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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 November 2016 (17.11.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/182654 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 11/00* (2006.01)
H04L 29/08 (2006.01) *G06F 12/14* (2006.01)
G06F 7/04 (2006.01) *G06F 12/16* (2006.01)

(21) International Application Number:
PCT/US2016/026856

(22) International Filing Date:
11 April 2016 (11.04.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/159,862 11 May 2015 (11.05.2015) US
15/069,981 15 March 2016 (15.03.2016) US

(71) Applicant: **FINJAN MOBILE, INC.** [US/US]; 2000 University Avenue, East Palo Alto, California 94303 (US).

(72) Inventors: **GODLEWSKI, Michael**; 413 Capp Street, San Francisco, California 94110 (US). **HOUSE, Geoffrey**; 413 Capp Street, San Francisco, California 94110 (US). **TONG, Winnie**; 338 Spear Street, Apartment #37D, San Francisco, California 94105 (US). **MUTTER, Rudolph**; 349 El Camino Real, Apartment #1, Millbrae, California 94030 (US). **FEORE, Bay Lee**; 641 27th Avenue, San Francisco, California 94121 (US). **SHIPMAN, Timothy**; 1112 Larkin Street, Apartment #205, San Francisco, California 94109 (US). **SCHERBA, Anthony**; 333 Harrison Street, Apartment #602, San Francisco, California 94105 (US). **MCDOLE, Lee**; 528 66th Street, Apartment #3, Oakland, California 94609 (US). **KREMER, Alexander Lin**; 2810 Alvarado Avenue, San Mateo, California 94403 (US). **MAR-SPINOLA, Julie**; 4925Portmamoch Court, San Jose, California 95138 (US).

(74) Agent: **BERGER, Marc**; Soquel Group LLC, P. O. Box 691, Soquel, California 95073 (US).

(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, 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, ST, 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: MALWARE WARNING

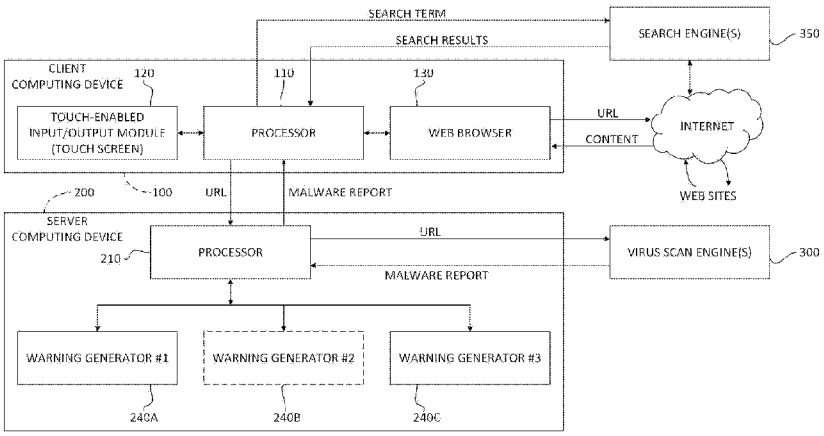

FIG. 15

(57) Abstract: A malware warning system, including a client sending requests to and receiving replies from a server, and a server, including a first warning generator sending to the client a warning including a threat level of content located at a web site, in response to receiving from the client a URL for accessing content at the web site, a second warning generator sending to the client a warning including information about at least one of the nature of the threat of the content located at the web site and a location of the web site, in response to receiving from the client a request for more information about the nature of the threat, and a third warning generator, sending to the client a warning including an instruction to perform a swipe gesture to confirm a request to access the URL, in response to receiving that request from the client.

WO 2016/182654 A1

MALWARE WARNING

PRIORITY REFERENCES

[0001] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/159,862, entitled SECURE BROWSER APPLICATION, and filed on May 11, 2015 by inventors Mike Godlewski, Geoff House, Winnie Tong, Rudolph Mutter, Baylee Feore, Timothy Shipman, Tony Scherba and Julie Mar-Spinola.

[0002] This application also claims benefit of and hereby incorporates by reference US Patent Application No. 15/069,981, entitled MALWARE WARNING, and filed on March 15, 2016 by inventors Michael Godlewski, Geoffrey House, Winnie Tong, Rudolph Mutter, Bay Lee Feore, Timothy Shipman, Anthony Scherba and Julie Mar-Spinola.

FIELD OF THE INVENTION

[0004] The present invention relates to computer security and in particular to warning a user about malware to prevent virus attacks on computing devices.

BACKGROUND OF THE INVENTION

[0005] Users are adept today at touch-based input for many kinds of computing devices, and are able to perform tasks such as touch-keystrokes at a rapid-fire rate, even with small touch areas. This makes it difficult for users to make an abrupt stop when a malware application is encountered, and prevent its activation. Even though a user has installed an anti-virus application, and a malware warning message appears, the user may react "*one touch too late*", after the malware has been launched.

[0006] The damage caused by malware may be enormous. Malware can wipe out a smartphone or tablet computer, and/or extract sensitive data enabling a hacker to cause financial or other harm.

[0007] Sometimes an anti-virus application flags an unrecognized web site, application or file as being suspicious, when a user knows that the application or file is safe, a condition referred to as a "*false positive*". In such case, the user intentionally ignores a malware warning message.

[0008] Thus what is needed to prevent a user from unintentionally ignoring a malware warning message is a new type of malware warning mechanism.

SUMMARY

[0009] Embodiments of the present invention provide multiple warning modules, systems and methods that generate important information about specific malware that a user is encountering, and that require a confirmatory action from the user that is different than a simple touch prior to accessing a suspicious web site, application or file, thus preventing the "*one touch too late*" catastrophe.

[0010] There is thus provided in accordance with an embodiment of the present invention a non-transitory computer readable medium storing instructions, which, when executed by a processor of an electronic device, cause the processor to (i) receive an identifier for accessing content at a destination web site, (ii) in response to receiving the identifier, generate a warning comprising a threat level of content located at the destination web site, (iii) receive a request for more information about the nature of the threat, (iv) in response to receiving the request for more information, generate a warning comprising information about at least one of (i) the nature of the threat of the content, and (ii) a location of the destination web site, (v) receive a request to access the content, and (vi) in response to receiving the request to access the content, generating a warning comprising an instruction to perform a confirmatory touch gesture to confirm the request to access the content.

[0011] There is additionally provided in accordance with an embodiment of the present invention a malware warning module for an electronic device, including one or more touch-enabled input devices, receiving user input, a first warning generator, generating a warning comprising a threat level of content located at a destination web site, in response to the one or more input devices receiving an identifier for accessing content at the

destination web site, a second warning generator, generating a warning including information about at least one of (i) the nature of the threat of the content, and (ii) a location of the destination web site, in response to the one or more input devices receiving a request for more information about the nature of the threat; and a third warning generator, generating a warning including an instruction to perform a confirmatory touch gesture to confirm a request to access the content, in response to the one or more input devices receiving a request to access the content.

[0012] There is further provided in accordance with an embodiment of the present invention a malware warning system, including a touch-enabled client computer device sending requests to and receiving replies from a server computing device, and a server computing device receiving the requests from the client, including a first warning generator, sending to the client a warning including a threat level of content located at a destination web site, in response to receiving from the client an identifier for accessing content at the destination web site, a second warning generator, sending to the client a warning comprising information about at least one of (i) the nature of the threat of the content, and (ii) a location of the destination web site, in response to receiving from the client a request for more information about the nature of the threat, and a third warning generator, sending to the client a warning including an instruction to perform a swipe gesture to confirm a request to access the content, in response to receiving from the client a request to access the content.

[0013] There is yet further provided in accordance with an embodiment of the present invention a non-transitory computer readable medium storing instructions, which, when executed by a processor of an electronic

device, cause the processor to (i) receive an identifier for accessing content at a destination web site, (ii) in response to receiving the identifier, generate a warning comprising a threat level of content located, (iii) receive a request to access the content, and (iv) in response to receiving the request to access the content, generate a warning including an instruction to perform a confirmatory touch gesture to confirm the request to access the content.

[0014] There is moreover provided in accordance with an embodiment of the present invention a malware warning module for an electronic device, including one or more touch-enabled input devices receiving user input, a first warning generator, generating a warning including a threat level of content located at a destination web site, in response to the one or more input devices receiving an identifier for accessing content at the destination web site, and a second warning generator, generating a warning including an instruction to perform a confirmatory touch gesture to confirm a request to access the content, in response to the one or more input devices receiving a request to access the content.

[0015] There is additionally provided in accordance with an embodiment of the present invention a malware warning system, including a touch-enabled client computer device sending requests to and receiving replies from a server computing device, and a server computing device receiving the requests from the client computer device, including a first warning generator, sending to the client a warning including a threat level of content located at a destination web site, in response to receiving from the client an identifier for accessing content at the destination web site, and a second warning generator, sending to the client a warning including an instruction to perform a confirmatory touch gesture to confirm a

request to access the content, in response to receiving from the client a request to access the content.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The present invention will be more fully understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

[0018] **FIG. 1** is a simplified diagram of a client-based embodiment of a malware warning module for URLs, in accordance with an embodiment of the present invention;

[0019] **FIG. 2** is a simplified flowchart of a client-based method for malware warning for URLs, in accordance with an embodiment of the present invention;

[0020] **FIG. 3** is a screen shot of a simple interface display via which a user is prompted to enter a URL using a touch-based keyboard, in accordance with an embodiment of the present invention;

[0021] **FIG. 4** is a screen shot showing that the user has input a specific identifier, in accordance with an embodiment of the present invention;

[0022] **FIG. 5** is a screen shot showing a message, "*This is taking longer than expected*", displayed while a processor is waiting for scan results, in accordance with an embodiment of the present invention;

[0023] **FIG. 6** is a screen shot of a threat level of "*DANGER*" for a web site, in accordance with an embodiment of the present invention;

[0024] **FIG. 7** is a screen shot of a second warning displayed, including the nature of a "*DANGER*" threat and a location of an identified web site, in accordance with an embodiment of the present invention;

[0025] **FIG. 8** is a screen shot of a threat level of "*CAUTION*" for a web site, in accordance with an embodiment of the present invention;

[0026] **FIG. 9** is a screen shot of a second warning displayed, including the nature of a "*CAUTION*" threat and a location of the identified web site, in accordance with an embodiment of the present invention;

[0027] **FIG. 10** is a screen shot of a threat level of "*SAFE*" for a web site, in accordance with an embodiment of the present invention;

[0028] **FIG. 11** is a message indicating that a "*SAFE*" web site does not have any malicious code or phishing tactics, in accordance with an embodiment of the present invention;

[0029] **FIG. 12** is a screen shot showing a threat warning for a web site displayed by a processor, requiring a user to perform a swipe gesture in order to access a suspicious web site, in accordance with an embodiment of the present invention;

[0030] **FIG. 13** is a screen shot of a swipe gesture being performed to access a suspicious web site, in accordance with an embodiment of the present invention;

[0031] **FIG. 14** is a simplified flow diagram using display screens to illustrate stages of a client-based malware warning mechanism, in accordance with an embodiment of the present invention;

[0032] **FIG. 15** is a simplified diagram of a server-based embodiment of a malware warning system for URLs, in accordance with an embodiment of the present invention;

[0033] **FIG. 16** is a simplified flowchart of a server-based method for malware warning for URLs, in accordance with an embodiment of the present invention;

[0034] **FIG. 17** is a simplified flow diagram using display screens to illustrate stages of a server-based malware warning mechanism, in accordance with an embodiment of the present invention;

[0035] **FIG. 18** is a simplified flowchart of a client-based method for malware warning for search results, in accordance with an embodiment of the present invention;

[0036] **FIG. 19** is a screen shot of a warning regarding potential risks of search results in accordance with an embodiment of the present invention; and

[0037] **FIG. 20** is a screen shot of a safe assessment of search results in accordance with an embodiment of the present invention;

[0038] **FIG. 21** is a simplified flowchart of a server-based method for malware warning for search results, in accordance with an embodiment of the present invention; and

[0039] **FIG. 22** is a simplified flow diagram using display screens to illustrate stages of a server-based malware warning mechanism for web search results, in accordance with an embodiment of the present invention.

[0040] For reference to the figures, the following index of elements and their numerals is provided. Similarly numbered elements represent elements of the same type, but they need not be identical elements.

Table of elements in the figures	
Element	**Description**
100	client computing device
110	client processor
120	touch-enabled input/output module
125	touch-based keyboard
130	web browser
140A	first warning generator
140B	second warning generator (optional)
140C	third warning generator
200	server computing device
210	server processor
240A	first warning generator
240B	second warning generator (optional)
240C	third warning generator
300	virus scan engine(s)
350	search engine(s)
410 – 460	display screens

[0041] Elements numbered in the **1000**'s are operations of flow charts.

DETAILED DESCRIPTION

[0042] In accordance with embodiments of the present invention, modules, systems and methods are provided for warning a user about specific malware that he is encountering, and requiring a confirmatory action from the user that is different than a simple touch prior to accessing a suspicious web site, application or file. As described below, the present invention may be embodied inter alia with or without use of a server computer.

