



(51) International Patent Classification:

H04L 12/46 (2006.01) H04L 12/58 (2006.01)  
H04L 12/26 (2006.01) H04L 9/00 (2006.01)

(21) International Application Number:

PCT/CA2013/050480

(22) International Filing Date:

21 June 2013 (21.06.2013)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

13/545,988 11 July 2012 (11.07.2012) US

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

(71) Applicant (for MG only): **IBM CANADA LIMITED-IBM CANADA LIMITEE** [CA/CA]; 3600 Steeles Avenue East, Markham, Ontario L3R 9Z7 (CA).

(72) Inventors: **BANK, Judith Helen**; 3039 East Cornwallis Road, Research Triangle Park, North Carolina 27709 (US). **HARPUR, Liam**; IBM Ireland Technology Campus, Damastown Industrial Estate, Dublin (IE). **LYLE, Ruthie D.**; 4205 S. Miami Boulevard, Durham, North Carolina 27703 (US). **O'SULLIVAN, Patrick Joseph**; IBM Ireland Technology Campus, Damastown Industrial Estate, Dublin (IE).

**LIN, Sun**; 3039 Cornwallis Road, Research Triangle Park, North Carolina 27709 (US).

(74) Agent: **WANG, Peter**; IBM Canada Limited, 3600 Steeles Avenue East, Markham, Ontario L3R 9Z7 (CA).

(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, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

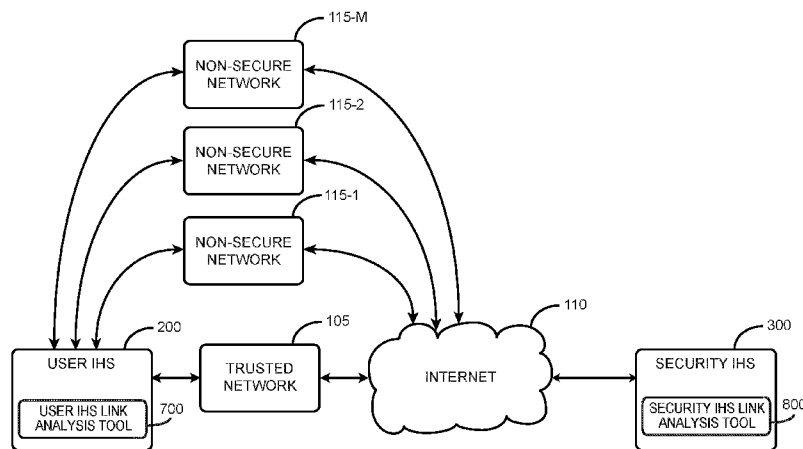
Published:

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

(54) Title: NETWORK SELECTION TOOL FOR INFORMATION HANDLING SYSTEM

FIG. 1

100



(57) Abstract: A user information handling system (IHS) link analysis tool intercepts requests to navigate to a webpage, such as a link. The user IHS link analysis tool transmits the link to a security IHS link analysis tool. The user IHS link analysis tool receives a network selection message from the security IHS indicating which network the user IHS should utilize based upon the content of the link.

WO 2014/008590 A1

## NETWORK SELECTION TOOL FOR INFORMATION HANDLING SYSTEM

### CROSS REFERENCE TO RELATED PATENT APPLICATIONS

**[0001]** This patent application is related to the copending patent application entitled "Link Analysis Tool For Security Information Handling System" by Bank, et al., (Docket Number AUS920120120US1), filed concurrently herewith and assigned to the same Assignee, the disclosure of which is incorporated herein by reference in its entirety.

### BACKGROUND

**[0002]** The disclosures herein relate generally to information handling systems (IHSs) that interact with other IHSs via a network connection. More specifically, the disclosure relates to an IHS that may connect to another IHS via multiple available networks.

### BRIEF SUMMARY

**[0003]** In one embodiment, a method is disclosed that includes receiving, by a user information handling system (IHS), a request to navigate to an IHS other than the user IHS, the request including a link. The method also includes intercepting, by the user IHS, the request to navigate to an IHS other than the user IHS. The method further includes transmitting, by the user IHS, the link to a security IHS. The method still further includes receiving, by the user IHS, a network selection message from the security IHS, the network selection message indicating a particular network for the user IHS to employ in communicating with a target of the link.

**[0004]** In another embodiment, a user information handling system (IHS) is disclosed that includes a processor. The user IHS also includes a memory that is coupled to the processor. The memory is configured with a user IHS link analysis tool that receive a request to navigate to an IHS other than the user IHS, the request including a link. The memory is also configured to intercept the request to navigate to an IHS other than the user IHS. The memory is further configured to transmit the link to a security IHS. The memory is still further configured to receive a network selection message from the security IHS, the network selection message indicating a particular network for the user IHS to employ in communicating with a target of the link.

**[0005]** In yet another embodiment, a user IHS link analysis tool computer program product is disclosed that includes a non-transitory computer readable storage medium. The user IHS link analysis tool includes first instructions that receive a request to navigate to an IHS other than the user IHS, the request including a link. The user IHS link analysis tool also includes second instructions that intercept the request to navigate to an IHS other than the user IHS. The user IHS link analysis tool further includes third instructions that transmit the link to a security IHS. The user IHS link analysis tool still further includes fourth instructions that receive a network selection message from the security IHS, the network selection message indicating a particular network for the user IHS to employ in communicating with a target of the link. The first, second third and fourth instructions are stored on the non-transitory computer readable storage medium.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0006]** The appended drawings illustrate only exemplary embodiments of the invention and therefore do not limit its scope because the inventive concepts lend themselves to other equally effective embodiments.

**[0007]** Fig. 1 is a block diagram of one embodiment of the disclosed network selection system.

**[0008]** Fig. 2 is a block diagram of the disclosed user information handling system (IHS) including a user IHS link analysis tool.

**[0009]** Fig. 3 is a block diagram of the disclosed security IHS including a security IHS link analysis tool.

**[0010]** Fig. 4 shows a representative email in that the disclosed user IHS link analysis tool may employ.

**[0011]** Fig. 5 shows a representative webpage in that the disclosed security IHS link analysis tool may employ.

**[0012]** Fig. 6 shows a representative override network selection message prompt that the disclosed user IHS link analysis tool may generate.

**[0013]** Fig. 7 is a flowchart of process flow in the disclosed user IHS link analysis tool.

**[0014]** Fig. 8 is a flowchart of process flow in the disclosed security IHS link analysis tool.

## DETAILED DESCRIPTION

**[0015]** The disclosed user information handling system (IHS) includes a “user IHS link analysis tool” that intercepts requests to navigate to respective websites,. These requests may include links. The user IHS link analysis tool transmits a link from such a request to a security IHS via a trusted network. A “security IHS link analysis tool” in the security IHS determines if the target of the link contains sensitive content. The security IHS link analysis tool also determines which network of multiple networks the user IHS should use to navigate to the target of the link and further creates a network selection message. The security IHS link analysis tool transmits the network selection message to the user IHS using the trusted network. The user IHS link analysis tool receives the network selection message and prompts the user to follow the network selection message to navigate to the target of the link using the preferred network of the network selection message or to override the network selection message and navigate to the target of the link using another network.

**[0016]** Fig. 1 is a block diagram of one embodiment of a disclosed network selection system 100 that employs user IHS link analysis tool 700 and security IHS link analysis tool 800 to determine the appropriate network to employ for navigation to particular content. A user may employ a user IHS 200 in an attempt to navigate to the target of a link, for example, a webpage. The user IHS link analysis tool 700 intercepts the attempt to navigate to the target of a link and generates a navigation request. In one embodiment, the navigation request may contain the link, the current local time at user IHS 200, a list of networks available to user IHS 200 and other relevant data.

**[0017]** User IHS link analysis tool 700 transmits the navigation request over trusted network 105 via the Internet 110 to security IHS 300. Trusted network 105 may be a network connection over which the user has some control, for example an Internet service provider (ISP) or a cellular communications carrier. In one embodiment, a trusted network is a network that includes at least some security features. A trusted network may also be a network that the user or others regard as secure, or that is generally accepted as secure. Security IHS link analysis tool 800 receives the navigation request from user IHS 700 and navigates to the target of the link contained therein. Security IHS link analysis tool 800 parses the target of the link and determines if the target of the link contains sensitive content. A representative process of determining if the target of the link contains sensitive content is described in detail below. The security IHS link analysis tool 800 generates a network selection message that specifies which one of the available networks that user IHS 200 should employ to navigate to the target of the link. In other words, the network selection message may specify one of trusted network 105, non-secure network 115-1, non-secure network 115-2, ... , and non-secure network 115-M, for use by user IHS 200 to navigate to the target of the link.

**[0018]** The security IHS link analysis tool 800 transmits the network selection message via the Internet 110, through trusted network 105 to user IHS 200. In one embodiment, the user IHS link analysis tool 700 receives the network selection message and navigates to the target of the link using the network that the network selection message specifies. In one embodiment, trusted network 105, non-secure network 115-1, non-secure network 115-2, ... , non-secure network 115-M may include wired and/or wireless networks. For example, non-secure network 115-1 could be a Wi-Fi hotspot at a coffee shop where the user is not in control of the network. In another example, non-secure network 115-2 could be a business network where the user is not in control of the network.

