(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007575 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US01/32361

(22) International Filing Date: 16 October 2001 (16.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/901,350 9 July 2001 (09.07.2001) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/901,350 (CON)
Filed on 9 July 2001 (09.07.2001)

(71) Applicant *(for all designated States except US)*: **INGRIAN SYSTEMS, INC.** [US/US]; 3071 Edison Way, Redwood City, CA 94063 (US).

(72) Inventors; and

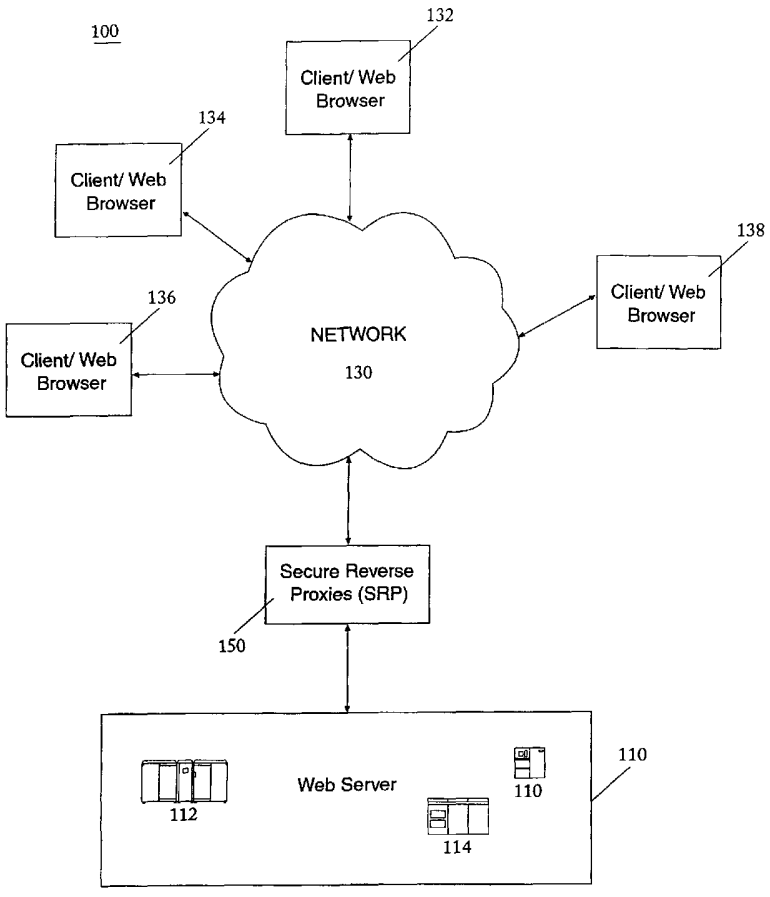
(75) Inventors/Applicants *(for US only)*: **CHAWLA, Rajeev** [US/US]; 5819 Carmel Way, Union City, CA 94587 (US). **PANAGIOTIS, Tsirigotis** [GR/US]; 231 Acalanes Drive #9, Sunnyvale, CA (US). **BONEH, Dan** [IL/US]; 3349 Louis Road, Palo Alto, CA 94303 (US).

(74) Agents: **GREGORY, Richard, L., Jr.** et al.; Perkins Coie LLP, P.O. Box 2168, Menlo Park, CA 94026 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR CACHING SECURE WEB CONTENT



(57) Abstract: A method and system for securing network communications are provided. In a network a Secure Reverse Proxy ("SRP") is placed among a server and a client where the client and SRP establish a secure connection using TLS protocol. Upon receiving a request from the client for a secure HTTP page, the SRP determines if the secure page is maintained in its cache. If the page is present, the SRP responds to the client by sending the requested secure HTTP page without contacting the server. If the page is not contained within the SRP's cache, the SRP establishes secure TLS connection with the server and forwards the request for the HTTP page. Receiving the HTTP page from the server, the SRP places it in its cache for future use. Having the page in its cache the SRP retrieves the page, encrypts it, and sends it to the requesting client. Subsequent requests for the same page do not involve the server enhancing the efficiency of network operations.

WO 03/007575 A1

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR CACHING SECURE WEB CONTENT

FIELD OF THE INVENTION

The field of the invention is secure content in a network system. More particularly the invention is in the field of secure content transfer in a network using caching techniques.

