2012 International Conference on Management and Education Innovation
IPEDR vol.37 (2012) © (2012) IACSIT Press, Singapore

An Overview of Hypertext Transfer Protocol service Security on Business Domain

Burra Venkata Durga Kumar[+]
Taylor's Business School, Taylor's University-Malaysia

Abstract. Network protocols define the way data is transported between computers in a networked environment. Network protocols completely hide business functionality from higher level services and protocols, which can simply assume that, by providing the assigned name of another computer and company can transit a message or open a continuous communication stream without dealing with the intricacies of data transport. Populates Internet began to grow rapidly like expands with new tools, that is the new standard Hypertext Transfer Protocol and Hypertext Markup Language were introduced to the public. Hypertext Transfer Protocol to make accessing information through the Transfer Control Protocol or Internet Protocol is easier than ever.
Hypertext Markup Language allows people to present information that is visually more interesting. Appearance of Hypertext Transfer Protocol and Hypertext Markup Language made people knows so popular, that is often considered synonymous with the Internet itself to the World Wide Web. The purpose of this paper is that knowing what kinds of security methods are appropriate for this Hypertext Transfer Protocol service and then explanations on World Wide Web and Hypertext Transfer Protocol works mechanisms. Proving the security methods of the answers obtained from what are assumed from the issues and included all models.

Keywords: Network Protocols, Hypertext Transfer Protocol, Hypertext Markup Language, Transfer Control Protocol, Security, Business.

1. Introduction

Nowadays, Internet service become very widely in business purpose and functionality, and for two popular internet services that common used by people, such as FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol). HTTP is similar to FTP in that it implements simple read/write data transfer of file over the network. The HTTP service provides a context to the receiving client to inform the client what type of data is contained in file transfer and therefore how data should be present to the user. HTTP clients called Web browsers, which interpret the transmitted files according to the MIME (Multipurpose Internet Mail Extensions) type to present HTML (Hypertext Markup Language), pictures, or other data type for which a registered browser plug-in is available [1]. A World Wide Web server provides a way to place documents like text, pictures, forms, and data of all kinds on a network for user to view and downloads, using a web browser such as Netscape navigator, Microsoft internet explorer, Opera, I cab, Hot java, Lynx, and others. We can place a web server on an intranet or an internet, where it is accessible to anybody with a computer and a web browser [2]. For examples, we might set up a customer data base and order entry system on company internet with a front end running from a web server. Company sales representatives would then use business web browsers to connect to all the customer information company need. Next on the Internet is a global network that connects a network with other networks around the world. TCP (Transfer Control Protocol) / IP (Internet Protocol) protocol into the link between networks vary around the world to be able to communicate. WWW (World Wide Web) is part of the Internet's fastest growing and the most popular.

[+] Tel: +603 5629 5681; Fax +603 5629 5141
Email address: BurraVenkata.DurgaKumar@Taylors.edu.my

WWW works Based on the following mechanisms:

1.1. Internet Protocol

Standard protocol rules in use to communicate on the computer networking, HTTP is a protocol for the WWW. A number of protocols are found in the internet layer, including the most important protocol in the entire suite, the internet protocol or known as IP. The transport layer cannot communicate at all without communicating through IP in the internet layer [6].

1.2. Address

WWW address naming rules of the web address: URL (Uniform Resource Locator) is used as the standard Internet address. The most fundamental element of the IP is the address space that IP uses. Each machine on a network is given a unique 32-bit address called an internet address or IP address [6].

1.3. Html

HTML is used to create a document that can be accessed via the web. HTML is the standard language used to display the document web. HTML is an easy-to-use language that the text files for display at web browsers. The main purpose at HTML is to allow clients to flip through web documents in a manner similar to flipping through a book, magazine, or catalog [9].

1.4. URL

URL is the basis for locating resources in WWW. URL consists of a string of character that uniquely identifies a resource. A client can connect to resources by typing the URL in browser window or by clicking on hyperlink that implicitly invokes a URL [9].