Client-Based Embodiment

[0043] Reference is made to **FIG. 1**, which is a simplified diagram of a client-based embodiment of a malware warning module for URLs, in accordance with an embodiment of the present invention. Shown in **FIG. 1** is a client device **100** with a processor **110**, a touch-enabled input/output (I/O) module **120**, such as a touch screen, and a web browser **130**. Client **100** also includes a data bus and memory modules that store data and instructions; the memory modules being accessible by processor **110**, via the data bus, for processor **110** to perform read and write operations.

[0044] In accordance with an embodiment of the present invention, client device **100** is an electronic computing device, including inter alia mobile devices such as smartphones, tablets, and laptops that have processors, memory and communication interfaces. Client device **100** may be programmed and configured to perform the methods of the present invention described below with reference to **FIGS. 2 – 22**. Depending on the operating system of client device **100**, standard appropriate programming languages for developing and testing

applications, including application program interfaces (APIs), pop-up windows and animations, can implement the methods of the present invention.

[0045] I/O module **120** provides for touch and gesture input to processor **110**, in response to a user touching a surface of the device with an object such as a finger, or sliding his finger along the surface of the device to perform a gesture such as the familiar "*swipe*" gesture. Web browser **130** may be, for example, the familiar ANDROID®-based or SAFARI® web browsers.

[0046] Shown in **FIG. 1** are three warning generators, **140A**, **140B** and **140C**. Operation of these warning generators is described below with reference to **FIGS. 2 – 14**. Warning generators **140A**, **140B** and **140C** may be three separate modules, as shown in **FIG. 1**, they may be combined into fewer modules, or they may be separated into more modules. Warning generators **140A**, **140B** and **140C** may be software, firmware or hardware modules, or a combination of software, firmware and hardware modules.

[0047] Also shown in **FIG. 1** are one or more virus scan engines **300**, and one or more search engines **350**. Scan engine(s) **300** scan content at a designated URL address for malicious or potentially malicious malware code. Scan engine(s) **300** may be a physical gateway capable of scanning content at a URL address, and/or may be a cloud-based content scanning service. Search engine(s) **350** may be a physical or cloud-based search service, such as Microsoft BING®.

[0048] Reference is made to **FIG. 2**, which is a simplified flowchart **1000** of a client-based method for malware warning for URLs, in accordance with an embodiment of the present invention. Flowchart

1000 of **FIG. 2** is divided into three columns. The left column includes operations performed by a user of device **100**, the middle column includes operations performed by device **100**, and the right column includes operations performed by scan engine(s) **300**.

[0049] At the beginning of method **1000**, the user is prompted to enter an identifier, such as a URL, for accessing web content. In this regard, reference is made to **FIG. 3**, which is a screen shot of a simple interface display via which a user is prompted to enter a URL using a touch-based keyboard **125** displayed in I/O module **120**, in accordance with an embodiment of the present invention. At operation **1005**, the user enters an identifier for accessing content at a web site that is identified by the identifier. In this regard, reference is made to **FIG. 4**, which is a screen shot showing that the user has entered a specific identifier, namely, "*finjan.com*", in accordance with an embodiment of the present invention.

[0050] At operation **1010**, device **100** passes the URL to scan engine(s) **300** for analysis. Alternatively, instead of invoking scan engine(s) **300**, device **100** may consult a database that stores malware information for each of a plurality of URLs. If the specific URL input by the user does not reside in the database, or if it does reside in the database but its information is out of date, only then does device **100** pass the URL to scan engine(s) **300** to perform a scan of the URL. Operation **1010** may be performed inter alia by invoking remote or third-party scanners, such as the VirusTotal scanner at https://www.virustotal.com, using an API key. VirusTotal provides security results from many different scan engines. More time is required when the URL needs to be scanned, and device **100** may display a message to the user in response to which the

user may either wait or cancel the scan. In this regard, reference is made to **FIG. 5**, which is a screen shot of a message, "*This is taking longer than expected*", displayed while device **100** is waiting for scan results, in accordance with an embodiment of the present invention.

[0051] At operation **1015**, scan engines(s) **300** scan the content at the URL, generate a malware report for the content, and return the report to device **100**.

[0052] At operation **1050**, warning generator **140A** generates a first warning including a threat level of the content located at the identified web site.

[0053] In accordance with one embodiment of the present invention, threat levels include "*SAFE*", "*CAUTION*" and "*DANGER*". Reference is made to **FIG. 6**, which is a screen shot of a threat level of "*DANGER*" for the web site finjan.com, in accordance with an embodiment of the present invention.

[0054] At operation **1055** the user requests more information about the nature of the threat. At operation **1060** warning generator **140B** generates a second warning including the nature of the threat and the location of the identified web site. In this regard, reference is made to **FIG. 7**, which is a screen shot of a warning displayed by warning generator **140B**, including the nature of the "*DANGER*" threat and a location of the identified web site, in accordance with an embodiment of the present invention. Specifically **FIG. 7** shows that the threat is phishing malware that steals personal information, and that the web site is categorized as "*phishing*", "*malware*" and "*malicious*", and resolves to a domain located in Russia.

[0055] Reference is made to **FIG. 8**, which is a screen shot of a threat level of "*CAUTION*" for the web site finjan.com, in accordance with an embodiment of the present invention. Reference is made to **FIG. 9**, which is a screen shot of a warning displayed by warning generator **140B**, including the nature of the "*CAUTION*" threat and a location of the identified web site, in accordance with an embodiment of the present invention. **FIG. 9** shows that the threat is phishing malware that steals personal information, and that the web site is categorized as "*news & media*" and resolves to a domain located in the United States.

[0056] Reference is made to **FIG. 10**, which is a screen shot of a threat level of "*SAFE*" for the web site finjan.com, in accordance with an embodiment of the present invention. Reference is made to **FIG. 11**, which is a screen shot of a message displayed by warning generator **140B** indicating that the "*SAFE*" web site does not have any malicious code or phishing tactics, in accordance with an embodiment of the present invention. **FIG. 11** shows that the web site is categorized as "*technology*" and resolves to a domain located in the United States.

[0057] At operation **1065** the user requests access to the content at the identified web site. At operation **1070**, warning generator **140C** prompts the user to perform a confirmatory gesture, such as a swipe gesture. Such a prompt is shown in **FIG. 12**.

[0058] Reference is made to **FIG. 12**, which is a screen shot showing a threat warning for a web site displayed by warning generator **140C**, requiring a user to perform a swipe gesture in order to access a suspicious web site, in accordance with an embodiment of the present invention. **FIG. 12** shows a threat warning for the web site "*gooogel.com*" displayed by warning generator **140C**, in accordance with

an embodiment of the present invention. The warning includes the text "*WARNING*" displayed with a caution sign, and a warning message indicating that accessing the identified web site may be harmful to device **100** or may compromise sensitive information of the user. The warning also provides touch controls for the user to "*GO BACK*" and not access the identified web site, or to "*LEARN MORE*" about the nature of the threat. If the user wishes nevertheless to access the identified web site, then the use is required to perform a swipe gesture on I/O module **120**, to slide the warning message off of the display.

[0059] At operation **1075** the user reviews the message and decides nevertheless to perform the confirmatory gesture. In this regard, reference is made to **FIG. 13**, which is a screen shot of a swipe gesture being performed on I/O module **120** to access the identified web site, in accordance with an embodiment of the present invention. As the swipe gesture is being performed and the warning message slides out of the display, another message, "*VISIT DANGEROUS SITE*", slides into the display. As such, it will be appreciated by those skilled in the art that it is highly unlikely that the user access the identified web site unintentionally.

[0060] At operation **1080**, in response to the user having performed the confirmatory gesture at operation **1075**, web browser **130** attempts to access the identified web site. However, it may be that the identified web site redirects web browser **130** using a different identifier than that received at operation **1005**. Device **100** may register itself to listen to redirection events for web browser **130** and, as such, is able to hook web browser **130** before it accesses the different identifier. At decision **1085**, device **100** decides whether or not web browser **130** has been redirected. If so, processing returns to operation **1010**, where device

100 passes the different identifier to scan engine(s) **300** for analysis. Otherwise, if decision **1085** decides that web browser **130** has not been redirected, processing advances to operation **1090**, where web browser **130** accesses the content that the user requested at operation **1065**. The user then views and interacts with the content at operation **1095**, thereby completing flowchart **1000**.

[0061] In an alternative embodiment of the present invention, warning generator **140B** of **FIG. 1** may be eliminated and, correspondingly, method **1000** of **FIG. 2** may advance directly from operation **1050** to operation **1065**. As such, the tri-warning module, system and method of **FIGS. 1** and **2** may optionally be a bi-warning module, system and method, respectively, without using the intermediate informational warnings, such as the warnings shown in **FIGS. 7**, **9** and **11**. Instead, after displaying the threat level of an identified web site, the user is required to perform a confirmatory gesture in order to access the site. To indicate this alternative embodiment, warning generator **140B** is drawn with a dashed rectangle in **FIG. 1**, operation **1060** is drawn with a dashed rectangle in **FIG. 2**, and an arrow from operation **1050** to operation **1065** is drawn with a dashed line in **FIG. 2**.

[0062] Classification of malware threats by warning generator **140A** into types "*DANGER*", "*CAUTION*" and "*SAFE*" may be based on statistics of the virus scan results provided to warning generator **140A** from virus scan engine(s) **300**. In one exemplary embodiment, categorization may be based on statistical conditions such as those shown in **TABLE I** below.

TABLE I: Statistical breakdown of scan engine results into threat types	
Threat Type	**Condition**
DANGER	> 75% of the scan engines indicate threat
CAUTION	5% - 75% of the scan engines indicate threat
SAFE	<5% of the scan engines indicate threat

[0063] Reference is made to **FIG. 14**, which is a simplified flow diagram using display screens to illustrate stages of a client-based malware warning mechanism, in accordance with an embodiment of the present invention. **FIG. 14** includes virus scan engine(s) **300**. Screen **410** is a landing screen, e.g., the screen shown in **FIG. 3**, prompting a user to enter a URL. Screen **420** is a loading screen, e.g., the screen shown in **FIG. 4**. While screen **420** is being displayed, warning generator **140A** determines the security threat of the URL that was entered in screen **410**. If this security information is not readily available, then warning generator **140A** queries virus scan engine(s) **300** for the information about the URL. After determining the security threat, warning generator **140A** displays either a "*DANGER*" screen **431**, e.g., the screen shown in **FIG. 6**, or a "*CAUTION*" screen **432**, e.g., the screen shown in **FIG. 8**, or a "*SAFE*" screen **433**, e.g., the screen shown in **FIG. 10**.

[0064] Device **100** then performs the warning method of **FIG. 2** beginning at operation **1025**. Upon request by the user of information about the nature of the threat, warning generator **140B** generates warning screens, such as the screens shown in **FIGS. 7**, **9** and **11**, with warning information for the respective "*DANGER*", "*CAUTION*" and "*SAFE*" threat levels.

[0065] If the user decides to access the content at the URL, then warning generator **140C** requires that the user perform a confirmatory

gesture. Upon performing the confirmatory gesture, web browser **130** attempts to access the URL. If web browser is re-directed to another URL, then device **100** hooks the re-direction event and displays screen **420**, prior to web browser **130** accessing the other URL.

Server-Based Embodiment

[0066] In the embodiment of the **FIG. 1**, I/O module **120**, web browser **130** and the warning generators are components of the same device, namely, client device **100**. In another embodiment of the present invention, module **120** and web browser **130** are components of one device, namely, client device **100**, and the warning generators are components of another device, namely, a server computing device **200**.

[0067] Reference is made to **FIG. 15**, which is a simplified diagram of a server-based embodiment of a malware warning system for URLs, in accordance with an embodiment of the present invention. As shown in **FIG. 15** server **200** includes three warning generators, **240A**, **240B** and **240C**. Warning generators **240A**, **240B** and **240C** may be three separate modules, as shown in **FIG. 15**, they may be combined into fewer modules, or they may be separated into more modules.

[0068] It will be appreciated by those skilled in the art that a client-server architecture affords many variations in distribution of processing labor between the client and the server, all of which are contemplated by the present invention. Thus, referring to **FIG. 15**, server **200**, instead of device **100**, may pass the search terms to search engine(s) **350** and receive the results therefrom.

[0069] Similarly, referring to **FIG. 15**, the three warning generators may instead be components of device **100**, as in **FIG. 1**, and server **200** may

be operative only to receive a URL and return a malware report, as in **FIG. 16**. Operation of such an embodiment is illustrated in **FIG. 16**.

[0070] Reference is made to **FIG. 16**, which is a simplified flowchart **1100** of a server-based method for malware warning for URLs, in accordance with an embodiment of the present invention. Flowchart **1100** of **FIG. 16** is divided into four columns. The left-most column includes operations performed by a user of device **100**, the second-from-leftmost column includes operations performed by device **100**, the second-from rightmost column indicates operations performed by server **200**, and the right column includes operations performed by scan engine(s) **300**.

