



US 20080201344A1

(19) **United States**(12) **Patent Application Publication**
Levergood et al.(10) **Pub. No.: US 2008/0201344 A1**(43) **Pub. Date: Aug. 21, 2008**(54) **INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS**

09/548,235, filed on Apr. 12, 2000, which is a continuation of application No. 09/548,237, filed on Apr. 12, 2000.

(76) Inventors: **Thomas Mark Levergood**,
Hopkinton, MA (US); **Lawrence C. Stewart**, Burlington, MA (US);
Stephen Jeffrey Morris, Westford, MA (US); **Andrew C. Payne**,
Lincoln, MA (US); **George Winfield Treese**, Newton, MA (US)**Publication Classification**(51) **Int. Cl.**
H04L 9/32 (2006.01)
G06F 21/00 (2006.01)
G06F 17/30 (2006.01)
G06Q 30/00 (2006.01)

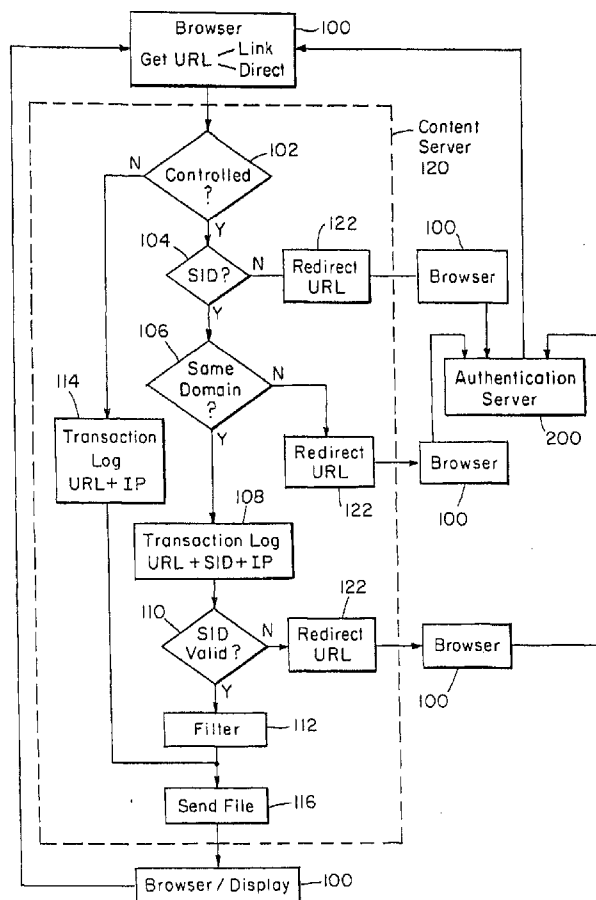
Correspondence Address:

James M. Smith, Esq.
HAMILTON, BROOK, SMITH & REYNOLDS,
P.C.**Two Militia Drive**
Lexington, MA 02173(52) **U.S. Cl. 707/100; 726/3; 726/7; 705/39;**
705/40; 707/E17.009(57) **ABSTRACT**

This invention relates to methods for controlling and monitoring access to network servers. In particular, the process described in the invention includes client-server sessions over the Internet. In this environment, when the user attempts to access an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon such verification, the user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain.

(21) Appl. No.: **12/109,443**(22) Filed: **Apr. 25, 2008****Related U.S. Application Data**

(63) Continuation of application No. 11/300,245, filed on Dec. 13, 2005, which is a continuation of application No. 09/005,479, filed on Jan. 12, 1998, now Pat. No. 7,272,639, which is a continuation of application No.