1.5. TCP/IP

TCP/IP is true client/server platform, and TCP/IP is also a cross-platform communication medium, and TCP/IP has a rich set of connectivity protocols. These include the FTP (File Transfer Protocol), the SMTP (Simple Mail Transport Protocol), and the TELNET (Terminal access protocol) [7].

1.6. Clients and Servers

Network has two categories of computers, those that access the networked resources (clients) and those that provide the resources (server). The clients are any PC or other computers system that make use at network resources is a clients or workstations or web browser. And the server is managing the network's shared resources. A small network may have only one server, but corporate setup may have loads, each performing a specific task [8].

2. Issues

Next on the security issues web server that included protecting the sever contents from being seen, preventing the contents from being changed or damaged, and protecting the server itself from damage as shown in the following situation:

2.1. Assumption of the server

Many web servers either contain or have access to sensitive data. A server used for electronic commerce may contain customer records and credit card information, all of which must be kept from prying eyes. If company server has different access levels, we might display same information to the general public, with other information available only to pay subscribers [2]. An important problem related to the client-server nature of the web is that a web server can easily become overloaded. A practical solution employed in many designs is to simply replicate a server on a cluster of workstations, and use a front-end to redirect client requests and get response from the server as shown in Figure 3, and next is the security issues based on assumption of the client which is company need to keep business data safely.

2.2. Assumption of the client

Client interacts with web servers through a special application know as a browser. Browser accepts input from a user mostly by letting the user select a reference to another document, which it then subsequently fetches and displays. This leads to overall architecture shown in Figure 1 [3] and the client can request each of these operations to be carried out at the server by sending a request message containing the operation desired to sever.

2.3. Assumption from both parties

All communication between a client and server takes place through messages. HTTP is just simple no security provided and HTTP allow only request and response messages. When a web browser requests some web peg and the web services will receive all information detected. In run the web receives all users or clients needed as shown in Figure 2 [3].

If the client and server need a simple to secure business data just using proxies and firewalls together, the great thing about using firewalls is that it is not an either or situation because the two products work at different stages of the user's access, company can be implemented on the same network as shown in Figure 4.