BACKGROUND OF THE INVENTION

Web caches are network applications used to reduce network traffic and improve response times. Web caches work by storing static content on a network at intermediate locations. Static content encompasses items that rarely change. Once stored the information is available for repeated transmissions of the same content over an abbreviated portion of the network. By eliminating the need for the server to produce all of the requested information for each request, the effective bandwidth of the network is increased. Unfortunately, web caching does not currently apply to secure web content. Secure web content is sent encrypted using various protocols such as Transport Layer Security ("TLS") or Secure Socket Layer ("SSL"). Such secure protocols use unique encryption keys known only to the connection endpoints. Each message therefore is independently secure. Consequently, intermediate web caches in a computer network do not store and retransmit secure static content since they cannot examine it to determine if it has changed. As far as the cache is concerned each message is unique effectively eliminating the purpose of a cache entirely. Hence, TLS and SSL are incompatible with the existing web caching architecture.

Transport Layer Security protocol is one of the most widely deployed protocols for securing communications on the World Wide Web ("WWW") and is used by most E-commerce and financial web sites. It guarantees privacy and authenticity of information exchanged between a web server and a web browser. Currently, the number of web sites using TLS or SSL to secure web traffic is growing at a phenomenal rate. As the services provided by the World Wide Web continue to expand, so will the need for security. Unfortunately, TLS and SSL are incompatible with the current network design methodologies used in the Internet.

This incompatibility stems from the inherent nature of how a secure session is established. A TLS session, for example, between a web server and a web browser occurs

in a number of phases. When a web browser first connects to a web server using TLS, the browser and server execute the TLS handshake protocol. The outcome of this protocol is a session encryption key and a session integrity key. These keys are known only to the web server and the web browser.

Once the session keys are established, the browser and server begin exchanging data. The data is encrypted using the session encryption key and protected from tampering using the session integrity key. When the browser and server are done exchanging data the connection between them is closed. If the browser and server subsequently reestablish a secure connection the browser and server may execute a resume handshake or establish a new set of session keys. A resume handshake protocol causes both server and browser to reuse the session key previously established during the initial handshake, and is more efficient, but requires the connection between the web server and web browser to be continuous. Thereafter, all application data is encrypted and protected using the previously established session keys.

Web caches are typically located on the network between the user and the web server being accessed. The web cache inspects all responses coming back from the server and stores in its memory all content that changes infrequently. This information is called static content. Examples of static content include the banner and the navigation buttons on the page. The next time a user requests this information the cache responds immediately with the information without contacting the web server. As a result, web caches dramatically reduce traffic on the network and reduce the response times to user requests.

A reverse proxy is similar to a web cache. The difference lies in where the reverse proxy is located and the type of content cached. While web caches are located close to the client processor so as to minimize response time, the reverse proxy is typically located close to the web server with the most common location being at the same site as the web server. The main goal of the reverse proxy is to reduce the load on the web server. Any time a request is received at the web site the reverse proxy first determines whether the response is already cached. If so, the reverse proxy responds itself without contacting the web server. Otherwise the request is sent to the web server. Inherent to the reverse proxy function is its ability to examine the request as well as the content of the cache to determine if the information stored fulfills the request.

Web caches and reverse proxies are ineffective when dealing with secure content. The problem lies in identification of repeated information. Secure content passing through

these appliances is encrypted using a key known only to the end points, namely the web server and the web browser. Each web browser connected to the proxy passes through information that is unrecognizable to the cache. The web cache or the reverse proxy cannot interpret the data to determine if the data should be stored or if the data request matches any stored data. Hence it is useless to cache the encrypted information. Consequently, the existing infrastructure designed to make the Internet more efficient and faster becomes ineffective when dealing with secure content.

SUMMARY OF THE INVENTION

A method and system are provided for caching secure content on a computer network. One embodiment establishes a reverse proxy logically located between a web server and connections to the outside world that is capable of interpreting and storing secure content.

The Secure Reverse Proxy ("SRP") in one embodiment intercepts request for secure content prior to the demand being received by the web server. The SRP establishes an encrypted session with the web browser to facilitate the SRP's ability to examine the secure content. Once the secure request is decrypted, the SRP examines its cache and determines if the requested content available. If the requested content is available, the SRP encrypts it using the established session keys with the web browser and transmits the information. In this embodiment the web browser never directly contacts the web server nor does the web server need to respond to the request.

In an additional embodiment the SRP determines if the requested information is not available in the SRP's cache. Upon determining that the information is not cached, the SRP establishes a secure connection with the web server using TLS, SSL or other secure protocol. The SRP forwards the web browser's request for information to the web server and the web server responds to the SRP as if it was the web browser. Upon receiving the information the SRP stores it in the cache for future use in either encrypted or clear-text form. With the information requested by the browser now available in the SRP's cache, the SRP retrieves the information and encrypts it using the session keys established between the SRP and the web browser. The SRP then transmits the information to the web browser. Since the requested information is now contained in the SRP's cache, subsequent requests from this or other browsers for the same information will not require any interaction with

the web server. Thus the efficiency of the network is increased and the load upon the server is diminished.