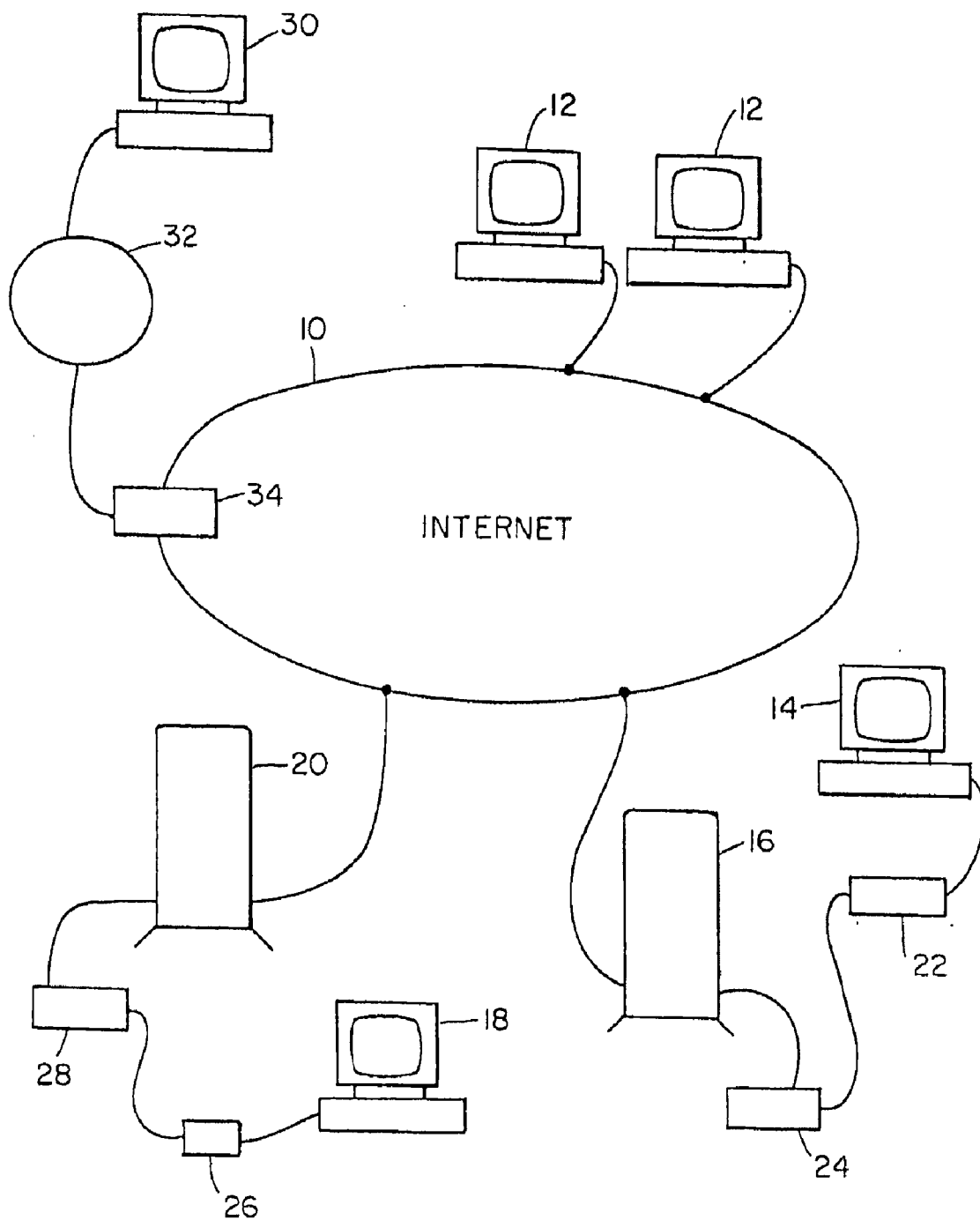


FIG. 1

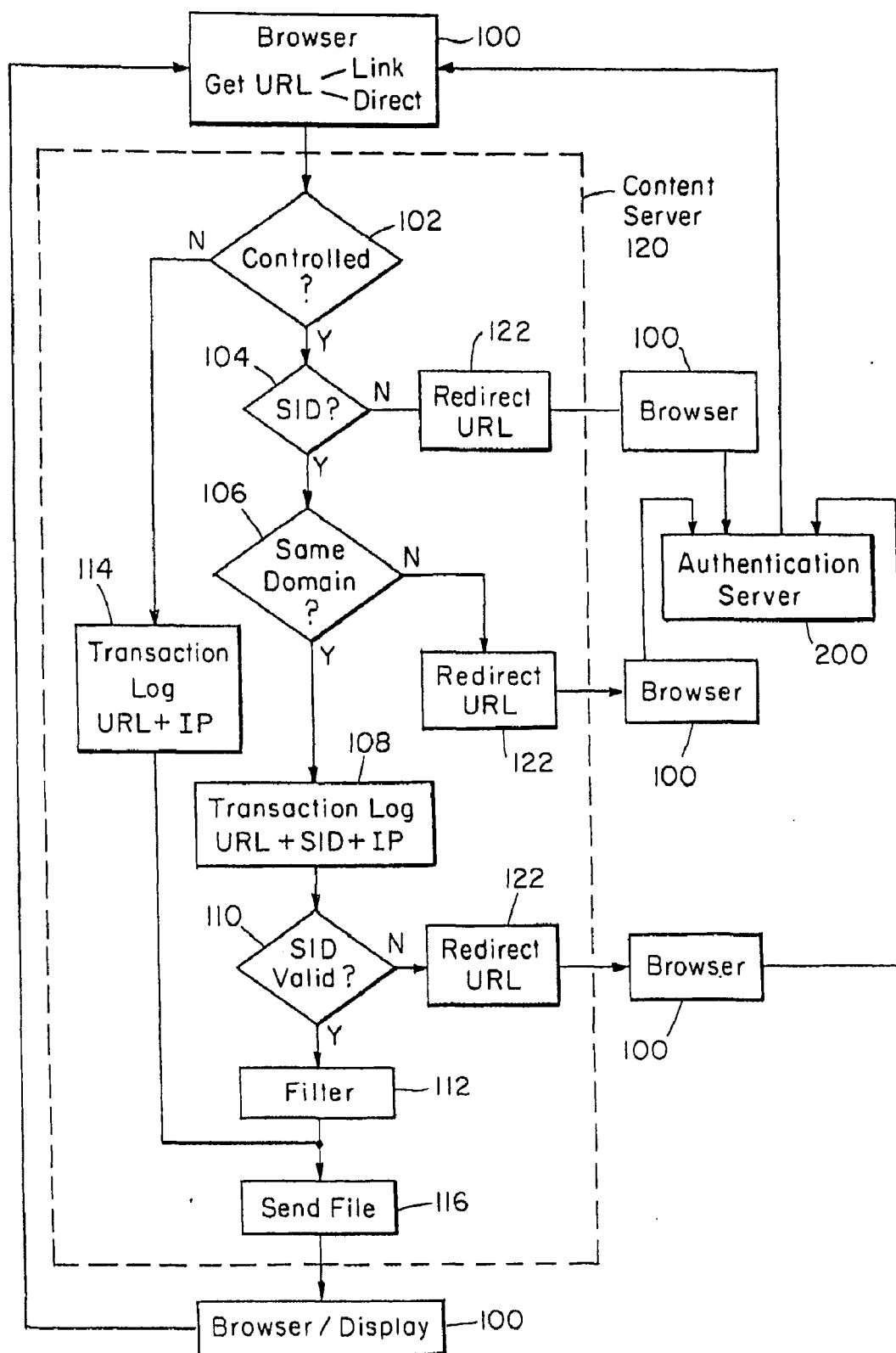


FIG. 2A

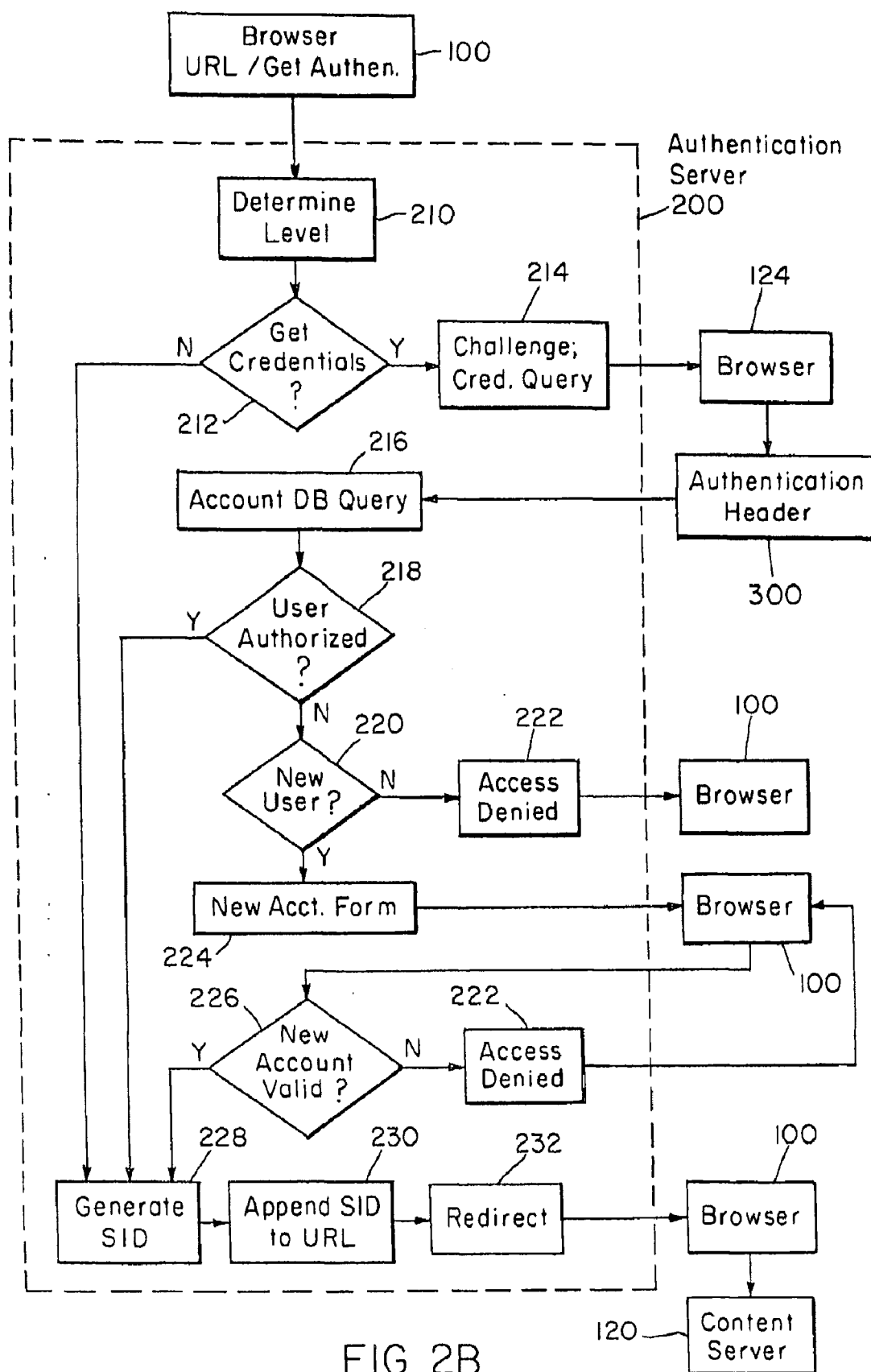


FIG. 2B

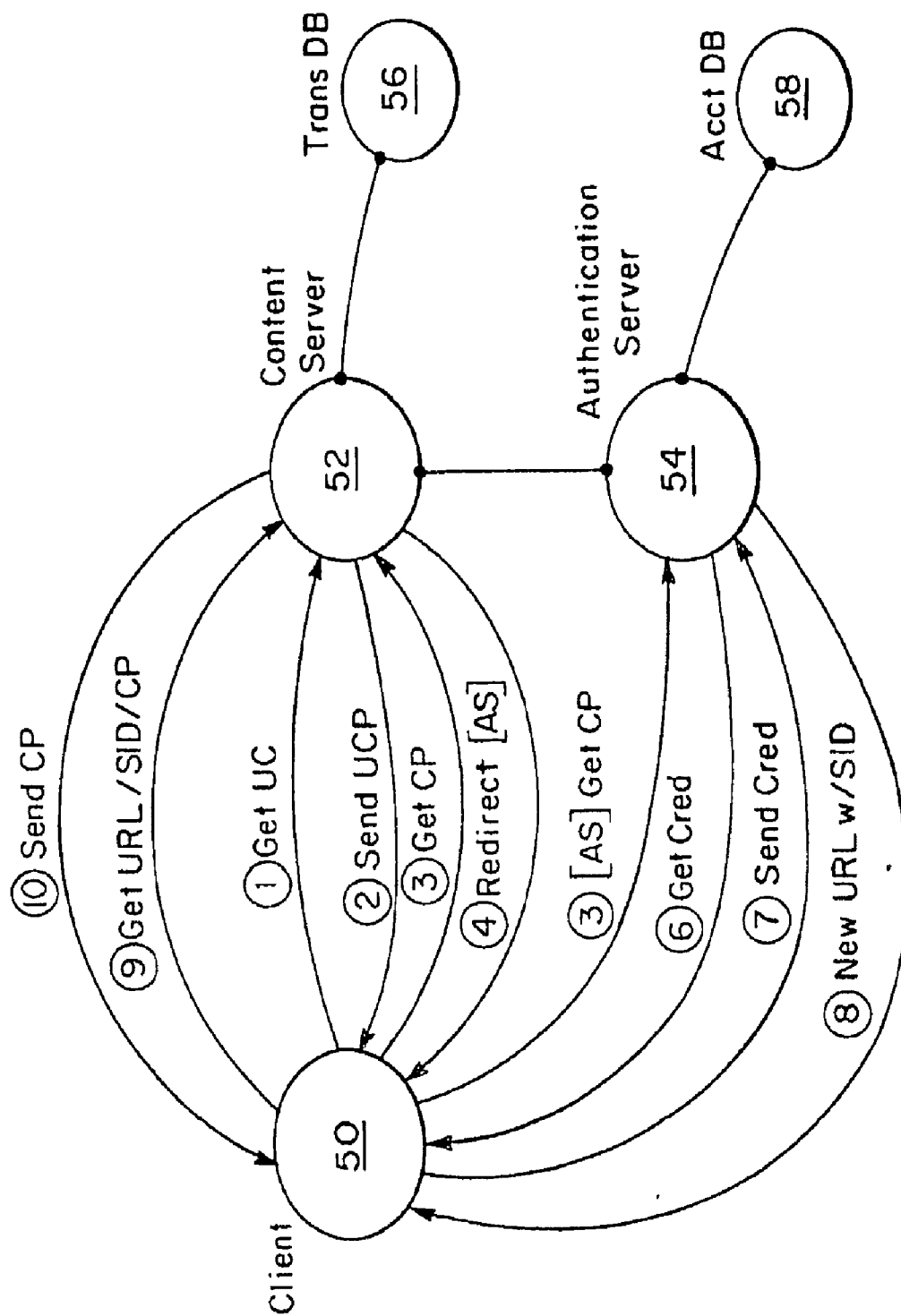


FIG. 3

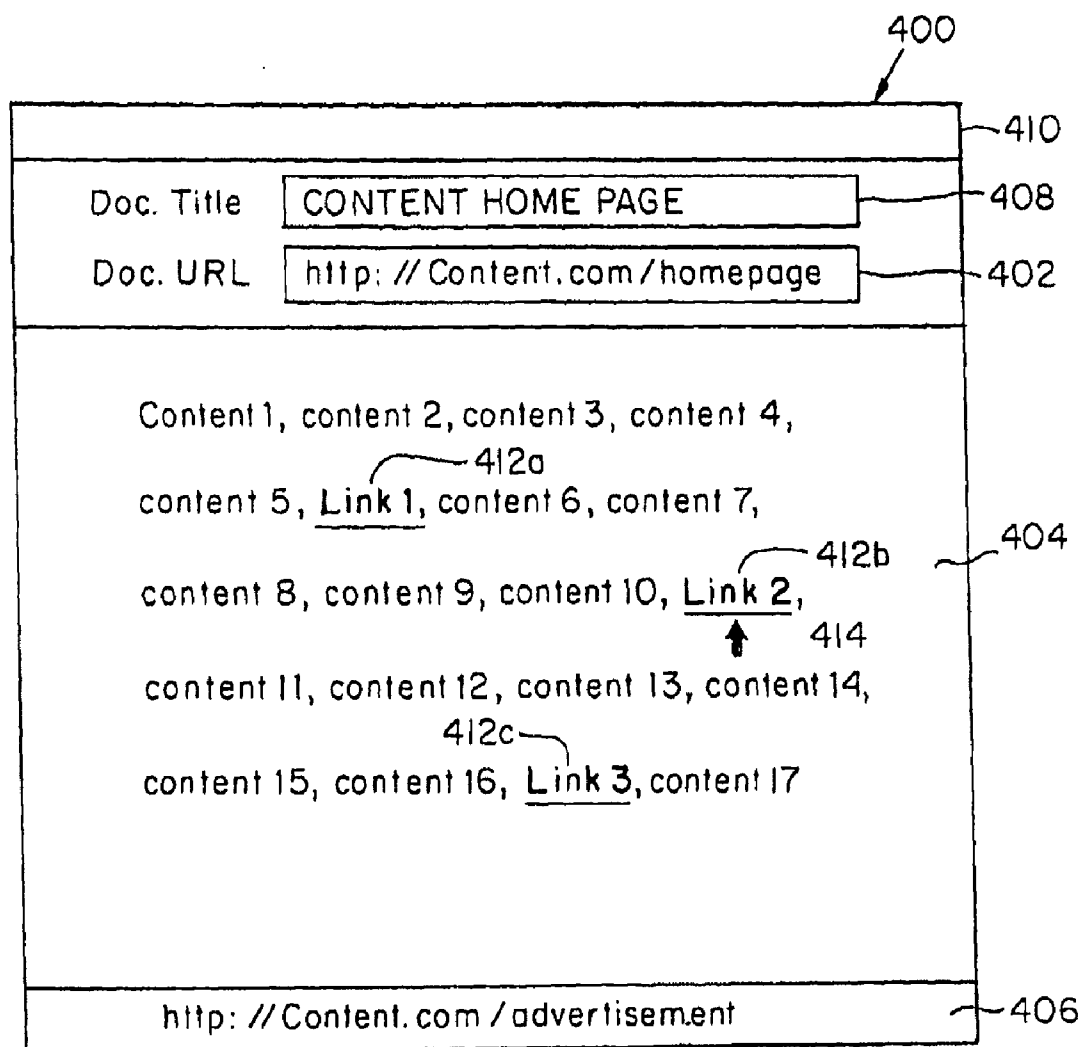


FIG. 4

Document View	
File Options Navigate Annotate Documents Help	
Title:	<input style="width: 90%;" type="text" value="How to join"/>
URL:	<input style="width: 90%;" type="text" value="http: //auth. com/ service/ nph- createacct. cgi"/>

