

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 November 2008 (13.11.2008)

PCT

(10) International Publication Number
WO 2008/137387 A1

- (51) International Patent Classification:
G06F 15/16 (2006.01) **G06F 17/00** (2006.01)
- (21) International Application Number:
PCT/US2008/061792
- (22) International Filing Date: 28 April 2008 (28.04.2008)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
11/742,539 30 April 2007 (30.04.2007) US
- (71) Applicant (for all designated States except US):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. [US/US]; 20555 S.h. 249, Houston, TX 77070 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **WALKER, Philip, M.** [US/US]; 3404 E. Harmony Road, Fort Collins, CO 80528 (US). **MCCOLLOM, William, G.** [US/US]; 3404 E. Harmony Road, Fort Collins, CO 80528 (US). **MINER,**

Kathy, L. [US/US]; 3404 E. Harmony Road, Fort Collins, CO 80528 (US). **SRINIVAS, Pulle** [IN/IN]; HP Ave., 39/40, Electronics City Hosur Road, Bengalooru 560100 (IN).

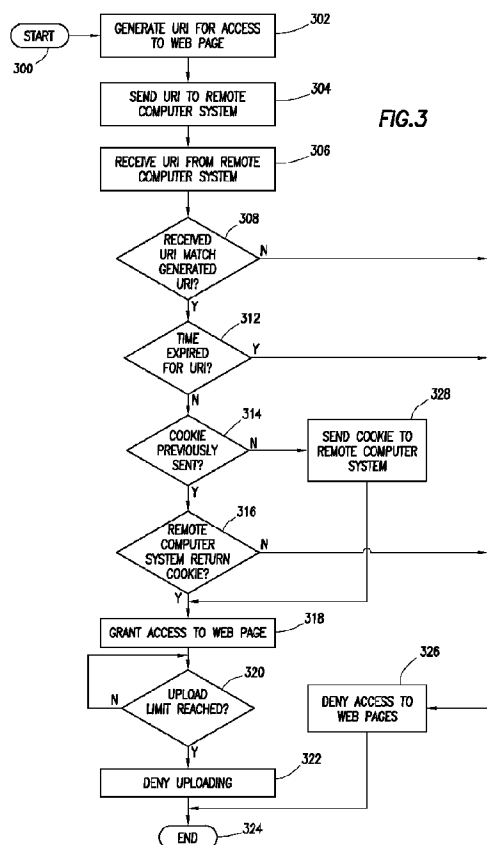
(74) Agents: **HARTNETT, Clare** et al.; Hewlett-Packard Company, Intellectual Property Administration, Mail Stop 35, P.O. Box 272400, Fort Collins, CO 80527-2400 (US).

(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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

[Continued on next page]

(54) Title: METHOD AND SYSTEM OF VERIFYING PERMISSION FOR A REMOTE COMPUTER SYSTEM TO ACCESS A WEB PAGE



(57) Abstract: Methods and systems of verifying permission for a remote computer system to access a web page. At least some of the illustrative embodiments are methods comprising receiving (306) a request from a remote computer (10, 16, 102) to access a web page stored on a server (20), verifying (308, 312, 314, 316) permission of the remote computer to access the web page without the remote computer system (10, 16, 102) sending a user name and password, and granting (318) the remote computer (10, 16, 10) access to the web page if permission is verified.



GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report*

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

METHOD AND SYSTEM OF VERIFYING PERMISSION FOR A REMOTE COMPUTER SYSTEM TO ACCESS A WEB PAGE

BACKGROUND

[0001] Limiting access to web pages, both with respect to viewing the web pages and modifying the web pages, is a cumbersome process. For each web page or series of web pages which a person seeks to view and/or modify for which access is limited, the person is assigned a user name and password which are used to authenticate each new session. In some cases, the passwords automatically expire after a pre-determined amount of time, thus forcing the person to periodically generate and remember a new password periodically. While user names and passwords are not complicated pieces of information, the person may have a user name and password for a host of websites (*e.g.*, banking website, stock trading website, online auction website, electronic travel ticketing website, or warranty registration websites, just to name a few), and keeping track of all the varying user names and passwords is difficult. Likewise, the entity providing the web pages has a large administrative burden regarding, for example, assigning user names to new users, assigning and modifying privileges for each user, ensuring login privileges are revoked for users whose no longer have permission to access the web pages.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] For a detailed description of exemplary embodiments, reference will now be made to the accompanying drawings in which:

[0003] Figure 1 shows a system in accordance with at least some embodiments;

[0004] Figure 2 shows in greater detail a home network server in accordance with at least some embodiments; and

[0005] Figure 3 shows a method in accordance with at least some embodiments.

NOTATION AND NOMENCLATURE

[0006] Certain terms are used throughout the following description and claims to refer to particular system components. As one skilled in the art will appreciate, computer companies may refer to a component by different names. This document does not intend to distinguish between components that differ in name but not function. In the following discussion and in the claims, the terms “including” and “comprising” are used in an open-ended fashion, and thus should be interpreted to mean “including, but not limited to... .”