BRIEF DESCRIPTION OF THE FIGURES

The present invention is illustrated by way of example in the following diagrams and flow charts in which like references indicate similar elements. The following diagrams and flow charts disclose various embodiments of the present invention for purposes of illustration only and are not intended to limit the scope of the invention.

Figure 1 is a block diagram of an embodiment of a network system for improving secure communications.

Figure 2 is a flow diagram illustrating a method for secure reverse proxy caching of secure content for one embodiment of the present invention.

DETAILED DESCRIPTION

A method and system are provided for secure reverse proxies capable of caching secure content. These Secure Reverse Proxies ("SRP") are, in one embodiment, installed logically between the web server and the connection to the outside world with all incoming secure requests being first sent to the SRP rather than directly to the server.

Normally, a request to establish a secure connection is received by the server from a web browser. In one embodiment the request message, such as a request to establish a TLS session, is referred to as a client hello and is directed to the SRP instead of the server. The SRP responds to the request by sending back a TLS server hello message containing the server certificate. After performing the TLS key exchange protocol the SRP and the requesting browser share a secret encryption key and a secret integrity key. These keys are used to protect the rest of the session and are appropriately called session keys.

With a TLS session established between the SRP and the web browser the requesting web browser sends an encrypted HTTP request using the TLS protocol and the session keys. The SRP receives the request, decrypts it using the session keys and checks whether the local cache contains an appropriate response to the incoming inquiry. If the SRP contains the requested information, the SRP encrypts the response using the current session keys and sends the result to the requesting web browser. Up to this point the web server has never seen the request.

If the request received by the SRP is not contained in the local cache the SRP must forward the request to the web server. This requires the SRP and the web server to establish a secure session, independent of the secure session between the SRP and the web browser. The request to the web server is thereafter secured using a secure protocol such as TLS so that is does not appear as clear-text on the network. In another embodiment all communication between the SRP and the web server takes place over a private network at the web site or by an inherently secure connection such as fiber optic or copper cable. If such a connection between the server and the SRP is present it is possible for the SRP to send the request to the web server using clear-text HTTP. This reduces the load on the web server since the web server need not perform any expensive secure handshake computations.

With communication between the web server and the SRP established either through a secure network protocol or an inherently secure connection, the web server sends a response to the query back to the SRP. Having received a response from the web server, the SRP caches the information in either cipher or clear-text format. Now possessing the requested information in the local cache, the SRP encrypts the requested information using the current SRP / browser session keys and sends the result to the requesting web browser. While the SRP can maintain numerous secure connections with a number of web browsers using a number of session keys, the SRP need only maintain one secure connection with the server. Thus the load on the server is dramatically reduced and the efficiency of the network is significantly improved.

In one embodiment the SRP stores the cached information locally within the server or on a non-volatile medium such as magnetic tape, optical disks, by a third party, or using other techniques known in the art. To ensure the information remains secure, information is stored on non-volatile mediums encrypted under a separate key known only to the server. The server maintains the key to the information using a tamper resistant non-volatile card.

Figure 1 shows one embodiment for enhancing secure network communications. The system 100 includes multiple client computers 132,134,136, and 138, which are coupled to a server system 110 through a network 130. The network 130 can be any network, such as a local area network, a wide area network, or the Internet. Coupled among the server system 110 and the network 130 is a Secure Reverse Proxy 150. While shown as a separate entity, the SRP 150 can be located independently of the server system, the network environment or distributed among any number of server sites 112, 114 and 116.

The client computers each include one or more processors and one or more storage devices. Each of the client computers also includes a display device, and one or more input devices. The SRP can be one or more devices, each including one or more processors and storage devices.

All of the storage devices store various data and software programs. In one embodiment, the method for improving TLS is carried out on the system 100 by software instructions executing on one or more of the server sites 112, 114 and 116. The software instructions may be stored on the server system 110 any one of the server sites 112 - 116 on any one of the client computers 132 - 138 or any number of SRPs. For example, one embodiment presents a hosted application where an enterprise requires secure communications with the server. The software instructions to enable the communication to be cached by the SRP are stored on the server. In other embodiments, the software instructions and the caching process may be stored and executed on the client computers. Data required for the execution of the software instructions can also be accessed via the network and can be stored anywhere on the network.

