INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS

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)

Assignee: Soverain Software LLC, Chicago, IL (US)

Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

Filed: Jan. 12, 1998

Related U.S. Application Data

Continuation of application No. 08/474,096, filed on Jun. 7, 1995, now Pat. No. 5,708,780.

Int. Cl.
G06F 15/16 (2006.01)

U.S. Cl. ...................... 709/218; 709/203; 709/229

Field of Classification Search ............... 709/217, 709/218, 219, 225, 229

See application file for complete search history.

References Cited

U.S. PATENT DOCUMENTS

4,305,059 A 12/1981 Beaton
4,528,643 A 7/1985 Freeny, Jr.
4,529,870 A 7/1985 Chaum

FOREIGN PATENT DOCUMENTS

EP 0172670 2/1986

OTHER PUBLICATIONS


Primary Examiner—Patrice Winder
Attorney, Agent, or Firm—Jones Day

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.

79 Claims, 7 Drawing Sheets


Bellecore Internal Email, Nov. 24, 1993.


Amazon.com’s Reply in Support of Renewed Motion to Stay, dated Apr. 25, 2005, pp. 1-5.


Motion to Stay [Renewed] by Amazon.com (Attachments: # 1 Affidavit # 2 Text of Proposed Order) (Nelson, Justin) (Entered: Apr. 5, 2005).
Notice by Amazon.com re Answer to Amended Complaint, Counterclaim Of Rejection Of Claims 1-45 of U.S. Patent No. 5,708,780, dated Mar. 25, 2005, pp. 1-3, with Exhibit A.
Order Denying Amazon’s Motion to Stay Proceedings Pending Completion of the Reexamination, dated Apr. 20, 2005.
Sovran’s Opposition to Amazon’s Renewed Motion to Stay, dated Apr. 20, 2005, pp. 1-12.
Sovran’s Reply to Amazon.com’s Amended Counterclaims, dated Jan. 14, 2005.
Sovran’s Reply to Response to Motion re: Motion to Stay, dated Apr. 26, 2005.
Sovran’s Answer to Counterclaim (Amazon’s Third Amended Counterclaim) by Sovran Software LLC. (Seraphine, Jennifer) (Entered: Mar. 17, 2005).
Sovran’s Fourth Supplemental Responses to Amazon’s First Set of Interrogatories (Nos. 1-14) dated Mar. 21, 2005.
Sovran’s Responses to Amazon’s First Set of Requests for Admission to Plaintiff Sovran Software (Nos. 1-100) dated Mar. 21, 2005.
Sovran’s Responses to Interrogatory Nos. 22, 23, 26 and 36 of Amazon’s Third Set of Interrogatories (Nos. 17-368) dated Mar. 21, 2005.
Third Supplement to Defendant Amazon’s Initial Disclosures, dated Mar. 4, 2005.
Transcript of the Markman Hearing Before the Honorable Leonard David United States District Judge, Jan. 6, 2005.
Videotaped Deposition of Andrew Payne dated Mar. 11, 2005.
Videotaped Deposition of Glenn Crocker with Exhibits (Mar. 10, 2005).
Videotaped Deposition of Glenn Trewitt dated Jan. 25, 2005 (2 parts).
Videotaped Deposition of Mark Levergood dated Mar. 8, 2005 (2 Parts).
Amazon.com Inc.’s Unopposed Motion for Leave to Amend Its Answer to Include Allegations Regarding Stuff.com, dated May 18, 2005, pp. 1-9.
Deposition of Joshua Smith with Exhibits (Mar. 2, 2005).
Deposition of Michael Lazzaro with Exhibits (Mar. 9, 2005).
Deposition of Thomas Soulanielle with Exhibits (Mar. 14, 2005).
Exhibit 2 of Geringer Declaration: E-mail from Brooks Cutter to Mike Kuniavsky (Jun. 14, 1994).
Exhibit 6 of Geringer Declaration: E-mail from Andrew Payne to Winfield Teese et al. (Jun. 15, 1994).
Exhibit 7 of Geringer Declaration: Excerpts of Deposition of Winfield Teese (Oct. 27, 2004).
Videotaped Deposition of Guy Henry Haskin with Exhibits (Mar. 18, 2005).
Videotaped Deposition of Kevin Ming-Wei Kadla Hughes with Exhibits (Mar. 21, 2005).
Videotaped Deposition of Michael Kuniavsky with Exhibits (Feb. 22, 2005).
Videotaped Deposition of Phillip Hallam-Baker with Exhibits (Mar. 11, 2005).
“Mall Offers Holiday Treat for Hackers,” Advertising Age, Nov. 13, 1985, p. 76.
Allen & Hamilton, How to Buy Information with a First Virtual Assistant, Apr. 11, 1994, pp. 3-71.
Case Study: The CIRRUS Banking Network; Comm. ACM 8, 28 pp. 797-8078; Aug. 1985.
Consumers Plugging into New Electronic Mall, Advertising Age, Mar. 4, 1985, p. 74.