[0007] Also, the term “couple” or “couples” is intended to mean either an indirect, direct, optical or wireless electrical connection. Thus, if a first device couples to a second device, that connection may be through a direct electrical connection, through an indirect electrical connection via other devices and connections, through an optical electrical connection, or through a wireless electrical connection.

[0008] The term “Universal Resource Indicator” or URI shall mean a set of characters (*e.g.*, letters, numbers and symbols) that identify a resource accessible through networking protocols, and the URI also comprises any information that may be included with the information that identifies the resource (*e.g.*, information that identifies the referring page, the search terms to use on the requested page, unsubscribe information, or authentication information, expiration information, information regarding for whom the URI was generated).

DETAILED DESCRIPTION

[0009] The following discussion is directed to various embodiments. Although one or more of these embodiments may be preferred, the embodiments disclosed should not be interpreted, or otherwise used, as limiting the scope of the disclosure, including the claims. In addition, one skilled in the art will understand that the following description has broad application, and the discussion of any embodiment is meant only to be exemplary of that embodiment, and not intended

to intimate that the scope of the disclosure, including the claims, is limited to that embodiment.

[0010] Figure 1 illustrates a system 1000 in accordance with at least some embodiments. In particular, the system 1000 comprises a home network system 100 and communicatively coupled to a remotely located computer system 102 (*i.e.*, computer system 102 physically located an appreciable distance (*e.g.*, miles) from the home network system). The home network system 100 comprises an illustrative desktop computer system 10 coupled to the Internet 12 by way of a router 14. The home network system 100 also comprises a second computer system, in this case a portable computer system 16, coupled to the Internet 12 by way of the router 14. In the embodiments illustrated in Figure 1, desktop computer system 10 couples to the router by way of a hardwired connection 18 (*e.g.*, an Ethernet connection) and illustrative portable computer system 16 couples to the router 14 wirelessly (*e.g.*, IEEE 802.11, Bluetooth). However, computer systems may couple to the router in a hardwired fashion and/or wirelessly without regard to their portability. Further, while the home network system 100 of Figure 1 shows only one desktop computer system 10 and one portable computer system 16, any number of computer systems may be coupled to the router using any networking functionality.

[0011] The home network system 100 of Figure 1 also comprises a home network server 20 coupled to the router 14. The home network server 20 is a storage device and/or server available to any computer system of the home network system 100 (*e.g.*, desktop computer system 10 or portable notebook computer system 16), and in some cases the home network server 20 is also available to the remote computer system 102. The home network server 20 may be, for example, the central repository for data generated by computer systems of the home network system 100 and the server from which family web pages are hosted. The storage implemented by home network server 20 is accessible to other computer systems by way of any suitable currently available networking communication protocol (*e.g.*, Internet Protocol (IP), Transmission Control Protocol/Internet Protocol (TCP/IP), server message block (SMB)/common internet file system (CIFS)), or any after-developed networking protocol. Thus,

the home network server 20 operates, at least in part, as a network attached storage (NAS) device.

[0012] Figure 2 illustrates in greater detail an embodiment of the home network server 20. In particular, home network sever 20 comprises a processor 24 coupled to a main memory array 26 and various other components through host bridge 28. The processor 24 couples to the host bridge 28 (sometimes referred to as a “north bridge” because of its location in computer system drawings) by way of a host bus 30, or the host bridge 28 may be integrated into the processor 24. The processor 24 may be one of many available processors, and thus the home network server 20 may implement other bus configurations or bus-bridges in addition to, or in place of, those shown in Figure 2.

[0013] Main memory array 26 couples to the host bridge 28 through a memory bus 32. The host bridge 28 comprises a memory control unit that controls transactions to the main memory 26 by asserting control signals for memory accesses. The main memory array 26 functions as the working memory for the processor 24 and comprises a memory device or array of memory devices in which programs, instructions and data are stored. The main memory array 26 may comprise any suitable type of memory such as dynamic random access memory (DRAM) or any of the various types of DRAM devices such as synchronous DRAM (SDRAM), extended data output DRAM (EDODRAM), or Rambus DRAM (RDRAM).

[0014] Still referring to Figure 2, the home network server 20 also comprises a second bridge 34 that bridges the primary expansion bus 36 to various secondary expansion buses, such as the peripheral component interconnect (PCI) bus 38 and the low pin count (LPC) bus 44. The second bridge 34 may be referred to as the “south bridge” because of its location in computer system drawings. Read only memory (ROM) 42 couples to the south bridge 34, such as by the LPC bus 44. The ROM 42 contains software programs executable by the processor 24 to enable the computer system components to perform tasks such as acting as a network attached storage device, and to simplify authentication of access to web pages hosted on the home network server (discussed more below).