Figure 2 is a flow diagram for enhancing secure content on a network using reverse proxies of an embodiment. The process begins with a request by the web browser to establish a secure connection 210. The SRP responds with a hello message 220 and a TLS key is exchanged and validated between the browser and the SRP 230. With the establishment of the secure session 240 the SRP receives an HTTP request 250. The SRP examines the local cache 260 and if the content is not cached, forwards the request to the web server 270. This forwarding is through an independent TLS session established between the SRP and the web server. The web server responds with the secure content 280 which is locally cached at the SRP 285 and then forwarded to the web browser 290 via the earlier established session keys.

While TLS and other secure network protocols typically prevent the intermediate storing of secure static content on a reverse proxy, the architecture described herein enables such content to be cached. Hence, the web browser continues to receive encrypted content yet requests for encrypted material at the server are significantly reduced. The secure protocol between the SRP and the web browser preserves the confidentiality of the communication, as does the connection between the SRP and the web server. This connection provides no clear-text traffic from which an eavesdropper or active attacker can

gain information. In addition to this security benefit there is also a significant performance advantage since the web server responds to minimal browser requests.

Performance is also enhanced by reducing the costly protocol of establishing a secure connection. When an SRP is not used, the web server must perform an initial TLS or equivalent handshake with every new user that connects to the site. The TLS handshake is expensive and slows down the network. In one embodiment, the web server sees only connections from the SRP as the need to establish multiple TLS connections is displaced to the SRP. Having once established a secure connection, the SRP and the server can utilize a more efficient resume handshake rather than having to reinitiate the creation of a unique session key. Consequently, the need to perform and handle TLS handshakes repetitively is eliminated and only one TLS handshake with the SRP need be accomplished. The resulting reduced load on the sever increases effective network bandwidth and reduces cost.

From the above description and drawings, it will be understood by those of ordinary skill in the art that the particular embodiments shown and described are for purposes of illustration only and are not intended to limit the scope of the invention. Those of ordinary skill in the art will recognize that the invention may be embodied in other specific forms without departing from its spirit or essential characteristics.

CLAIMS

What is claimed is:

1. A method for caching secure network communications in a computer network, comprising placing at least one secure reverse proxy among at least one web server and at least one web browser, wherein the at least one secure reverse proxy caches secure content.

2. A method for secure network communications, comprising:

coupling at least one network appliance among at least one web server and at least one web browser;

establishing a secure session between the at least one network appliance and the at least one web browser, wherein the at least one web browser sends an encrypted request for content using a secure session protocol;

decrypting the encrypted request for content at the at least one network appliance;

examining at least one network appliance's local cache to locate the content;

encrypting the content from the at the at least one network appliance's local cache using an established secure protocol; and

sending the content to the at least one web browser, wherein reducing the number of requests at the web server for establishing a secure network connection improves network efficiency.

3. The method of claim 2, wherein the local cache includes non-volatile memory.

4. The method of claim 2, wherein the at least one network appliance and the at least one Web server are collocated.

5. The method of claim 2, wherein the content includes an HTTP page.

6. The method of claim 2, wherein decrypting further includes:

determining the content requested by the at least one web browser is not present in the at least one network appliance's local cache;

forwarding the request for content to the at least one web server using a separate secure session;

receiving back from the at least one web server to the at least one network appliance a response containing the requested content, wherein communication between the at least one network appliance and the at least one web server is secure; and

caching the requested content locally at the network appliance for future requests.

7. The method of claim 2, wherein the secure session uses Transport Layer Security protocol.

8. The method of claim 2, wherein the secure session uses Secure Socket Layer protocol.

9. The method of claim 2, wherein the secure session uses Internet Protocol Secure ("IPSec") techniques.

10. A method for caching secure network communications, comprising:

coupling at least one Secure Reverse Proxy ("SRP") among at least one web server and at least on web browser wherein the at least one SRP intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server;

establishing a first secure session using a first secure session protocol between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;

decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;

retrieving the HTTP page if available from the local cache;

encrypting the HTTP page retrieved from the local cache using the first secure session protocol;

sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;

establishing a second secure session using a second secure session protocol with the at least on web server if the HTTP page is not available from the local cache, wherein the second secure session is maintained;

encrypting the request for a HTTP page using the second secure session protocol;

forwarding the request for a HTTP page encrypted using the second secure session to the at least one web server:

receiving from the at least one web server an encrypted HTTP page using the second secure session;

decrypting the encrypted HTTP page using the second secure session protocol;

storing the HTTP page in the at least one SRP's local cache;

encrypting the HTTP page using the first secure session protocol; and

sending the HTTP page to the at least one web browser using the first secure session.