**[0019]** Fig. 2 is a block diagram of a user information handling system (IHS) 200 that employs the disclosed user IHS link analysis tool methodology to prevent navigation on an undesired network. User IHS 200 includes a processor 205 that may include multiple cores. User IHS 200 processes, transfers, communicates, modifies, stores or otherwise handles information in digital form, analog form or other form. User IHS 200 includes a bus 210 that couples processor 205 to memory 215 via a memory controller 220 and memory bus 225. System memory 215 may also be referred to as main memory. System memory 215 may be a static random access memory (SRAM) array or a dynamic random access memory (DRAM) array. Processor 205 may also include local memory such as L1, L2 and L3 caches. A video graphics controller 230 couples display 235 to bus 210. Nonvolatile storage 240, such as a hard disk drive, solid state drive (SSD), CD drive, DVD drive, or other nonvolatile storage couples to bus 210 to provide user IHS 200 with permanent storage of information. System memory 215 and nonvolatile storage 240 are both forms of memory stores. Nonvolatile storage 240 stores an operating system 245 (OPERATING SYS) that governs operation of user IHS 200. I/O devices 250, such as a keyboard and a pointing device, couple to bus 210 via I/O controller 255 and I/O bus 260. I/O devices 250 may also include, but are not limited to: capacitive sensors, image sensors, audio input devices, touchscreen devices, video devices, and stereographic devices.

**[0020]** One or more expansion busses 265, such as USB, IEEE 1394 bus, ATA, SATA, PCI, PCIE, DVI, HDMI and other busses, couple to bus 210 to facilitate the connection of peripherals and devices to user IHS 200. A network interface controller 270 couples to bus 210 to enable user IHS 200 to connect by wire or wirelessly to a network and other information handling systems. Network interface controller 270 may also be called a network communication adapter or a network adapter. While Fig. 2 shows one IHS that employs processor 205, the IHS may take many forms. For example, user IHS 200 may take the form of a desktop, server, portable, laptop, notebook, tablet, or other form factor computer or data processing system. User IHS 200 may take other form factors such as a gaming device, a personal digital assistant (PDA), a portable telephone device, a communication device or other devices that include a processor and memory.

**[0021]** User IHS 200 includes a user IHS link analysis tool computer program product 700 on digital media 275 such as a CD, DVD or other media. In one embodiment, user IHS link analysis tool 700 is within user IHS 200 as shown in Fig. 1. User IHS link analysis tool 700 may also be an add-in that the user or other entity installs in user IHS 200 at the user's convenience. In actual practice, user IHS 200 may store user IHS link analysis tool 700 in nonvolatile storage 240 as user IHS link analysis tool 700'. User IHS 200 may also store operating system 245 (OPERATING SYS) in nonvolatile storage 240. When user IHS 200 initializes, the IHS loads operating system 245 into system memory 215 for execution as operating system 245'. User IHS 200 also loads user IHS link analysis tool 700' into system memory 215 for execution as user IHS link analysis tool 700'', respectively.

**[0022]** Fig. 3 is a block diagram of a security information handling system (IHS) 300 that employs the disclosed security IHS link analysis tool methodology to determine which networks should be utilized based upon the content of the link. Security IHS 300 includes a processor 305 that may include multiple cores. Security IHS 300 processes, transfers, communicates, modifies, stores or otherwise handles information in digital form, analog form or other form. Security IHS 300 includes a bus 310 that couples processor 305 to memory 315 via a memory controller 320 and memory bus 325. System memory 315 may also be referred to as main memory. System memory 315 may be a static random access memory (SRAM) array or a dynamic random access memory (DRAM) array. Processor 305 may also include local memory such as L1, L2 and L3 caches. A video graphics controller 330 couples display 335 to bus 310. Nonvolatile storage 340, such as a hard disk drive, solid state drive (SSD), CD drive, DVD drive, or other nonvolatile storage couples to bus 310 to provide security IHS 300 with permanent storage of information. System memory 315 and nonvolatile storage 340 are both forms of memory stores. Nonvolatile storage 340 stores an operating system 345 (OPERATING SYS) that governs operation of security IHS 300. I/O devices 350, such as a keyboard and a pointing device, couple to bus 310 via I/O controller 355 and I/O bus 360. I/O devices 350 may also include, but are not limited to: capacitive sensors, image sensors, audio input devices, touchscreen devices, video devices, and stereographic devices.

**[0023]** One or more expansion busses 365, such as USB, IEEE 1394 bus, ATA, SATA, PCI, PCIE, DVI, HDMI and other busses, couple to bus 310 to facilitate the connection of peripherals and devices to security IHS 300. A network interface controller 370 couples to bus 310 to enable security IHS 300 to connect by wire or wirelessly to a network and other information handling systems. Network interface controller 370 may also be called a network communication adapter or a network adapter. While Fig. 3 shows one IHS that employs processor 305, the IHS may take many forms. For example, security IHS 300 may take the form of a desktop, server, portable, laptop, notebook, tablet, or other form factor computer or data processing system. Security IHS 300 may take other form factors such as a gaming

device, a personal digital assistant (PDA), a portable telephone device, a communication device or other devices that include a processor and memory.

**[0024]** Security IHS 300 includes a security IHS link analysis tool computer program product 800 on digital media 375 such as a CD, DVD or other media. In one embodiment, security IHS link analysis tool 800 is within security IHS 300 as shown in Fig. 1. Security IHS link analysis tool 800 may also be an add-in that the user or other entity installs in security IHS 300 at the user's convenience. In actual practice, security IHS 300 may store security IHS link analysis tool 800 in nonvolatile storage 340 as security IHS link analysis tool 800'. Security IHS 300 may also store operating system 345 (OPERATING SYS) in nonvolatile storage 340. When security IHS 300 initializes, the IHS loads operating system 345 into system memory 315 for execution as operating system 345'. Security IHS 300 also loads security IHS link analysis tool 800' into system memory 315 for execution as security IHS link analysis tool 800", respectively.

**[0025]** Fig. 4 shows an example of an email message 400 that user IHS 200 may display on display 235. An email message may include a FROM field 405, a TO field 410, a TITLE field 415 and a message field 420. In one embodiment, the message field 420 may include a message to the user and links such as link 425-1, link 425-2, link 425-3, ... , link 425-M. These links, namely link 425-1, link 425-2, link 425-3, ... , link 425-M, may be links to webpages. For example, link 425-1 may be a link to webpage 525.

**[0026]** In one scenario, the user may select link 425-1. User IHS link analysis tool 700 intercepts the request to navigate to webpage 525, the target of link 425-1. The user IHS link analysis tool 700 may generate a navigation request. In one embodiment, the navigation request may contain link 425-1, the current location time at user IHS 200, and a list of networks available to user IHS 200, namely: trusted network 105, non-secure network 115-1, non-secure network 115-2, ... , non-secure network 115-M. The user IHS link analysis tool 700 may transmit the navigation request through trusted network 105, via the Internet 110, to security IHS 300. The user IHS 200 and security IHS 300 may communication with one another, back and forth, via the Internet 110, and trusted network 105.

**[0027]** Fig. 5 shows an example of a webpage 525 that link 425-1 may target. In one embodiment, the security IHS link analysis tool 800 receives the navigation request and navigates to the target of link 425-1, namely webpage 525. Fig. 5 shows an example of a webpage 525 in a browser 500 that security IHS 300 may display on display 335. Browser 500 may include a backward button 505, forward button 510, refresh button 515 and a uniform resource locator (URL) field 520.

**[0028]** In one embodiment, security IHS link analysis tool 800 parses the webpage 525 and URL field 520 for content. Security IHS link analysis tool 800 may accumulate content and determine to which

user-defined category or categories the content belongs. For example, security IHS link analysis tool 800 may parse URL field 520 for content. In this scenario, 'http' indicates an unsecure hypertext transport protocol communication. Other types of communication may be, hypertext transfer protocol over secure socket layer (HTTPS), file transfer protocol (FTP), secure shell file transfer protocol (SFTP) and others. Security IHS link analysis tool 800 may determine this content belongs to a user-defined category, "unsecure communication."

**[0029]** Security IHS link analysis tool 800 may also parse 'ibm.com' of URL field 520 as content and may further determine that this content belongs to multiple user-defined categories such as "trusted websites", "business" and "commerce". Security IHS link analysis tool 800 may parse 'newproduct.html' as content and may further determine that this content does not belong to a user-defined category. In response to this determination, security IHS link analysis tool 800 may transmit an instruction to the user IHS 200 instructing the user IHS link analysis tool 700 to generate a dialog box to notify the user that this particular content is not currently categorized. The user may or may not respond by selecting an appropriate category for this content, or by creating a new category for this content. The user IHS link analysis tool 700 may transmit the user's response to security IHS 300.

**[0030]** In another embodiment, based upon user settings, i.e. preferences, the security IHS link analysis tool 800 may determine that 'newproduct.html' does not belong to a user-defined category and, in response to this determination, may flag the content for later review by the user for categorization.

**[0031]** In another embodiment, based upon user settings, the security IHS link analysis tool 800 may determine that 'newproduct.html' does not belong to a user-defined category. However, in this embodiment, security IHS link analysis tool 800 may use past browsing history, time of previous access to similar content, similar content which has been categorized, and other factors to determine an appropriate category for the content. In this scenario, the security IHS link analysis tool 800 may autonomously determine a category for the content without user intervention.