[0015] The home network server 20 further comprises a drive controller 46 coupled to the south bridge 34 by way of the illustrative PCI bus 38. In alternative embodiments, the drive controller may couple to the primary expansion bus 36, or any other currently available or after-developed expansion bus. The drive controller 46 controls the non-volatile memory 48, such as a hard drive or optical drive. In some embodiments, the home network server 20 implements a single hard drive where computer systems of the home network can store and retrieve data and programs. In alternative embodiments, the home network server 20 implements a redundant array of independent (or inexpensive) devices (RAID) system where the data and instructions written to the home network server are duplicated across multiple hard drives to implement fault tolerance.

[0016] Also coupled to the illustrative PCI bus 38 is a network interface card (NIC) 50. In alternative embodiments, the functionality of the NIC 50 is integrated onto the motherboard along with the bridges 28 and 34. Regardless of the precise location where the NIC is implemented, the NIC 50 enables the home network storage 20 to communicate with other computer systems on the home networking system 100 (through the router 14 of Figure 1) such that the home network server can assist in automatic publishing of user content to web pages.

[0017] Because the home network server 20 is designed to act as a server for the home network system 100, and possibly to reduce cost, in accordance with at least some embodiments, the home network server 20 does not support direct coupling of a display device and/or keyboard. Thus, in some embodiments a home network sever 20 does not comprise a graphics controller that would couple to a display, and also does not comprise an input/output (I/O) controller that would couple to I/O devices such as a keyboard and mouse. To the extent administration is performed on the home network server 20, the administration may be accomplished remotely using other computer systems (*e.g.*, desktop computer system 10 or portable computer system 16) in the home network system 100.

[0018] In accordance with the various embodiments, the home network server 20 simplifies the process of authenticating access to (*i.e.*, verifying permission to access) web pages hosted on the home network server 20, the

simplification both for locally coupled computer systems (*e.g.*, computer systems 10 and 16) and for remotely coupled computer systems (*e.g.*, computer system 102). The discussion from this point forward is based on authenticating access attempts of the remote computer system 102 to view and/or modify web pages hosted on the home network server 20, but the discussion is equally applicable to locally coupled computer systems as well.

[0019] Rather than using user various forms of user-supplied information (*e.g.*, names and passwords, and/or biometric information) as the primary mechanism to authenticate access by the remote computer system 102, access to particular web pages hosted by the home network server 20 is based, at least in part, on an invitation process. In order to view a web page (*e.g.*, containing family pictures) hosted on the home network server 20, the home network server 20 is configured to send (*e.g.*, by way of an electronic mail message) to the remote computer system 102 a Universal Resource Indicator (URI) that identifies the web page. In some embodiments, the home network server sends the URI to the remote computer system 102 in the form of a hypertext link in an electronic mail message. For example, the home network server 20 may send an electronic mail message having a hypertext link “<http://familypictures.com/Vegas>.” Upon activating the link on the remote computer system 102 (*e.g.*, double-clicking the link), a browser program is invoked which searches for and attempts to display the page “<http://familypictures.hp.com/Vegas>” if available.

[0020] While sending URIs from the home network server 20 may dissuade some unauthorized access because of limited knowledge of the domain name and particular web page, “web crawlers” exist on the Internet which systematically scan the Internet for web pages, and make note of the content of identified web pages. Thus, though only a small trusted group of people may receive invitations to view the web pages hosted on the home network server 20, the existence and content of the web pages may nevertheless become known to the general population. In order to at least partially address these concerns, in accordance with at least some embodiments, each URI sent by the home network server 20 contains authentication information. When an access by a remote computer system is attempted, if the URI provided by the remote computer system does not

have authentication information, or correct authentication information, then access is denied.

[0021] In particular, in accordance with at least some embodiments, each URI generated by the home network server 20 contains an address portion and an authentication portion. The address portion and authentication portion are used to ensure that the URI was generated by the home network server 20. While the authentication portion may take many forms, in some embodiments the authentication portion is created as a one-way hash of the address portion along with other information, such as a private key associated with the home network server 20. One-way hash functions are characterized in that while it is computationally easy to compute the hash value given the source information, it is extremely difficult (*e.g.*, hundreds of computers thousands of hours) to calculate the source information given the hash value and less than all of the source information. A one-way hash may be equivalently referred to as: a compression function; contraction function; message digest; fingerprint; cryptographic checksum; message integrity check (MIC); or manipulation detection code (MDC). Thus, a URI generated in accordance with at least some embodiments may take the illustrative form:

“http://familypictures.com/Vegas&MAC=[HASH VALUE]”

where “http://familypictures.com/Vegas” is the address portion and “&MAC=[HASH VALUE]” is the illustrative authentication portion calculated using the address portion and other secret information, such as a private key of the home network server 20. In accordance with some embodiments, the hash value is a 32-character string, but any string length may be equivalently used.

