE GRAPHICAL RENDERING OF THE CANDIDATE DESTINATION WITH A CORRESPONDING TEXT VERSION AND GRAPHICAL RENDERING OF A STORED DESTINATION
104
GENERATE A FRAUD WARNING
106
108
IDENTIFY A CANDIDATE DESTINATION AS CLEAN
IDENTIFY A CANDIDATE DESTINATION AS UNKNOWN ORIGIN
110

FIG. 2

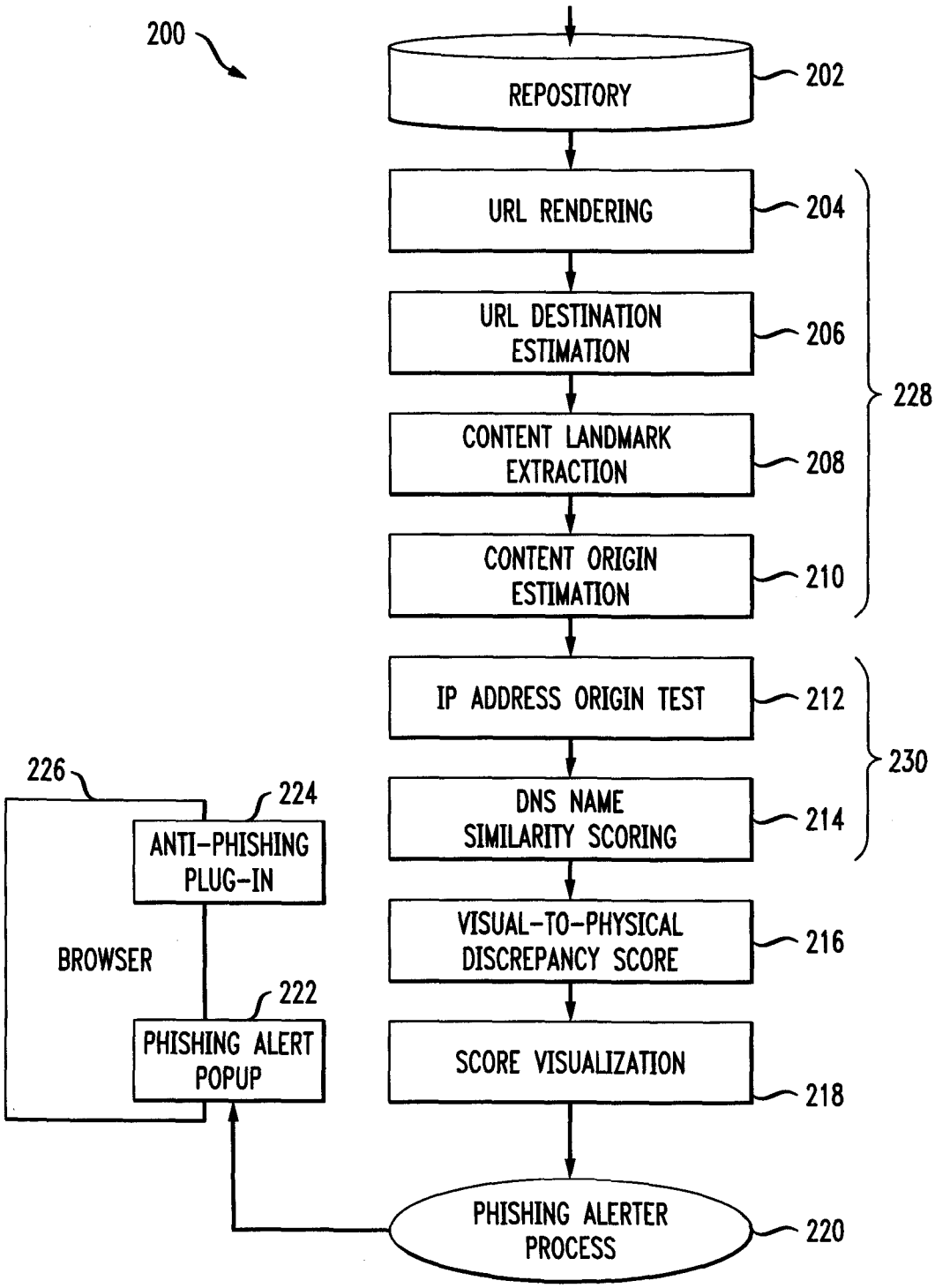

200
REPOSITORY
202
URL RENDERING
204
URL DESTINATION ESTIMATION
206
CONTENT LANDMARK EXTRACTION
208
CONTENT ORIGIN ESTIMATION
210
228
IP ADDRESS ORIGIN TEST
212
DNS NAME SIMILARITY SCORING
214
230
VISUAL-TO-PHYSICAL DISCREPANCY SCORE
216
SCORE VISUALIZATION
218
PHISHING ALERTER PROCESS
220
226
224
ANTI-PHISHING PLUG-IN
BROWSER
222
PHISHING ALERT POPUP