3. Models

3.1. Overall models

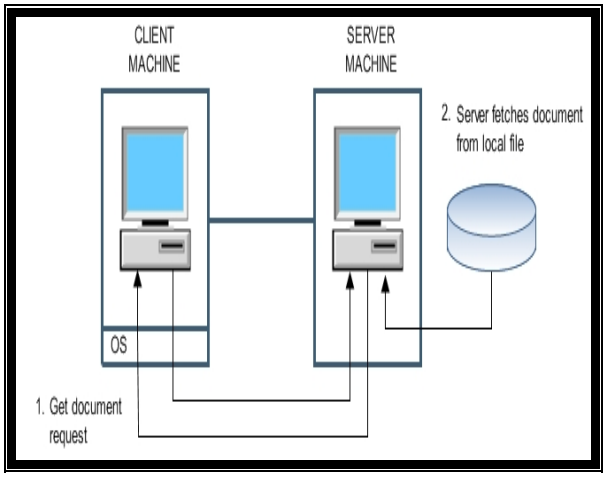


Figure 1.The overall organization

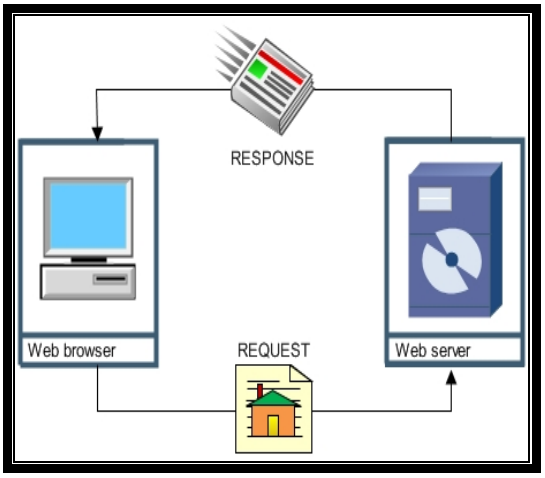
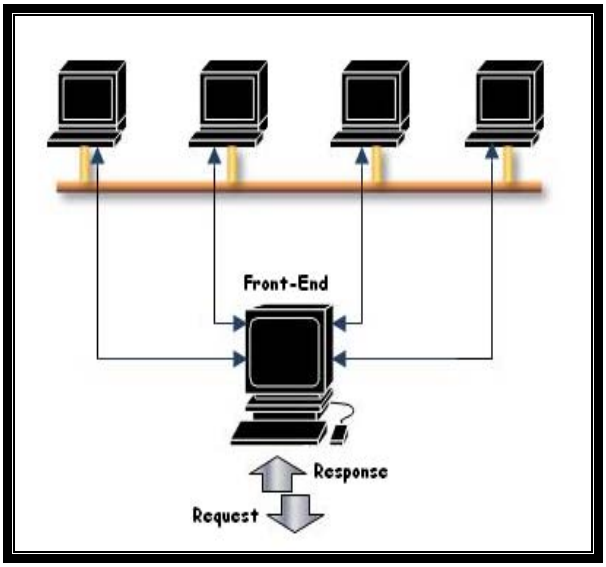


Figure 2: Request / Response cycle [3]

3.2. Solution Models



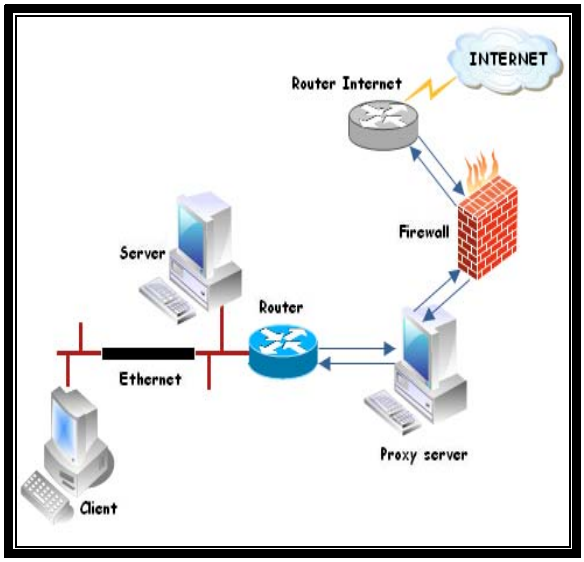
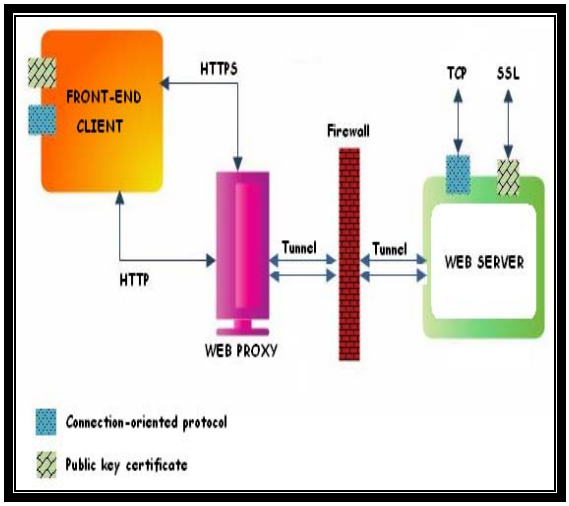


Figure 3: Using a cluster of workstations

Figure 4: Using proxy and firewall together [3]



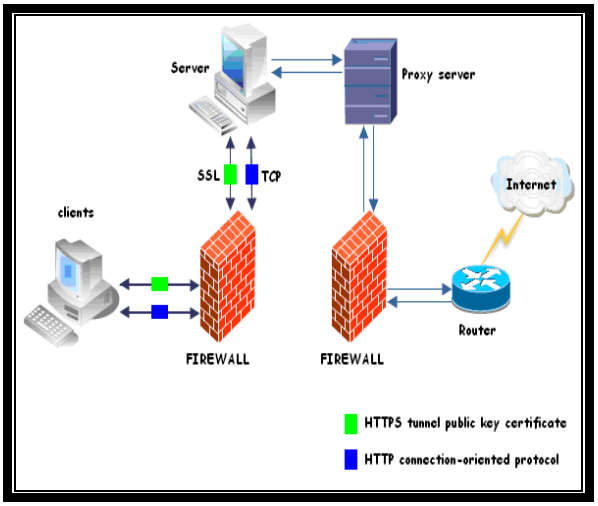


Figure 5.HTTPS and HTTP Client request (WAN) Figure 6.HTTPS and HTTP Client request