Gifford, David R.; “Cryptographic Scaling for Information Secrecy and Authentication”; Stanford University and Xerox Palo Alto Research Center; Communications of the ACM; vol. 25, No. 4; Apr. 1982.


Hirschfeld, Rafael; “Making Electronic Refunds Safer”; Sections 1, 2, and 3; 1992.


Arnon, Dan, et al., Electronic Mail to multiple recipients of the www-talk list (www-talk@info.cern.ch) on “Access and session control” dated Sep. 15, 1994.

Bateaen, Butler; Chan; Chen; Evenchick; Hughes; Jen; Jeng; Millett; Riccio; Skoudis; Starace; Stoddard; “An Internet Billing Server Prototype Design”; Carnegie Mellon University; 1992.


Derler, Christian, “The World-Wide Web Gateway to Hyper-G: Using a Connectionless Protocol to Access Session-Oriented Ser-
services", Institut für Informationsverarbeitung and Computergestützte
neue Medien, Graz, Austria, dated Mar. 1995.
Dukach, Seymour, "Proof of Concept Implementation of the SNPP Protocol;
English, Joe, Electronic Mail to multiple recipients of the www-talk
list (www-talk@info.cern.ch) on "Re: Identifying Mosaic session"
Ferrarin, E., "Flight of Fancy: Goodbye Travel Agent", Business
1, Jun. 1999, pp. 1-140.
Fielding, Roy, et al., "Principled Design of the Modern Web
Architecture" ACM Transactions on Internet Technology 2, 2 pp.
115-150 (May 2002).
Fielding, Roy, software distribution archive for the HTTP log file
analysis program, wwwstat v.1.01, dated Apr. 24, 1994, published at
Foster, David & Stuart Finn, "Insurers Can Benefit From E-Mail
Networks", National Underwriter Property & Casualty-Risk &
Gifford, Stewart, Payne, Treese, "Payment Switches for Open
San Francisco, CA.
Hall, Devra, et al., "Build a Web Site: The Programmer's Guide to
Creating, Building, and Maintaining a Web Presence", published
Hughes, Kevin, source code file for the HTTP log file analysis
com/software/getstats/getstats.html—Version 1, 64 pages.
Hughes, Kevin, source code file for the HTTP log file analysis
com/software/getstats/getstats.html Version 2, 64 pages.
It will happen, article excerpt from infoHighway, vol. 2-1, Jan.
1995.
Leggett, John, et al., "Hypermail: Using Extensibility to Develop
Dynamic, Open and Distributed Hypertext Systems" (1992).
Maren, Michael, "The Age of E-Mail", Home Office Computing,
McCartney, Todd, Message posted to Usenet public discussion
group, rec.arts.disney, dated Nov. 21, 1993.
NCSA HTTPd release notes at http://hooho.ncsa.uiuc.edu/docs/
Upgrade.html (last updated Aug. 1, 1995).
O'Mahony, Donald, Michael Pearce, & Hitesh Tewari, Electronic
Pitkov, et al., "Results from the First World Wide Web Use Survey",
presented at the First International Conference on the World Wide
www94.web.cern.ch/www94/PrelimProc.html on Jun. 2, 1994,
and reprinted in the Journal of Computer Networks and ISDN
Smithson, Brain, and Singer, Barbara, An Information Clearing-
Stallings, William, Data & Computer Communications, MacMillan
The Major BBS: Collection of Information and Advertisements
concerning The Major BBS (Fall 1993).
Trettw, Glenn, "Using Tel to Process HTML Forms", Digital
Equipment Corporation, Network Systems Laboratory TN-14,
Trip et al., "Cookies" (client-side persistent information) and their
use, Netscape Technical Note 20019, Netscape Communications
wwwstat/readme, dated May 18, 2005.
Ohmori et al., "An On-line Shopping System Protecting User's
Privacy", Information Communication Laboratory of Mitsubishi
Electric Industrial Co., Ltd., pp. 25-32. Note: 12 Pages of Translation
Soverain Software LLC. Amazon.Com, Inc. and The Gap, Inc.,
Form of Stipulated Request for Final Dismissal of the Actions, filed
Soverain Software LLC v. Amazon.Com, Inc. and The Gap, Inc.,
Bina et al., "Secure Access to Data Over the Internet", Natl. Center
for Supercomputing Applns., Univ. Of Illinois, Champaign, Illinois,
Farber, David, "Interesting-People Message—RSA/NCDSA/EIT
Announcement on Secure Mosaic" Palo Alto, California, Apr. 12,
1994, 4 pages.
Kent, Stephen T., "Internet Privacy Enhanced Mail", 8070 Com-
munications of the ACM 36, New York, Aug. 1993, pp. 48-60.
Kohn, Dan, "Prior Art on Open Market Patents", e-mail message
dated Mar. 9, 1998, 1 page.
Lewis, Peter H., "Attention Shoppers: Internet is Open", 2 pages.
Medvinsky et al., Netsmash: A Design for Practical Electronic
Currency on the Internet, Information Sciences Institute, University
Schaefer et al., "Networked Information Discovery and Retrieval
Tools: Security Capabilities and Needs", The MITRE Corporation,
Kahan, Jose "Un nouveau modele d'autorisation pour les systemes
de consultation d'information multimedia reprise", pp. 45-57.
Kahan, Jose, "A New Authorization Model for Distributed Multi-
* cited by examiner
Doc. Title  CONTENT HOME PAGE
Doc. URL    http://Content.com/homepage

