

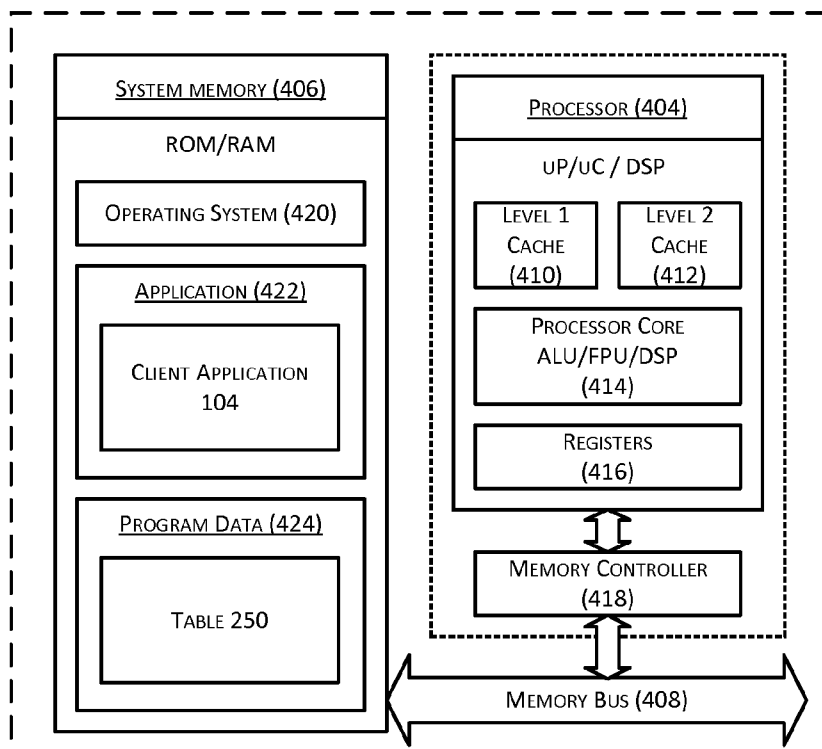


- (51) **International Patent Classification:**
G06F 11/00 (2006.01)
- (21) **International Application Number:**
PCT/US2012/049697
- (22) **International Filing Date:**
6 August 2012 (06.08.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant (for all designated States except US):** **EMPIRE TECHNOLOGY DEVELOPMENT LLC** [US/US];
2711 Centerville Road, Suite 400, Wilmington, DE 19808 (US).
- (72) **Inventor; and**
- (75) **Inventor/Applicant (for US only):** **UR, Shmuel** [IL/IL];
Shorashim, 20164 Galil (IL).
- (74) **Agent:** **LEE, David, S.**; Brundidge & Stanger, P.c., 2318
Mill Road, Suite 1020, Alexander, VA 22314 (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, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

- (54) **Title:** DEFENDING AGAINST BROWSER ATTACKS



- (57) **Abstract:** In one example the opening of a primary browser to a URL may be detected, a reference browser may then be opened to the same URL, data input to respective data fields on the primary browser may be copied to respectively corresponding data fields on the reference browser, and security on the primary browser may be evaluated based on, at least, the data copied to the reference browser.

WO 2014/025334 A1



Published:

— *with international search report (Art. 21(3))*

DEFENDING AGAINST BROWSER ATTACKS**TECHNICAL FIELD**

[0001] The embodiments described herein pertain generally to implementing one or more safeguards against unauthorized transactions that may be executed due to browser attacks.

BACKGROUND

[0002] As the proportion of commerce that is conducted online increases, so do attempts to exploit the technology that enables and facilitates such transactions for illegal gain. In particular, browser attacks may be utilized to exploit a user's legitimate access to a website for a financial institution or place of commerce by conducting stealth transactions.

SUMMARY

[0003] In one example embodiment, a computer-readable medium stores one or more computer-executable instructions that cause one or more processors to detect that a primary browser has opened to a URL, open a reference browser to the URL, copy data input to respective data fields on the primary browser to respectively corresponding data fields on the reference browser, and evaluate security on the primary browser based on, at least, the data copied to the reference browser.

[0004] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described

above, further aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] In the detailed description that follows, embodiments are described as illustrations only since various changes and modifications will become apparent to those skilled in the art from the following detailed description. The use of the same reference numbers in different figures indicates similar or identical items.

[0006] **FIG. 1** shows an example system configuration in which browser attacks may be defended against, arranged in accordance with at least some embodiments described herein;

[0007] **FIG. 2** shows an example configuration of a reference browser relative to the example system of **FIG. 1**, arranged in accordance with at least some embodiments described herein;

[0008] **FIG. 3** shows an example configuration of a processing flow of operations for defending against browser attacks, in accordance with at least some embodiments described herein; and

[0009] **FIG. 4** shows a block diagram illustrating an example computing device by which various example solutions described herein may be implemented, arranged in accordance with at least some embodiments described herein.

DETAILED DESCRIPTION

[0010] In the following detailed description, reference is made to the accompanying drawings, which form a part of the description. In the drawings, similar symbols typically identify similar components, unless context dictates otherwise. Furthermore, unless otherwise noted, the description of each successive drawing may reference features from one or more of the previous drawings to provide clearer context and a more substantive explanation of the current example embodiment. Still, the example embodiments described in the detailed description, drawings, and claims are not meant to be limiting. Other embodiments may be utilized, and other changes may be made, without departing from the spirit or scope of the subject matter presented herein. It will be readily understood that the aspects of the present disclosure, as generally described herein and illustrated in the drawings, may be arranged, substituted, combined, separated, and designed in a wide variety of different configurations, all of which are explicitly contemplated herein.

[0011] FIG. 1 shows an example system configuration 100 in which browser attacks may be defended against, arranged in accordance with at least some embodiments described herein. As depicted, configuration 100 includes, at least, a client device 102 with an instance of a browser 104 and a reference browser 106 hosted thereon, and an internet destination 108. Non-limiting examples of internet destination 108 may include a website for a financial institution or a website for a place of commerce.