[0071] At operation **1105**, the user enters an identifier, such as a URL, for accessing content at a web site identified by the identifier. At operation **1110**, device **100** passes the identifier to server **200** for analysis, thereby relieving device **100** from this task. At operation **1115**, server **200** passes the identifier to scan engine(s) **300** for analysis. Alternatively, instead of invoking scan engine(s) **300**, server **200** may consult a database that stores malware information for each of a plurality of URLs. If the specific URL input by the user does not reside in the database, or if it does reside in the database but its information is out of date, only then does server **200** pass the URL to scan engine(s) **300** to perform a scan of the URL.

[0072] At operation **1120**, scan engine(s) scan the identified content for potential malware, and return a malware report to server **200**. At operation **1125**, server **200** passes the scan results to device **100**.

[0073] Subsequent operations **1150** – **1195** are similar to correspondingly numbered operations **1050** – **1095**, which were described above with reference to **FIG. 2**.

[0074] Reference is made to **FIG. 17**, which is a simplified flow diagram using display screens to illustrate stages of a server-based malware warning mechanism, in accordance with an embodiment of the present invention. **FIG. 17** includes server **200** and virus scan engine(s) **300**. Screen **410** is a landing screen, e.g., the screen shown in **FIG. 3**, prompting a user to enter a URL. Screen **420** is a loading screen, e.g., the screen shown in **FIG. 4**. While screen **420** is being displayed, device **100** sends the URL that was entered in screen **410** to server **200** for analysis. If security information for the URL is not readily available to server **200**, then server **200** queries virus scan engine(s) **300** for the information about the URL. After receiving a malware report for the URL from server **200**, warning generator **140A** sends a malware report to device **100**, and device **100** displays either a "*DANGER*" screen **431**, e.g., the screen shown in **FIG. 6**, or a "*CAUTION*" screen **432**, e.g., the screen shown in **FIG. 8**, or a "*SAFE*" screen **433**, e.g., the screen shown in **FIG. 10**.

[0075] Device **100** then performs the warning method of **FIG. 16** beginning at operation **1115**. Upon request by the user of information about the nature of the threat, warning generator **140B** generates warning information, such as the information shown in **FIGS. 7**, **9** and **11** for the respective "*DANGER*", "*CAUTION*" and "*SAFE*" threat levels.

[0076] If the user decides to access the content at the URL, then warning generator **140C** requires that the user perform a confirmatory gesture. Upon performing the confirmatory gesture, web browser **130**

attempts to access the URL. If web browser is re-directed to another URL, then device **100** hooks the re-direction event, reports the re-direction event to server **200**, which then invokes scan engine(s) **300** to analyze the other URL.

Malware Warnings for Search Results

[0077] It will be appreciated by those skilled in the art that the warning modules, systems and methods of the present invention are of widespread advantage to many client-server applications. In some embodiments, the present invention is applied to search engines, to provide warning modules, systems and methods for potential malware in web search results. These applications may be embodied inter alia with or without use of a server computer.

[0078] Reference is made to **FIG. 18**, which is a simplified flowchart **1200** of a client-based method for malware warning for search results, in accordance with an embodiment of the present invention. Flowchart **1200** of **FIG. 18** is divided into four columns. The left-most column includes operations performed by a user, the second-from-leftmost column includes operations performed by device **100**, the second-from rightmost column indicates operations performed by search engine(s) **350**, and the right column includes operations performed by scan engine(s) **300**.

[0079] At operation **1205**, the user enters either an identifier, such as a URL, or a search term. At decision **1210**, device **100** decides whether or not the user entered a search term. For example, device **100** may examine the text string input by the user for the presence of a domain name extension such as "*.com*". If decision **1210** determines that the

user did not enter a search term, then the user input is an identifier, and at operation **1215** flowchart **1200** advances to operation **1010** of **FIG. 2**; namely, a method for malware warning for identifiers.

[0080] If decision **1210** determines that the user entered a search term, then at operation **1220** device **100** passes the search term to search engine(s) **350**. At operation **1225** search engine(s) **350** perform their search and return their search results to device **100**. At operation **1230** device **100** in turn passes a batch of the search results to scan engine(s) **300**, for inspection of each result for potential malware. Search results are sent to scan engine(s) **300** in batches, since there may be a large number of results, and it is not necessary for device **100** to wait for scan engine(s) **300** to scan all of the results. Each batch may be inter alia a display page worth of results. At operation **1235** scan engine(s) **300** analyze the batch of search results and returns their malware reports to device **100**.

[0081] At operation **1250**, warning generator **140A** displays a list of the search results in the batch together with the threat levels of content located at each result. Reference is made to **FIG. 19**, which is a screen shot of a warning regarding potential risks of search results in accordance with an embodiment of the present invention. Reference is made to **FIG. 20**, which is a screen shot of a safe assessment of search results in accordance with an embodiment of the present invention.

[0082] At operation **1255**, the user requests more information about the nature of the threat for one or more of the search results in the list; e.g., the result marked "*CAUTION*" in **FIG. 19**. At operation **1260**, warning generator **140B** displays information about the nature of the threat and/or the location of the one or more search result.

[0083] At operation **1265**, after having seen the information displayed by warning generator **140B**, the user requests access to one of the search results. At operation **1270**, warning generator **140C** displays a warning instructing the user to perform a confirmatory gesture, such as a swipe gesture, to confirm his request. At operation **1275**, the user performs the confirmatory gesture.

[0084] At operation **1280**, in response to the user having performed the confirmatory gesture at operation **1275**, web browser **130** attempts to access the requested search result. However, it may be that the requested search result redirects web browser **130** to a different web site. Device **100** may register itself to listen to redirection events for web browser **130** and, as such, is able to hook web browser **130** before it accesses the different web site. At decision **1285**, device **100** decides whether or not web browser **130** has been redirected. If so, processing returns to operation **1010** of **FIG. 2**, where device **100** passes an identifier for the redirected web site to scan engine(s) **300** for analysis. Otherwise, if decision **1285** decides that web browser **130** has not been redirected, processing advances to operation **1290**, where web browser **130** accesses the content that the user requested at operation **1265**. The user then views and interacts with the content at operation **1295**, thereby completing flowchart **1200**.

[0085] Reference is made to **FIG. 21**, which is a simplified flowchart **1300** of a server-based method for malware warning for search results, in accordance with an embodiment of the present invention. The flowchart of **FIG. 21** is divided into five columns. The leftmost column indicates operations performed by a user, the second-from-leftmost column indicates operations performed by device **100**, the middle column

indicates operations performed by search engine(s) **350**, the second-from-rightmost column indicates operations performed by server **200**, and the rightmost column indicates operation performed by scan engine(s) **300**.

[0086] At operation **1305** the user enters either an identifier for web site content, or a search term. At decision **1310** device **100** decides whether or not the user entered a search term. Decision **1310** may be performed as described above with reference to decision **1210** of **FIG. 18**. If decision **1310** decides that the user did not enter a search term, then at operation **1315** flowchart **1300** advances to operation **1110** of **FIG. 16**; namely, a method for malware warning for identifiers.

[0087] Otherwise, if decision **1310** decides that the user did enter a search term, then at operation **1320** device **100** passes the search term to search engine(s) **350**. At operation **1325** search engine(s) **350** perform their search and return their search results to device **100**. At operation **1330** device **100** receives the search results, but prior to displaying them to the user, device **100** passes a batch of the search results to server **200** for a malware check.

[0088] At operation **1335** server **200** passes a batch of search results to scan engine(s) **300** for scanning. At operation **1340**, scan engine(s) **300** scan the batch of search results, and return malware reports to server **200**. At operation **1345** server **200** passes the reports back to device **100**.

[0089] Subsequent operations **1350** – **1395** are similar to correspondingly numbered operations **1250** – **1295** of **FIG. 18**.

[0090] As described above, in an alternative embodiment of the present invention, server 200, instead of device 100, passes the search terms to

search engine(s) 350. In this case, instead of operation **1330**, device **100** passing the search results to server **200** subsequent to operation **1325**, device **100** instead passes the search terms to server **200** prior to operation **1325**.

[0091] Reference is made to **FIG. 22**, which is a simplified flow diagram using display screens to illustrate stages of a server-based malware warning mechanism for web search results, in accordance with an embodiment of the present invention. **FIG. 22** includes server **200**, virus scan engine(s) **300** and search engine(s) **350**. Screen **440** is a landing screen, prompting a user to enter a search expression. Screen **450** is a loading screen. While screen **420** is being displayed, device **100** sends the search expression that was entered in screen **410** to search engine(s) **350**. After receiving a page of search results, device **100** sends the results to server **200**, which sends the URLs of the search results to virus scan engine(s) **300** for analysis. Server **200** returns the malware reports to client **100**, and warning generator **140A** displays a list of results together with their levels of threat, as shown in screen **460**.

[0092] If the user touches one of the results to request information about the nature of the threat, then processor **210** performs the warning method of **FIG. 2** beginning at operation **1015**, and warning generator **140B** generates warning information, such as the information shown in **FIGS. 7**, **9** and **11** for the respective "*DANGER*", "*CAUTION*" and "*SAFE*" threat levels.

[0093] Thus is will be appreciated by those skilled in the art that the present invention prevents a "*one touch too late*" catastrophe and ensures that a user does not access suspect malware unintentionally, by provide multiple warnings about specific malware that a user is

encountering, and by requiring a confirmatory action from the user that is different than a simple touch, prior to accessing a suspicious web site, application or file.

[0094] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made to the specific exemplary embodiments without departing from the broader spirit and scope of the invention. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A non-transitory computer readable medium storing instructions, which, when executed by a processor of an electronic device, cause the processor to:

receive an identifier for accessing content at a destination web site;

in response to receiving the identifier, generate a warning comprising a threat level of content located at the destination web site;

receive a request for more information about the nature of the threat;

in response to receiving the request for more information, generate a warning comprising information about at least one of (i) the nature of the threat of the content, and (ii) a location of the destination web site;

receive a request to access the content; and

in response to receiving the request to access the content, generating a warning comprising an instruction to perform a confirmatory touch gesture to confirm the request to access the content.

2. The computer readable medium of claim **1** wherein the identifier is a URL.

3. The computer readable medium of claim **1** wherein the confirmatory touch gesture is a swipe gesture.

4. The computer readable medium of claim **1** wherein the instructions further cause the processor to:

in response to detecting the confirmatory touch gesture, attempt to access the content at the destination web site;

recognize an event that the identifier is being re-directed by the destination web site to another identifier; and

prior to accessing the content using the other identifier, repeating operations of claim **1** using the other identifier.

5. A malware warning module for an electronic device, comprising:

a touch-enabled input module, receiving touch-based user input;

a first warning generator, generating a warning comprising a threat level of content located at a destination web site, in response to said one or more input devices receiving an identifier for accessing content at the destination web site;

a second warning generator, generating a warning comprising information about at least one of (i) the nature of the threat of the content, and (ii) a location of the destination web site, in response to said one or more input devices receiving a request for more information about the nature of the threat; and

a third warning generator, generating a warning comprising an instruction to perform a confirmatory touch gesture to confirm a request to access the content, in response to said one or more input devices receiving a request to access the content.

6. The module of claim **5** wherein the identifier is a URL.

7. The module of claim **5** wherein the confirmatory touch gesture is a swipe gesture.

8. The module of claim **5** further comprising a content accessor, attempting to access the content in response to detecting the confirmatory touch gesture, recognizing an event that the identifier is being re-directed by the destination web site to another identifier, and re-invoking said first, second and third warning generators with the other identifier, prior to accessing the content using the other identifier.

9. A malware warning system, comprising:

a touch-enabled client computing device sending requests to and receiving replies from a server computing device; and

a server computing device receiving the requests from the client, comprising:

a first warning generator, sending to the client a warning comprising a threat level of content located at a destination web site, in response to receiving from the client an identifier for accessing content at the destination web site;

a second warning generator, sending to the client a warning comprising information about at least one of (i) the nature of the threat of the content, and (ii) a location of the destination web site, in response to receiving from the client a request for more information about the nature of the threat; and

a third warning generator, sending to the client a warning comprising an instruction to perform a swipe gesture to confirm a

request to access the content, in response to receiving from the client a request to access the content.

10. The system of claim **9** wherein the identifier is a URL.

11. The system of claim **9** wherein the confirmatory touch gesture is a swipe gesture.

12. The system of claim **9** wherein said server further comprises a content accessor, attempting to access the content in response to detecting that the confirmatory touch gesture has been performed on said client, recognizing an event that the identifier is being re-directed by the destination web site to another identifier, and re-invoking said first, second and third warning generators with the other identifier, prior to accessing the content using the other identifier.

13. A non-transitory computer readable medium storing instructions, which, when executed by a processor of an electronic device, cause the processor to:

receive an identifier for accessing content at a destination web site;

in response to receiving the identifier, generate a warning comprising a threat level of content located;

receive a request to access the content; and

in response to receiving the request to access the content, generate a warning comprising an instruction to perform a confirmatory touch gesture to confirm the request to access the content.

14. The computer readable medium of claim **13** wherein the identifier is a URL.

15. The computer readable medium of claim **13** wherein the confirmatory touch gesture is a swipe gesture.

16. The computer readable medium of claim **13** wherein the instructions further cause the processor to:

in response to detecting the confirmatory touch gesture, attempt to access the content at the destination web site;

recognize an event that the identifier is being re-directed by the destination web site to another identifier; and

prior to accessing the content using the other identifier, repeating operations of claim **13** using the other identifier.