1. First name
2. Last name
3. Choose a screen name (no more than 15 characters)
4. Choose a password (no more than 15 characters)
 Password:

 Re-enter password:
5. E-mail address
6. Your birthdate (MM/DD/YY)
7. U. S. zip code, or country code
 Zip/postal code:

 ISO country code

FIG. 5

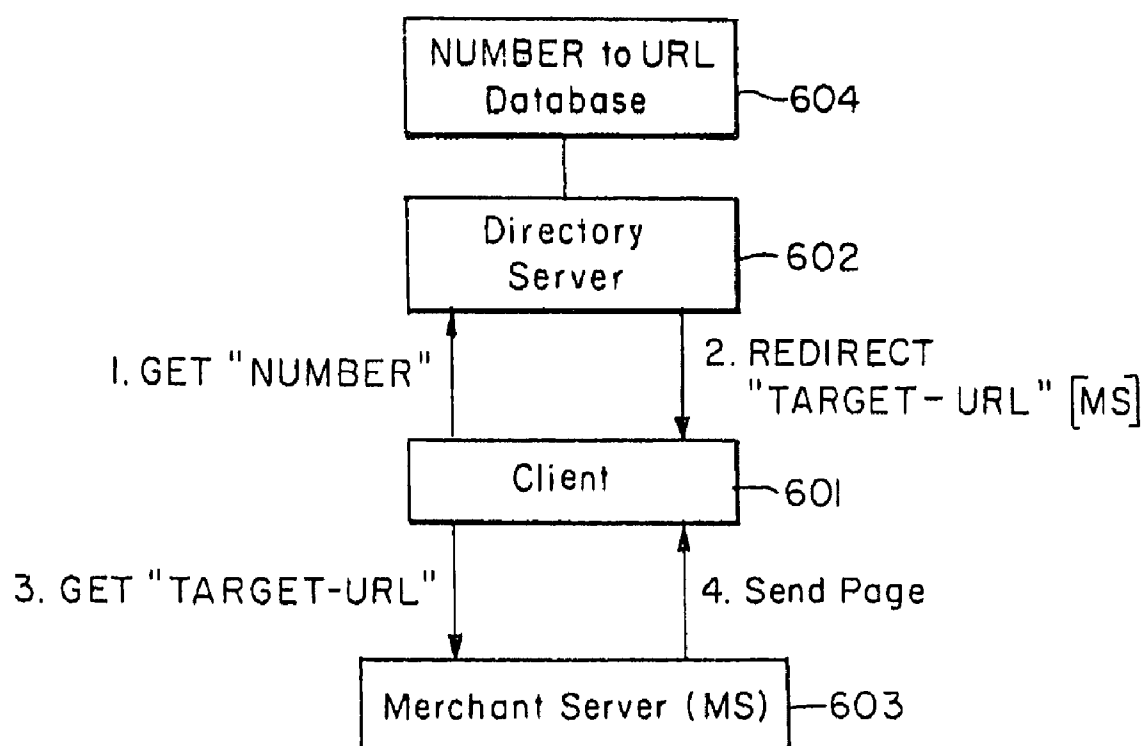


FIG. 6

INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS

RELATED APPLICATION

[0001] This application is a Continuation of U.S. Ser. No. 11/300,245, which is a Continuation of (1) U.S. Ser. No. 09/005,479 filed Jan. 12, 1998 and now U.S. Pat. No. 7,272,639, and (2) U.S. Ser. No. 09/548,235 filed Apr. 12, 2000, and (3) U.S. Ser. No. 09/548,237 filed Apr. 12, 2000, each of which claims priority to U.S. Ser. No. 08/474,096 filed on Jun. 7, 1995, now U.S. Pat. No. 5,708,780. The entire disclosure of each of these prior applications are incorporated herein by reference.

BACKGROUND TO THE INVENTION

[0002] The Internet, which started in the late 1960s, is a vast computer network consisting of many smaller networks that span the entire globe. The Internet has grown exponentially, and millions of users ranging from individuals to corporations now use permanent and dial-up connections to use the Internet on a daily basis worldwide. The computers or networks of computers connected within the Internet, known as “hosts”, allow public access to databases featuring information in nearly every field of expertise and are supported by entities ranging from universities and government to many commercial organizations.

[0003] The information on the Internet is made available to the public through “servers”. A server is a system running on an Internet host for making available files or documents contained within that host. Such files are typically stored on magnetic storage devices, such as tape drives or fixed disks, local to the host. An Internet server may distribute information to any computer that requests the files on a host. The computer making such a request is known as the “client”, which may be an Internet-connected workstation, bulletin board system or home personal computer (PC).

[0004] TCP/IP (Transmission Control Protocol/Internet Protocol) is one networking protocol that permits full use of the Internet. All computers on a TCP/IP network need unique ID codes. Therefore, each computer or host on the Internet is identified by a unique number code, known as the IP (Internet Protocol) number or address, and corresponding network and computer names. In the past, an Internet user gained access to its resources only by identifying the host computer and a path through directories within the host’s storage to locate a requested file. Although various navigating tools have helped users to search resources on the Internet without knowing specific host addresses, these tools still require a substantial technical knowledge of the Internet.

[0005] The World-Wide Web (Web) is a method of accessing information on the Internet which allows a user to navigate the Internet resources intuitively, without IP addresses or other technical knowledge. The Web dispenses with command-line utilities which typically require a user to transmit sets of commands to communicate with an Internet server. Instead, the Web is made up of hundreds of thousands of interconnected “pages”, or documents, which can be displayed on a computer monitor. The Web pages are provided by hosts running special servers. Software which runs these Web servers is relatively simple and is available on a wide range of computer platforms including PC’s. Equally available is a form of client software, known as a Web “browser”, which is used to display Web pages as well as traditional

non-Web files on the client system. Today, the Internet hosts which provide Web servers are increasing at a rate of more than 300 per month, en route to becoming the preferred method of Internet communication.

[0006] Created in 1991, the Web is based on the concept of “hypertext” and a transfer method known as “HTTP” (Hypertext Transfer Protocol). HTTP is designed to run primarily over TCP/IP and uses the standard Internet setup, where a server issues the data and a client displays or processes it. One format for information transfer is to create documents using Hypertext Markup Language (HTML). HTML pages are made up of standard text as well as formatting codes which indicate how the page should be displayed. The Web client, a browser, reads these codes in order to display the page. The hypertext conventions and related functions of the world wide web are described in the appendices of U.S. patent application Ser. No. 08/328,133, filed on Oct. 24, 1994, by Payne et al. which is incorporated herein by reference.

[0007] Each Web page may contain pictures and sounds in addition to text. Hidden behind certain text, pictures or sounds are connections, known as “hypertext links” (“links”), to other pages within the same server or even on other computers within the Internet. For example, links may be visually displayed as words or phrases that may be underlined or displayed in a second color. Each link is directed to a web page by using a special name called a URL (Uniform Resource Locator)—URLs enable a Web browser to go directly to any file held on any Web server. A user may also specify a known URL by writing it directly into the command line on a Web page to jump to another Web page.

[0008] The URL naming system consists of three parts: the transfer format, the host name of the machine that holds the file, and the path to the file. An example of a URL may be: <http://www.college.Univ.edu/Adir/Bdir/Cdir/page.html>, where “http” represents the transfer protocol; a colon and two forward slashes (://) are used to separate the transfer format from the host name; “www.college.univ.edu” is the host name in which “www” denotes that the file being requested is a Web page; “/Adir/Ddir/Cdir” is a set of directory names in a tree structure, or a path, on the host machine; and “page.html” is the file name with an indication that the file is written in HTML.