11. The method of claim 10, wherein coupling includes connecting the SRP and web server using a dedicated line.

12. The method of claim 10, wherein coupling includes having the web server and SRP collocated.

13. The method of claim 10, wherein storing includes using non-volatile media to store the content.

14. The method of claim 10, wherein storing includes encrypting the content using a third secure session protocol.

15. The method of claim 10, wherein the first secure session protocol includes Transport Layer Security protocol.

16. The method of claim 10, wherein the second secure session protocol includes Transport Layer Security protocol.

17. The method of claim 10, wherein the third secure session protocol includes Transport Layer Security protocol.

18. The method of claim 10, wherein the first secure session protocol includes Secure Socket Layer protocol.

19. The method of claim 10, wherein the second secure session protocol includes Secure Socket Layer protocol.

20. The method of claim 10, wherein the third secure session protocol includes Secure Socket Layer protocol.

21. The method of claim 10, wherein the first secure session protocol includes Internet Protocol Secure ("IPSec") techniques.

22. The method of claim 10, wherein the second secure session protocol includes Internet Protocol Secure ("IPSec") techniques.

23. The method of claim 10, wherein the third secure session protocol includes Internet Protocol Secure ("IPSec") techniques.

24. A method for caching secure content in a Secure Reverse Proxy ("SRP") in an secure network, comprising:

coupling at least one SRP among at least one web browser and at least one web server wherein the at least one SRP receives from the at least one web browser requests for establishing a first secure session;

establishing the first secure session using a first secure session protocol between the at least one SRP and the at least on web browser, wherein the web browser sends an encrypted request for content to the at least one SRP;

decrypting the encrypted request for content from the at least one web browser at the at least one SRP using the first secure session protocol, wherein the at least one SRP determines that the at least one SRP does not possess the requested content;

establishing a second secure session using a second secure session protocol between the at least one SRP and the at least one web server, wherein the second secure session is maintained;

encrypting the request for content from the at least one web browser using the second secure session protocol;

sending the encrypted request for content to the at least one web server using the second secure session;

receiving the content from the at least on web server at the least one SRP using the second secure session;

decrypting the content using the second secure session protocol;

storing the requested content locally in a memory at the at least one SRP;

and retrieving the content from the memory at the at least one SRP upon subsequent requests for the content.

25. The method of claim 24, wherein storing includes encrypting the content using a third secure session protocol, wherein the third secure session protocol is known only to the at least one SRP.

26. The method of claim 24, wherein storing includes using non-volatile media.

27. The method of claim 24, wherein coupling includes establishing a dedicated secure line between the SRP and the web server.

28. The method of claim 24, wherein coupling includes collocating the web server and the SRP.

29. The method of claim 24, wherein content includes an HTTP page.

30. The method of claim 24, wherein the first secure session includes Transport Layer Security protocol.

31. The method of claim 24, wherein the second secure session includes Transport Layer Security protocol.

32. The method of claim 24, wherein the first secure session includes Secure Socket Layer protocol.

33. The method of claim 24, wherein the second secure session includes Secure Socket Layer protocol.

34. The method of claim 24, wherein the first secure session includes Internet Protocol Secure ("IPSec") techniques.

35. The method of claim 24, wherein the second secure session includes Internet Protocol Secure ("IPSec") techniques.

36. The method of claim 24, wherein storing includes encrypting the requested HTTP page.

37. A system for caching secure communications in a network comprising:

at least one web server;

at least one web browser;

at least one Secure Reverse Proxy ("SRP") coupled among the at least one web server and the at least one web browser, wherein the at least one SRP caches secure content.

38. The system of claim 37, wherein the at least one web browser, the at least one web server, and at least one SRP use Transport Layer Security protocol to establish a secure session.

39. The system of claim 37, wherein the at least one web browser, the at least one web server, and at least one SRP use Secure Socket Layer protocol to establish a secure session.

40. The system of claim 37, wherein the at least one web browser, the at least one web server, and at least one SRP use Internet Protocol Secure ("IPSec") techniques to establish a secure session.

41. A method for secure communications in a network, comprising:

caching responses including secure content from at least one web server to at least one web browser in at least one Secure Reverse Proxy ("SRP"), wherein the at least one SRP is coupled among the at least one web server and the at least one web browser; and

enabling future requests for the same secure content to be processed by the at least one SRP.