[0012] Client device 102 may refer to a processor-based electronic device on which an instance of browser 104 and reference browser 106 may be hosted to implement at least some aspects of defending against browser attacks. Further, client device 102 may be configured to transmit and receive data over a communication link to internet destination

108 by further connecting to a mobile communications network provided by a wireless service provider (not shown). Client device 102 may be implemented as a mobile (or portable) electronic device such as a mobile phone, cell phone, smartphone, personal data assistant (PDA), a personal media player device, an application specific device, or a hybrid device that includes any of the above functions. Client device 102 may also be implemented as a personal computer including tablet, laptop computer, and non-laptop computer configurations, which may be connected to the aforementioned mobile communications network or, alternatively, to a wired network.

[0013] The aforementioned wireless service provider for implementing communications for client device 102 may also be known as a mobile network carrier, wireless carrier, or even cellular company. Regardless of the alternate reference, the wireless service provider may provide services for mobile communications subscribers.

[0014] Client device 102 may further include an operating system (OS) configuration of various components or modules, *e.g.*, implemented by a framework of hardware, software, firmware, or any combination thereof. Such software and/or firmware may include one or more computer-readable media including but not limited to Application Specific Integrated Circuit (ASIC) or Customer Specific Integrated Circuit (CSIC). The various components or modules corresponding to the aforementioned OS configuration may include, but are not limited to, browser 104 and reference browser 106.

[0015] Browser 104 may refer to a component or module running on the OS that is configured to facilitate user interaction with at least internet destination 108. By way of example, upon opening up on a display of client device 102, browser 104 may refer to a software application for retrieving, presenting, and otherwise traversing information on the

internet by presenting the user of client device 102 with a web-based user interface, command line interface, or touch user interface. Of course, the embodiments of defending against browser attacks are not limited to such interfaces, and should be interpreted as encompassing any and all embodiments of direct manipulation interfaces.

[0016] Typical of web browsers, browser 104 may facilitate electronic commerce, whereby a user of client device 102 may purchase goods or services over the internet using credit cards, debit cards, debiting existing accounts, *etc.* In addition to such “business-to-consumer” online shopping, electronic commerce facilitated by browser 104 may further include financial management with banks or other financial institutions, transaction processing, account management, inventory management, *etc.* The examples of commerce, electronic data exchanges, *etc.*, that may be facilitated by browser 104 and to which the embodiments of defending against browser attacks may be applicable are unbounded.

[0017] Data input 103 represents the inputting of data, as described herein, into appropriate data fields on browser 104 via the user interface on browser 104. Such data input may be implemented by user interaction with the user interface provided by browser 104, with data being input by means of a keyboard, a mouse, a stylus, multi-touch input, or even voice-commands. Further still, examples of such data input may include programmatic input, *i.e.*, by program and/or process.

[0018] Browser 104 may facilitate electronic commerce, in part, by transmitting to internet destination 108 authentication data that is input to appropriate data fields on browser 104 by user interaction with the user interface on browser 104. The authentication data may then be sent to internet destination 108 by clicking or otherwise activating a “send” or other button on the user interface. When the transmitted authentication

information is verified at or by internet destination 108, the intended transaction may be further executed utilizing input from client device 102, via the user interface on browser 104. In some embodiments, such input may be automated.

[0019] Reference browser 106 may refer to a component or module running on the aforementioned OS that is configured to run as a “stealth” browser on client device 102. Alternatively, reference browser 106 may run on a remote server to which client device is communicatively connected. Regardless, in stealth mode, reference browser is not intended to be viewed on the display of client device 102, although alternative embodiments of defending against browser attacks may contemplate means and methods for reference browser 106 to be displayed on, at least, a display of client device 102.

[0020] Further, reference browser 106 may or may not be communicatively coupled to the internet, although browser 104 is coupled in order to conduct electronic commerce. Further still, while reference browser 106 is intended to mimic browser 104, some embodiments of reference browser 106 may remain static, *i.e.*, do not accept add-ons from any internet source. Thus, reference browser 106 may not duplicate browser 104 in design or even protocol, but for the structure, *i.e.*, data fields, and data input thereto.

[0021] Reference browser 106 may open or activate when browser 104 is detected as opening or activating to a URL (uniform resource locator), or any other identifier of an internet resource, corresponding to internet destination 108. Reference browser 106 may be configured, designed, and/or programmed to mimic browser 104 by at least duplicating data fields displayed on browser 104 and copying data input thereto to the appropriately corresponding data fields. That is, data entered onto data fields on browser 104 is copied onto corresponding data fields on reference browser 106.

[0022] Data transmission 105 represents the copying of data from data fields on browser 104 onto corresponding data fields on reference browser 106, in accordance with at least some embodiments described herein.

[0023] When data input to the data fields on browser 104 is transmitted to internet destination 108, at the URL or other identifier identified by browser 104, reference browser 106 records the data input to the data fields of browser 104. The recorded data may be stored in a static or dynamic memory of client device 102.

[0024] Data transmission 107 represents the storing of the data recorded by reference browser 106 onto the static or dynamic memory of client device 102.

[0025] Reference browser 106 may then evaluate the security of browser 104 by comparing the recorded data to the data that is actually transmitted by browser 104 to internet destination 108. More particularly, reference browser 106 may be configured, designed, and/or programmed to further access a web cache or other repository of temporary internet files on client device 102 and compare the recorded data that was entered into the data fields on browser 104 to the data that was actually transmitted to internet destination 108.

[0026] If the comparison of the recorded data to the data that was actually transmitted to internet destination 108 reveals a discrepancy, an alarm component (not shown) on the OS of client device 102 may activate a visual or audible warning to inform the user of client device 102 that a browser attack has occurred and that the security of browser 104 has been compromised.

[0027] Alternatively, if the comparison of the recorded data to the data that was actually transmitted to internet destination 108 reveals no discrepancy, the operation of

reference browser 106 remains in the background, unannounced to the user of client device 102.