**[0032]** Security IHS link analysis tool 800 may parse new product video 530 as content and determine it belongs to multiple categories: "advertisement" and "high-bandwidth video". Security IHS link analysis tool 800 may parse user ID 535, password 540, and login 545 as content and determine they belong to category "user login website". Security IHS link analysis tool 800 may also determine that password 540 does not use a proper hypertext markup language (HTML) form field and as content belongs to category "security risk" as well as "user login website".

**[0033]** Security IHS link analysis tool 800 may parse link 550-1, link 550-2, link 550-3, ... , link 550-M and determine some, or all parts of the link 550-1, link 550-2, link 550-3, ... , link 550-M constitute content



and belong to categories. For example, link 550-1 may link to “www.medicalsupply.com/newproduct.html”. Security IHS link analysis tool 800 may parse “medicalsupply.com” as content and may further determine that this content belongs to multiple categories, such as “medical” and “business”. Security IHS link analysis tool 800 may parse “newproduct.html” as content, determine that this content is similar to “newproduct.html” from URL field 520 and identify the content as belonging to the same category as the content from “newproduct.html” from URL field 520, as discussed above. Identifying each content portion and appending each content portion to one or more categories is discussed in more detail below with respect to TABLE 1.

**[0034]** Security IHS link analysis tool 800 may parse additional data, but is not limited to the examples above, wherein portions of webpage 525 may be hidden to the user, such as metadata, image tags, and other data. In one embodiment, security IHS link analysis tool 800, based on user settings, assesses the respective weights of categories and the number of instance of those categories identified on webpage 525 and determines a sensitivity level of webpage 525 in accordance with those user settings. The security IHS link analysis tool determines the sensitivity level which may be a number greater than or equal to 0 but less than or equal to 1. Security IHS link analysis tool 800, based upon a user-defined sensitivity threshold and the determined sensitivity level of webpage 525, generates a network selection message. The user-defined sensitivity threshold may be a number greater than or equal to 0 but less than or equal to 1 and is discussed in more detail below with reference to TABLE 2. The network selection message includes the suggested network to be used for navigation by user IHS 200.

**[0035]** Referring now to TABLE 1, the user may define a weight for a category to increase with the perceived sensitivity or importance of the category. For example, a user wishing to only browse medical information on a trusted network may assign

the maximum weight, in this case “1”, to the “MEDICAL” category, as shown in TABLE 1.

TABLE 1

CATEGORY	WEIGHT	NUMBER OF INSTANCES
MEDICAL	1	1
BUSINESS	0	3
SOCIAL	0.6	13

In this scenario, security IHS link analysis tool 800 may determine that the presence of the “MEDICAL” category would be above the user-defined sensitivity threshold and therefore garner the maximum sensitivity level. The security IHS link analysis tool 800 may generate a network selection message that

the trusted network 105, namely the default network with the highest sensitivity threshold, be used by the user IHS 200 to navigate to webpage 525. In one embodiment, trusted network 105 exhibits the highest security of networks available to user IHS 200 for communication with other IHSs such as an IHS hosting a webpage on the Internet.

**[0036]** In another example, a user unconcerned with browsing information relating to business on a secure network may assign the minimum weight, in this case “0”, to the “BUSINESS” category, as shown in TABLE 1 above. The user may be concerned with browsing information relating to social media on a secure network, and may assign a weight of “0.6” to the “SOCIAL” category, as shown in TABLE 1. In this scenario, security IHS link analysis tool 800 may determine that the presence of the “SOCIAL” category may not be above the user-defined sensitivity threshold and therefore not garner the maximum sensitivity level. The security IHS link analysis tool 800 may generate a network selection message that the non-secure network 115-1, a network below the sensitivity threshold, be used by the user IHS 200 to navigate to webpage 525.

**[0037]** In another example, the security IHS link analysis tool 800 parses webpage 525 and determines that one (1) content portion belongs to the “MEDICAL” category. The security IHS link analysis tool 800 may append “1” as the “NUMBER OF INSTANCES” in the “MEDICAL” row of TABLE 1. The security IHS link analysis tool 800 may determine that 3 content portions belong to the “BUSINESS” category. The security IHS link analysis tool 800 may append “3” as the “NUMBER OF INSTANCES” in the “BUSINESS” row of TABLE 1. The security IHS link analysis tool 800 may determine that 13 content portions belong to the “SOCIAL” category. The security IHS link analysis tool 800 may append “13” as the “NUMBER OF INSTANCES” in the “SOCIAL” row of TABLE 1. Each time that the security IHS link analysis tool 800 determines that a content portion belongs to a category, the security IHS link analysis tool 800 increments the “NUMBER OF INSTANCES” of that category by one (1).

**[0038]** In one embodiment, the user may set individual sensitivity thresholds on a per network basis. For example, a user may set a sensitivity threshold of “0.9” for trusted network 105, a sensitivity threshold of “0.75” for non-secure network 115-1, and a sensitivity threshold of “0.5” for non-secure network 115-2, such as shown in TABLE 2 below. The security IHS link analysis tool 800, based upon a user-defined sensitivity threshold and the determined sensitivity level of webpage 525 generates a network selection message.

TABLE 2

NETWORKS	SENSITIVITY THRESHOLDS
trusted network 105	0.9
non-secure network 115-1	0.75
non-secure network 115-2	0.5

**[0039]** In another embodiment, the user may set SENSITIVITY THRESHOLDS for GROUPS of NETWORKS as shown in TABLE 3 below. A user may set the SENSITIVITY THRESHOLD for group G1 to “0.95”. The SENSITIVITY THRESHOLD for trusted network 105 may then be set to “0.95”. A user may set the SENSITIVITY THRESHOLD for group G2 to “0.6”. The SENSITIVITY THRESHOLD for non-secure network 115-1 and non-secure network 115-2 may then be set to “0.6”. A user may set the SENSITIVITY THRESHOLD for group G3 to “0.2”. The SENSITIVITY THRESHOLD for non-secure network 115-M may then be set to “0.2”. The security IHS link analysis tool 800, based upon a user-defined sensitivity threshold and the determined sensitivity level of webpage 525 generates a network selection message.

TABLE 3

GROUPS	NETWORKS	SENSITIVITY THRESHOLDS
G1	trusted network 105	0.95
G2	non-secure network 115-1, non-secure network 115-2	0.6
G3	non-secure network 115-M	0.2

**[0040]** In another embodiment, the user may set a time period for which an individual network, or group of networks, exhibits different sensitivity thresholds. For example, a user may set a sensitivity threshold of “0.9” for trusted network 105. In this scenario, the user may set the sensitivity threshold for trusted network 105 to be “0.7” during the local hours of user IHS 200 from 8:00 to 17:00, i.e. a time period.

**[0041]** In another embodiment, the user may set a time period for which a category exhibits different weights. For example, a user may set a weight of “0.3” for category “SOCIAL”. In this scenario, the user may set the weight for category “SOCIAL” to be “0.7” during the local hours of user IHS 200 from 8:00 to 15:00, i.e. a time period.

**[0042]** In another embodiment, the user may change the default link depth option from “0” to one of “1”, “2”, “3”, ... , “M”. “Link depth” refers to how many levels of links the security IHS link analysis tool 800 navigates to and analyzes. With a link depth of “0”, the security IHS link analysis tool 800 may analyze only the target of the link and not further. With a link depth of “1”, the security IHS link analysis tool 800 may analyze the target of the link and the targets of the target of the link. With a link depth of “2”, the security IHS link analysis tool 800 may analyze the target of the link, the targets of the target of the link, and the targets of the targets of the target of the link, and so on according to increasing link depth. In this scenario, the user increases the link depth option from “0” to “1”. The security IHS analysis tool 800 responds by navigating to not only webpage 525 to parse for content, but also by navigating to the target of link 550-1, link 550-2, link 550-3, ... , link 550-M to parse for content. Link 550-1, link 550-2, link 550-3, ... , link 550-M are 1 link depth away from webpage 525. With the link depth set to “1”, the security IHS link analysis tool 800, based upon a user-defined sensitivity threshold and the determined sensitivity level of webpage 525, link 550-1, link 550-2, link 550-3, ... , link 550-M generates a network selection message. The network selection message includes the suggested network to be used for navigation by user IHS 200.

**[0043]** Security IHS link analysis tool 800 transmits a network selection message, via Internet 110, through trusted network 105, to user IHS 200. User IHS link analysis tool 700 of user IHS 200 receives the network selection message and may generate an override network selection message prompt 600. Fig. 6 shows an example of an override network selection message prompt 600 that user IHS 200 may display on display 235. In this scenario, the network selection message suggests that the content on webpage 525 is sensitive, and should be navigated to using trusted network 105. Override network selection message prompt 600 displays information indicating that the link to be navigated to is not suitable for a non-secure connection.

**[0044]** If the user selects YES button 605, user IHS link analysis tool 700 navigates to webpage 525 through trusted network 105. However, if the user selects USE NON-SECURE NETWORK 115-1, user IHS link analysis tool 700 navigates to webpage 525 through non-secure network 115-1. If the user selects USE NON-SECURE NETWORK 115-2, user IHS link analysis tool 700 navigates to webpage 525 through non-secure network 115-2. If the user selects USE NON-SECURE NETWORK 115-M, user IHS link analysis tool 700 navigates to webpage 525 through non-secure network 115-M.