[0009] The Internet maintains an open structure in which exchanges of information are made cost-free without restriction. The free access format inherent to the Internet, however, presents difficulties for those information providers requiring control over their Internet servers. Consider for example, a research organization that may want to make certain technical information available on its Internet server to a large group of colleagues around the globe, but the information must be kept confidential. Without means for identifying each client, the organization would not be able to provide information on the network on a confidential or preferential basis. In another situation, a company may want to provide highly specific service tips over its Internet server only to customers having service contracts or accounts.

[0010] Access control by an Internet server is difficult for at least two reasons. First, when a client sends a request for a file on a remote Internet server, that message is routed or relayed by a web of computers connected through the Internet until it reaches its destination host. The client does not necessarily know how its message reaches the server. At the same time, the server makes responses without ever knowing exactly who the client is or what its IP address is. While the server

may be programmed to trace its clients, the task of tracing is often difficult, if not impossible. Secondly, to prevent unwanted intrusion into private local area networks (LAN), system administrators implement various data-flow control mechanisms, such as the Internet "firewalls", within their networks. An Internet firewall allows a user to reach the Internet anonymously while preventing intruders of the outside world from accessing the user's LAN.

SUMMARY OF THE INVENTION

[0011] The present invention relates to methods of processing service requests from a client to a server through a network. In particular the present invention is applicable to processing client requests in an HTTP (Hypertext Transfer Protocol) environment, such as the World-Wide Web (Web). One aspect of the invention involves forwarding a service request from the client to the server and appending a session identification (SID) to the request and to subsequent service requests from the client to the server within a session of requests. In a preferred embodiment, the present method involves returning the SID from the server to the client upon an initial service request made by the client. A valid SID may include an authorization identifier to allow a user to access controlled files.

[0012] In a preferred embodiment, a client request is made with a Uniform Resource Locator (URL) from a Web browser. Where a client request is directed to a controlled file without an SID, the Internet server subjects the client to an authorization routine prior to issuing the SID, the SID being protected from forgery. A content server initiates the authorization routine by redirecting the client's request to an authentication server which may be at a different host. Upon receiving a redirected request, the authentication server returns a response to interrogate the client and then issues an SID to a qualified client. For a new client, the authentication server may open a new account and issue an SID thereafter. A valid SID typically comprises a user identifier, an accessible domain, a key identifier, an expiration time such as date, the IP address of the user computer, and an unforgeable digital signature such as a cryptographic hash of all of the other items in the SID encrypted with a secret key. The authentication server then forwards a new request consisting of the original URL appended by the SID to the client in a REDIRECT. The modified request formed by a new URL is automatically forwarded by the client browser to the content server.

[0013] When the content server receives a URL request accompanied by an SID, it logs the URL with the SID and the user IP address in a transaction log and proceeds to validate the SID. When the SID is so validated, the content server sends the requested document for display by the client's Web browser.

[0014] In the preferred embodiment, a valid SID allows the client to access all controlled files within a protection domain without requiring further authorization. A protection domain is defined by the service provider and is a collection of controlled files of common protection within one or more servers.

[0015] When a client accesses a controlled Web page with a valid SID, the user viewing the page may want to traverse a link to view another Web page. There are several possibilities. The user may traverse a link to another page in the same path. This is called a "relative link". A relative link may be made either within the same domain or to a different domain. The browser on the client computer executes a relative link by rewriting the current URL to replace the old controlled page

name with a new one. The new URL retains all portions of the old, including the SID, except for the new page name. If the relative link points to a page in the same protection domain, the SID remains valid, and the request is honored. However, if the relative link points to a controlled page in a different protection domain, the SID is no longer valid, and the client is automatically redirected to forward the rewritten URL to the authentication server to update the SID. The updated or new SID provides access to the new domain if the user is qualified.

[0016] The user may also elect to traverse a link to a document in a different path. This is called an "absolute link". In generating a new absolute link, the SID is overwritten by the browser. In the preferred embodiment, the content server, in each serving of a controlled Web page within the domain, filters the page to include the current SID in each absolute URL on the page. Hence, when the user elects to traverse an absolute link, the browser is facilitated with an authenticated URL which is directed with its SID to a page in a different path. In another embodiment, the content server may forego the filtering procedure as above-described and redirect an absolute URL to the authentication server for an update.

[0017] An absolute link may also be directed to a controlled file in a different domain. Again, such a request is redirected to the authentication server for processing of a new SID. An absolute link directed to an uncontrolled file is accorded an immediate access.

[0018] In another embodiment, a server access control may be maintained by programming the client browser to store an SID or a similar tag for use in each URL call to that particular server. This embodiment, however, requires a special browser which can handle such communications and was generally not suitable for early browser formats common to the Web. However, it may now be implemented in cookie compatible browsers.

[0019] Another aspect of the invention is to monitor the frequency and duration of access to various pages both controlled and uncontrolled. A transaction log within a content server keeps a history of each client access to a page including the link sequence through which the page was accessed. Additionally, the content server may count the client requests exclusive of repeated requests from a common client. Such records provide important marketing feedback including user demand, access pattern, and relationships between customer demographics and accessed pages and access patterns.

[0020] The above and other features of the invention including various novel details of construction and combinations of parts will now be more particularly described with reference to the accompanying drawings and pointed out in the claims. It will be understood that the particular devices and methods embodying the invention are shown by way of illustration only and not as limitations of the invention. The principles and features of this invention may be employed in varied and numerous embodiments without departing from the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIG. 1 is a diagram illustrating the Internet operation.

[0022] FIG. 2A is a flowchart describing the preferred method of Internet server access control and monitoring.

[0023] FIG. 2B is a related flowchart describing the details of the authentication process.

[0024] FIG. 3 illustrates an example of a client-server exchange session involving the access control and monitoring method of the present invention.

[0025] FIG. 4 is an example of a World Wide Web page.

[0026] FIG. 5 is an example of an authorization form page.

[0027] FIG. 6 is a diagram describing the details of the translation of telephone numbers to URL5.

DETAILED DESCRIPTION OF THE INVENTION

[0028] Referring now to the drawings, FIG. 1 is a graphical illustration of the Internet. The Internet 10 is a network of millions of interconnected computers 12 including systems owned by Internet providers 16 and information systems (BBS) 20 such as Compuserve or America Online. Individual or corporate users may establish connections to the Internet in several ways. A user on a home PC 14 may purchase an account through the Internet provider 16. Using a modem 22, the PC user can dial up the Internet provider to connect to a high speed modem 24 which, in turn, provides a full service connection to the Internet. A user 18 may also make a somewhat limited connection to the Internet through a BBS 20 that provides an Internet gateway connection to its customers.

[0029] FIG. 2A is a flowchart detailing the preferred process of the present invention and FIG. 4 illustrates a sample Web page displayed at a client by a browser. The page includes text 404 which includes underlined link text 412. The title bar 408 and URL bar 402 display the title and URL of the current web page, respectively. As shown in FIG. 4, the title of the page is "Content Home Page" and the corresponding URL is "http://content.com/homepage". When a cursor 414 is positioned over link text 412b, the page which would be retrieved by clicking a mouse is typically identified in a status bar 406 which shows the URL for that link. In this example the status bar 406 shows that the URL for the pointed link 412b is directed to a page called "advertisement" in a commercial content server called "content". By clicking on the link text, the user causes the browser to generate a URL GET request at 100 in FIG. 2A. The browser forwards the request to a content server 120, which processes the request by first determining whether the requested page is a controlled document 102. If the request is directed to an uncontrolled page, as in "advertisement" page in this example, the content server records the URL and the IP address, to the extent it is available, in the transaction log 114. The content server then sends the requested page to the browser 116 for display on the user computer 117.