[0028] As indicated above, reference browser 106 may or may not be communicatively coupled to the internet. However, reference browser 106 is communicatively coupled to browser 104 and may even be further communicatively coupled to other client applications on client device 102, particularly those by which internet-based communication is facilitated between client device 102 and internet destination 108. Non-limiting examples of such client applications may include proprietary applications designed by or for an entity represented by internet destination 108, *e.g.*, e-mail applications, *e.g.*, Outlook, *etc.*; applications for a bank or other financial institution; applications for a store or other place of commerce; applications for a service provider; applications for a consumer rewards program, *etc.* Thus, data transmission 105 may further represent the data received by client device 102 from internet destination 108 or a corresponding domain being communicated to reference browser 106, with the data being received by browser 104 or another client application on client device 102.

[0029] Thus, when a confirmation communication is transmitted from internet destination 108 or from a corresponding domain on the internet, reference browser 106 or another component on the OS of client device 102 may detect the incoming confirmation communication. In at least some embodiments of defending against browser attacks, a URL or other identifier to which data is transmitted may be cached for at least such purposes, *i.e.*, detecting an incoming confirmation communication. Subsequently, reference browser 106 or the aforementioned another component on the OS of client device 102 may compare the recorded data, *i.e.*, the data entered into the data fields of browser 104, to the data

corresponding to those data fields as indicated in the detected confirmation communication when displayed on browser 104.

[0030] If the comparison of the recorded data to the data that is indicated in the confirmation communication, when displayed on browser 104, reveals a discrepancy, an alarm component on the OS of client device 102 may activate a visual or audio warning to inform the user of client device 102 that a browser attack has occurred and that the security of browser 104 had been compromised.

[0031] Alternatively, if the comparison of the recorded data to the data that is indicated in the confirmation communication reveals no discrepancy, the operation of reference browser 106 remains in the background, unannounced to the user of client device 102.

[0032] Internet destination 108 may refer to a website to which at least browser 104 is directed for retrieving, presenting, and otherwise traversing information on the internet to conduct electronic commerce, in accordance with embodiments described herein. Internet destination 108 may be identified on browser 104 by a URL, or some other identifier, on an address field thereof. The URL and a domain to which the virtual address space of the URL correspond may be saved in a static or dynamic memory on client device 102.

[0033] In some embodiments, internet destination 108 may be regarded as a cloud-based service and storage platform owned and/or operated by a third-party service provider. Internet destination 108 may include a framework of hardware, software, firmware, or any combination thereof, through which or to which digital data and information may be stored, passed, or shared with regard to a transaction for which at least

one subscriber to the hosted service, including client device 102, is a party. Internet destination 108 may also be implemented as a web-based storage and sharing service to which client device 102 register prior to use.

[0034] Thus, **FIG. 1** shows an example implementation of transaction verification in accordance with various embodiments of defending against browser attacks.

[0035] One type of attack that may produce a discrepancy between the recorded data and at least one of the data transmitted by browser 104 to internet destination 108 and the data that is indicated in the confirmation communication may be referred to a “man-in-the-browser” (MitB) attack. While MitB is just one of myriad attacks that may be defended against by the embodiments described herein, a description thereof provides a glimpse of context with regard to the unwitting transactions that may be executed even after proper authentication has been procured. MitB attacks may provide illicit access to the internet-based communication capabilities of browser 104 by exploiting common facilities provided to enhance browser capabilities, *e.g.*, browser extensions and add-ons. Thus, defense against such attacks need be more concerned with transaction verification as opposed to credential validation.

[0036] **FIG. 2** shows an example configuration 200 of a reference browser relative to the example system of **FIG. 1**, arranged in accordance with at least some embodiments described herein. As depicted, example configuration 200 of reference browser 106, hosted on client device 102, includes an outgoing content verifier 202, and an incoming content verifier 204. However, this configuration is an example only, and is not intended to be limiting in any manner.

[0037] Outgoing content verifier 202 may refer to a component or module on the OS of client device 102 that is configured, designed, and/or programmed to verify that data sent from browser 104 to internet destination 108 is the same as the data entered into data fields on browser 104 by a user of client device 102.

[0038] By way of example, reference browser 106 records, in a static or dynamic memory of client device 102, data that is input to the data fields on browser 104. When the data input to the data fields on browser 104 is transmitted to internet destination 108, outgoing content verifier 202 may compare the recorded data to the data that is actually transmitted by browser 104 to internet destination 108. Outgoing content provider 202 may be configured, designed, and/or programmed to access a web cache or other repository of temporary internet files on client device 102 and implement logic to compare the recorded data that was entered into the data fields on browser 104 to the data that was actually transmitted to internet destination 108.

[0039] If outgoing content verifier 202 reveals a discrepancy between the recorded data and the data that was actually transmitted to internet destination 108, an alarm component on the OS of client device 102 may activate a warning to inform the user of client device 102 that a browser attack has occurred and that the security of browser 104 has been compromised.

[0040] Alternatively, if outgoing content verifier 202 reveals no discrepancy between the recorded data and the data that was actually transmitted to internet destination 108, the operation of reference browser 106 remains in the background, unannounced to the user of client device 102.

[0041] Incoming content verifier 204 may refer to a component or module on the OS of client device 102 that is configured, designed, and/or programmed to verify that data received at browser 104 or some other client application on client device 102 is the same as the data entered into data fields on browser 104 by a user of client device 102.

[0042] By way of example, when a confirmation communication is transmitted from internet destination 108 or from a corresponding domain on the internet, incoming content verifier 204 or another component on the OS of client device 102 may detect the incoming confirmation communication. Then, incoming content verifier 204 may implement logic to compare the recorded data, *i.e.*, the data entered into the data fields of browser 104, to the data corresponding to those data fields as indicated in the detected confirmation communication when displayed on browser 104.