**[0045]** In another embodiment, the user IHS link analysis tool 700 may transmit a response to security IHS 300 through trusted network 105, via Internet 110. The response may include the user’s selection of whether or not to override the network selection message and which network was selected for navigation. Security IHS link analysis tool 800 may use some or all information available, including but not limited to,

past user decisions, time of decisions, available networks, content accessed, categories and more to choose the appropriate network.

**[0046]** In another embodiment, after transmitting the network selection message to the user IHS 200, the security IHS link analysis tool 800 may prefetch additional content. It is likely that after navigating to webpage 525, the user may decide to select one of link 550-1, link 550-2, link 550-3, ... link 550-M to navigate to next. The security IHS analysis tool 800 responds by navigating to the target of link 550-1, link 550-2, link 550-3, ... , link 550-M to parse the targets for content. Security IHS link analysis tool 800, based upon a user-defined sensitivity threshold and the determined sensitivity level of link 550-1, link 550-2, link 550-3, ... link 550-M generates a network selection message for each link. Each network selection message includes the suggested network to be used for navigation by user IHS 200 in the event that the user selects one of those links for future navigation. The above actions may speed up processing time as perceived by the user of user IHS 200, by effectively anticipating the next link clicked by the user. Depending on user settings, security IHS link analysis tool 800 may prefetch content N levels deep, wherein N is an integer. For example, one level deep (N=1), corresponds to the security IHS link analysis tool 800 prefetching additional content of the targets of the target of the link. Two levels deep (N=2), corresponds to the security IHS link analysis tool 800 prefetching additional content of the targets of targets of the target of the link.

**[0047]** In another embodiment, multiple users may use the disclosed network selection system 100. For example, multiple users User A, User B, User C, and User D may use network selection system 100. User A and User B both configured security IHS link analysis tool 800 to suit their respective network needs. User C may instruct security IHS link analysis tool 800 to use settings similar to those User A uses, but not similar to those User B uses. User D may instruct security IHS link analysis tool 800 to use settings similar to those of User B, but not similar to those of User A.

**[0048]** Fig. 7 is a flowchart that shows process flow of the user IHS link analysis tool 700 that executes on user IHS 200 in cooperation with security IHS link analysis tool 800 that executes on security IHS 300. Process flow commences when user IHS 200 initializes and launches user IHS link analysis tool 700, as per start block 705. The user attempts to attempt to navigate, for example, to webpage 525, that is the target of link 425-1, as per block 710. The user IHS link analysis tool 700 intercepts the user's attempt to navigate, as per block 715. The user IHS link analysis tool 700 may transmit the link to security IHS 300 through trusted network 105, via the Internet 110, as per block 720.

**[0049]** The user IHS 200 receives a network selection message from security IHS 300 via the Internet, through trusted network 105. The user IHS link analysis tool 700 intercepts the network selection message, as per block 725. The user IHS link analysis tool 700 displays, for example, an override

network selection message prompt 600 on display 235, that informs the user of the indicated network and other network choices, as per block 730. The user may choose to select the indicated network or override and choose another network, as per decision block 735. If the user does not override the network selection message, as per decision block 735, the user IHS link analysis tool 200 navigates to the target of the link using the indicated network, as per block 740. After navigating to the link by using the indicated network, as per block 740, the process flow may end, as per block 745. Alternatively, process flow may continue back to start block 705 and the process starts anew.

**[0050]** However, if the user chooses to override the indicated network, as per decision block 735, the user selects which network to use, as per block 745. The user IHS link analysis tool 700 navigates to the target of the selected link using the selected network, as per block 750. After navigating to the link using the indicated network, as per block 750, the process flow may end, as per block 745. Alternatively, process flow may continue back to start block 705 and the process starts anew.

**[0051]** Fig. 8 is a flowchart that shows process flow of the security IHS link analysis tool 800 when it executes on security IHS 300 in cooperation with user IHS link analysis tool 700 that executes on security IHS 200. Process flow commences when security IHS 300 initializes and launches security IHS link analysis tool 800, as per start block 805. Security IHS link analysis tool 800 of security IHS 300 may receive a link from user IHS 200 via the Internet, over trusted network 105, as per block 810.

**[0052]** Security IHS link analysis tool 800 conducts a test to determine if the link was analyzed previously, as per decision block 815. If the link was not previously analyzed, security IHS link analysis tool 800 analyzes the link for content, as per block 820. If the link was previously analyzed for content, security IHS link analysis tool 800 determines if the link contains sensitive content, namely content above the sensitivity threshold, as per decision block 825. If the security IHS link analysis tool 800 determines that the link does not contain sensitive content, the security IHS link analysis tool may transmit a network selection message to the user IHS 200 that indicates that user IHS 200 may use a non-secure network, as per block 830.

**[0053]** If the security IHS link analysis tool 800 determines that the link does contain sensitive content, the security IHS link analysis tool may transmit a network selection message to the user IHS 200 that user IHS 200 may use trusted network 105, as per block 835. The security IHS link analysis tool 800 determines if any more links need to be analyzed, per user settings, as per block 840. If security IHS link analysis tool 800 determines that link analysis is complete, process flow ends, as per block 845. If security IHS link analysis tool 800 determines that link analysis is not complete, security IHS link analysis tool 800 analyzes the remaining links, per user settings, as per block 850. After security IHS link analysis

tool 800 has analyzed the links, process flow ends, as per block 845. Alternatively, process flow may continue back to start block 805 and the process starts anew.

**[0054]** As will be appreciated by one skilled in the art, aspects of the disclosed methodology may be embodied as a system, method or computer program product. Accordingly, aspects of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present invention may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

**[0055]** Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

**[0056]** Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

**[0057]** Aspects of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the Figures 7 and 8 flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowcharts of Figures 7 and 8 and/or block diagram block or blocks.

**[0058]** These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

**[0059]** The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowcharts of Figures 7 and 8 described above.

**[0060]** The flowcharts of Figures 7 and 8 illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products that perform network analysis in accordance with various embodiments of the present invention. In this regard, each block in the flowcharts of Figures 7 and 8 may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in Figures 7 and 8. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of Figures 7 and 8 and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.



**[0061]** The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

**[0062]** The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

## CLAIMS

What is claimed is:

1. A method, comprising:
  - receiving, by a user information handling system (IHS), a request to navigate to an IHS other than the user IHS, the request including a link;
  - intercepting, by the user IHS, the request to navigate to an IHS other than the user IHS;
  - transmitting, by the user IHS, the link to a security IHS; and
  - receiving, by the user IHS, a network selection message from the security IHS, the network selection message indicating a particular network for the user IHS to employ in communicating with a target of the link.
2. The method of claim 1, wherein the request to navigate is a request to navigate to a webpage.
3. The method of claim 1, wherein the user IHS receives the network selection message from the security IHS via a trusted network.
4. The method of claim 1, wherein the network selection message is a non-secure network selection message that designates a particular non-secure network for communication between the user IHS and the target of the link.
5. The method of claim 3, wherein the network selection message is a trusted network selection message that designates the trusted network for communication between the user IHS and the security IHS.
6. The method of claim 1, further comprising displaying, by the user IHS, an override prompt when the user IHS receives a network selection message.
7. The method of claim 6, wherein the user IHS receives an override selection in response to the override prompt, the user IHS employing a particular network indicated in the override selection for communication with the target of the link.
8. The method of claim 7, further comprising transmitting, by the user IHS, the override selection to the security IHS via the trusted network.

9. The method of claim 1, wherein the network selection message designates one of a plurality of non-secure networks for communication between the user IHS and the target of the link.
10. A user information handling system (IHS), comprising:  
a processor;  
a memory, coupled to the processor, the memory being configured with a user IHS link analysis tool to:  
receive a request to navigate to an IHS other than the user IHS, the request including a link;  
intercept the request to navigate to an IHS other than the user IHS;  
transmit the link to a security IHS; and  
receive a network selection message from the security IHS, the network selection message indicating a particular network for the user IHS to employ in communicating with a target of the link.
11. The user IHS of claim 10, wherein the request to navigate is a request to navigate to a webpage.
12. The user IHS of claim 10, wherein the user IHS receives the network selection message from the security IHS via a trusted network.
13. The user IHS of claim 10, wherein the network selection message is a non-secure network selection message that designates a particular non-secure network for communication between the user IHS and the target of the link.
14. The user IHS of claim 12, wherein the network selection message is a trusted network selection message that designates the trusted network for communication between the user IHS and the security IHS.
15. The user IHS of claim 10, wherein the user IHS displays an override prompt when the user IHS receives a network selection message.
16. The user IHS of claim 15, wherein the user IHS receives an override selection in response to the override prompt, the user IHS employing a particular network indicated in the override selection for communication with the target of the link.
17. The user IHS of claim 16, wherein the user IHS transmits the override selection to the security IHS via the trusted network.