42. A system for enhancing secure communications in a computer network, comprising:

at least one Secure Reverse Proxy ("SRP") coupled among at least one web server and at least one browser, wherein the at least one SRP establishes a secure session between the at least one SRP and the at least one web browser;

the at least one web browser sending to the at least one SRP an HTTP page request encrypted using the secure session protocol;

the at least one SRP decrypting the HTTP page request, wherein the SRP examines a local cache to locate the HTTP page, retrieves the HTTP page, encrypts the HTTP page from the local cache using the established secure session protocol, and sends the HTTP page to the at least one web browser using the secure session reducing the messages sent to the web server improving the efficiency of the network.

43. The system of claim 42, wherein the secure session is established using Transport Layer Security protocol.

44. The system of claim 42, wherein the secure session is established using Secure Socket Layer protocol.

45. The system of claim 42, wherein the secure session is established using Internet Protocol Secure ("IPSec") techniques.

46. The system of claim 42, further comprising:

the at least one SRP establishing a separate secure session with the at least one web server, wherein the at least on web server forwards the HTTP page request to the at least one web server using a separate secure session;

the at least one web server sending to the at least one SRP a response containing the requested HTTP page, wherein communication between the at least one SRP and the at least one web server is secure using the separate secure session; and

the at least one SRP caching the requested HTTP page for future requests.

47. A computer-readable medium, comprising executable instructions for caching secure content in computer network which, when executed in a processing system, causes the system to:

couple at least one Secure Reverse Proxy ("SRP") among at least one web server and at least one browser;

direct requests for establishing a secure connection from the at least one web browser to the at least one SRP, wherein the SRP responds by initiating an initial secure handshake;

establish a secure session between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an HTTP page request encrypted using a secure session protocol;

decrypt the HTTP page request at the at least one SRP, wherein the SRP examines a local cache to locate the HTTP page;

retrieve the HTTP page from the local cache;

encrypt the HTTP page from the local cache at the at least one SRP using the established secure protocol; and

send the HTTP page to the at least one web browser, wherein contact with the at least one web server is reduced improving the effective efficiency of the network.

48. The computer readable medium of claim 47, further comprising instructions that when executed in a processing system cause the system to:

forward the HTTP page request to the at least one web server using a separate secure session when the HTTP page is not present in the local cache;

receive from the at least one web server to the at least one SRP a response containing the requested HTTP page wherein communication between the at least one SRP and the at least one web server is secure using a separate secure session; and

cache the requested HTTP page locally at the SRP for future requests.

49. An electromagnetic medium containing executable instructions for improving secure connections in computer network communications which, when executed in a processing system, causes the system to:

couple at least one Secure Reverse Proxy ("SRP") among at least one web server and at least one browser;

direct requests for establishing a secure connection from the at least one web browser to the at least one SRP, wherein the SRP responds by initiating an initial secure handshake;

establish a secure session between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an HTTP page request encrypted using a secure session protocol;

decrypt the HTTP page request at the at least one SRP, wherein the SRP examines a local cache to locate the HTTP page;

retrieve the HTTP page from the local cache;

encrypt the HTTP page from the local cache at the at least one SRP using the established secure protocol; and

send the HTTP page to the at least one web browser, wherein contact with the at least one web server is reduced improving the effective efficiency of the network.

50. The electromagnetic medium of claim 49, further comprising instruction that when executed in a processing system cause the processing system to:

forward the HTTP page request to the at least one web server using a separate secure session when the HTTP page is not present in the local cache;

receive from the at least one web server to the at least one SRP a response containing the requested HTTP page wherein communication between the at least one SRP and the at least one web server is secure using a separate secure session; and

cache the requested HTTP page locally at the SRP for future requests.