[0043] Once again, if incoming content verifier 204 reveals a discrepancy between the recorded data and the data that is indicated in the confirmation communication, when displayed on browser 104 an alarm component on the OS of client device 102 may activate a warning to inform the user of client device 102 that a browser attack has occurred and that the security of browser 104 had been compromised.

[0044] Alternatively, if incoming content verifier 204 reveals no discrepancy between the recorded data and the data that is indicated in the confirmation communication, the operation of reference browser 106 remains in the background, unannounced to the user of client device 102.

[0045] Thus, FIG. 2 show an example configuration of transaction verification in accordance with various embodiments of a reference browser.

[0046] FIG. 3 shows an example configuration of a processing flow 300 of operations for defending against browser attacks, in accordance with at least some embodiments described herein. As depicted, processing flow 300 includes sub-processes executed by various components that are part of the OS on client device 102, including but not limited to browser 104 and/or reference browser 106. However, processing flow 300 is not limited to such components, as obvious modifications may be made by re-ordering two or more of the sub-processes described here, eliminating at least one of the sub-processes, adding further sub-processes, substituting components, or even having various components assuming sub-processing roles accorded to other components in the following description. Processing flow 500 may include various operations, functions, or actions as illustrated by one or more of blocks 302, 304, 306, 308, and/or 310. Processing may begin at block 302.

[0047] Block 302 (Detect Browser Opening) may refer to a component or module on the OS of client device 102 detecting that browser 104 has opened or activated to a URL or other identifier corresponding to internet destination 108. Processing may proceed from block 302 to block 304.

[0048] Block 304 (Open Reference Browser) may refer to a component or module on the OS of client device 102, which may or may not include reference browser 106, opening or activating reference browser 106. Reference browser 106, if communicatively connected to the internet, may open or activate to the same URL as browser 104, and then mimic at least the data fields displayed thereat. Alternatively, reference browser 106 may open at any time that the OS of client device 102 is running, and then mimic the data fields displayed on browser 104 as previously described. Further still, if reference browser 106 is not communicatively coupled to the internet, reference browser may mimic at least the

data fields displayed on browser 104, as retrieved by transmission 105. Processing may proceed from block 304 to block 306.

[0049] Block 306 (Copy Data from Browser to Reference Browser) may refer to reference browser 106 or some other component running on the OS of client device 102 implementing logic to copy data entered onto data fields on browser 104 onto corresponding data fields on reference browser 106. Processing may proceed from block 306 to block 308.

[0050] Block 308 (Evaluate Security Based on Outgoing Data) may refer to outgoing content verifier 202 or another module on the OS of client device 102 verifying that data sent from browser 104 to internet destination 108 is the same as the data entered into data fields on browser 104 by a user of client device 102.

[0051] Reference browser 106, by outgoing content verifier 202 or the aforementioned other module on the OS of client device 102, may record, in a static or dynamic memory of client device 102, data that is input to the data fields on browser 104. Outgoing content verifier 202 may compare the recorded data to the data that is actually transmitted by browser 104 to internet destination 108 by accessing a web cache or other repository of temporary internet files on client device 102 and implementing logic to compare the recorded data that was entered into the data fields on browser 104 to the data that was actually transmitted to internet destination 108. If outgoing content verifier 202 reveals a discrepancy between the recorded data and the data that was actually transmitted to internet destination 108, an alarm component on the OS of client device 102 may activate a visual or audio warning to inform the user of client device 102 that a browser attack has occurred and that the security of browser 104 has been compromised.

Alternatively, if outgoing content verifier 202 reveals no discrepancy between the recorded data and the data that was actually transmitted to internet destination 108, the operation of reference browser 106 remains in the background. Processing may proceed from block 308 to block 310.

[0052] Block 310 (Evaluate Security Based on Incoming Data) may refer to incoming content verifier 204 or other module on the OS of client device 102 verifying that data received at browser 104 or some other client application on client device 102 is the same as the data entered into data fields on browser 104 by a user of client device 102.

[0053] When a confirmation communication is transmitted from internet destination 108 or from a corresponding domain on the internet, reference browser 106, by incoming content verifier 204 or another component on the OS of client device 102, may detect the incoming confirmation communication. Incoming content verifier 204 may implement logic to compare the recorded data to the data corresponding to those data fields as indicated in the detected confirmation communication when displayed on browser 104. If incoming content verifier 204 reveals a discrepancy between the recorded data and the data that is indicated in the confirmation communication when displayed, an alarm component on the OS of client device 102 may activate a visual or audio warning to inform the user of client device 102 that a browser attack has occurred and that the security of browser 104 had been compromised. Alternatively, if incoming content verifier 204 reveals no discrepancy between the recorded data and the data that is indicated in the confirmation communication, the operation of reference browser 106 remains in the background.

[0054] Thus, **FIG. 3** shows an example processing flow for evaluating security on a browser by verifying a transaction implemented thereby.

[0055] **FIG. 4** shows a block diagram illustrating an example computing device 400 by which various example solutions described herein may be implemented, arranged in accordance with at least some embodiments described herein.

[0056] More particularly, **FIG. 4** shows an illustrative computing embodiment, in which any of the processes and sub-processes described herein may be implemented as computer-readable instructions stored on a computer-readable medium. The computer-readable instructions may, for example, be executed by a processor of a device, as referenced herein, having a network element and/or any other device corresponding thereto, particularly as applicable to the applications and/or programs described above corresponding to the configuration 100 for defending against browser attacks.

[0057] In a very basic configuration, a computing device 400 may typically include one or more processors 404 and a system memory 406. A memory bus 408 may be used for communicating between processor 404 and system memory 406.

[0058] Depending on the desired configuration, processor 404 may be of any type including but not limited to a microprocessor (μ P), a microcontroller (μ C), a digital signal processor (DSP), or any combination thereof.

[0059] Depending on the desired configuration, system memory 406 may be of any type including but not limited to volatile memory (such as RAM), non-volatile memory (such as ROM, flash memory, etc.) or any combination thereof. System memory 406 may include an operating system 420, one or more applications 422, and program data 424.