[0022] When remote computer system 102 attempts to access web pages stored on the home network server 20, the URI provided by the browser of the remote computer system 102 is parsed to extract the address portion and the authentication portion. The home network server 20 calculates the one-way hash of the address portion and the home network server's 20 private key. If the one-way hash created by the home network server 20 using the address portion of the URI and the private key does not match the authentication portion of the URI, then access is denied. For example, a set of pictures from a family vacation to

Las Vegas may be posted on the home network server at "http://familypictures.com/Vegas." If a person has previously been authorized to access other pictures and knows the domain name "familypictures.com," a person may attempt an unauthorized access to the family's Las Vegas pictures by appending the "/Vegas" to the domain name. While the address portion of the URI provided in the attempted access may indeed identify web pages on the home network server, if no authentication information is included then access is denied by the home network server 20. Likewise, if the URI provided in the attempted access contains an authentication portion that is fabricated or concocted, then the hash value calculated by the home network server 20 in an attempt to authenticate the access will not match, and again access is denied. Authentication based on the URI containing an address portion and an authentication portion thus thwarts those "guessing" web page addresses based on knowledge of the domain name alone, and further thwarts automatic web crawling programs from accessing the web pages.

[0023] Having the home network server 20 send invitations to view and/or access web pages, having the home network server 20 send the URI with embedded authentication information, and having the home network server verify the authentication information prior to granting access significantly limits access to the home network server 20 (*i.e.*, secures access to the home network server) without using user names and passwords. In some situations, particularly for web pages hosted on a home network server 20 containing relatively benign information (*e.g.*, family pictures), the level of protection provided may be sufficient. However, for more private information, or for situations where the URIs with embedded authentication information are subject to widespread dissemination (*e.g.*, inadvertently or malicious posting, inadvertent or malicious forwarding of the electronic mail containing the URI to others), further protections may be desirable.

[0024] One such protection against inadvertent or malicious dissemination of the URI information is an automatically expiring invitation. In particular, in some embodiments the URI provided by the home network server 20 to the remote computer system 102 expires after a predetermined amount of time (*e.g.*,

calculated from generation and sending of the URI, or alternatively from a first use of the URI). During the unexpired period, the URI provided by the home network server 20 may be used repeatedly, but after expiration of the predetermined period of time, requests to view the web page identified by the URI are denied. Implementing the expiration of the URI may take many forms. In some embodiments the expiration time is embedded within the URI, either directly or cryptographically. For example, a URI with an embedded expiration time may take the form:

“http://familypictures.com/Vegas&MAC=[HASH VALUE]&EXP=[time]”

where “http://familypictures.com/Vegas” is the address portion, “&MAC=[HASH VALUE]” is the authentication portion, and “&EXP=[time]” is the expiration portion. The expiration date/time of the URI may be encrypted using the private key of the home network server 20. When authenticating an attempted access, the home network server 20 parses the expiration portion, decrypts the expiration portion using the private key of the home network server 20, and grants access only if the current date is prior to the expiration date. In other embodiments an indication of the person to whom the invitation is directed is embedded within the URI, either directly or cryptographically. For example, a URI with an embedded identification portion may take the form:

“http://familypictures.com/Vegas&MAC=[HASH VALUE]&ID=[user]”

where “http://familypictures.com/Vegas” is the address portion, “&MAC=[HASH VALUE]” is the authentication portion, and “&ID=[user]” is the identification portion. When authenticating an attempted access, the home network server 20 parses the identification portion, decrypts the identification portion, and thus identifies the person to whom the URI was directed. Once the person is identified, then the home network server can view other information (e.g., a table) to determine if that person's predetermined access period has expired.

[0025] Another protection against inadvertent or malicious wide spread dissemination is based on the use of HTTP cookies (equivalently referred to as web cookies or just cookies). Cookies are small pieces of data generated by the home network server 20 and provided to the browser of the remote computer system 102 during an initial interaction. During subsequent interactions between

the home network server 20 and the browser of the remote computer system 102, the remote computer system 102 provides the cookie, unchanged, to the home network server 20. Such an interaction enables the home network server 20 to determine whether the particular remote computer system 102 has previously interacted with the home network server 20. In the context of authenticating access to the home network server 20, delivery of the cookie to the remote computer system 102 takes place on the initial use of a URI, but not on subsequent uses. Once a URI has been used to access the home network server 20, the URI will be authenticated if the remote computer system 102 can supply the cookie. Thus, even though a malicious attempt to access a web page may use a URI whose authentication portion is consistent with the address portion and the private key of the home network server, if the remote computer system is unable to supply the cookie, access is denied.

[0026] In some embodiments, once authenticated the remote computer system 102 has the ability not only to view the web pages, but also to upload data (e.g., pictures) to the home network server 20 for publication on the web pages. For relatively benign data such as family vacation pictures, the inadvertent authentication and viewing by an otherwise unauthorized person is not particularly troublesome. However, when the inadvertent authentication provides for upload ability, the potential for abuse is significant. Thus, yet other protections implemented in at least some embodiments deal with upload parameters. In particular, in some embodiments each user with upload authority is given a certain upload size limitation (e.g., ten megabytes). Once the user has uploaded to his or her quota, no further uploading may occur until approval by the administrator of the home network server 20. In yet other embodiments, the user may upload, but the uploaded data is not published to the web page unless and until approved by the administrator. Thus, for example, the family teenager may be granted access to view and upload pictures to the family web page, but those pictures are not published until, for example, a parent, acting as an administrator, approves the publication. Moreover, the upload size limits and pre-publication approval may be combined in some embodiments.