[0030] If the request is directed to a controlled page, the content server determines whether the URL contains an SID 102. For example, a URL may be directed to a controlled page name "report", such as "http://content.com/report", that requires an SID. If no SID is present, as in this example, the content server sends a "REDIRECT" response 122 to the browser 100 to redirect the user's initial request to an authentication server 200 to obtain a valid SID. The details of the authentication process are described in FIG. 2B and will be discussed later, but the result of the process is an SID provided from the authentication server to the client. In the above example, a modified URL appended with an SID may be: "http://content.com/{SID}/report". The preferred SID is a sixteen character ASCII string that encodes 96 bits of SID data, 6 bits per character. It contains a 32-bit digital signature, a 16-bit expiration date with a granularity of one hour, a 2-bit key identifier used for key management, an 8-bit domain comprising a set of information files to which the current SID

authorizes access, and a 22-bit user identifier. The remaining bits are reserved for expansion. The digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers.

[0031] If the initial GET URL contains a SID, the content server determines whether the request is directed to a page within the current domain 106. If the request having a SID is directed to a controlled page of a different domain, the SID is no longer valid and, again, the user is redirected to the authentication server 122.

[0032] If the request is for a controlled page within the current domain, the content server proceeds to log the request URL, tagged with SID, and the user IP address in the transaction log 108. The content server then validates the SID 110. Such validation includes the following list of checks: (1) the SID's digital signature is compared against the digital signature computed from the remaining items in the SID and the user IP address using the secret key shared by the authentication and content servers; (2) the domain field of the SID is checked to verify that it is within the domain authorized; and (3) the EXP field of the SID is checked to verify that it is later than the current time,

[0033] If the validation passes, the content server searches the page to be forwarded for any absolute URL links contained therein 112, that is, any links directed to controlled documents in different content servers. The content server augments each absolute URL with the current SID to facilitate authenticated accesses across multiple content servers. The requested page as processed is then transmitted to the client browser for display 117. The user viewing the requested Web page may elect to traverse any link on that page to trigger the entire sequence again 100.

[0034] FIG. 2B describes the details of the authentication process. The content server may redirect the client to an authentication server. The REDIRECT URL might be: "http://auth.com/authenticate?domain=[domain]&URL=http://content.com/report". That URL requests authentication and specifies the domain and the initial URL. In response to the REDIRECT, the client browser automatically sends a GET request with the provided URL.

[0035] Whenever the content server redirects the client to the authentication server 200, the authentication server initiates the authorization process by validating that it is for an approved content server and determining the level of authentication required for the access requested 210. Depending on this level, the server may challenge the user 212 for credentials. If the request is for a low level document, the authentication may issue an appropriate SID immediately 228 and forego the credential check procedures. If the document requires credentials, the authentication server sends a "CHALLENGE" response which causes the client browser to prompt the user for credentials 214. A preferred credential query typically consists of a request for user name and password. If the user is unable to provide a password, the access is denied. The browser forms an authorization header 300 from the information provided, and resends a GET request to the authentication server using the last URL along with an authorization header. For example, a URL of such a GET request may be: "http://auth.com/authenticate?domain=[domain]&URL=http://content.com/report and the authorization header may be: "AUTHORIZE: [authorization]".

[0036] Upon receiving the GET request, the authentication server queries an account database 216 to determine whether

the user is authorized **218** to access the requested document. A preferred account database may contain a user profile which includes information for identifying purposes, such as client IP address and password, as well as user demographic information, such as user age, home address, hobby, or occupation, for later use by the content server. If the user is authorized, an SID is generated **228** as previously described. If the user is not cleared for authorization, the authentication server checks to see if the user qualifies for a new account **220**. If the user is not qualified to open a new account, a page denying access **222** is transmitted to the client browser **100**. If the user is qualified, the new user is sent a form page such as illustrated in FIG. 5 to initiate a real-time on-line registration **224**. The form may, for example, require personal information and credit references from the user. The browser is able to transmit the data entered by the user in the blanks **502** as a "POST" message to the authentication server. A POST message causes form contents to be sent to the server in a data body other than as part of the URL. If the registration form filled out by the new user is valid **226**, an appropriate SID is generated **228**. If the registration is not valid, access is again denied **222**.

[0037] An SID for an authorized user is appended ("tagged") **230** to the original URL directed to a controlled page on the content server. The authentication server then transmits a REDIRECT response **232** based on the tagged URL to the client browser **100**. The modified URL, such as "http://content.com/[SID]/report" is automatically forwarded to the content server **120**.

[0038] FIG. 3, illustrates a typical client-server exchange involving the access control and monitoring method of the present invention. In Step 1, the client **50** running a browser transmits a GET request through a network for an uncontrolled page (UCP). For example, the user may request an advertisement page by transmitting a URL "http://content.com/advertisement", where "content.com" is the server name and "advertisement" is the uncontrolled page name. In Step 2, the content server **52** processes the GET request and transmits the requested page, "advertisement". The content server also logs the GET request in the transaction database **56** by recording the URL, the client IP address, and the current time.

[0039] In Step 3, the user on the client machine may elect to traverse a link in the advertisement page directed to a controlled page (CP). For example, the advertisement page may contain a link to a controlled page called "report". Selecting this link causes the client browser **50** to forward a GET request through a URL which is associated with the report file "http://content.com/report". The content server **52** determines that the request is to a controlled page and that the URL does not contain an SID. In Step 4, the content server transmits a REDIRECT response to the client, and, in Step 5, the browser automatically sends the REDIRECT URL to the authentication server **54**. The REDIRECT URL sent to the authentication server may contain the following string: "http://auth.com/authenticate?domain=[domain]&URL=http://content.com/report".

[0040] The authentication server processes the REDIRECT and determines whether user credentials (CRED) are needed for authorization. In Step 6, the authentication server transmits a "CHALLENGE" response to the client. As previously described, typical credentials consist of user name and password. An authorization header based on the credential information is then forwarded by the client browser to the authentication server. For example, a GET URL having such an authorization header is: "http://auth.com/authenticat-

e?domain=[domain]&URL=http://content.com/report and the authorization header may be: "AUTHORIZE: [authorization]".

The authentication server processes the GET request by checking the Account Database **58**. If a valid account exists for the user, an SID is issued which authorizes access to the controlled page "report" and all the other pages within the domain.

[0041] As previously described, the preferred SID comprises a compact ASCII string that encodes a user identifier, the current domain, a key identifier, an expiration time, the client IP address, and an unforgeable digital signature. In Step 8, the authentication server redirects the client to the tagged URL, "http://content.com/[SID]/report", to the client. In Step 9, the tagged URL is automatically forwarded by the browser as a GET request to the content server. The content server logs the GET request in the Transaction database **56** by recording the tagged URL, the client IP address, and the current time. In Step 10, the content server, upon validating the SID, transmits the requested controlled page "report" for display on the client browser.

[0042] According to one aspect of the present invention, the content server periodically evaluates the record contained in the transaction log **56** to determine the frequency and duration of accesses to the associated content server. The server counts requests to particular pages exclusive of repeated requests from a common client in order to determine the merits of the information on different pages for ratings purposes. By excluding repeated calls, the system avoids distortions by users attempting to "stuff the ballot box."

[0043] In one embodiment, the time intervals between repeated requests by a common client are measured to exclude those requests falling within a defined period of time.