[0060] Application 422 may be configured to transmit or receive identification information pertaining to client device 102, verify or validate such identifying data, and transmit device data as described previously with respect to **FIGS. 1 - 3**. Further, application 422 may be configured to detect the opening of browser 104, and implement the logic for comparing stored data to data transmitted from or to browser 104 or some other client application on client device 102. Program data 424 may include a table 450, which may be useful for implementing actuation of appropriate components or modules as described herein.

[0061] System memory 406 is an example of computer storage media. Computer storage media may include, but not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may be accessed by computing device 400. Any such computer storage media may be part of computing device 400.

[0062] The network communication link may be one example of a communication media. Communication media may typically be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and may include any information delivery media. A “modulated data signal” may be a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio

frequency (RF), microwave, infrared (IR) and other wireless media. The term computer readable media as used herein may include both storage media and communication media.

[0063] There is little distinction left between hardware and software implementations of aspects of systems; the use of hardware or software is generally (but not always, in that in certain contexts the choice between hardware and software can become significant) a design choice representing cost vs. efficiency tradeoffs. There are various vehicles by which processes and/or systems and/or other technologies described herein may be implemented, *e.g.*, hardware, software, and/or firmware, and that the preferred vehicle may vary with the context in which the processes and/or systems and/or other technologies are deployed. For example, if an implementer determines that speed and accuracy are paramount, the implementer may opt for a mainly hardware and/or firmware vehicle; if flexibility is paramount, the implementer may opt for a mainly software implementation; or, yet again alternatively, the implementer may opt for some combination of hardware, software, and/or firmware.

[0064] The foregoing detailed description has set forth various embodiments of the devices and/or processes for system configuration 100 via the use of block diagrams, flowcharts, and/or examples. Insofar as such block diagrams, flowcharts, and/or examples contain one or more functions and/or operations, it will be understood by those within the art that each function and/or operation within such block diagrams, flowcharts, or examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. In one embodiment, several portions of the subject matter described herein may be implemented via Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs), digital signal

processors (DSPs), or other integrated formats. However, those skilled in the art will recognize that some aspects of the embodiments disclosed herein, in whole or in part, can be equivalently implemented in integrated circuits, as one or more computer programs running on one or more computers, *e.g.*, as one or more programs running on one or more computer systems, as one or more programs running on one or more processors, *e.g.*, as one or more programs running on one or more microprocessors, as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing the code for the software and or firmware would be well within the skill of one of skill in the art in light of this disclosure. In addition, those skilled in the art will appreciate that the mechanisms of the subject matter described herein are capable of being distributed as a program product in a variety of forms, and that an illustrative embodiment of the subject matter described herein applies regardless of the particular type of signal bearing medium used to actually carry out the distribution. Examples of a signal bearing medium include, but are not limited to, the following: a recordable type medium such as a floppy disk, a hard disk drive, a CD, a DVD, a digital tape, a computer memory, etc.; and a transmission type medium such as a digital and/or an analog communication medium (e.g., a fiber optic cable, a waveguide, a wired communications link, a wireless communication link, etc.).

[0065] Those skilled in the art will recognize that it is common within the art to describe devices and/or processes in the fashion set forth herein, and thereafter use engineering practices to integrate such described devices and/or processes into data processing systems. That is, at least a portion of the devices and/or processes described herein can be integrated into a data processing system via a reasonable amount of experimentation. Those having skill in the art will recognize that a typical data processing

system generally includes one or more of a system unit housing, a video display device, a memory such as volatile and non-volatile memory, processors such as microprocessors and digital signal processors, computational entities such as operating systems, drivers, graphical user interfaces, and applications programs, one or more interaction devices, such as a touch pad or screen, and/or control systems including feedback loops and control motors, *e.g.*, feedback for sensing position and/or velocity; control motors for moving and/or adjusting components and/or quantities. A typical data processing system may be implemented utilizing any suitable commercially available components, such as those typically found in data computing/communication and/or network computing/communication systems.

[0066] The herein described subject matter sometimes illustrates different components contained within, or connected with, different other components. It is to be understood that such depicted architectures are merely examples, and that in fact many other architectures can be implemented which achieve the same functionality. In a conceptual sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermedial components. Likewise, any two components so associated can also be viewed as being "operably connected", or "operably coupled", to each other to achieve the desired functionality, and any two components capable of being so associated can also be viewed as being "operably couplable", to each other to achieve the desired functionality. Specific examples of operably couplable include but are not limited to

physically mateable and/or physically interacting components and/or wirelessly interactable and/or wirelessly interacting components and/or logically interacting and/or logically interactable components.

[0067] Lastly, with respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0068] It will be understood by those within the art that, in general, terms used herein, and especially in the appended claims, *e.g.*, bodies of the appended claims, are generally intended as “open” terms, *e.g.*, the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” *etc.* It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases “at least one” and “one or more” to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles “a” or “an” limits any particular claim containing such introduced claim recitation to embodiments containing only one such recitation, even when the same claim includes the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an,” *e.g.*, “a” and/or “an” should be interpreted to mean “at least one” or “one or more;” the same holds true for the use of definite articles used to introduce

claim recitations. In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should be interpreted to mean at least the recited number, *e.g.*, the bare recitation of "two recitations," without other modifiers, means at least two recitations, or two or more recitations. Furthermore, in those instances where a convention analogous to "at least one of A, B, and C, *etc.*" is used, in general such a construction is intended in the sense one having skill in the art would understand the convention, *e.g.*, "a system having at least one of A, B, and C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, *etc.* In those instances where a convention analogous to "at least one of A, B, or C, *etc.*" is used, in general such a construction is intended in the sense one having skill in the art would understand the convention, *e.g.*, "a system having at least one of A, B, or C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, *etc.* It will be further understood by those within the art that virtually any disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms. For example, the phrase "A or B" will be understood to include the possibilities of "A" or "B" or "A and B."