17. A malware warning module for an electronic device, comprising:

one or more touch-enabled input devices receiving user input;

a first warning generator, generating a warning comprising a threat level of content located at a destination web site, in response to said one or more input devices receiving an identifier for accessing content at the destination web site; and

a second warning generator, generating a warning comprising an instruction to perform a confirmatory touch gesture to confirm a request to access the content, in response to said one or more input devices receiving a request to access the content.

18. The module of claim **17** wherein the identifier is a URL.

19. The module of claim **17** wherein the confirmatory touch gesture is a swipe gesture.

20. The module of claim **17** further comprising a content accessor, attempting to access the content in response to detecting the confirmatory touch gesture, recognizing an event that the identifier is being re-directed by the destination web site to another identifier, and re-invoking said first, second and third warning generators with the other identifier, prior to accessing the content using the other identifier.

21. A malware warning system, comprising:

a touch-enabled client computer device sending requests to and receiving replies from a server computing device; and

a server computing device receiving the requests from the client computer device, comprising:

a first warning generator, sending to the client a warning comprising a threat level of content located at a destination web site, in response to receiving from the client an identifier for accessing content at the destination web site; and

a second warning generator, sending to the client a warning comprising an instruction to perform a confirmatory touch gesture to confirm a request to access the content, in response to receiving from the client a request to access the content.

22. The system of claim **21** wherein the identifier is a URL.

23. The system of claim **21** wherein the confirmatory touch gesture is a swipe gesture.

24. The system of claim **21** wherein said server further comprises a content accessor, attempting to access the content in response to detecting that the confirmatory touch gesture has been performed on said client, recognizing an event that the identifier is being re-directed by the destination web site to another identifier, and re-invoking said first, second and third warning generators with the other identifier, prior to accessing the content using the other identifier.

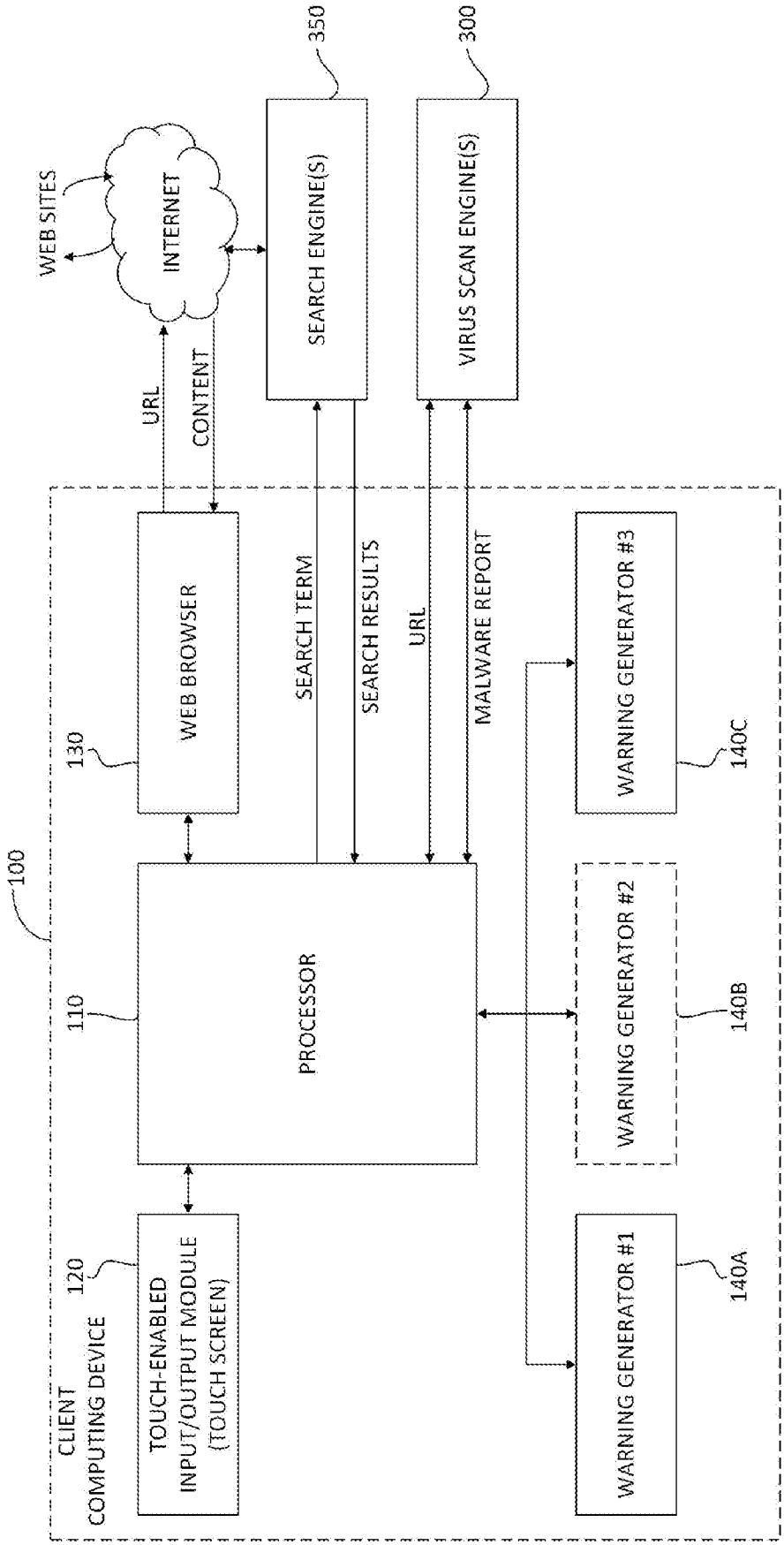
WEB SITES
INTERNET
350
SEARCH ENGINE(S)
300
VIRUS SCAN ENGINE(S)
URL
CONTENT
SEARCH TERM
SEARCH RESULTS
URL
MALWARE REPORT
100
130
WEB BROWSER
110
PROCESSOR
WARNING GENERATOR #3
140C
WARNING GENERATOR #2
140B
WARNING GENERATOR #1
140A
CLIENT COMPUTING DEVICE
120
TOUCH-ENABLED INPUT/OUTPUT MODULE (TOUCH SCREEN)

FIG. 1

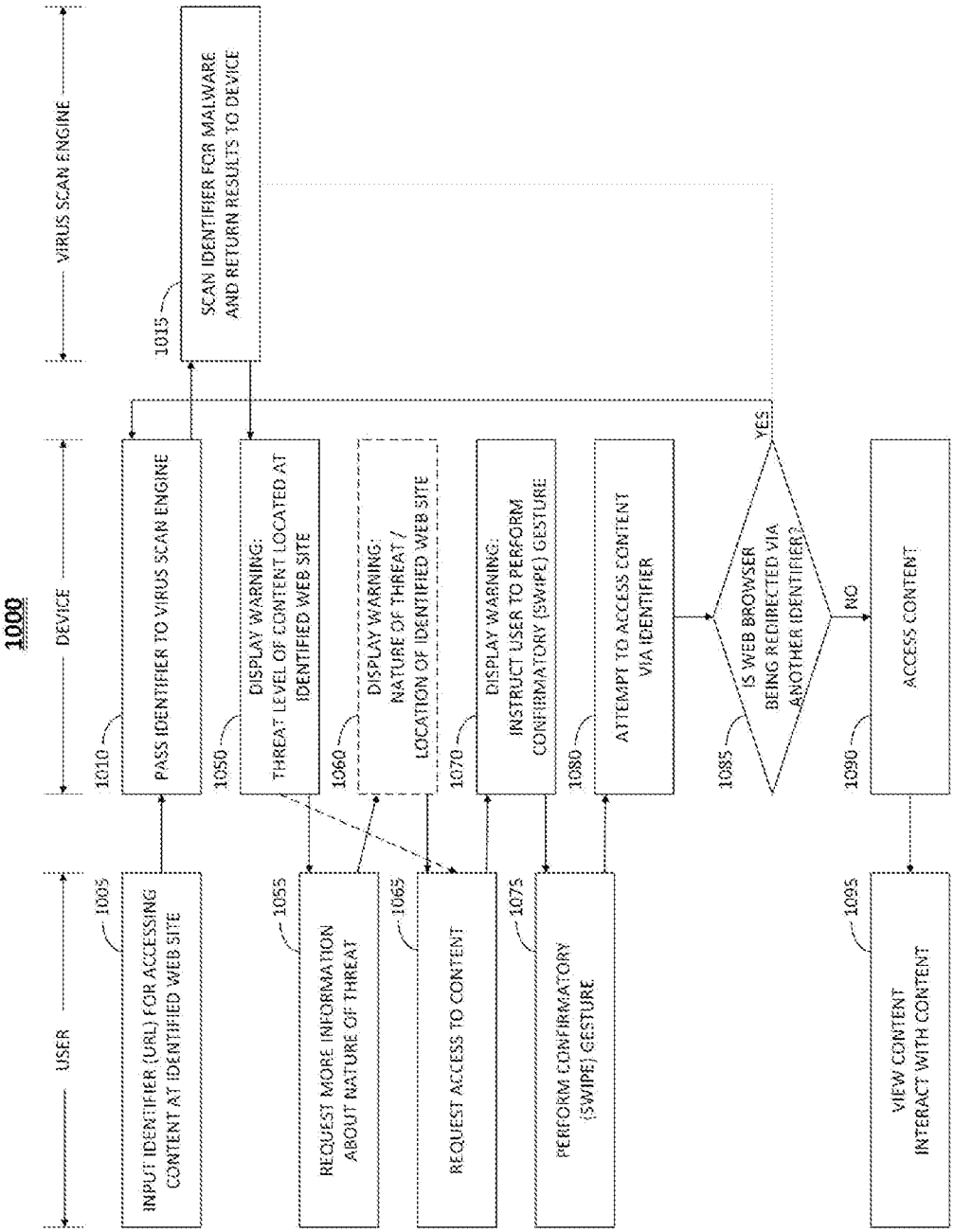
1000
USER
DEVICE
VIRUS SCAN ENGINE
1005
INPUT IDENTIFIER (URL) FOR ACCESSING CONTENT AT IDENTIFIED WEB SITE
1010
PASS IDENTIFIER TO VIRUS SCAN ENGINE
1015
SCAN IDENTIFIER FOR MALWARE AND RETURN RESULTS TO DEVICE
1050
DISPLAY WARNING: THREAT LEVEL OF CONTENT LOCATED AT IDENTIFIED WEB SITE
1055
REQUEST MORE INFORMATION ABOUT NATURE OF THREAT
1060
DISPLAY WARNING: NATURE OF THREAT / LOCATION OF IDENTIFIED WEB SITE
1065
REQUEST ACCESS TO CONTENT
1070
DISPLAY WARNING: INSTRUCT USER TO PERFORM CONFIRMATORY (SWIPE) GESTURE
1075
PERFORM CONFIRMATORY (SWIPE) GESTURE
1080
ATTEMPT TO ACCESS CONTENT VIA IDENTIFIER
1085
IS WEB BROWSER BEING REDIRECTED VIA ANOTHER IDENTIFIER?
YES
NO
1090
ACCESS CONTENT
1095
VIEW CONTENT
INTERACT WITH CONTENT

FIG. 2

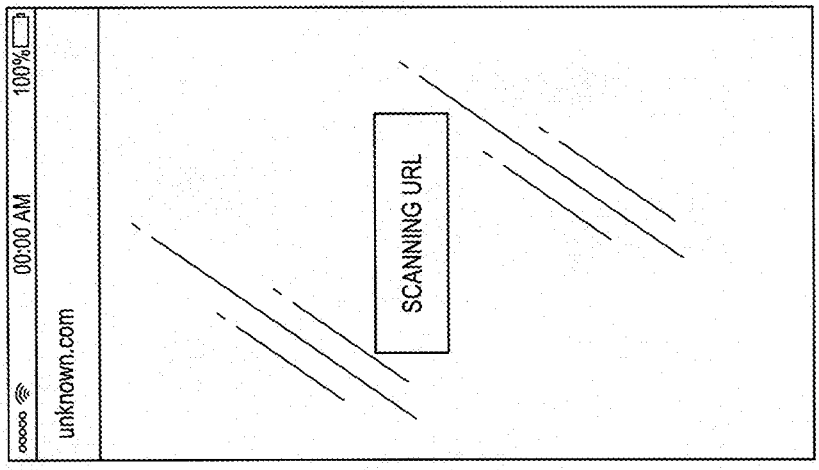
00:00 AM
100%
unknown.com
SCANNING URL

FIG. 4

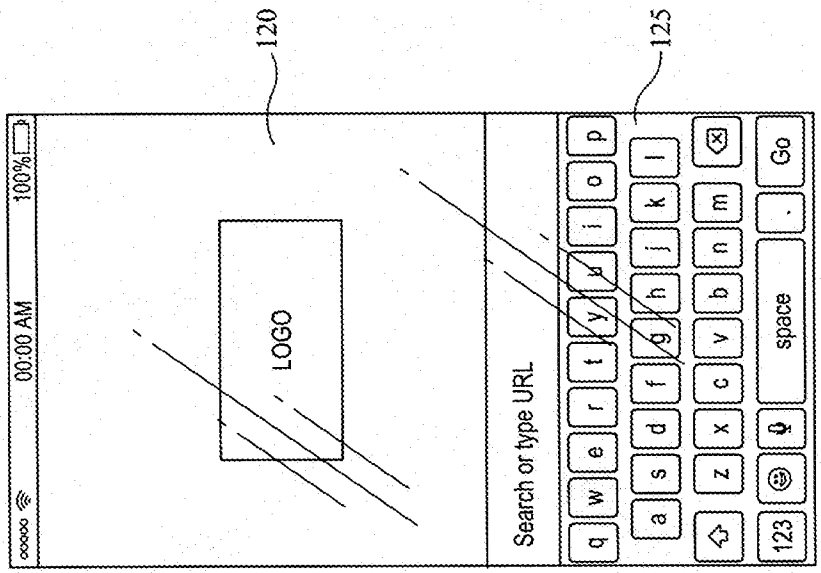
120
125
00:00 AM
100%
LOGO
Search or type URL
Go
space