[0027] Figure 3 illustrates a method (*e.g.*, software) in accordance with at least some embodiments. The various method functions of Figure 3 are merely illustrative, as the particular functions may be equivalently performed in a different order, or some may be omitted. The method starts (block 300) and generates a URI for access to web pages (block 302). Generating the URI may take many forms. In some embodiments, the URI merely comprises an address portion. In other embodiments, the URI comprises the address portion along with an authentication portion. The authentication portion may be any suitable value used to later authenticate that the URI was generated by the server. In some embodiments, the authentication portion is created as the one-way hash of the address portion and a private key of the server. In yet still other embodiments, the URI comprise an expiration portion used to identify a predetermined time within which the URI is usable. In some embodiments, the expiration portion is an expiration time embedded in the URI (*e.g.*, directly embedded or cryptographically modified and then embedded). In other embodiments, the URI comprises an identification portion which identifies for whom the URI was generated. Regardless of the precise form of the URI, the URI is sent to the remote computer system, such as by way of an electronic mail message (block 304).

[0028] At some later time, the remote computer system attempts to access web pages using the URI, and thus a URI is received from the remote computer system (block 306). For embodiments that rely solely on the invitation in the form of URI without an authentication portion, access may be immediately granted (block 318), and in which case decisions 312, 314 and 316 would be omitted.

[0029] For embodiments where the URI contains an authentication portion, a determination is made as to whether the received URI matches the URI sent (block 308). Determining whether the received and previously sent URIs match may take many forms. In some embodiments the received URI is parsed into the address portion and the authentication portion. A test value is calculated as the one-way hash of the address portion and the private key of the server. In these embodiments, the determination as to whether the sent URI matches the

received URI is based on a determination of whether the test value matches the authentication portion.

[0030] If the sent URI matches the received URI, in embodiments where the sent URI is only usable for a limited time, a determination is made as to whether a predetermined time for use of the sent URI has expired (block 312). The determination may be made, for example, by inspection of an expiration portion of the URI. In other embodiments, a determination is made as to whom the URI was directed by way of an identification portion of the URI, and the server may consult a table to determine whether a predetermined time for use of the URI by that person has expired.

[0031] For embodiments that use cookies as a protection mechanism, the next step in the illustrative method is a determination as to whether a cookie was previously sent to the remote computer system (block 314). If a cookie was previously sent, then the illustrative method moves to a determination of whether the remote computer system returned the cookie in the current attempted access (block 316). If the remote computer system returned the cookie, then access is granted to the remote computer system (block 318). If the access attempt is the first use of the sent URI, then the illustrative process provides a cookie to the remote computer system (block 328), and access to the web pages is granted (block 318).

[0032] Once access to the web pages is granted, in some embodiments upload authority is given, a determination is made as to whether the remote computer system has reached an upload limit (block 320). If the upload limit has not been reached, then the illustrative process loops until the upload limit has been reached (again block 320). Once the upload limit is reached, further uploads by the user are denied (block 322), and the illustrative process ends (block 324).

[0033] Returning to the determination of whether the received URI matches the sent URI (block 308), in the event the received URI does not match the sent URI, then access to the web pages is denied (block 326), and the illustrative process ends (block 324). Likewise, if the predetermined time for use of URI has expired (block 312), access to the web pages is denied (block 326), and the illustrative process ends (block 324). Further still, if the cookie has previously been

provided, but the remote computer system cannot return the cookie (block 316), access to the web pages is denied (block 326), and the illustrative process ends (block 324).

[0034] From the description provided herein, those skilled in the art are readily able to combine software created as described with appropriate general purpose or special purpose computer software to create a computer system and/or computer subcomponents in accordance with the various embodiments, to create a computer system and/or computer subcomponents for carrying out the methods of the various embodiments and/or to create a computer-readable media for storing a software program (*e.g.*, an operating system), to implement the method aspects of the various embodiments.

CLAIMS

1. A method comprising:
receiving (306) a request from a remote computer (10, 16, 102) to access a web page stored on a server (20);
verifying (308, 312, 314, 316) permission of the remote computer to access the web page without the remote computer system (10, 16, 102) sending a user name and password; and
granting (318) the remote computer (10, 16, 102) access to the web page if permission is verified.
2. The method according to claim 1 wherein receiving the request further comprises receiving (306) a uniform resource indicator (URI) having an address portion and the authentication value appended to the address portion.
3. The method according to claim 1 wherein receiving the request further comprises receiving (305) a uniform resource indicator (URI) having an authentication value that is a one-way hash of the address portion and a private key of the associated with the server.
4. The method according to claim 1 wherein granting (318) the remote computer (10, 16, 102) access further comprises at least one selected from the group consisting of: granting the remote computer view-only access to the web page; granting the remote computer upload access to the web page; and granting the remote computer upload access to the web page within a predetermined upload size limit.
5. The method according to claim 1 further comprising:
determining (314) whether the request originated from the remote computer system (10, 16, 102) having a cookie previously provided to the remote computer system (10, 16, 102); and

granting (318) access to the web page if the cookie is present on the remote computer system (10, 16, 102).