Content 1, content 2, content 3, content 4,
content 5, Link 1, content 6, content 7,
content 8, content 9, content 10, Link 2,
content 11, content 12, content 13, content 14,
content 15, content 16, Link 3, content 17

http://Content.com/advertisement

FIG. 4
Document View

Title: How to join
URL: 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
   US

FIG. 5
NUMBER to URL Database

Directory Server

1. GET "NUMBER"

2. REDIRECT "TARGET-URL" [MS]

Client

3. GET "TARGET-URL"

4. Send Page

Merchant Server (MS)

FIG. 6
INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS

RELATED APPLICATION

This application is a Continuation of U.S. Ser. No. 08/474,096, filed Jun. 7, 1995, now U.S. Pat. No. 5,708,780 the entire teachings of which are incorporated herein by reference.

BACKGROUND TO THE INVENTION

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.

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).

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 navigational tools have helped users search resources on the Internet without knowing specific host addresses, these tools still require a substantial technical knowledge of the Internet.

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.

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, or browser, reads these codes in order to display the page. The hypertext conventions and related functions of the worldwide 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.

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.

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/Bdir/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.

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.

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

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.

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 therefor. 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.

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.

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.

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 contains 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 new SID provides access to the new domain if the user is qualified.

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.

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.

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.

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.

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

FIG. 1 is a diagram illustrating the Internet operation.
FIG. 2A is a flowchart describing the preferred method of Internet server access control and monitoring.
FIG. 2B is a related flowchart describing the details of the authentication process.
FIG. 3 illustrates an example of a client-server exchange session involving the access control and monitoring method of the present invention.
FIG. 4 is an example of a World Wide Web page.
FIG. 5 is an example of an authorization form page.
FIG. 6 is a diagram describing the details of the translation of telephone numbers to URLs.
Detailed Description of the Invention

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.

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 412, 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 412 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.

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.

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.

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.

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.

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.

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

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
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.

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 ranking purposes. By excluding repeated calls, the system avoids distortions by users attempting to "stuff the ballot box."

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.

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 traversal 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.

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.

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.

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 SIDs. 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.

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.

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 parentheses or dashes are not significant.

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.

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.

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.

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 URLs.

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.

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

Those skilled in the art will know, or be able to ascertain using no more than routine experimentation, many equivalents to the specific embodiments of 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 processing service requests from a client to a server system through a network, said method comprising the steps of forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

    returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent distinct requests to the server system; and

    appending the stored session identifier to each of the subsequent distinct requests from the client to the server system.

2. A method as claimed in claim 1 wherein the session identifier includes a user identifier.

3. A method as claimed in claim 1 wherein the session identifier includes an expiration time for the session.

4. A method as claimed in claim 1 wherein the server system records information from the session identifier in a transaction log in the server system.

5. A method as claimed in claim 4 wherein the server system tracks the access history of sequences of service requests within a session of requests.