FIG. 3

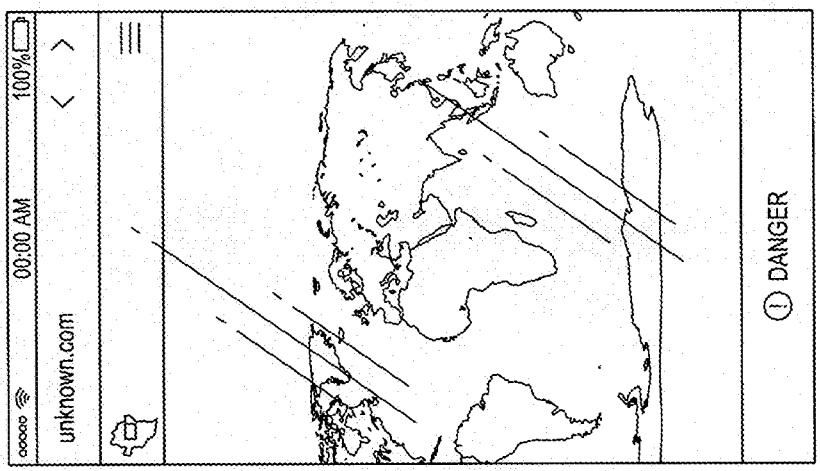
00:00 AM
100%
unknown.com
DANGER

FIG. 6

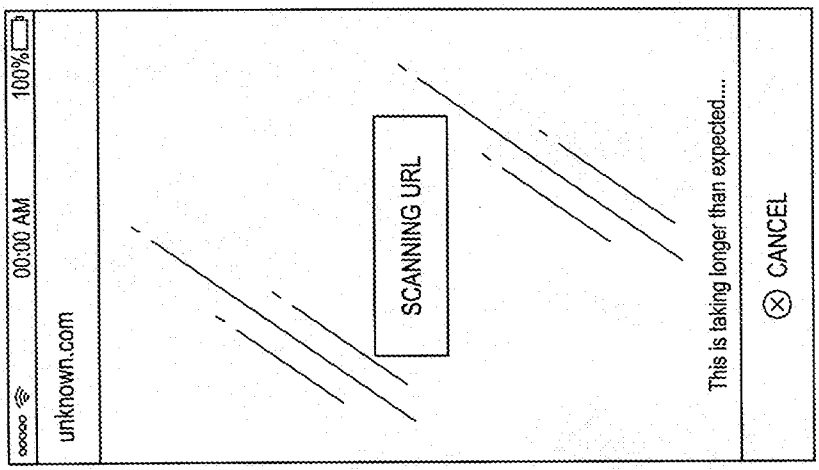
00:00 AM
100%
unknown.com
SCANNING URL
This is taking longer than expected....
CANCEL

FIG. 5

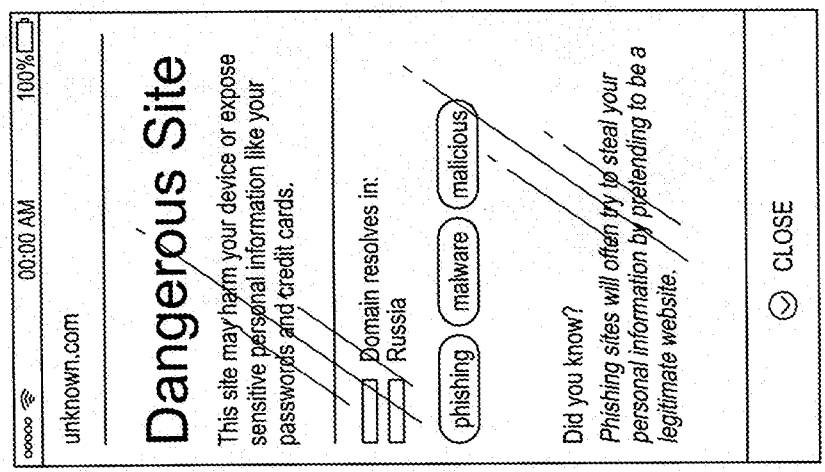
00:00 AM
100%
unknown.com
CAUTION

FIG. 8

00:00 AM
100%
unknown.com
Dangerous Site
This site may harm your device or expose sensitive personal information like your passwords and credit cards.
Domain resolves in:
Russia
phishing
malware
malicious
Did you know?
Phishing sites will often try to steal your personal information by pretending to be a legitimate website.
CLOSE

FIG. 7

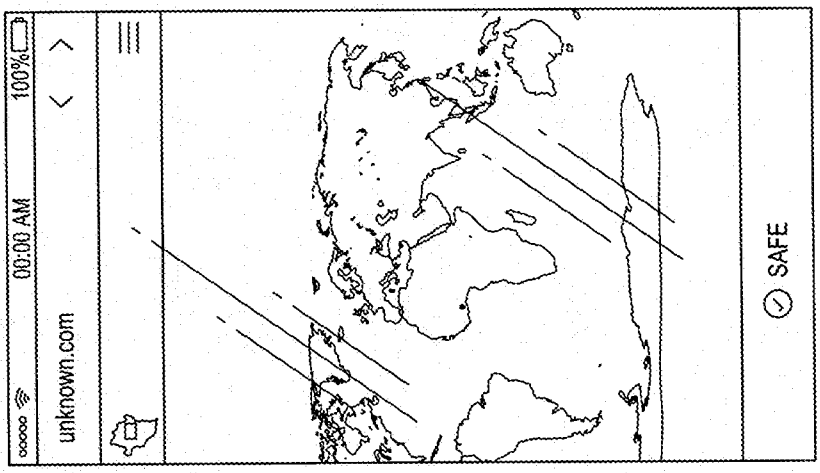
00:00 AM
100%
unknown.com
SAFE

FIG. 10

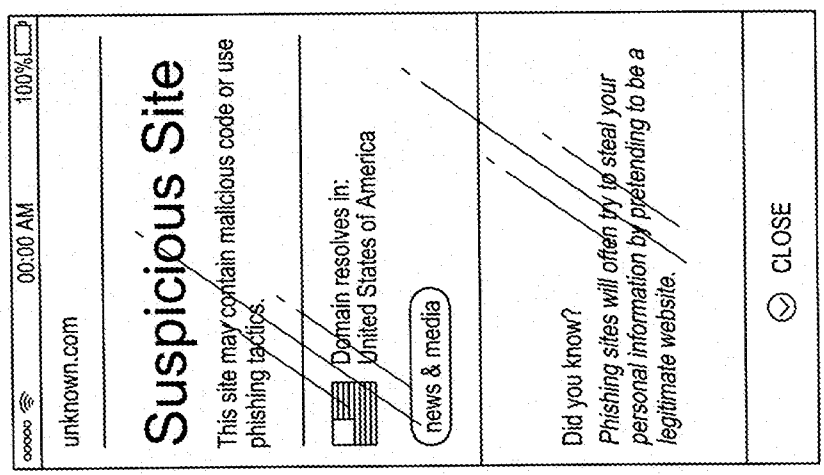
00:00 AM
100%
unknown.com
Suspicious Site
This site may contain malicious code or use phishing tactics.
Domain resolves in:
United States of America
news & media
Did you know?
Phishing sites will often try to steal your personal information by pretending to be a legitimate website.
CLOSE

FIG. 9

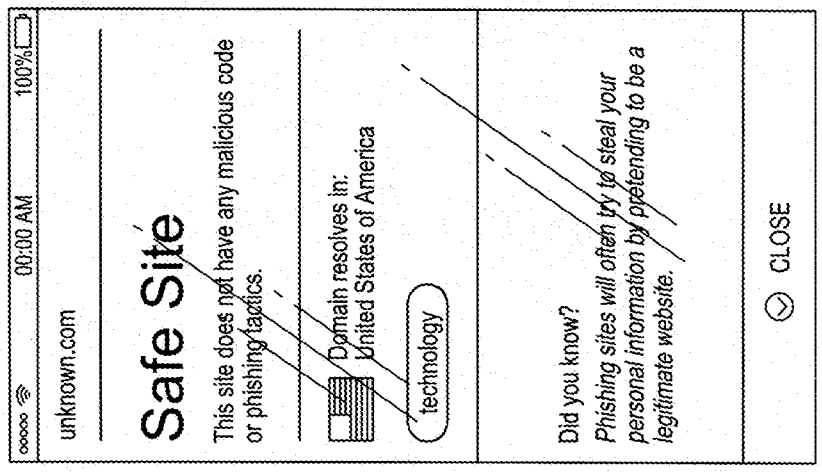
00:00 AM
100%
unknown.com
Safe Site
This site does not have any malicious code or phishing tactics.
Domain resolves in:
United States of America
technology
Did you know?
Phishing sites will often try to steal your personal information by pretending to be a legitimate website.
CLOSE

FIG. 11

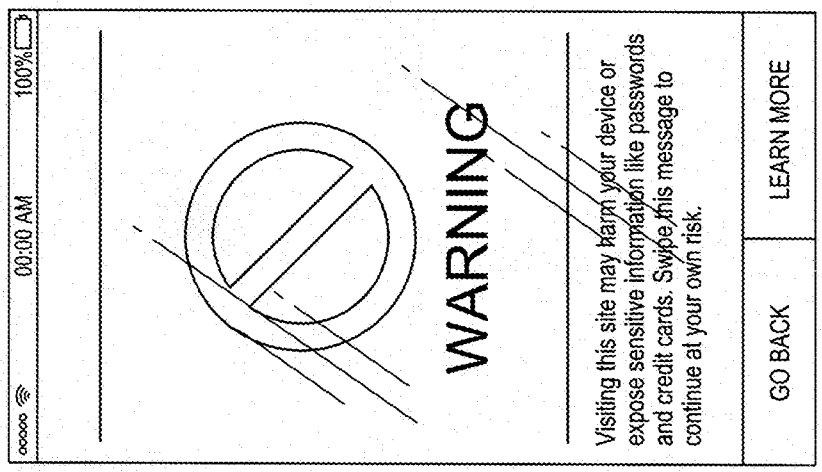
00:00 AM
100%
WARNING
Visiting this site may harm your device or expose sensitive information like passwords and credit cards. Swipe this message to continue at your own risk.
GO BACK
LEARN MORE

FIG. 12

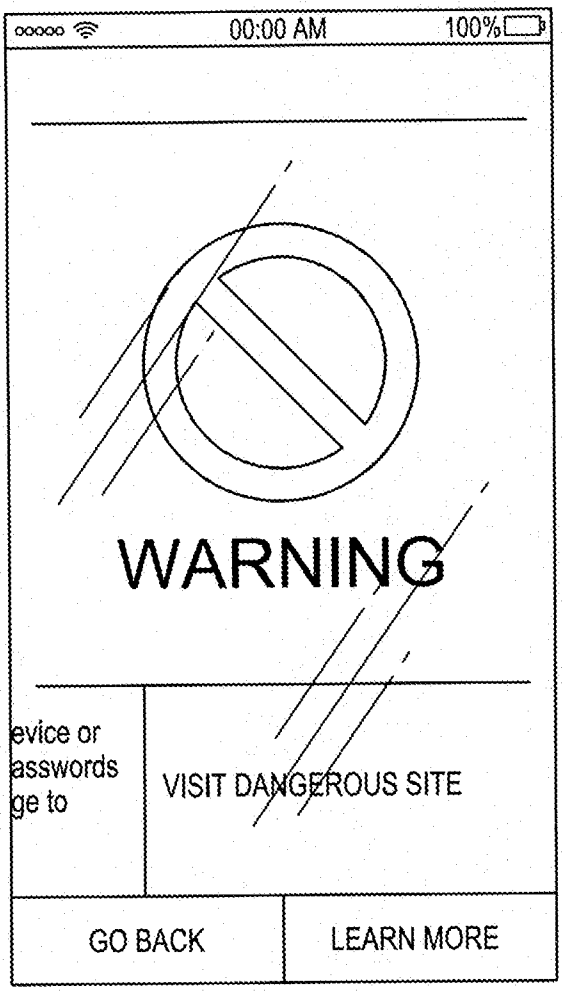
00:00 AM
100%
WARNING
evice or
asswords
ge to
VISIT DANGEROUS SITE
GO BACK
LEARN MORE