6. A network server (20) comprising:
 - a processor (24); and
 - a non-volatile memory device (48) coupled to the processor (24), the non-volatile memory device (48) stores a web page viewable using a web browser; andwherein the network server (20) is configured to determine whether a remote computer system (10, 16, 102) that requests the web page has permission to access the web page, the determination based on information contained within a Universal Resource Indicator (URI) provided by the remote computer system (10, 16, 102).
7. The network server according to claim 6 wherein in determining whether the remote computer system has permission to access the web page, the network server is configured to separate the URI into an address portion and an authentication value, calculate a test value using the address portion, and determine if the test value matches the authentication value.
8. The network server according to claim 6 wherein if the remote computer system has permission to access the web page, the network server is configured to at least one selected from the group consisting of: grant the remote computer view-only access to the web page; grant the remote computer upload access to the web page; grant the remote computer upload access to the web page within a predetermined upload size limit; and grant upload access to the web page without publication until approval of administrator of the network server.
9. The network server according to claim 6 wherein the network server is further configured to determine whether the URI originated from the remote computer system having a previously delivered cookie, and grant access to the web page if the cookie is present on the remote computer system.

10. The network server according to claim 6 wherein the network server, when verifying permission, is further configured to determine whether a predetermined amount of time has elapsed since the URI was provided.

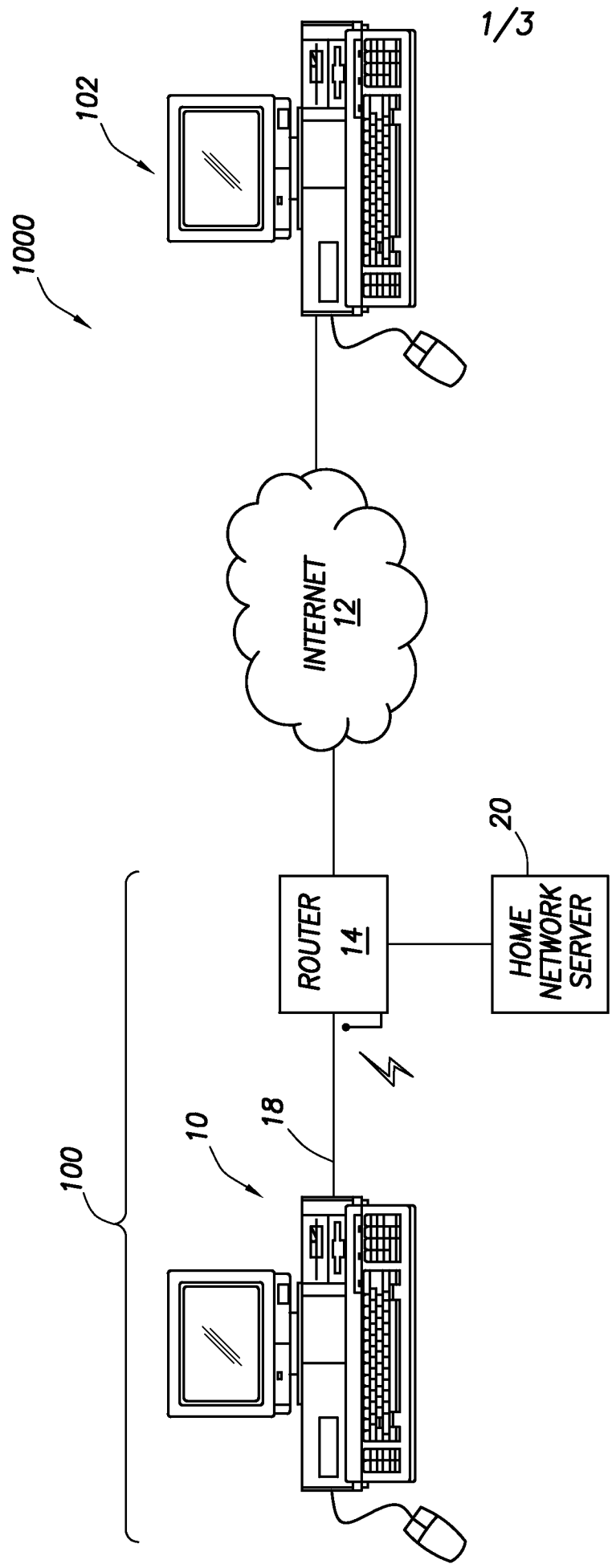
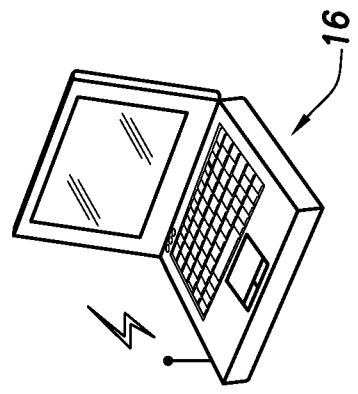