3.3. Definition Models

3.3.1 Overall models

Figure 1 show about Web browser uses HTTP to fetch the requested document from an appropriate website. Web browser a design to display information prepared in markup language, known as HTML. And then the server gives response from local file to client display. Figure 2 show about simple HTTP with no security provided and HTTP allow only request and response messages. When a web browser requests some web peg from the web server and client receive all information detected.

3.3.2 Solution Models

Figure 3 show the designs for the servers on a cluster to avoid overloaded documentation. And use a front-end to redirect client requests and get response from the server.

Figure 4 show about Using the proxies and then combination with the firewalls. These show how the local connection between the client request to server and then the server take information to internet by using proxy and firewall for security connection. Figure 5 shows about the main difference between HTTP and HTTPS connections from the web browser or client request for (WAN). And both connect to web proxy and then connect to web server. After server accept from both of the connection company will send the response with different front-end. Figure 6 show about the main difference between HTTP and HTTPS connections from the web browser or client request. And both connect to server and then connect to proxy server then take some information request from internet. After server accept from both of the connection company will send the response with different front-end.

4. Conclusion

All communication in the web between clients and servers is based on the HTTP. HTTP is a relatively simple client-server protocol. A client sends a request message to a server and waits for a response message. HTTP is base on TCP, whenever a client issues a request message along that connection. The same connection is use for receiving the response. By using TCP as its underlying protocol, HTTP need not be concerned about lost requests and response. Considering the open nature of the internet, devising a security architecture that protects and servers against various attacks is crucially important. Most of the security issues in the web deal with setting up a secure channel between a client and server. Author opinion about the server to secure business database and all documents safely, better company have to make HTTPS certificate that must be signed by a trusted certificate authority for the web browser to accept it. The upgrade message header is use to switch to another protocol. For example, client and server may use HTTP, when the client gives the request and the server may immediately respond with telling the client that it wants to continue

communication with a secure version of HTTP, such as HTTPS. In the case the server will send an upgrade message header with content “upgrade: HTTPS.” And HTTPS is combination of HTTP with SSL or TLS protocol which is included encryption and secure identification of the server as shown in figure 3. Or if the server and client need low cost to provide the security on HTTP, generally company just using the proxies and then combination with the firewalls. By using a firewall and a proxy server, the client can have control over who has access to the internet and what company can do once company get here, this tends to be the most comfortable level of internal internet security a client can have**.**

5. References

[1] Strebe, Matthew. (1999) “Net server 4 (24seven)”, United states of America: Network Press sybex,.

[2] Norton’s, Peter. Stockman, Mike (2000). “Network security fundamentals”, United States of America: Sam’s Publishing.

[3] Tanenbaum S, Andrew. Yansteen, Marten (2002). “Distribution systems: principles and paradigms”, vrije universities of Amsterdam, the Netherlands: prentice-hall, inc

[4] Baker H, Richard (1999) “Network security: how to plan for it and achieve it” Koga: McGraw-Hill international,

[5] Shapiro R, et al.,windows server (2003) bible, Canada: Wiley Publishing, Inc.,

[6] Rozell, Erik. Pablo, Mary.(2000) “MCSE test prop: TCP/IP, second edition” USA: new riders,

[7] Knnaman K, Dave (1999).” TCP/IP: accelerate MCSE study guide”, USA: the McGraw-Hill, Inc.

[8] Kendrick, Nigel. Meyers, Mike. (2002)” network +” , USA: the McGraw-Hill, inc. 2002.

[9] Umar, Amjad (1997). “Object-oriented client/server internet environments: the modern it infrastructure”, USA: Prentice Hall ptr, Inc.