FIG. 13

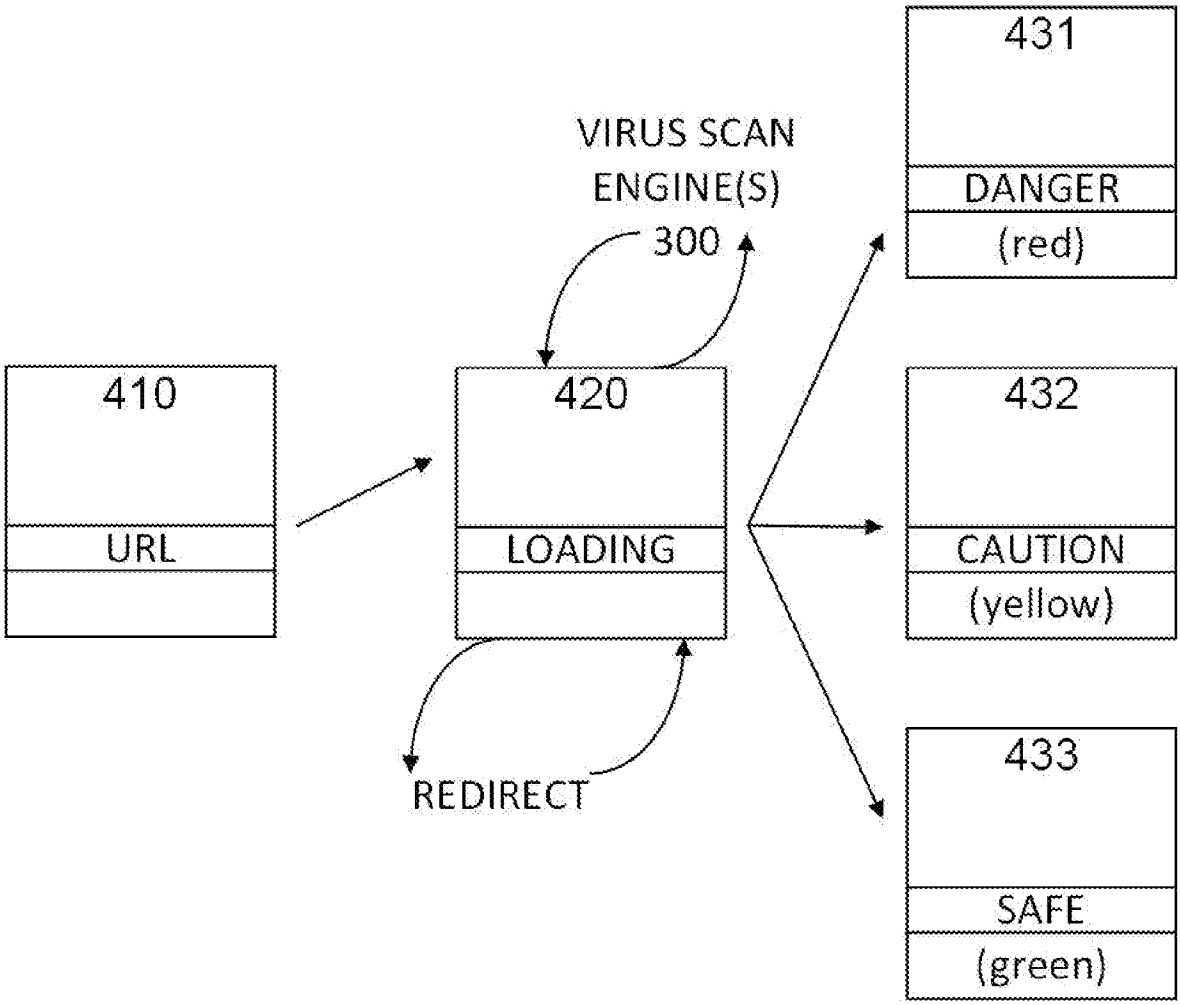
431
DANGER
(red)
VIRUS SCAN
ENGINE(S)
300
410
URL
420
LOADING
432
CAUTION
(yellow)
REDIRECT
433
SAFE
(green)

FIG. 14

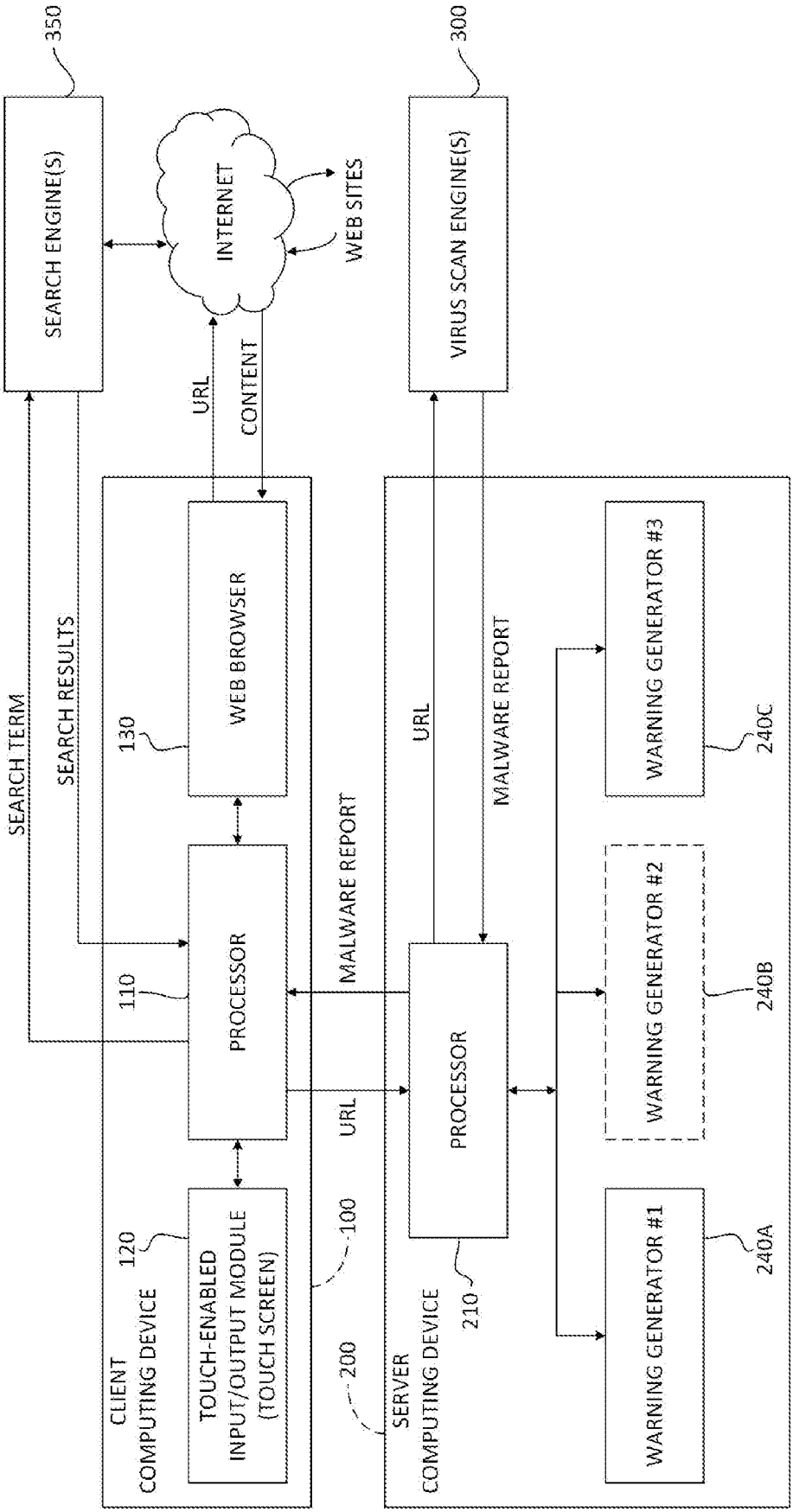
350
SEARCH ENGINE(S)
INTERNET
WEB SITES
300
VIRUS SCAN ENGINE(S)
URL
CONTENT
SEARCH TERM
SEARCH RESULTS
130
WEB BROWSER
110
PROCESSOR
MALWARE REPORT
URL
MALWARE REPORT
WARNING GENERATOR #3
240C
WARNING GENERATOR #2
240B
WARNING GENERATOR #1
240A
120
TOUCH-ENABLED INPUT/OUTPUT MODULE (TOUCH SCREEN)
CLIENT COMPUTING DEVICE
100
200
210
PROCESSOR
SERVER COMPUTING DEVICE

FIG. 15

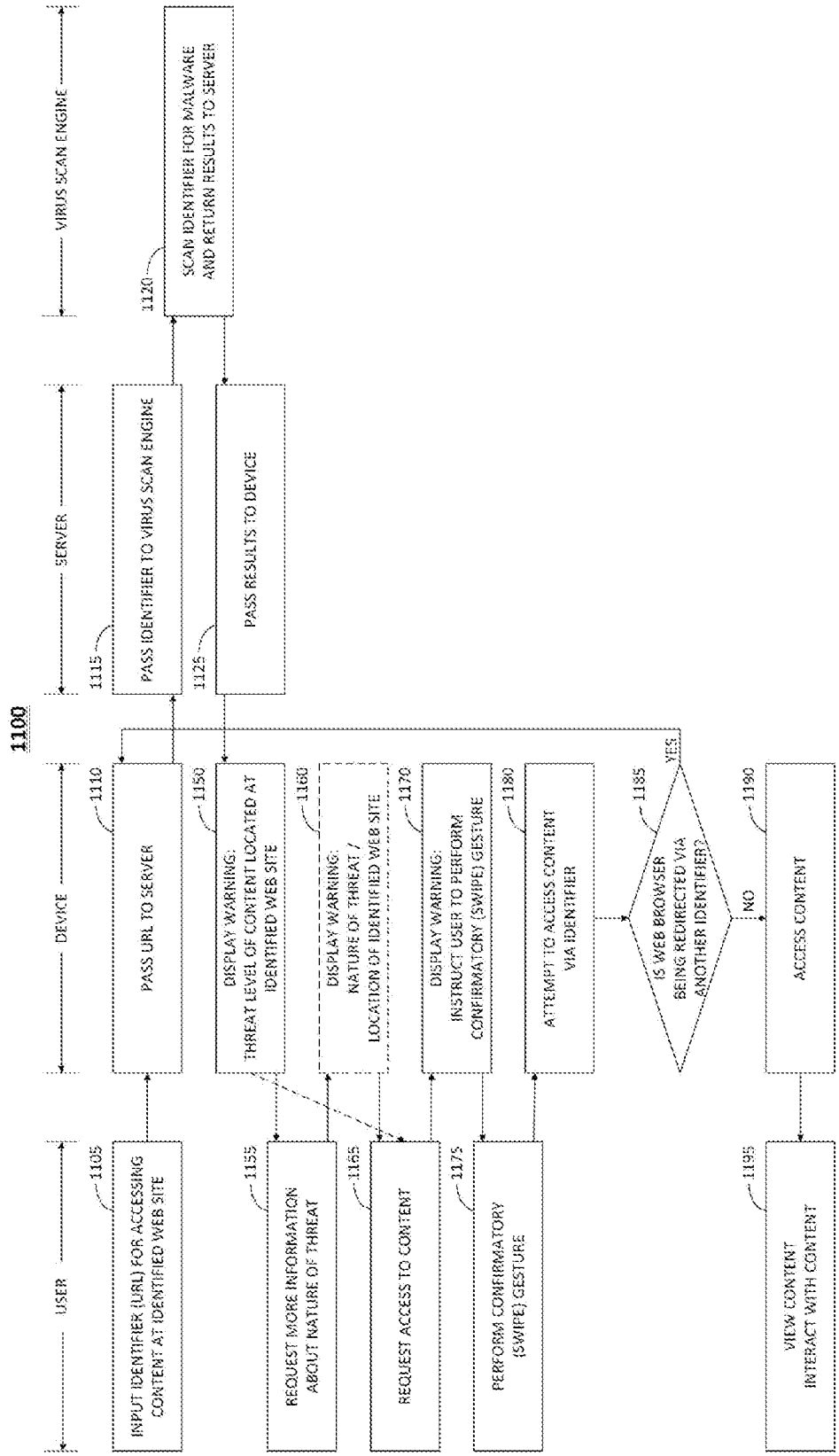
1100
USER
DEVICE
SERVER
VIRUS SCAN ENGINE
1105
INPUT IDENTIFIER (URL) FOR ACCESSING CONTENT AT IDENTIFIED WEB SITE
1110
PASS URL TO SERVER
1115
PASS IDENTIFIER TO VIRUS SCAN ENGINE
1120
SCAN IDENTIFIER FOR MALWARE AND RETURN RESULTS TO SERVER
1125
PASS RESULTS TO DEVICE
1150
DISPLAY WARNING: THREAT LEVEL OF CONTENT LOCATED AT IDENTIFIED WEB SITE
1155
REQUEST MORE INFORMATION ABOUT NATURE OF THREAT
1160
DISPLAY WARNING: NATURE OF THREAT / LOCATION OF IDENTIFIED WEB SITE
1165
REQUEST ACCESS TO CONTENT
1170
DISPLAY WARNING: INSTRUCT USER TO PERFORM CONFIRMATORY (SWIPE) GESTURE
1175
PERFORM CONFIRMATORY (SWIPE) GESTURE
1180
ATTEMPT TO ACCESS CONTENT VIA IDENTIFIER
1185
IS WEB BROWSER BEING REDIRECTED VIA ANOTHER IDENTIFIER?
YES
NO
1190
ACCESS CONTENT
1195
VIEW CONTENT INTERACT WITH CONTENT