18. The method of claim 10, wherein the network selection message designates one of a plurality of non-secure networks for communication between the user IHS and the target of the link.
19. A user IHS link analysis tool computer program product, comprising:  
a non-transitory computer readable storage medium;  
first instructions that receive a request to navigate to an IHS other than the user IHS, the request including a link;  
second instructions that intercept the request to navigate to an IHS other than the user IHS;  
third instructions that transmit the link to a security IHS; and  
fourth instructions that receive a network selection message from the security IHS, the network selection message indicating a particular network for the user IHS to employ in communicating with a target of the link;  
wherein the first, second third and fourth instructions are on the non-transitory computer readable storage medium.
20. The user IHS link analysis tool computer program product, of claim 19, wherein the request to navigate is a request to navigate to a webpage.
21. The user IHS link analysis tool computer program product, of claim 19, further comprising fifth instructions that receive the network selection message from the security IHS via a trusted network.
22. The user IHS link analysis tool computer program product, of claim 19, wherein the network selection message is a non-secure network selection message that designates a particular non-secure network for communication between the user IHS and the target of the link.
23. The user IHS link analysis tool computer program product of claim 21, wherein the network selection message is a trusted network selection message that designates the trusted network for communication between the user IHS and the security IHS.
24. The user IHS link analysis tool computer program product of claim 19, further comprising sixth instructions that display an override prompt when the user IHS receives a network selection message.

25. The user IHS link analysis tool computer program product of claim 24, further comprising seventh instructions that receive an override selection in response to the override prompt, the user IHS employing a particular network indicated in the override selection for communication with the target of the link.