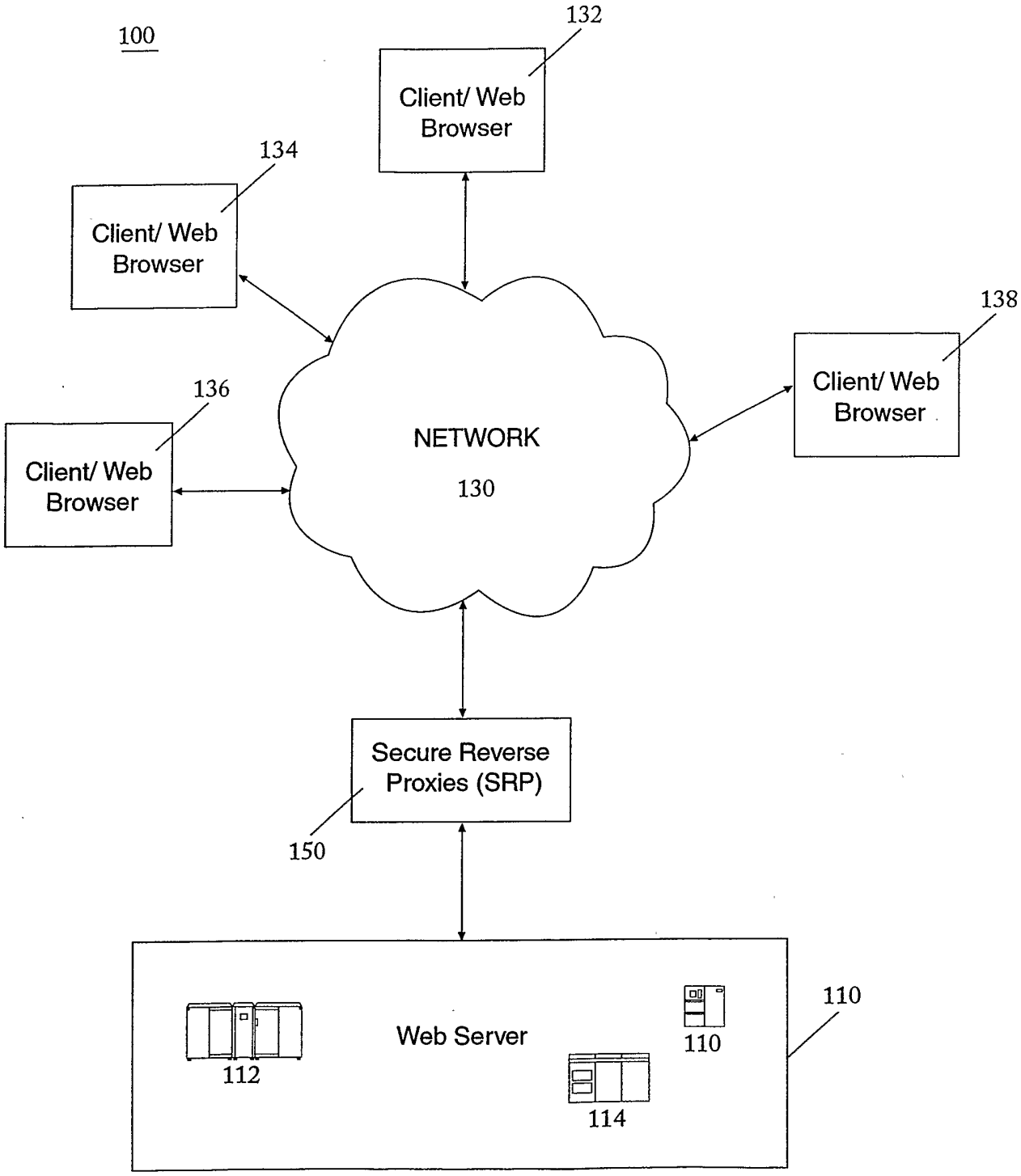

100
132
Client/ Web Browser
134
Client/ Web Browser
136
Client/ Web Browser
NETWORK
130
138
Client/ Web Browser
Secure Reverse Proxies (SRP)
150
Web Server
112
110
110
114