FIG. 3

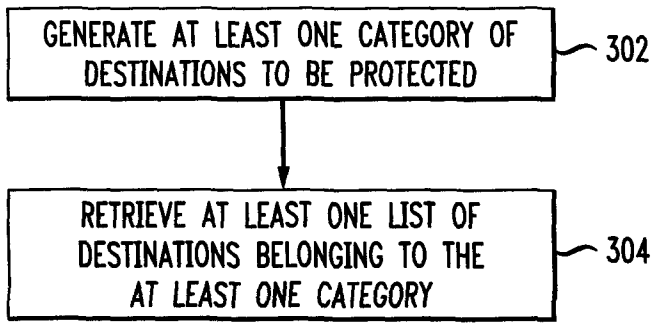
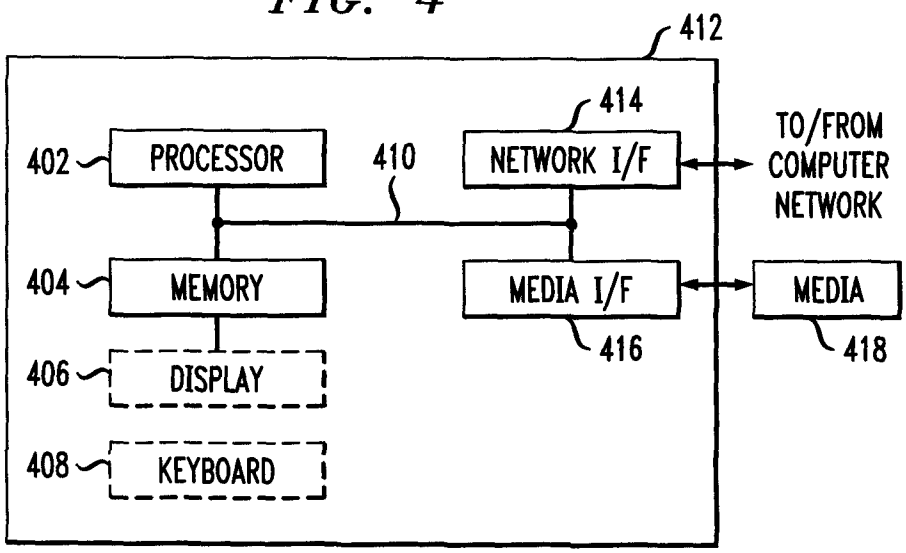

GENERATE AT LEAST ONE CATEGORY OF DESTINATIONS TO BE PROTECTED
302
RETRIEVE AT LEAST ONE LIST OF DESTINATIONS BELONGING TO THE AT LEAST ONE CATEGORY
304

FIG. 4


412
414
402
PROCESSOR
410
NETWORK I/F
TO/FROM COMPUTER NETWORK
404
MEMORY
MEDIA I/F
MEDIA
416
418
406
DISPLAY
408
KEYBOARD

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/063845

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/20 H04L29/06
ADD. G06F17/30

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 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 practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/026921 A (METASWARM HONGKONG LTD [CN]) 16 March 2006 (2006-03-16) page 6, line 17 - page 7, line 2 page 12, line 5 - page 13, line 10 page 16, lines 16-20 page 18, line 12 - page 20, line 1 page 24, line 16 - page 32, line 4 page 35, lines 4-13 page 36, lines 11-28 page 38, line 6 - page 41, line 21 page 43, line 6 - page 45, line 9	23-25, 34,35
A		1-22, 26-33

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 May 2008	28/05/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/063845

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/123157 A1 (ALAGNA MICHAEL ANTHONY [US] ET AL) 24 June 2004 (2004-06-24) paragraphs [0040] - [0053] paragraph [0063] paragraphs [0090] - [0101]	23-25, 34,35
A		1-22, 26-33

X	WO 2006/018647 A (PUGH RHODERICK JOHN KENNEDY [GB]) 23 February 2006 (2006-02-23) page 13, line 1 - page 14, line 1 page 16, line 25 - page 24, line 22	23-25, 34,35
A		1-22, 26-33

X	EP 1 681 825 A (STREAMSHIELD NETWORKS LTD [GB]) 19 July 2006 (2006-07-19) column 5, line 24 - column 8, line 48	23-25, 34,35
A		1-22, 26-33

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2007/063845

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers allsearchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search reportcovers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-22, 26-33

   phishing detection using graphical rendering and textual representation of destinations

   ---

2. claims: 23-25, 34, 35

   automatic generation of a database of destinations to be protected against computer fraud.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/063845

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006026921 A	16-03-2006	NONE	
US 2004123157 A1	24-06-2004	AU 2003293501 A1	09-07-2004
		EP 1586054 A2	19-10-2005
		WO 2004055632 A2	01-07-2004
WO 2006018647 A	23-02-2006	EP 1779216 A1	02-05-2007
EP 1681825 A	19-07-2006	GB 2422224 A	19-07-2006
		WO 2006120368 A1	16-11-2006