6. A method as claimed in claim 5 wherein the server system tracks the access history to determine service requests leading to a purchase made within the session of requests.

7. A method as claimed in claim 4 wherein the server system counts requests to particular services exclusive of repeated requests from a common client.

8. A method as claimed in claim 4 wherein the server system maintains a data base relating customer information to access patterns.

9. A method as claimed in claim 8 wherein the information includes customer demographics.

10. A method as claimed in claim 1 wherein the server system assigns the session identifier to an initial service request to the server system.

11. A method as claimed in claim 1 wherein the server system subjects the client to an authorization routine prior to issuing the session identifier and the session identifier is protected from forgery.
12. A method as claimed in claim 1 wherein the server system comprises plural servers including an authentication server which provides session identifiers for service requests to multiple servers.

13. A method as claimed in claim 12 wherein:
   a client directs a service request to a first server which is to provide the requested service;
   the first server checks the service request for a session identifier and only services a service request having a valid session identifier, and where the service request has no valid identifier:
   the first server returns a response to the client, the response redirecting the service request from the client to the authentication server;
   the authentication server subjects the client to an authorization routine and issues the session identifier to be appended to the service request to the first server;
   the client forwards the service request appended with the session identifier to the first server; and
   the first server recognizes the session identifier and services the service request to the client; and
   the client appends the session identifier to subsequent service requests to the server system and is serviced without further authorization.

14. A method as claimed in claim 13 wherein the session identifier includes a user identifier.

15. A method as claimed in claim 13 wherein the session identifier includes an expiration time for the session.

16. A method as claimed in claim 13 wherein the session identifier provides access to a protected domain to which the session has access authorization.

17. A method as claimed in claim 16 wherein the session identifier is modified for access to a different protected domain.

18. A method as claimed in claim 13 wherein the session identifier provides a key identifier for key management.

19. A method as claimed in claim 13 wherein the server system records information from the session identifier in a transaction log in the server system.

20. The method of claim 1 wherein the access rights of the client are fully contained within the session identifier.

21. A method as claimed in claim 1 wherein a service request is for a document and the session identifier includes a user identifier, further comprising:
   returning the requested document wherein the document is customized for a particular user based on the user identification of the session identifier.

22. A method as claimed in claim 1 wherein a service request is for a document which has been purchased by a user, the session identifier comprises an authorization identifier, and further comprising:
   returning the requested document if the authorization identifier indicates that the user is authorized to access the document.

23. A method as claimed in claim 1 wherein a service request is for a document wherein the session identifier comprises a user identifier, and further comprising:
   returning the requested document to the client; and charging the user identified in the identifier for access to the document.

24. The method of claim 1, wherein at least one service request comprises a request for a document which has been purchased by a user, and wherein the session identifier comprises an authorization identifier, the method further comprising:
   returning the requested document if the authorization identifier indicates that the user is authorized to access the document.

25. A method as claimed in claim 24, wherein the authorization identifier is encoded within a session identifier which is appended to the request.

26. The method of claim 24 wherein the authorization identifier is provided by the authentication server.

27. The method of claim 24, further comprising:
   identifying the user from the authorization identifier; and
   automatically charging the identified user for the document.

28. The method of claim 24, wherein the document is returned electronically.

29. The method of claim 24, wherein a physical copy of the document is sent.

30. The method of claim 24, wherein the authorization identifier is appended to a uniform resource locator.

31. The method of claim 1, wherein at least one service request comprises a request for a document, wherein the session identifier is designated by the server system, said method further comprising the steps of:
   returning the requested document to the client; and
   charging the user identified in the identifier for access to the document.

32. A method as claimed in claim 31, wherein a user identifier is encoded within a session identifier which is appended to the request.

33. The method of claim 1 wherein the session identifier is cryptographically generated.

34. The method of claim 1, further comprising:
   returning a response to the client, the response redirecting an initial service request to an authentication server, the authentication server providing the session identifier.

35. The method of claim 1, wherein the session identifier is appended to at least one path name in a document returned by the server system.

36. The method of claim 35, wherein the at least one path name is in a link in the returned document.

37. The method of claim 36 wherein the link is an absolute link.

38. The method of claim 36 wherein the link comprises a uniform resource locator.

39. The method of claim 35 wherein the step of appending the session identifier comprises filtering the requested document.