FIG. 16

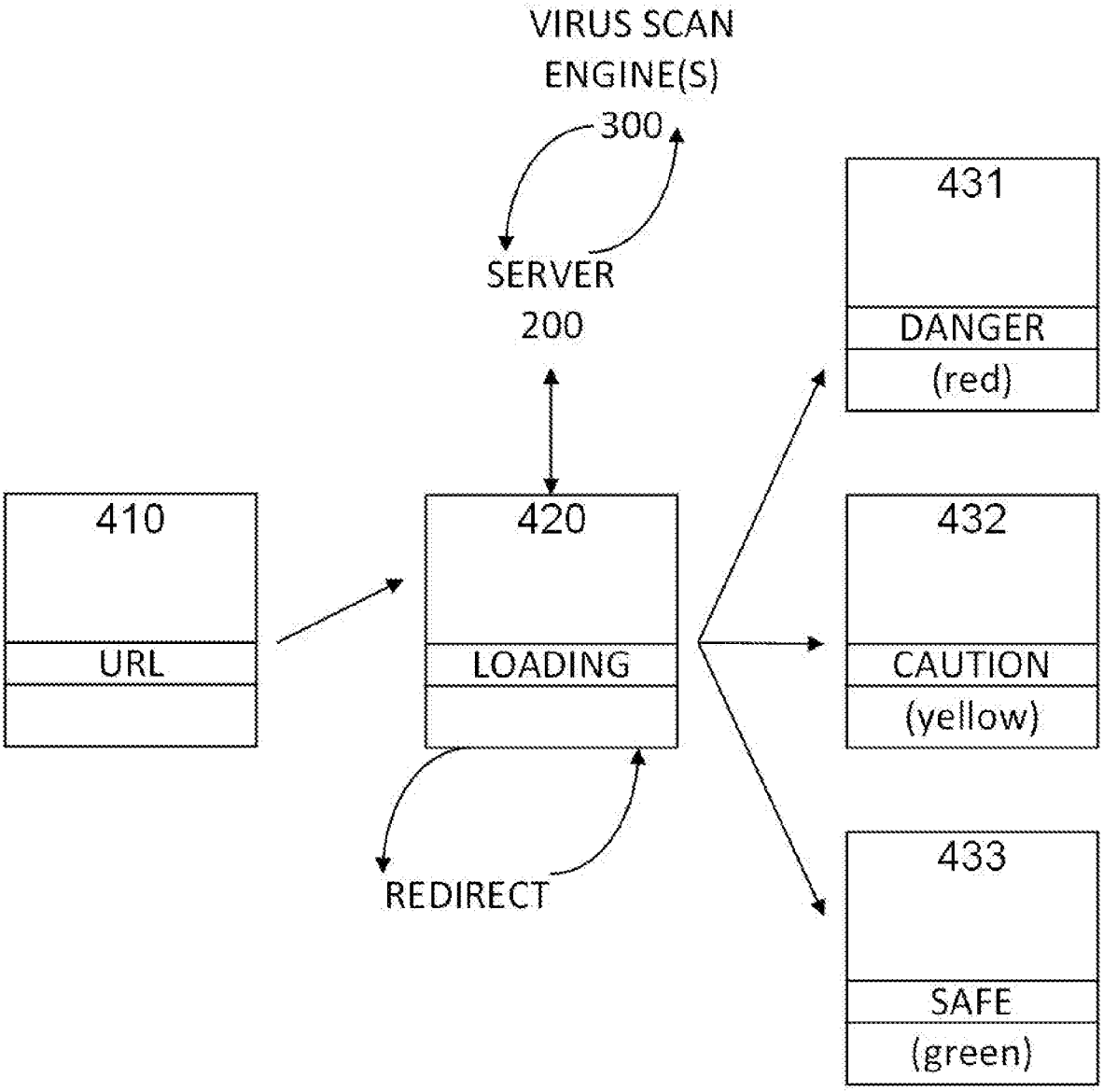
VIRUS SCAN
ENGINE(S)
300
SERVER
200
410
URL
420
LOADING
REDIRECT
431
DANGER
(red)
432
CAUTION
(yellow)
433
SAFE
(green)

FIG. 17

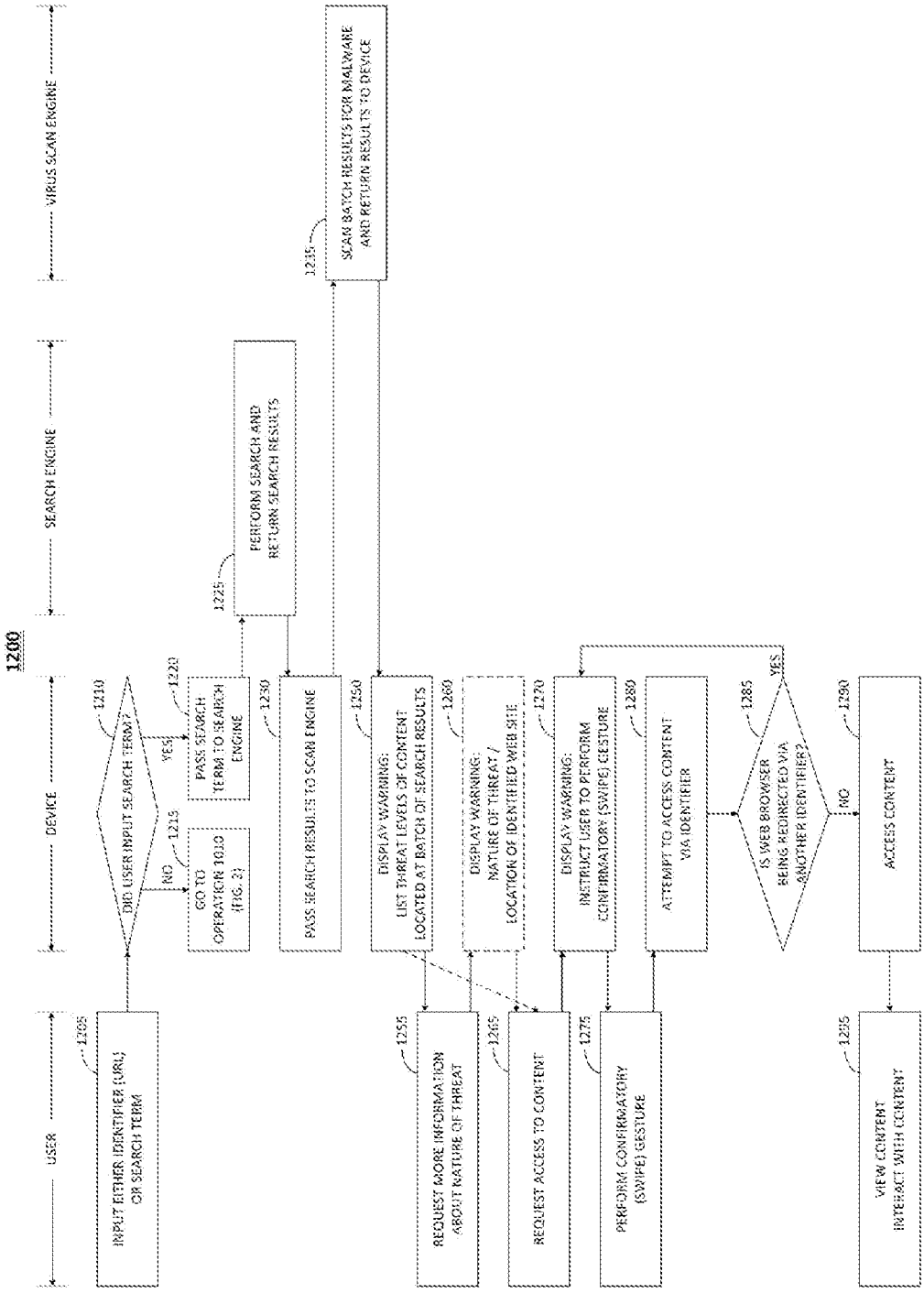
1200
USER
DEVICE
SEARCH ENGINE
VIRUS SCAN ENGINE
1205
INPUT EITHER IDENTIFIER (URL) OR SEARCH TERM
1210
DID USER INPUT SEARCH TERM?
YES
NO
1215
GO TO OPERATION 1010 (FIG. 2)
1220
PASS SEARCH TERM TO SEARCH ENGINE
1225
PERFORM SEARCH AND RETURN SEARCH RESULTS
1230
PASS SEARCH RESULTS TO SCAN ENGINE
1235
SCAN BATCH RESULTS FOR MALWARE AND RETURN RESULTS TO DEVICE
1250
DISPLAY WARNING: LIST THREAT LEVELS OF CONTENT LOCATED AT BATCH OF SEARCH RESULTS
1255
REQUEST MORE INFORMATION ABOUT NATURE OF THREAT
1260
DISPLAY WARNING: NATURE OF THREAT / LOCATION OF IDENTIFIED WEB SITE
1265
REQUEST ACCESS TO CONTENT
1270
DISPLAY WARNING: INSTRUCT USER TO PERFORM CONFIRMATORY (SWIPE) GESTURE
1275
PERFORM CONFIRMATORY (SWIPE) GESTURE
1280
ATTEMPT TO ACCESS CONTENT VIA IDENTIFIER
1285
IS WEB BROWSER BEING REDIRECTED VIA ANOTHER IDENTIFIER?
YES
NO
1290
ACCESS CONTENT
1295
VIEW CONTENT / INTERACT WITH CONTENT

FIG. 18

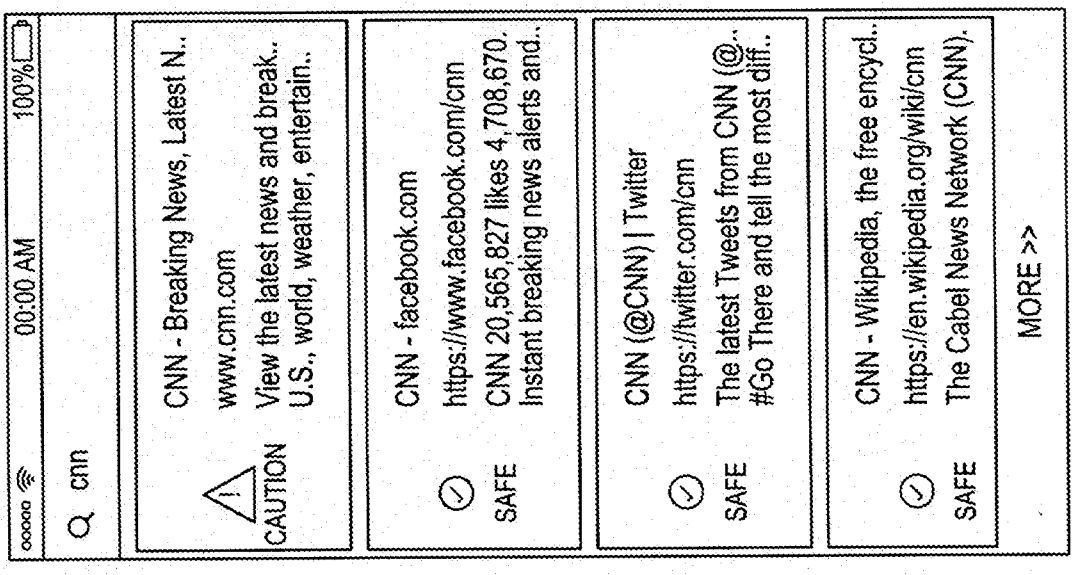
00:00 AM
100%
cnn
CNN - Breaking News, Latest N..
www.cnn.com
View the latest news and break..
U.S., world, weather, entertain..
CAUTION
CNN - facebook.com
https://www.facebook.com/cnn
CNN 20,565,827 likes 4,708,670.
Instant breaking news alerts and..
SAFE
CNN (@CNN) | Twitter
https://twitter.com/cnn
The latest Tweets from CNN (@..
#Go There and tell the most diff..
SAFE
CNN - Wikipedia, the free encycl..
https://en.wikipedia.org/wiki/cnn
The Cabel News Network (CNN).
SAFE
MORE >>