FIG. 1



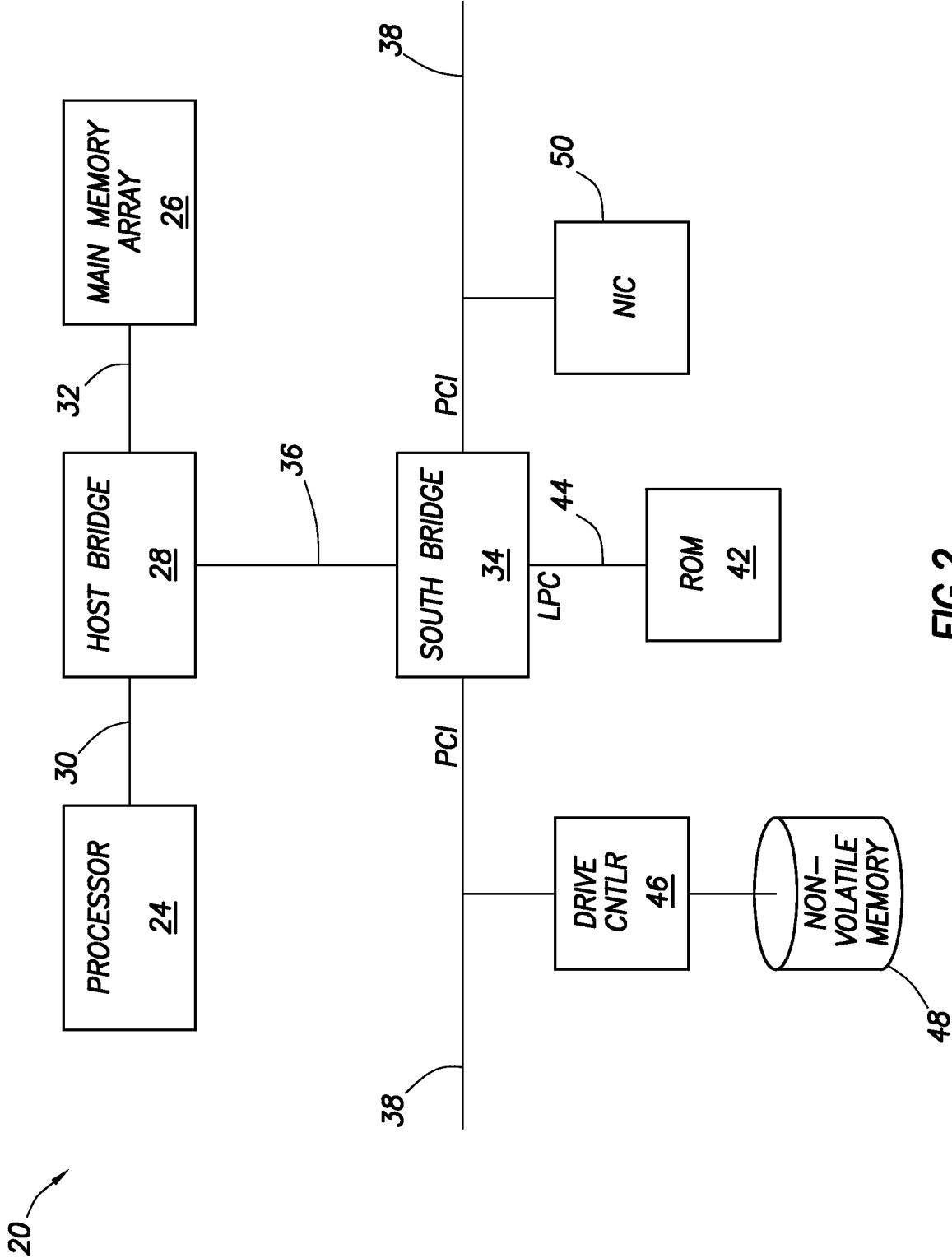
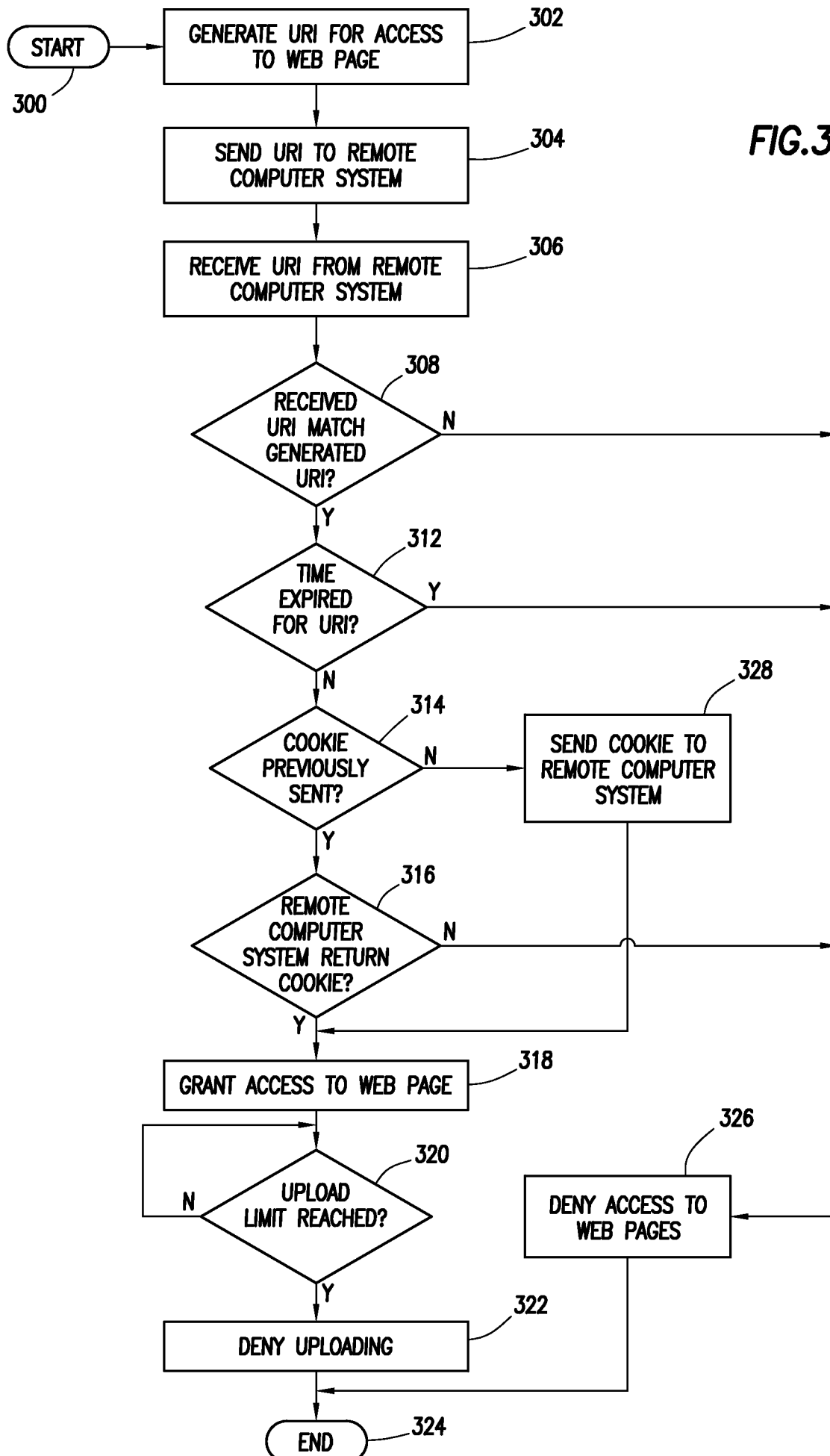