[0069] From the foregoing, it will be appreciated that various embodiments of the present disclosure have been described herein for purposes of illustration, and that various modifications may be made without departing from the scope and spirit of the present

disclosure. Accordingly, the various embodiments disclosed herein are not intended to be limiting, with the true scope and spirit being indicated by the following claims.

WE CLAIM

1. A computer-readable medium storing one or more computer-executable instructions that, when executed, cause one or more processors to:

detect that a primary browser has opened to a URL;

open a reference browser to the URL;

copy data input to respective data fields on the primary browser to respectively corresponding data fields on the reference browser; and

evaluate security on the primary browser based on, at least, the data copied to the reference browser.

2. The computer-readable medium of Claim 1, wherein the one or more computer-executable instructions further cause the one or more processors to:

detect that a transmission from the primary browser has occurred;

compare data included in the respective data fields transmitted from the primary browser against the data copied to the respectively corresponding data fields on the reference browser; and

issue a notification when the comparison results in a discrepancy.

3. The computer-readable medium of Claim 1, wherein the one or more computer-executable instructions further cause the one or more processors to:

detect an incoming confirmation transmission from a domain associated with the URL confirming transmission of data from the primary browser;

compare data included in respective data fields in the incoming confirmation transmission, when displayed on the primary browser, against data in the respectively corresponding data fields on the reference browser; and

issue a notification when the comparison results in a discrepancy.

4. The computer-readable medium of Claim 1, wherein the reference browser does not accept add-ons.

5. The computer-readable medium of Claim 1, wherein the data copied to the reference browser is not transmitted.

6. The computer-readable medium of Claim 2, wherein the notification includes a display of the data included in the respective data fields transmitted from the primary browser adjacent to the data copied to the respectively corresponding data fields on the reference browser.

7. The computer-readable medium of Claim 3, wherein the notification includes a display of the data included in the respective data fields transmitted in the incoming confirmation transmission adjacent to the data copied to the respectively corresponding data fields on the reference browser.

8. A system, comprising:

a first browser configured to:

open to a URL;
receive data input to respective data fields,
transmit data to a domain corresponding to the URL, and
receive a confirmation transmission from the domain corresponding to the URL;
a second browser configured to:
open to the URL, and
receive the data input to the respective fields of the first browser into corresponding replicated data fields; and
a reference application configured to:
evaluate security on the first browser based on, at least, the data input to the replicated data fields on the second browser.

9. The system of Claim 8, wherein the reference application is configured to evaluate security by comparing the data transmitted from the first browser to the domain corresponding to the URL against the data input to the replicated data fields of the second browser.

10. The system of Claim 9, wherein the reference application is further configured to display a notification when the comparison indicates a discrepancy.

11. The system of Claim 8, wherein the reference application is configured to evaluate security by comparing data included in the confirmation transmission received and

displayed by the first browser from the domain corresponding to the URL against the data input to the replicated data fields of the second browser.

12. The system of Claim 11, wherein the reference application is further configured to display a notification when the comparison indicates a discrepancy.

13. A method, comprising:

copying data input to data fields on a first browser into corresponding duplicate data fields on a reference browser;

transmitting data from the first browser to an internet destination;

detecting receipt of a confirmation message, including an alleged restatement of the data transmitted from the first browser to the internet destination;

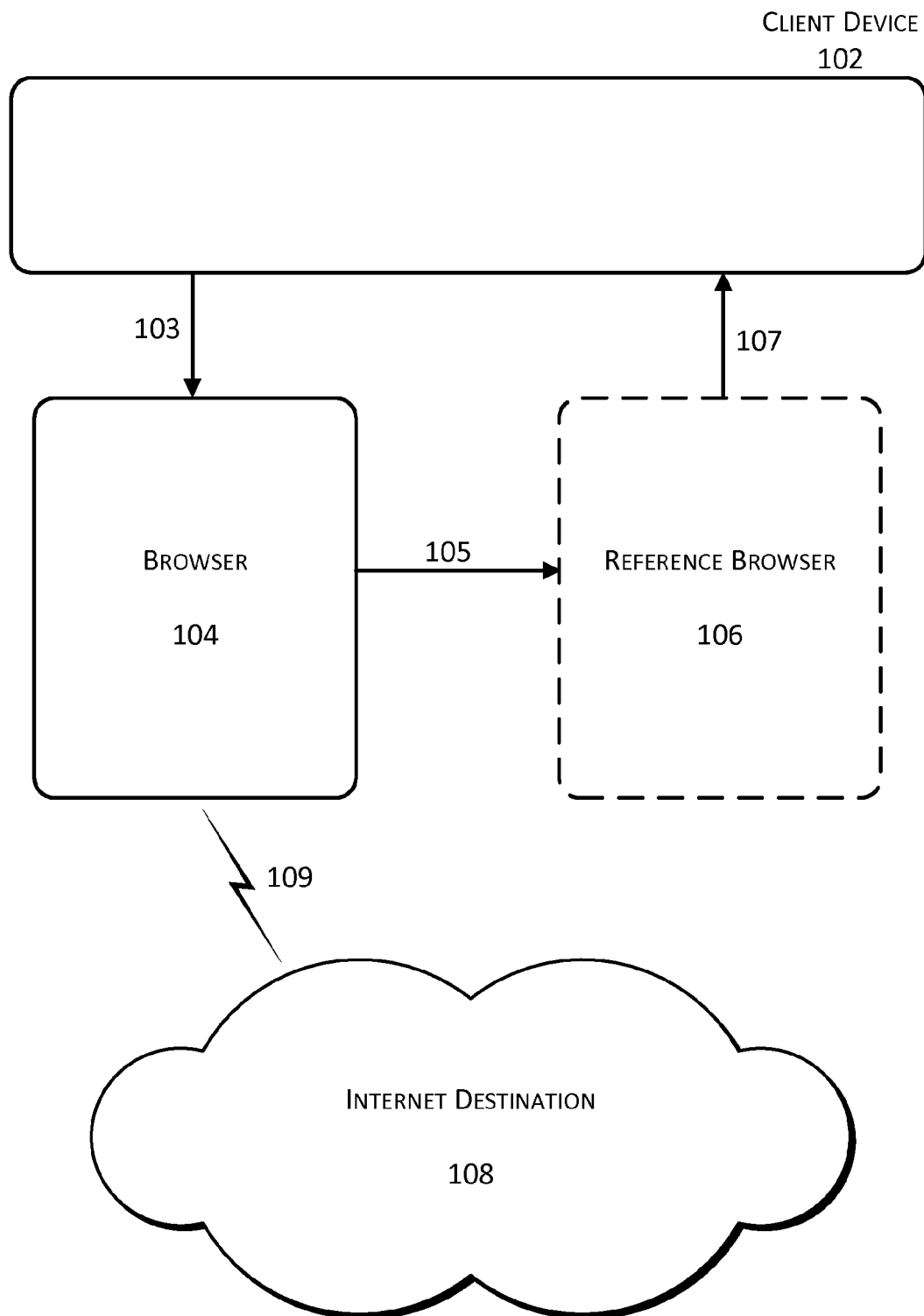
determining whether an attack has been made on the first browser using at least the copied data input to the duplicate data fields on the reference browser.