FIG. 19

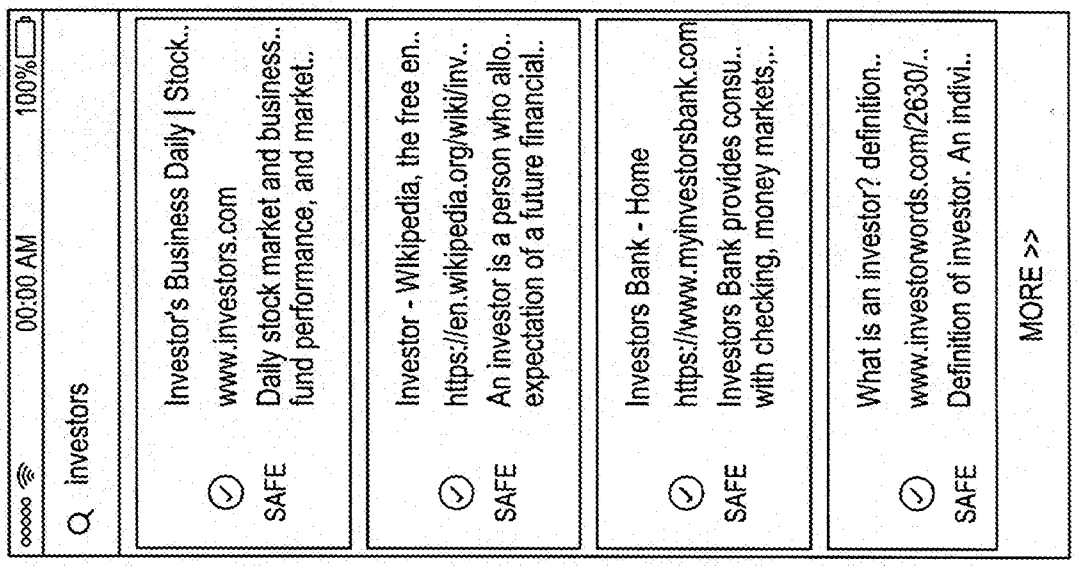
00:00 AM
100%
investors
Investor's Business Daily | Stock..
www.investors.com
Daily stock market and business..
fund performance, and market..
SAFE
Investor - Wikipedia, the free en..
https://en.wikipedia.org/wiki/inv..
An investor is a person who allo..
expectation of a future financial..
SAFE
Investors Bank - Home
https://www.myinvestorsbank.com
Investors Bank provides consu..
with checking, money markets,..
SAFE
What is an investor? definition..
www.investorwords.com/2630/..
Definition of investor. An indivi..
SAFE
MORE >>

FIG. 20

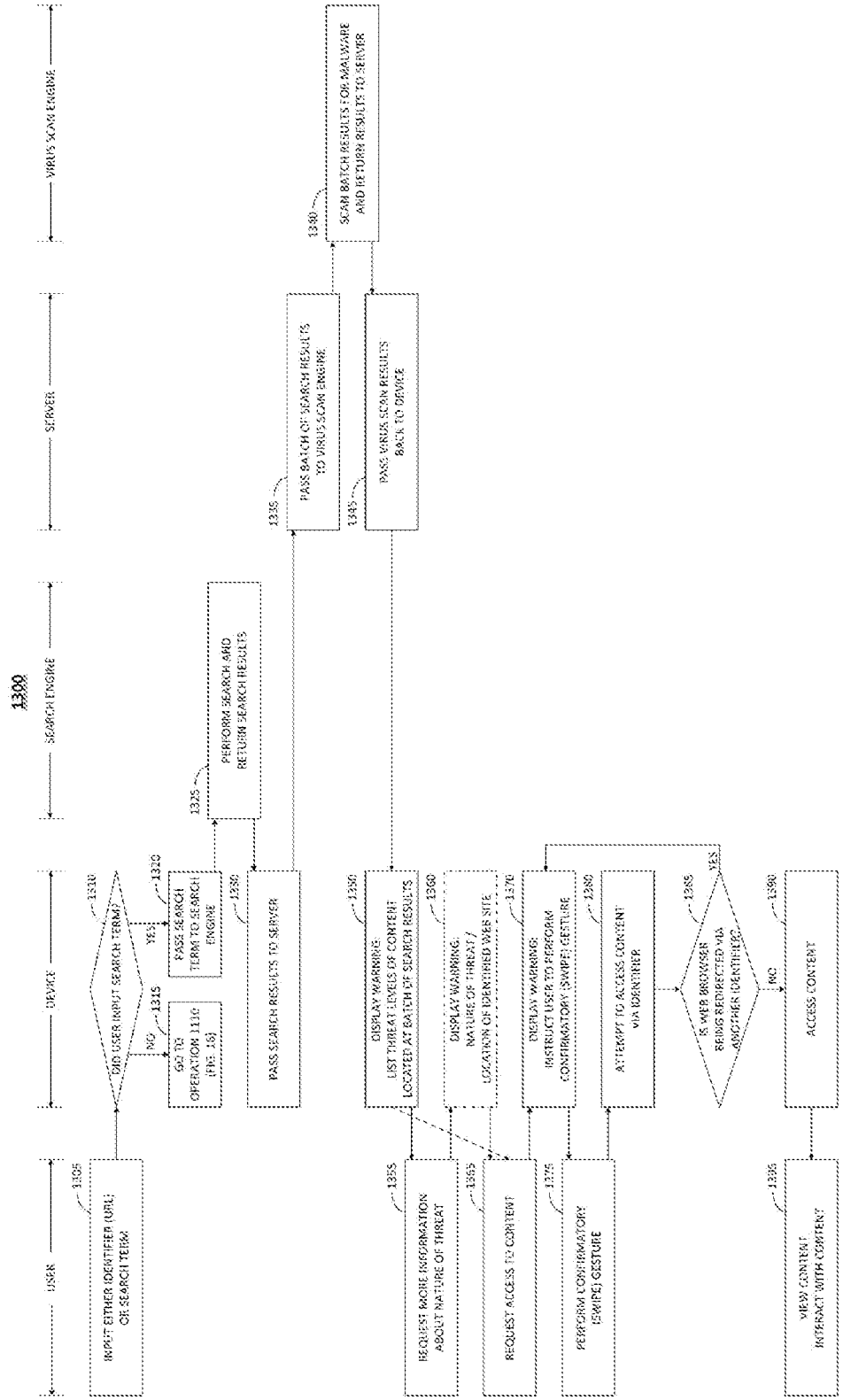
1300
USER
DEVICE
SEARCH ENGINE
SERVER
VIRUS SCAN ENGINE
INPUT EITHER IDENTIFIER (URL) OR SEARCH TERM
1305
DID USER INPUT SEARCH TERM?
1310
YES
PASS SEARCH TERM TO SEARCH ENGINE
1320
NO
GO TO OPERATION 1110 (FIG. 16)
1315
PERFORM SEARCH AND RETURN SEARCH RESULTS
1325
PASS SEARCH RESULTS TO SERVER
1330
PASS BATCH OF SEARCH RESULTS TO VIRUS SCAN ENGINE
1335
SCAN BATCH RESULTS FOR MALWARE AND RETURN RESULTS TO SERVER
1340
PASS VIRUS SCAN RESULTS BACK TO DEVICE
1345
DISPLAY WARNING: LIST THREAT LEVELS OF CONTENT LOCATED AT BATCH OF SEARCH RESULTS
1350
DISPLAY WARNING: NATURE OF THREAT / LOCATION OF IDENTIFIED WEB SITE
1360
DISPLAY WARNING: INSTRUCT USER TO PERFORM CONFIRMATORY (SWIPE) GESTURE
1370
ATTEMPT TO ACCESS CONTENT VIA IDENTIFIER
1380
IS WEB BROWSER BEING REDIRECTED VIA ANOTHER IDENTIFIER?
1385
YES
NO
ACCESS CONTENT
1390
REQUEST MORE INFORMATION ABOUT NATURE OF THREAT
1355
REQUEST ACCESS TO CONTENT
1365
PERFORM CONFIRMATORY (SWIPE) GESTURE
1375
VIEW CONTENT / INTERACT WITH CONTENT
1395

FIG. 21

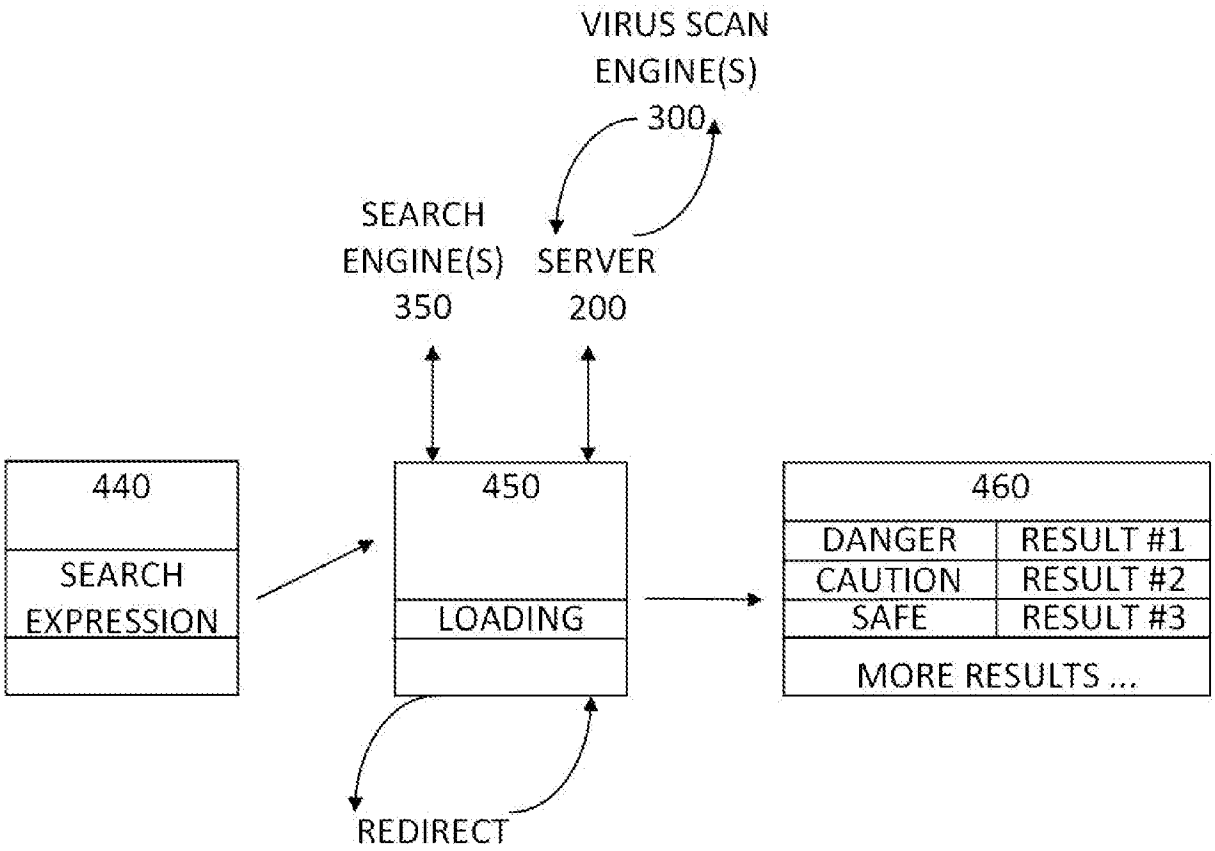
VIRUS SCAN ENGINE(S) 300
SEARCH ENGINE(S) 350
SERVER 200
440
SEARCH EXPRESSION
450
LOADING
460
DANGER
RESULT #1
CAUTION
RESULT #2
SAFE
RESULT #3
MORE RESULTS ...
REDIRECT

FIG. 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/026856

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 29/06; H04L 29/08; G06F 7/04; G06F 11/00; G06F 12/14; G06F 12/16 (2016.01)
CPC - H04L 63/1408; H04L 63/1416; H04L 63/1441; H04L 63/145; H04L 63/1483; H04L 67/02 (2016.02)
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(8) - G06F 7/04; G06F 11/00; G06F 12/14; G06F 12/16; G06F 21/00; G06F 21/50; G06F 21/56; G06Q 20/00; G06Q 20/10 (2016.01)
CPC - H04L 63/14; H04L 63/1408; H04L 63/1416; H04L 63/1441; H04L 63/145; H04L 63/1483; H04L 67/02; H04L 67/2814 (2016.02)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/52; 705/75; 713/188; 726/1; 726/5; 726/22; 726/23; 726/24; 726/25 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit, Google Patents, Google Scholar, Google
Search terms used: URL, malware, warning, threat, grant, access, confirmation, request, redirect, alert, mobile, device, swipe, gesture, touch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 8,869,271 B2 (JAYARAMAN et al) 21 October 2014 (21.10.2014) entire document	1-24
Y	US 2012/0047461 A1 (COLVIN et al) 23 February 2012 (23.02.2012) entire document	1-24
Y	US 8,904,495 B2 (BAGHDASARYAN et al) 02 December 2014 (02.12.2014) entire document	3, 7, 11, 15, 19, 23
A	US 2015/0067853 A1 (AMRUTKAR et al.) 05 March 2015 (05.03.2015) entire document	1-24
P,A	US 9,100,426 B1 (FANG) 04 August 2015 (04.08.2015) entire document	1-24
A	US 8,584,240 B1 (YANG et al.) 12 November 2013 (12.11.2013) entire document	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent 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
06 June 2016	11 JUL 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)