FIG.3



A. CLASSIFICATION OF SUBJECT MATTER**G06F 15/16(2006.01)i, G06F 17/00(2006.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 G06F

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

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

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

eKIPASS (KIPO internal) & keyword : "mail", "authentication", "access"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2001-0070869A (EOM, JANGPIL) 27 JULY 2001 see abstract, fig 1, figK2, fig7, fig8 and their corresponding specifications.	1-10
A	US 6005939 A(KEITH NEIL FORTENBERRY et al.) 21 DECEMBER 1999 see abstract, fig 4 and its corresponding specifications.	1-10
A	JP 11-149451 A (FUJITSU LTD.) 02 JUNE 1999 see abstract, fig 1 and its corresponding specifications.	1-10
A	WO 2006-046247 A2(SUPERNA LIMITED) 04 MAY 2006 abstract, fig 2a its corresponding specifications.	1-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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

25 SEPTEMBER 2008 (25.09.2008)

Date of mailing of the international search report

25 SEPTEMBER 2008 (25.09.2008)

Name and mailing address of the ISA/KR

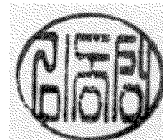
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-
gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Dong Sung

Telephone No. 82-42-481-8519



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/061792

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2001-0070869 A	27.07.2001	NONE	
US 6005939 A	21.12.1999	NONE	
JP 11-149451 A	02.06.1999	NONE	
WO 2006-046247 A2	04.05.2006	AU 2005-298253 AA	04.05.2006
		CA 2589065 AA	04.05.2006
		EP 1820118 A2	22.08.2007
		KR 10-2007-0111449 A	21.11.2007