FIG. 1

100

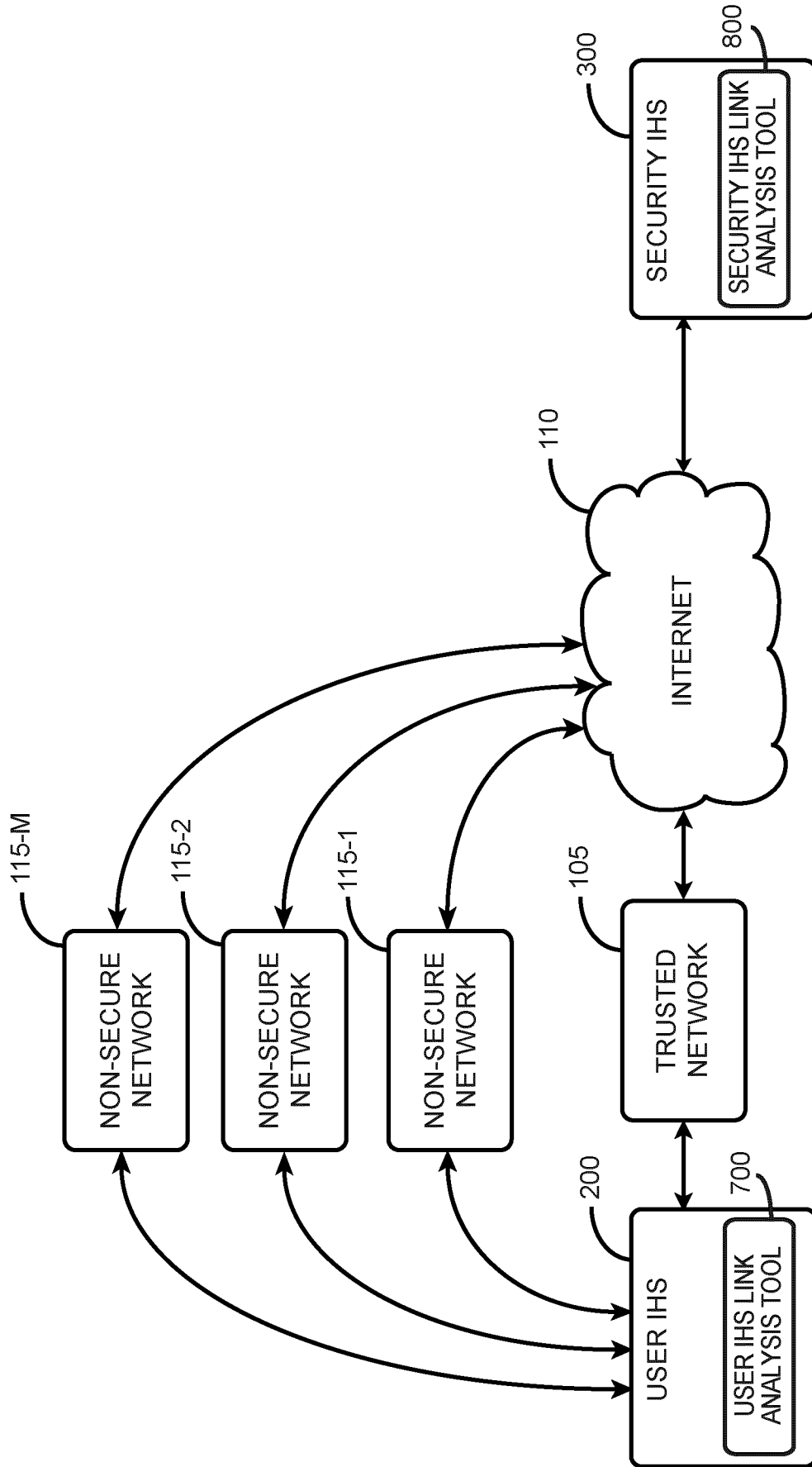


FIG. 2

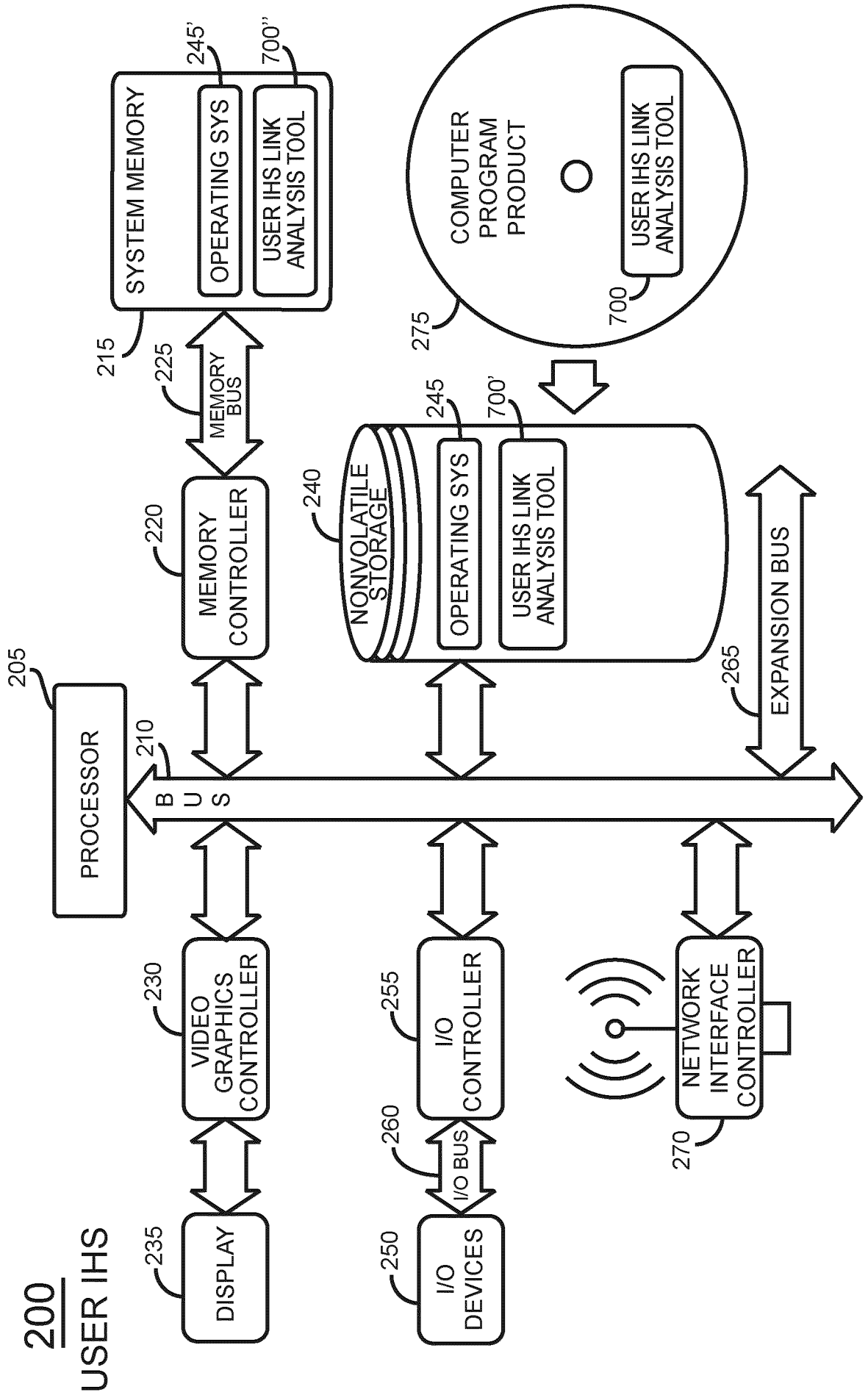


FIG. 3

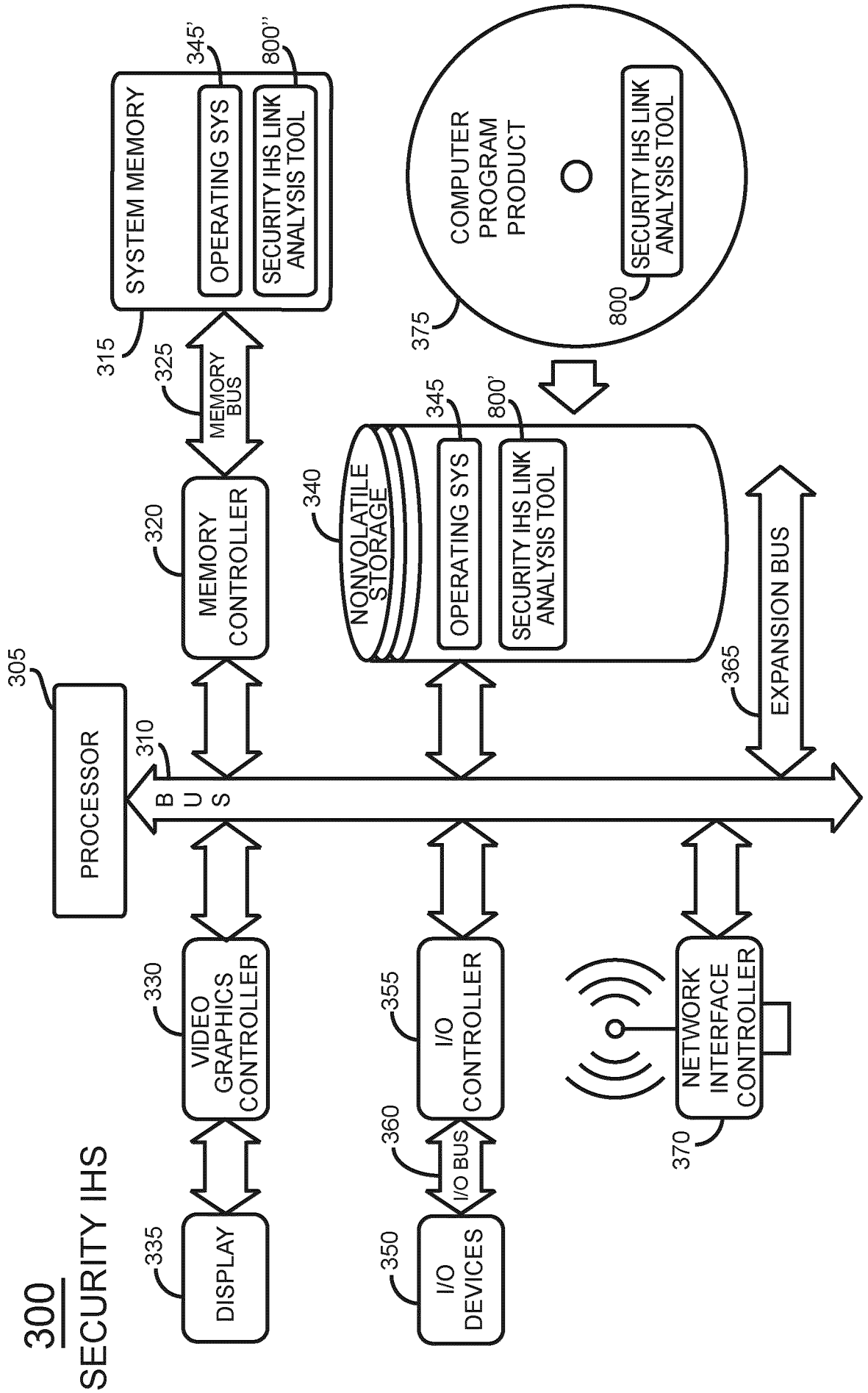
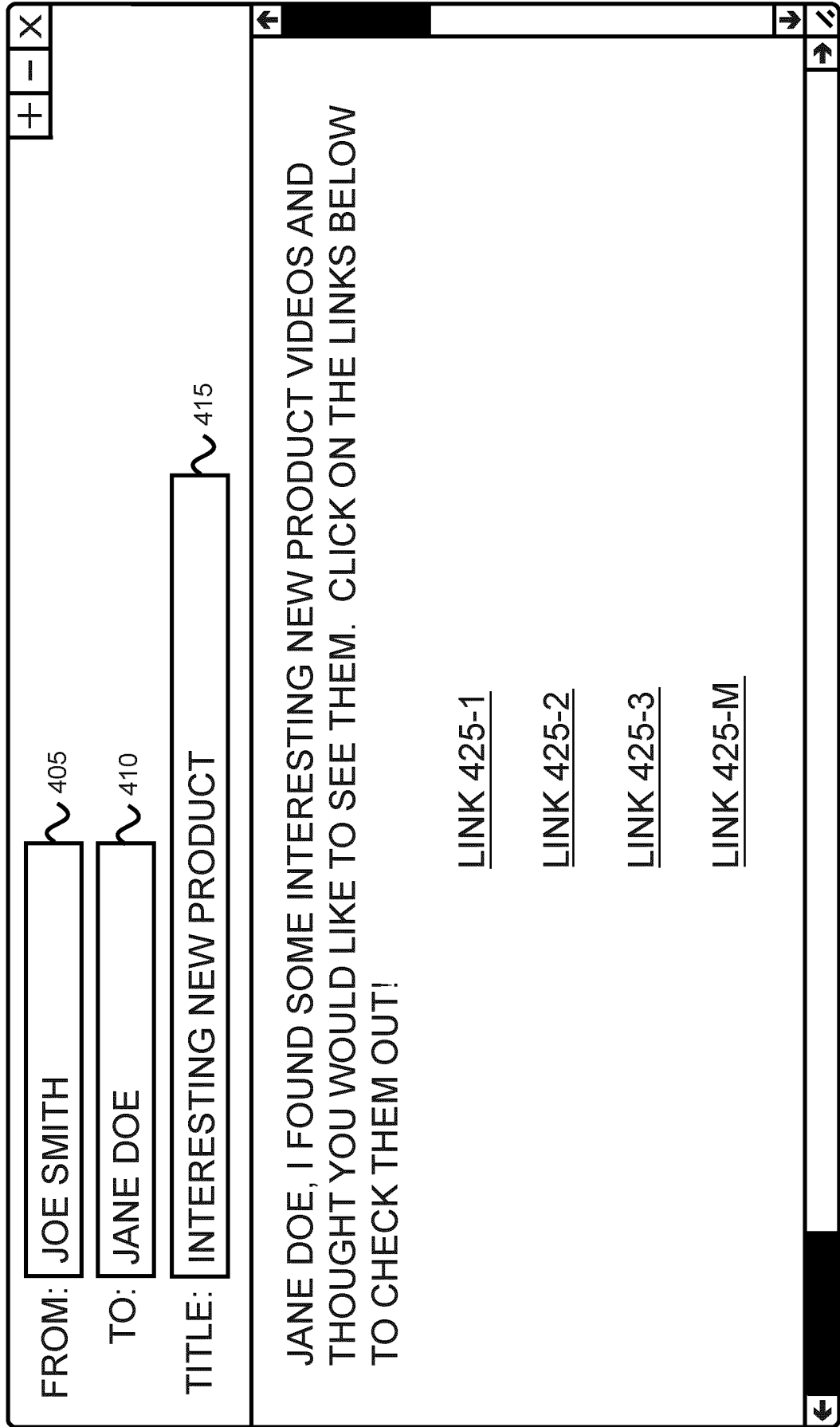