[0044] Additionally, the server may, at any given time, track access history within a client-server session. Such a history profile informs the service provider about link transversal frequencies and link paths followed by users. This profile is produced by filtering transaction logs from one or more servers to select only transactions involving a particular user ID (UID). Two subsequent entries, A and B, corresponding to requests from a given user in these logs represent a link traversal from document A to document B made by the user in question. This information may be used to identify the most popular links to a specific page and to suggest where to insert new links to provide more direct access. In another embodiment, the access history is evaluated to determine traversed links leading to a purchase of a product made within commercial pages. This information may be used, for example, to charge for advertising based on the number of link traversals from an advertising page to a product page or based on the count of purchases resulting from a path including the advertisement. In this embodiment, the server can gauge the effectiveness of advertising by measuring the number of sales that resulted from a particular page, link, or path of links. The system can be configured to charge the merchant for an advertising page based on the number of sales that resulted from that page.

[0045] According to another aspect of the present invention, a secondary server, such as the authentication server **200** in FIG. 2B, may access a prearranged user profile from the account database **216** and include information based on such a profile in the user identifier field of the SID. In a preferred embodiment, the content server may use such an SID to

customize user requested pages to include personalized content based on the user identifier field of the SID.

[0046] In another aspect of the invention, the user may gain access to domain of servers containing journals or publications through a subscription. In such a situation, the user may purchase the subscription in advance to gain access to on-line documents through the Internet. The user gains access to a subscribed document over the Internet through the authorization procedure as described above where an authorization indicator is preferably embedded in a session identifier. In another embodiment, rather than relying on a prepaid subscription, a user may be charged and billed each time he or she accesses a particular document through the Internet. In that case, authorization may not be required so long as the user is fully identified in order to be charged for the service. The user identification is most appropriately embedded in the session identifier described above.

[0047] In another aspect of the invention, facilities are provided to allow users to utilize conventional telephone numbers or other identifiers to access merchant services. These merchant services can optionally be protected using SID5. In a preferred embodiment, as shown in FIG. 6, a Web browser client **601** provides a “dial” command to accept a telephone number from a user, as by clicking on a “dial” icon and inputting the telephone number through the keyboard. The browser then constructs a URL of the form “http://directory.net/NUMBER”, where NUMBER is the telephone number or other identifier specified by the user. The browser then performs a GET of the document specified by this URL, and contacts directory server **602**, sending the NUMBER requested in Message 1.

[0048] In another embodiment, implemented with a conventional browser, client **601** uses a form page provided by directory server **601** that prompts for a telephone number or other identifier in place of a “dial” command, and Message 1 is a POST message to a URL specified by this form page.

[0049] Once NUMBER is received by directory server **601**, the directory server uses database **604** to translate the NUMBER to a target URL that describes the merchant server and document that implements the service corresponding to NUMBER. This translation can ignore the punctuation of the number, therefore embedded parenthesis or dashes are not significant.

[0050] In another embodiment an identifier other than a number may be provided. For example, a user may enter a company name or product name without exact spelling. In such a case a “soundex” or other phonetic mapping can be used to permit words that sound alike to map to the same target URL. Multiple identifiers can also be used, such as a telephone number in conjunction with a product name or extension.

[0051] In Message 2, Directory server **602** sends a REDIRECT to client **601**, specifying the target URL for NUMBER as computed from database **604**. The client browser **601** then automatically sends Message 3 to GET the contents of this URL. Merchant server **603** returns this information in Message 4. The server **602** might have returned a Web page to the client to provide an appropriate link to the required document. However, because server **602** makes a translation to a final URL and sends a REDIRECT rather than a page to client **601**, the document of message 4 is obtained without any user action beyond the initial dial input.

[0052] The Target URL contained in Message 3 can be an ordinary URL to an uncontrolled page, or it can be a URL that

describes a controlled page. If the Target URL describes a controlled page then authentication is performed as previously described. The Target URL can also describe a URL that includes an SID that provides a preauthorized means of accessing a controlled page.

[0053] Among benefits of the “dial” command and its implementation is an improved way of accessing the Internet that is compatible with conventional telephone numbers and other identifiers. Merchants do not need to alter their print or television advertising to provide an Internet specific form of contact information, and users do not need to learn about URL5.

[0054] In the approach a single merchant server can provide multiple services that correspond to different external “telephone numbers” or other identifiers. For example, if users dial the “flight arrival” number they could be directed to the URL for the arrival page, while, if they dial the “reservations” number, they would be directed to the URL for the reservations page. A “priority gold” number could be directed to a controlled page URL that would first authenticate the user as belonging to the gold users group, and then would provide access to the “priority gold” page. An unpublished “ambassador” number could be directed to a tagged URL that permits access to the “priority gold” page without user authentication.

[0055] This invention has particular application to network sales systems such as presented in U.S. patent application Ser. No. 08/328,133, filed Oct. 24, 1994, by Payne et al. which is incorporated herein by reference.

EQUIVALENTS

[0056] Those skilled in the art will know, or be able to ascertain using no more than routine experimentation, many equivalents to the specific embodiments or the invention described herein. These and all other equivalents are intended to be encompassed by the following claims.

What is claimed is:

1. A method of controlling access to protected content within a content server, comprising:
 - exchanging session data between a user computer system and a content server associated with a content server domain using a transfer format suitable for communication over the Internet to a user computer system that is configured to store the session data; and
 - receiving a request to access protected content from the user computer system at the content server, the request to access including at least a portion of the stored session data, the content server processing the request to access the protected content and using the portion of the stored session data to determine whether to allow the user computer system to access the protected content.
2. The method of claim 1, further comprising:
 - prompting the user computer system to provide credentials for accessing the protected content; and
 - comparing the user supplied credentials to information stored in a user account associated with the user computer system in order to authorize access to the protected content.
3. The method of claim 2, wherein the prompting and comparing steps precede the step of exchanging session data between the user computer system and the content server.
4. The method of claim 1, wherein the protected content is selected from the group consisting of an electronic document, a multimedia data file, an audio data file and a video data file.

5. The method of claim 1, wherein the session data includes a user identification associated with the user of the computer system and a domain identification associated with the content server domain, the method further comprising processing the user identification and the domain identification in order to authorize access to the protected content.

6. The method of claim 1, wherein the session data includes a user identification associated with the user of the computer system, the method further comprising processing the user identification in order to authorize access to the protected content.

7. The method of claim 1, wherein the session data includes a domain identification associated with the content server domain, the method further comprising processing the domain identification in order to authorize access to the protected content.

8. The method of claim 1, further comprising:

determining if credentials are required to access the protected content; and

if credentials are required to access the protected content, then prompting the user computer system to provide credentials for accessing the protected content.

9. The method of claim 8, wherein the determination of whether credentials are required to access the protected content is based upon an access level associated with the protected content.

10. The method of claim 1, further comprising:

determining an access level of the protected content; and accessing a user account associated with the user computer system in order to determine whether to authorize access to the protected content.

11. The method of claim 1, wherein at least a portion of the stored session data includes encrypted data.

12. The method of claim 1, wherein at least a portion of the stored session data is digitally signed.

13. The method of claim 1, further comprising:

receiving one or more requests from the user computer system to access protected content at the content server; in response to each request to access protected content, storing a content identifier in an access record associated with a user of the user computer system.

14. The method of claim 13, further comprising:

retrieving content identification data from the access record; and displaying the content identification data at the user computer system.

15. The method of claim 1, wherein the transfer format suitable for communication over the Internet is the hypertext transfer protocol.

16. The method of claim 1, further comprising:

maintaining a transaction log at the content server, the transaction log including session data associated with the access of protected content stored within the content server domain.

17. The method of claim 1, wherein the session data includes information from a user account profile stored in an account database, the method further comprising:

the content server using the information from the user account profile to customize communications to the user computer system.

18. The method of claim 17, wherein the customized communications include advertisements.

19. The method of claim 1, further comprising:

for each completed access to protected content by the user computer system from the content server, storing an access record in a transaction database.

20. The method of claim 19, further comprising:

transmitting an electronic access statement to the user computer system, the electronic access statement including links to the access records stored in the transaction database.