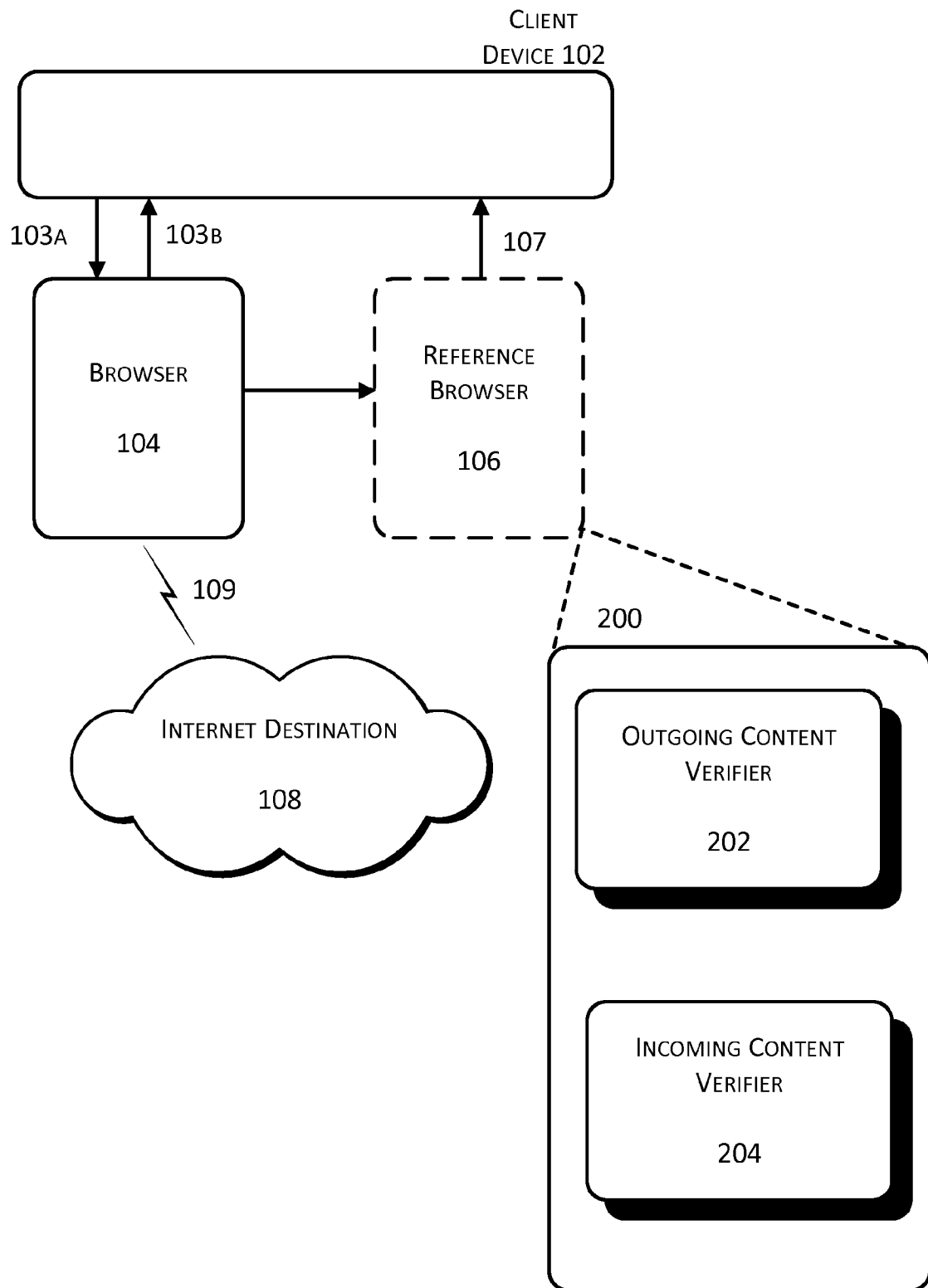
14. The method of Claim 13, wherein the determining includes comparing the data transmitted from the first browser to the internet destination against the copied data input to the duplicate data fields on the reference browser.