FIG. 4

400



420

FIG. 5

500

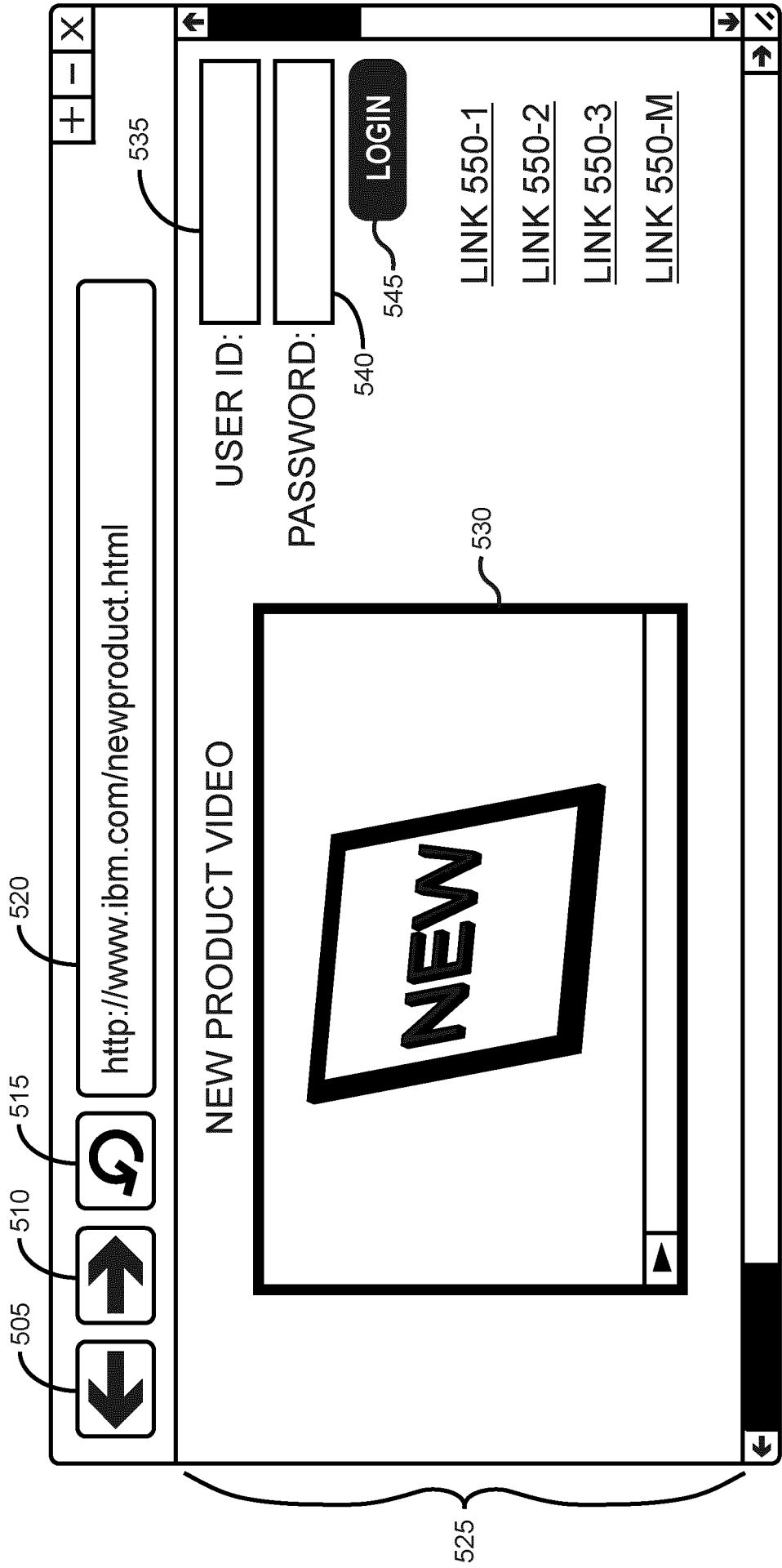


FIG. 6

600

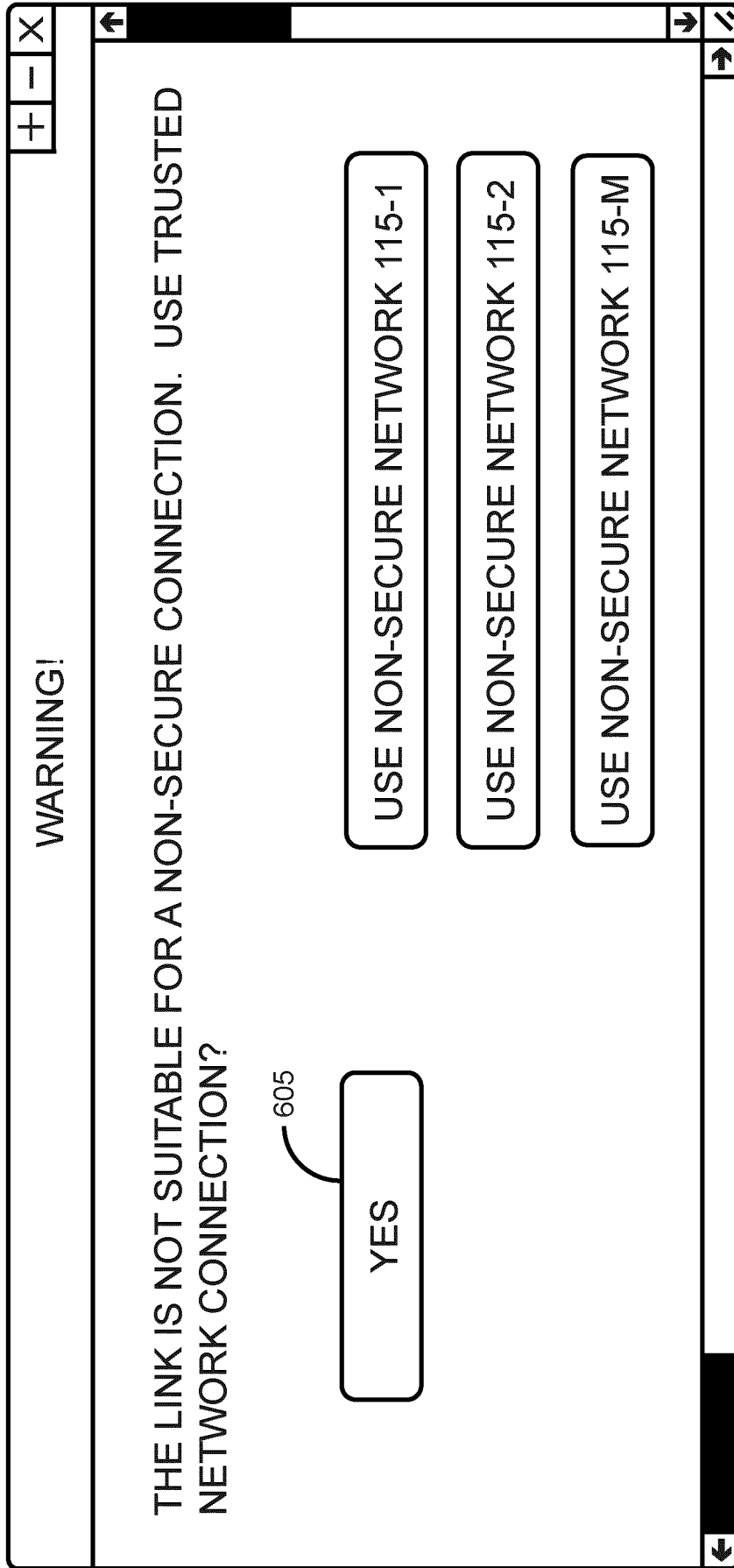


FIG. 7

700

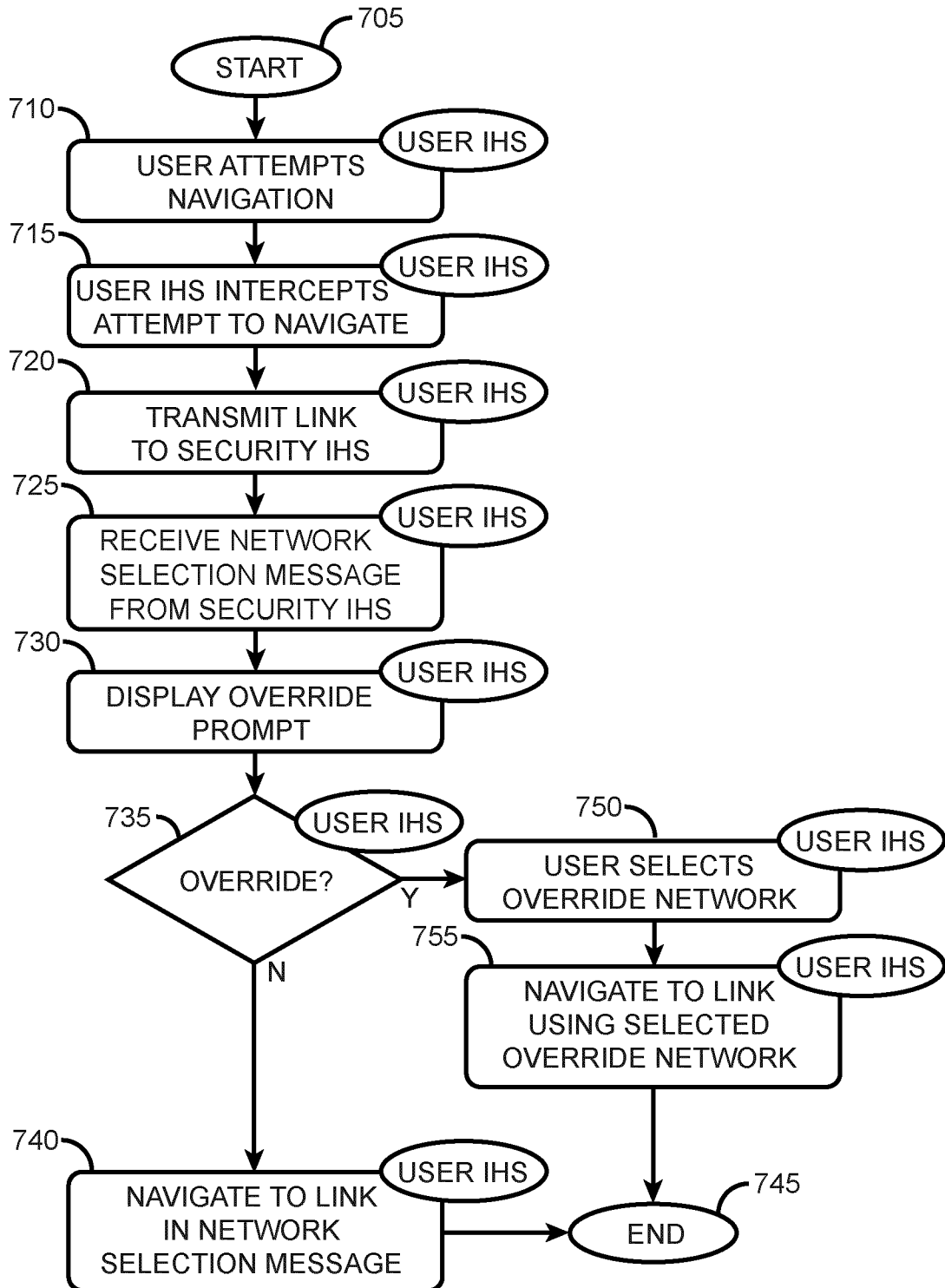
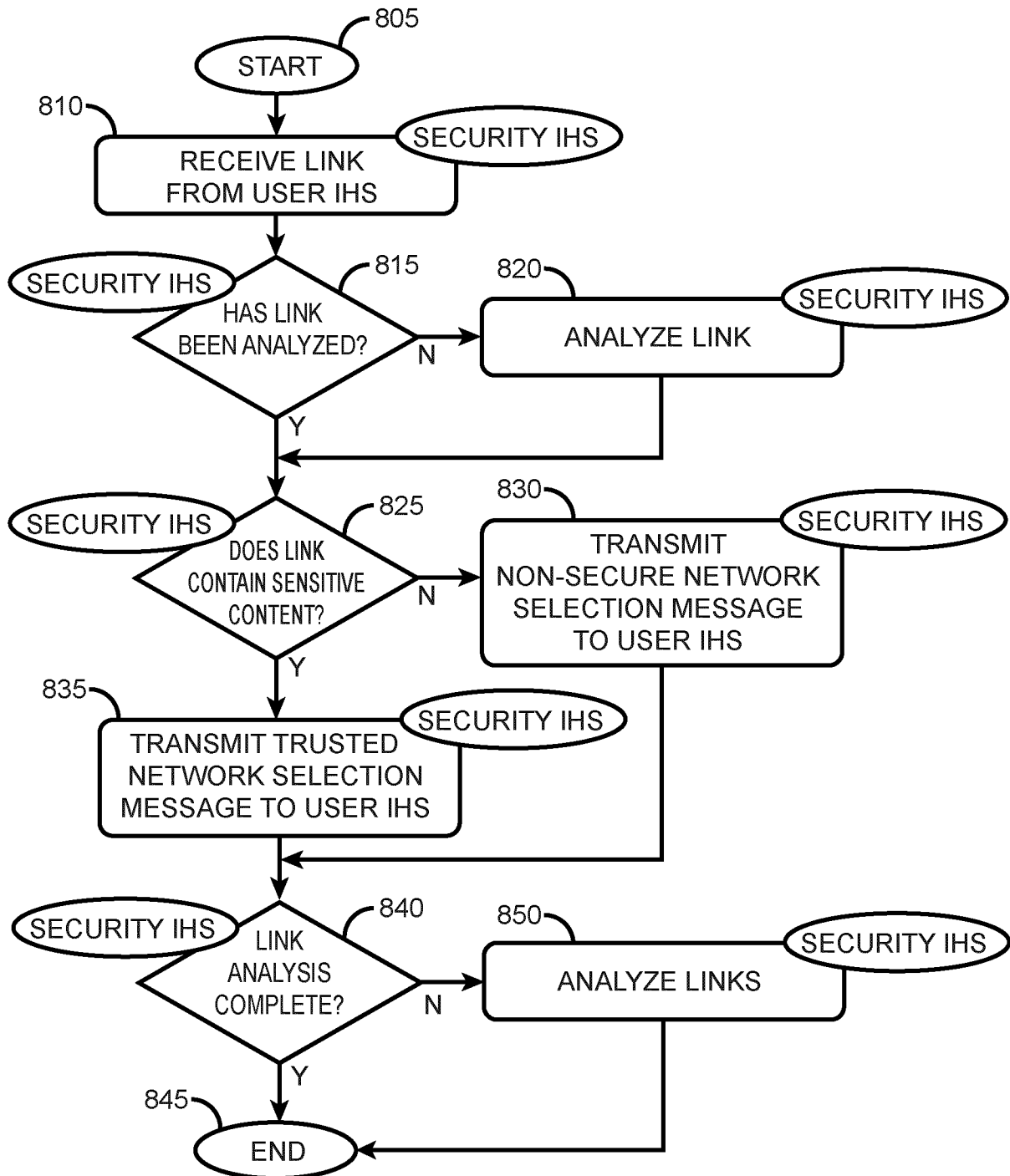


FIG. 8

800



**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/CA2013/050480

A. CLASSIFICATION OF SUBJECT MATTER  
 IPC: **H04L 12/46** (2006.01) , **H04L 12/26** (2006.01) , **H04L 12/58** (2006.01) , **H04L 9/00** (2006.01)  
 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: (2006.01): H04L 12/46, H04L 12/26, H04L 12/58, H04L 9/00

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)  
 EPOQUE (EPODOC, English Full Text), Google (switch, secure, rout+, browser, network, purchase, non-secure, unsecured, browser links, trusted, untrusted, select+, target, hyperlink, hyper+, location, choose, web+, content, filter)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 827 037 A2 (KARAGUZ) 29 August 2007 (29-08-2007) * whole document especially Figs 1-4, 7-8; par. 52, 54-59, 68, 156-157 *	1-25
A	EP 0 781 064 A2 (SEPPANEN et al.) 25 June 1997 (25-06-1997) * whole document *	1-25
A	EP 1 622 332 A1 (LIU et al.) 1 February 2006 (01-02-2006) * whole document *	1-25
A	US 2005/0238046 A1 (HASSAN et al.) 27 October 2005 (27-10-2005) * whole document *	1-25
A	US 2004/0143628 A1 (BRADFORD et al.) 22 July 2004 (22-07-2004) * whole document *	1-25
A	US 2003/0014659 A1 (ZHU ) 16 January 2003 (16-01-2003) * whole document *	1-25

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

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

Date of the actual completion of the international search 27 September 2013 (27-09-2013)	Date of mailing of the international search report 03 October 2013 (03-10-2013)
---	--

Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Authorized officer  <b>Mehdi Ghayour (819) 953-1566</b>
---	---

**INTERNATIONAL SEARCH REPORT**International application No.  
PCT/CA2013/050480

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/0105863 A1 (HEGLI et al.) 5 June 2003 (05-06-2003) * whole document *	1-25
A	US 2010/0058204 A1 (WILSON) 4 March 2010 (04-03-2010) * whole document *	1-25