21. The method of claim 20, further comprising:

selecting one of the links on the electronic access statement at the user computer system; and in response thereto, obtaining the access record from the transaction server.

22. The method of claim 21, further comprising:

transmitting the protected content to the user computer system.

23. The method of claim 20, wherein the electronic access statement includes links to access records that have occurred in a current month.

24. The method of claim 23, wherein the electronic access statement includes at least one link to access records that have occurred in a prior month.

25. The method of claim 20, wherein the electronic access statement is a web page.

26. The method of claim 20, wherein the electronic access statement is transmitted to the user computer system by e-mail.

27. The method of claim 1, further comprising:

transmitting an electronic access statement to the user computer system, the electronic access statement including information regarding protected content that has been accessed by the user computer system.

28. The method of claim 27, wherein the information included in the electronic access statement includes an identification of the protected content.

29. The method of claim 27, wherein the information included in the electronic access statement includes the date on which the protected content was accessed by the user computer system.

30. The method of claim 28, wherein the identification of the protected content on the electronic access statement includes information usable to access the protected content.

31. The method of claim 30, wherein the information usable to access the protected content is a Uniform Resource Locator (URL) link to the protected content.

32. The method of claim 31, further comprising:

receiving an URL link at the content server corresponding to the protected content identified on the electronic access statement; and transmitting additional data regarding the protected content to the user computer system.

33. The method of claim 32, wherein the additional data includes a description of the protected content.

34. The method of claim 32, further comprising:

transmitting the protected content associated with the URL link to the user computer system.

35. The method of claim 27, wherein the electronic access statement includes a customer service Uniform Resource Locator (URL) link.

36. The method of claim 35, further comprising:

receiving an URL link at the content server corresponding to the customer service URL link included in the electronic access statement; and

- transmitting a customer service document to the user computer system.
37. The method of claim 2, further comprising:
storing user demographic information in the user account;
and
determining whether to authorize access to the protected content based upon the user demographic information stored in the user account.
38. The method of claim 37, wherein the user demographic information includes an indication of the user's age.
39. The method of claim 1, further comprising:
determining whether to allow the user computer system to access the protected content according to a subscription with the content server.
40. The method of claim 39, wherein the subscription is a pre-paid subscription enabling the user computer system to access protected content within the content server.
41. The method of claim 1, further comprising:
charging the user computer system for accessing the protected content.
42. The method of claim 41, wherein the user computer system is charged each time protected content is accessed at the content server.
43. A system for providing controlled access to protected content, comprising:
a content server that exchanges session data with a user computer system using a transfer format suitable for communication over the Internet;
the content server transmitting the session data to the user computer system, which is configured to store the session data; and
the content server receiving a request to access protected content from the user computer system, the request to access including at least a portion of the stored session data, and processing the request to access the protected content using the portion of the stored session data to determine whether to allow the user computer system to access the protected content.
44. The system of claim 43, wherein the content server prompts the user computer system to provide credentials for accessing the protected content, and compares the user supplied credentials to information stored in a user account associated with the user computer system in order to authorize access to the protected content.
45. The system of claim 44, wherein the content server prompts the user computer system to provide credentials prior to transmitting the session data to the user computer system.
46. The system of claim 43, wherein the protected content is selected from the group consisting of an electronic document, a multimedia data file, an audio data file and a video data file.
47. The system of claim 43, wherein the session data includes a user identification associated with the user computer system and a domain identification associated with the content server domain, and wherein the content server is programmed to process the user identification and the domain identification in order to authorize access to the protected content.
48. The system of claim 43, wherein the session data includes a user identification associated with the user computer system, and wherein the content server is programmed to process the user identification in order to authorize access to the protected content.
49. The system of claim 43, wherein the session data includes a domain identification associated with the content server domain, and wherein the content server is programmed to process the domain identification in order to authorize access to the protected content.
50. The system of claim 43, wherein the content server determines if credentials are required to access the protected content, and if so, the content server prompts the user computer system to provide credentials for accessing the protected content.
51. The system of claim 43, wherein the content server determines if credentials are required based on an access level associated with the protected content.
52. The system of claim 43, wherein the content server determines an access level of the protected content and accesses a user account associated with the user computer system in order to determine whether to authorize access to the protected content.
53. The system of claim 43, wherein at least a portion of the stored session data includes encrypted data.
54. The system of claim 43, wherein at least a portion of the stored session data is digitally signed.
55. The system of claim 43, wherein the content server receives one or more requests to access protected content from the user computer system, and in response to each request to access protected content, stores a content identifier in an access record associated with a user of the user computer system.
56. The system of claim 55, wherein the content server retrieves content identification data from the access record and causes the content identification data to be displayed at the user computer system.
57. The system of claim 43, wherein the transfer format suitable for communication over the Internet is the hypertext transfer protocol.
58. The system of claim 43, wherein the content server maintains a transaction log including session data associated with the access of protected content stored within the content server domain.
59. The system of claim 43, wherein the session data includes information from a user account profile stored in an account database, the content server using the information from the user account profile to customize communications to the user computer system.
60. The system of claim 59, wherein the customized communications include advertisements.
61. The system of claim 43, wherein for each completed access to protected content by the user computer system from the content server, the content server stores an access record in a transaction database.
62. The system of claim 61, wherein the content server transmits an electronic access statement to the user computer system, the electronic access statement including links to the access records stored in the transaction database.
63. The system of claim 62, wherein the content server receives a selection of one of the links on the electronic access statement from the user computer system and, in response thereto, obtains the access record from the transaction server.
64. The system of claim 63, wherein the content server transmits the protected content to the user computer system.
65. The system of claim 64, wherein the electronic access statement includes links to access records that have occurred in a current month.

66. The system of claim 65, wherein the electronic access statement includes at least one link to access records that have occurred in a prior month.

67. The system of claim 64, wherein the electronic access statement is a web page.

68. The system of claim 64, wherein the electronic access statement is transmitted to the user computer system by e-mail.

69. The system of claim 43, wherein the content server transmits an electronic access statement to the user computer system, the electronic access statement including information regarding protected content that has been accessed by the user computer system.

70. The system of claim 69, wherein the information included in the electronic access statement includes an identification of the protected content.

71. The system of claim 69, wherein the information included in the electronic access statement includes the date on which the protected content was accessed by the user computer system.

72. The system of claim 70, wherein the identification of the protected content on the electronic access statement includes information usable to access the protected content.

73. The system of claim 72, wherein the information usable to access the protected content is a Uniform Resource Locator (URL) link to the protected content.

74. The system of claim 73, wherein the content server receives an URL link corresponding to the protected content identified on the electronic access statement and transmits additional data regarding the protected content to the user computer system.

75. The system of claim 74, wherein the additional data includes a description of the protected content.

76. The system of claim 74, wherein the content server transmits the protected content associated with the URL link to the user computer system.

77. The system of claim 64, wherein the electronic access statement includes a customer service Uniform Resource Locator (URL) link.

78. The system of claim 69, wherein the content server receives an URL link corresponding to the customer service URL link included in the electronic access statement and transmits a customer service document to the user computer system.

79. The system of claim 43, wherein the user account includes demographic information and the content server determines whether to authorize access to the protected content based upon the user demographic information stored in the user account.

80. The system of claim 79, wherein the user demographic information includes an indication of the user's age.

81. The system of claim 43, wherein the content server determines whether to allow the user computer system to access the protected content according to a subscription with the content server.

82. The system of claim 81, wherein the subscription is a pre-paid subscription enabling the user computer system to access protected content within the content server.

83. The system of claim 43, wherein the user computer system is charged for accessing the protected content.

84. The system of claim 83, wherein the use computer system is charged each time protected content is accessed at the content server.

* * * * *