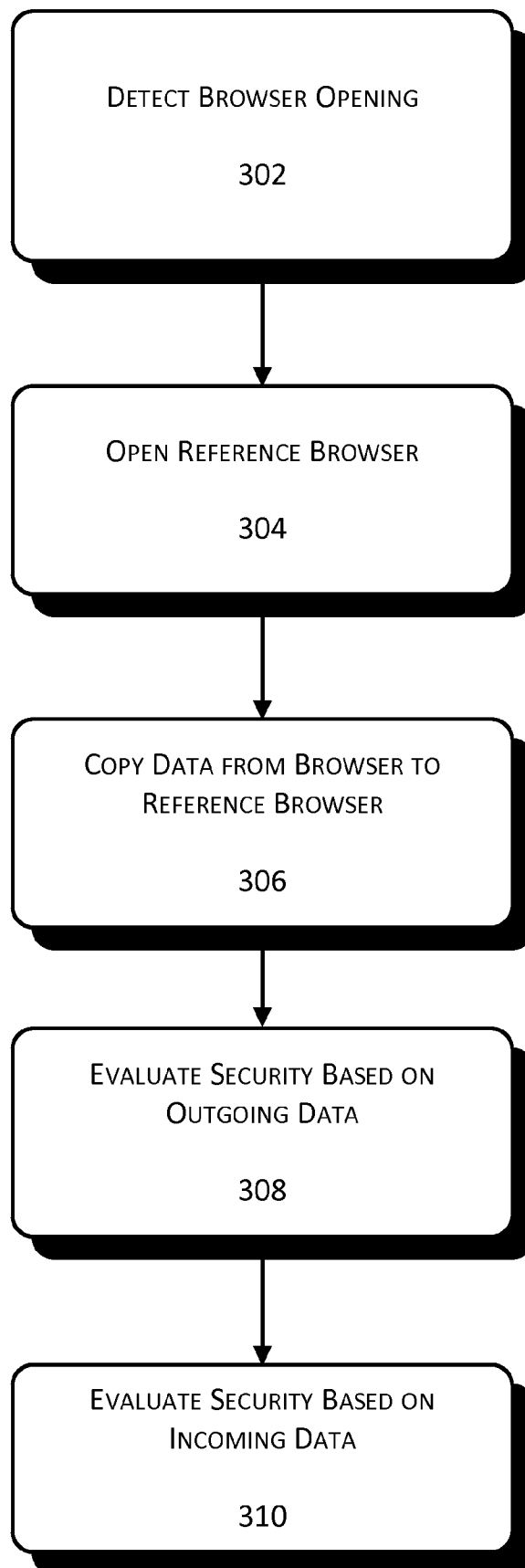
15. The method of Claim 13, wherein the determining includes comparing the alleged restatement of the data transmitted as displayed on the first browser against the copied data input to the duplicate data fields on the reference browser.

16. The method of Claim 13, wherein the determining includes determining whether a man-in-the-middle attack has been made on the first browser.

17. The method of Claim 13, further comprising displaying a notification when the determining indicates an attack has been made on the first browser.

100**FIG. 1**

**FIG. 2**

300**FIG. 3**

COMPUTING DEVICE (400)

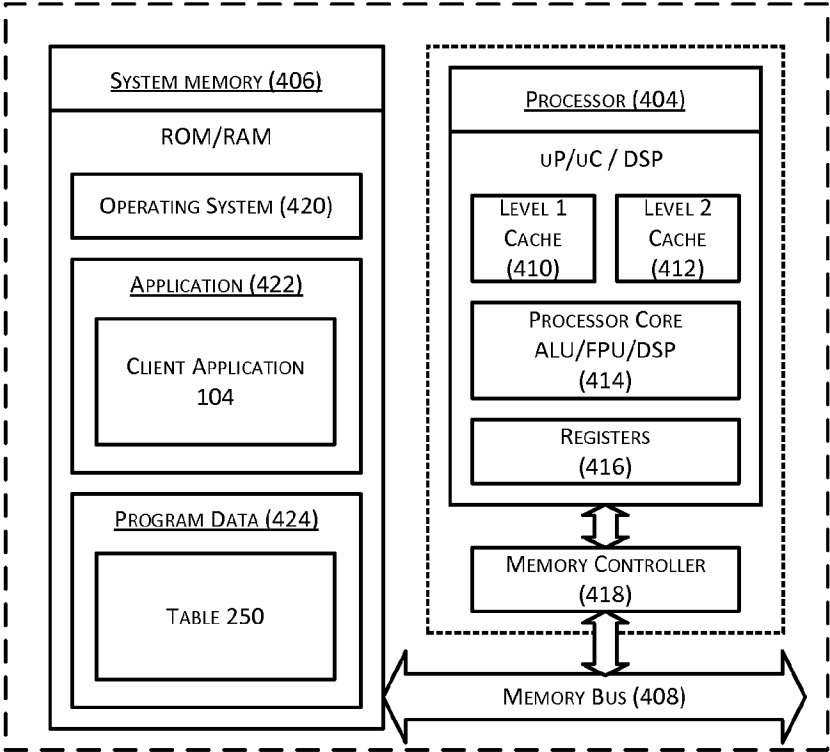


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 12/49697

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 11/00 (2012.01)

USPC - 726/22

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)

USPC: 726/22

IPC(8): G06F 11/00 (2012.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC: 726/22, 23; 713/187 (Keyword limited; terms below)

IPC(8): G06F 11/00 (2012.01) (Keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PubWEST (PGPB, USPT, EPAB, JPAB); Google (Scholar, Patents, Web)

Terms used: detect open url reference browser test measure security copy input compare form adjacent "man in the middle" add-on plug-in

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	US 7,343,626 B1 (Gallagher), 11 March 2008 (11.03.2008), entire document, especially Abstract; col 2, ln 65-67; col 5, ln 47-67; col 6, ln 58 to col 7, ln 29	13, 17 ----- 1-12, 14-16
Y	US 2011/0093773 A1 (Yee), 21 April 2011 (21.04.2011), entire document, especially Abstract, para [0024], [0050], [0081]	1-4, 5-7, 8-12
Y	US 2008/0172741 A1 (Reumann et al.), 17 July 2008 (17.07.2008), entire document, especially Abstract, para [0024], [0030]	2-3, 6-7, 9-12, 14-16
Y	US 7,051,285 B1 (Harrison et al.), 23 May 2006 (23.05.2006), entire document, especially Abstract; col 2, ln 60-67	4

☐

Further documents are listed in the continuation of Box C.

☐

* 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

03 October 2012 (03.10.2012)

Date of mailing of the international search report

12 OCT 2012

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774