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
**PCT/CA2013/050480**

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
EP1827037A2	29 August 2007 (29-08-2007)	CN101039481A EP1827037A3 TW200806056A TWI353801B US2007202915A1 US8155693B2 US2012196567A1	19 September 2007 (19-09-2007) 22 September 2010 (22-09-2010) 16 January 2008 (16-01-2008) 01 December 2011 (01-12-2011) 30 August 2007 (30-08-2007) 10 April 2012 (10-04-2012) 02 August 2012 (02-08-2012)
EP0781064A2	25 June 1997 (25-06-1997)	EP0781064A3 US5903832A	13 October 1999 (13-10-1999) 11 May 1999 (11-05-1999)
EP1622332A1	01 February 2006 (01-02-2006)	None	
US2005238046A1	27 October 2005 (27-10-2005)	US7761607B2	20 July 2010 (20-07-2010)
US2004143628A1	22 July 2004 (22-07-2004)	CN2462234Y EP1225391A2 EP1225391A3 US2002156838A1 US8065358B2 US2002093279A1 US2006039156A1	28 November 2001 (28-11-2001) 24 July 2002 (24-07-2002) 12 January 2005 (12-01-2005) 24 October 2002 (24-10-2002) 22 November 2011 (22-11-2011) 18 July 2002 (18-07-2002) 23 February 2006 (23-02-2006)
US2003014659A1	16 January 2003 (16-01-2003)	CN1529863A JP2004536407A WO03009172A2 WO03009172A3	15 September 2004 (15-09-2004) 02 December 2004 (02-12-2004) 30 January 2003 (30-01-2003) 26 February 2004 (26-02-2004)
US2003105863A1	05 June 2003 (05-06-2003)	AT484910T AU2002351237A1 AU2002351237B2 CA2465662A1 CA2465662C DE60237998D1 EP1461929A2 EP1461929B1 JP2005512211A JP4292403B2 US6947985B2 US2006031504A1 US7483982B2 WO03049403A2 WO03049403A3	15 October 2010 (15-10-2010) 17 June 2003 (17-06-2003) 07 June 2007 (07-06-2007) 12 June 2003 (12-06-2003) 15 February 2011 (15-02-2011) 25 November 2010 (25-11-2010) 29 September 2004 (29-09-2004) 13 October 2010 (13-10-2010) 28 April 2005 (28-04-2005) 08 July 2009 (08-07-2009) 20 September 2005 (20-09-2005) 09 February 2006 (09-02-2006) 27 January 2009 (27-01-2009) 12 June 2003 (12-06-2003) 27 November 2003 (27-11-2003)
US2010058204A1	04 March 2010 (04-03-2010)	EP2080127A2 GB0621752D0 US8539329B2 WO2008053228A2 WO2008053228A3 WO2008053228A9	22 July 2009 (22-07-2009) 13 December 2006 (13-12-2006) 17 September 2013 (17-09-2013) 08 May 2008 (08-05-2008) 08 January 2009 (08-01-2009) 19 March 2009 (19-03-2009)