FIGURE 1

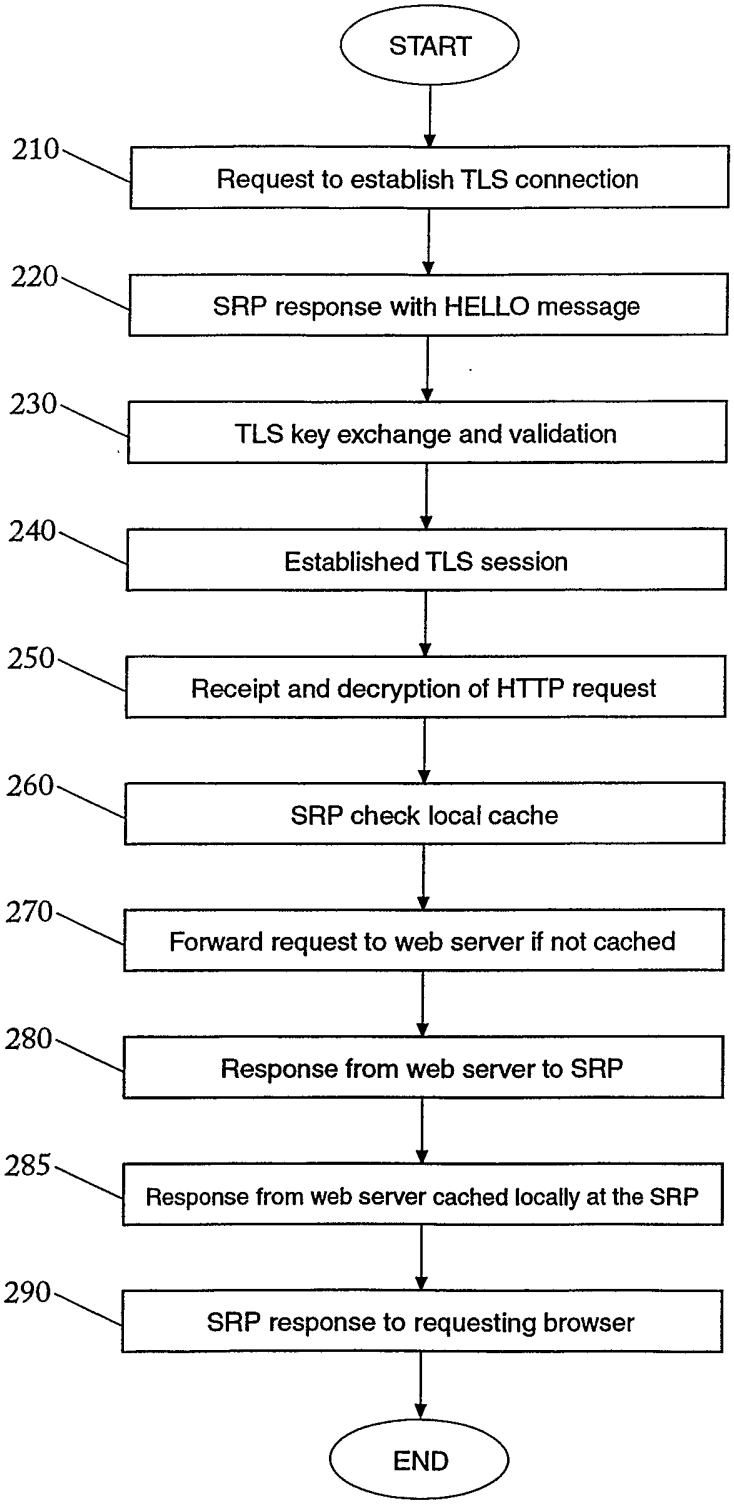

START
210
Request to establish TLS connection
220
SRP response with HELLO message
230
TLS key exchange and validation
240
Established TLS session
250
Receipt and decryption of HTTP request
260
SRP check local cache
270
Forward request to web server if not cached
280
Response from web server to SRP
285
Response from web server cached locally at the SRP
290
SRP response to requesting browser
END

FIGURE 2

INTERNATIONAL SEARCH REPORT

Inte | Application No
PCT/US 01/32361

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NETSCAPE: "Netscape Proxy Server 3.5 Administrator's Guide for Unix " NETSCAPE DOCUMENTATION, 'Online! 25 February 1998 (1998-02-25), XP002223540 Retrieved from the Internet: <URL:http://developer.netscape.com/docs/manuals/proxy/adminux/index.html> 'retrieved on 2002-12-04! Chapter 7, Secure Reverse Proxying Chapter 9, Chaching pages retrieved using HTTPS Chapter 14 --- -/--	1-50

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2002	19/12/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bertolissi, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr al Application No
PCT/US 01/32361

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 081 900 A (EBRAHIMI HASHEM M ET AL) 27 June 2000 (2000-06-27) abstract column 3, line 10 - line 65 column 6, line 40 -column 7, line 11 column 8, line 13 - line 46 column 10, line 5 - line 35	1-50
A	OPPLIGER R: "Authorization methods for e-commerce applications" RELIABLE DISTRIBUTED SYSTEMS, 1999. PROCEEDINGS OF THE 18TH IEEE SYMPOSIUM ON LAUSANNE, SWITZERLAND 19-22 OCT. 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 19 October 1999 (1999-10-19), pages 366-371, XP010357018 ISBN: 0-7695-0290-3 pag 367, 2. Certificate based authentication pag 369, col 2, lines 44-52	1-50
A	WO 01 03398 A (IBM UK ;IBM (US)) 11 January 2001 (2001-01-11) abstract	1-50

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter al Application No
PCT/US 01/32361

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6081900 A	27-06-2000	NONE	
WO 0103398 A	11-01-2001	AU 5554100 A	22-01-2001
		CN 1358386 T	10-07-2002
		CZ 20014650 A3	15-05-2002
		EP 1197052 A2	17-04-2002
		WO 0103398 A2	11-01-2001
		HU 0201706 A2	28-09-2002