40. The method of claim 35 wherein the session identifier is cryptographically generated.

41. The method of claim 35 wherein the session identifier is directed to an accessible domain.

42. The method of claim 35 wherein the session identifier comprises an expiration time.

43. The method of claim 35 wherein the session identifier comprises a date.

44. The method of claim 35 wherein the session identifier comprises a key identifier.

45. The method of claim 35 wherein the session identifier comprises an address of the client.

46. The method of claim 35 wherein the session identifier comprises a digital signature.

47. The method of claim 1, wherein the session identifier is designated by the server system, further comprising the steps of:
   validating, at the server system, the appended session identifier; and
   returning a controlled document if the appended session identifier is valid.

48. The method of claim 47 wherein the session identifier is cryptographically generated.

49. The method of claim 47 wherein the session identifier is directed to an accessible domain.
The method of claim 47 wherein the session identifier comprises an expiration time.

The method of claim 47 wherein the session identifier comprises a date.

The method of claim 47 wherein the session identifier comprises a key identifier.

The method of claim 47 wherein the session identifier comprises an address of the client.

The method of claim 47 wherein the session identifier comprises an unforgeable digital signature.

The method of claim 47 wherein the session identifier facilitates authenticated accesses across multiple content servers.

The method of claim 47 wherein the document is customized for a particular user based on a user identification of the session identifier.

The method of claim 47, wherein the session identifier is appended to at least one path name in a document returned by the server system.

The method of claim 57 wherein the step of appending the session identifier comprises filtering the requested document.

The method of claim 1, further comprising: servicing a request; and automatically charging a user identified by the session identifier for the service provided.

The method of claim 1, wherein at least one service request comprises a purchase request, the purchase request including an associated user identifier, the method further comprising: accessing, upon receipt of the purchase request at the server system, user information associated with the user identifier sufficient to charge to an account associated with the user, the purchase price of the product identified by the purchase request; charging the user for the product identified by the purchase request according to the user information; and fulfilling the purchase request based on the user information.

The method of claim 60, wherein the client includes the user identifier in a session identifier appended to the purchase request.

The method of claim 1, further comprising: under control of a client system, displaying information identifying a product; and in response to a user selection of a hyperlink associated with a product desired to be purchased, sending a request to purchase the item along with an identifier of a purchaser of the item to a server system; and, under control of the server system, upon receiving the request, retrieving additional information previously stored for the purchaser identified by the identifier in the received request; charging the user the purchase price of the product; and fulfilling the request for the product.

The method of claim 1, wherein the session identifier is appended by the client.

The method of claim 63, wherein the session identifier is cryptographically generated.

The method of claim 1, wherein a service request comprises a request to purchase a product.

The method of claim 65, wherein the product is transmitted over the network.

The method of claim 66, wherein the product is a newspaper/newsletter article.

The method of claim 65, wherein the product is a durable product.

An information system on a network, comprising: means for receiving service requests from a client and for determining whether a service request includes a session identifier, wherein communications to and from the client are according to hypertext transfer protocol; means for providing the session identifier in response to an initial service request from the client in a session of requests; means for storing, at the client, the session identifier for use in each communication to the server system; means for appending the stored session identifier to each of subsequent communications from the client to the server system; and means for servicing the subsequent service requests.

The information system of claim 69 wherein access rights of the client are fully contained within the session identifier.

An information system as claimed in claim 69 wherein the means for providing the session identifier is in a server system which services the requests.

An information system as claimed in claim 69 further comprising an authorization routine for authorizing the client prior to issuing the session identifier and means for protecting the session identifier from forgery.

An information server system as claimed in claim 69 further comprising a transaction log for recording information from the session identifier.

An information system as claimed in claim 69 further comprising means for tracking access history of sequences of service requests within the session of requests.

An information system as claimed in claim 69 further comprising means for counting requests to particular services exclusive of repeated requests from a common client.

An information system as claimed in claim 69 further comprising a database relating customer information to access patterns.

An information system as claimed in claim 76 wherein the information includes customer demographics.

A method of processing, in a server system, service requests from a client to the server system through a network, said method comprising the steps of: receiving, from the client, a service request to which a session identifier stored at the client has been appended by the client, wherein communications between the client and server system are according to hypertext transfer protocol; validating the session identifier appended to the service request; and servicing the service request if the appended session identifier is valid.

The method of claim 78, further comprising, in the server system: receiving an initial service request from the client; creating, responsive to the initial service request, the session identifier; and returning the session identifier to the client for storage by the client for use in subsequent distinct requests to the server system.