Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Overview of World Wide Web Protocol (Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure)

Sh. Rajinder Singh
Research Scholar PUSSGRC,
Hoshiarpur, Punjab, India

Dr. Satish Kumar
Research Supervisor PUSSGRC,
Hoshiarpur, Punjab, India

Abstract— HTTP is the main protocol of World Wide Web. It allows communication between varieties of clients. With the help of HTTP web-server are used to communicate with the nowadays available browser like Google Chrome, Mozilla Firefox, and internet Explorer etc. HTTPS (Hypertext Transfer Protocol Secure) is also used for the same purpose as HTTP but with additional features. In this paper a detail study of both the protocols has been made. Various features of both the protocols are also discussed.

Keywords: HTTP; HTTPS; SSL;

I. INTRODUCTION

HTTP and HTTPS both the protocols are used by the web browser to transmit and receive information on the internet. HTTP means Hypertext Transfer Protocol and it is used for exchanging information between the web-server and client. This protocol is used for delivering virtually all files like image files, text files and video files etc. With the help of HTTP web-server communicate with the browser like Google Chrome, Mozilla Firefox, and internet Explorer etc. HTTPS means hypertext transfer protocol secure and it is used to establish secure connection across the internet. Communications between the client side browser and web-server is encrypted by a secure certificate known as an SSL. This encryption of the information helps from preventing sniffing of the information by hackers [1].

II. WHAT IS HTTP?

HTTP is the main protocol used by World Wide Web for communication. HTTP defines how the messages are formatted and transmitted across the internet. HTTP protocol is based on client server model. A browser is like client because it is used to send request to server. Server then sends the response back to the client. The default port for the server to listen for the request is 80. HTTP protocol is a request/response stateless protocol [2]. Main function of HTTP is to transmit resources across the internet. A resource can be a file, A CGI script, or a document written in any available languages. The format of the request and response message is very much similar.

An HTTP request has mainly three parts: a) request line, b) HTTP header, and c) an optional HTTP body.

An example of HTTP request is given below

GET /xyz1.html HTTP/1.1

Means client is instructing the server to GET the xyz1.html file by using HTTP/1.1 protocol.

Next information needed by server is HTTP header. HTTP header contains the information about the request and information about the client such as browser type or connection information.

Final part of the HTTP request is HTTP body which is optional. It is used when client want to transfer specific data to server [3][12].

Main Features of HTTP:

Main features of HTTP are given below:

a) HTTP is connectionless protocol. It means client or a browser makes an HTTP request and then it disconnects from the server and waits for response from the server. The server after processing the request sends response back to the client.
b) HTTP is media independent protocol means any type of data can be sent by HTTP.
c) HTTP is stateless protocol means the server and client are in touch with each other only during current request [12].

Main methods used by HTTP are i) GET ii) HEAD iii) POST

GET: It is the most common method used by HTTP. It is used to retrieve the requested information. If the requested file is an HTML file then its content will be displayed at the browser side. If the requested file is a dynamic ASP file, then the server first process this file, executes its commands and finally the output of those command is send to the requesting Browser.

HEAD: This method is almost similar to GET method but it does not return the requested data. It is used to transfer header section, status line, server response code etc.

POST: This method is used to send data to server and then act on it. POST methods are used when the CGI or server side scripting is involved [11].

III. HTTPS (S FOR SECURE)

HTTPS (Hypertext Transfer Protocol Secure) is used for achieving security of data across the internet. It is combination HTTP with SSL/TLS protocol. HTTP is not a secure protocol. So when users communicate across the network by using HTTP protocol, anyone can eavesdrop communication between client and the web server easily. So if users want to transfer sensitive information across the internet, then this information needs to be secured and it should be accessible to authorized users only. For these purposes HTTPS is used [5][10].

Mainly HTTPS protocol is used in the following websites:
Shopping Websites, Banking Websites, Payment Gateway, Login Pages, and Email Apps etc [6].

IV. WORKING OF HTTPS

HTTPS protocol is used to provide secure connection between client and web server. HTTPS insert a layer of encryption/decryption between HTTP and TCP. It is a Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

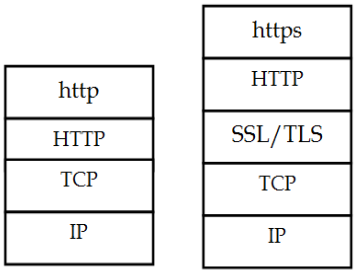

Figure 1 SSL/TLS Layer between HTTP and TCP

SSL uses RSA and public-key cryptography [7]. Pictures given below show facebook and gmail websites both are using HTTPS protocol. Important point to note here is that in this case URL starts with HTTPS:// and not with HTTP://

Figure 2 facebook using https

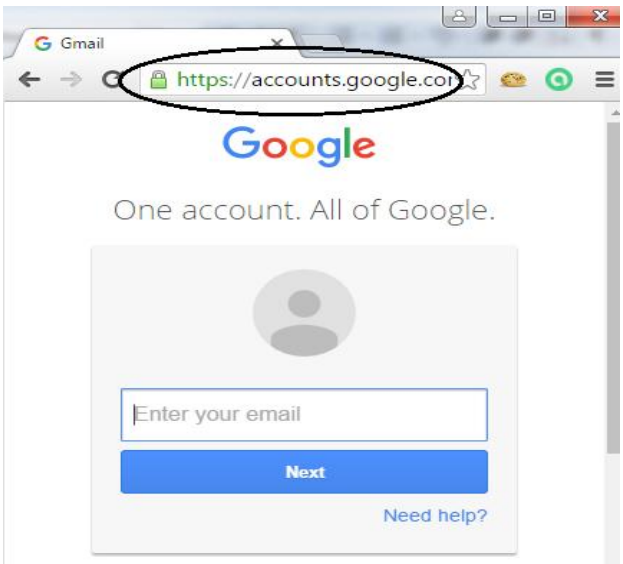

Figure 3 gmail using https

The SSL layer serves two main purposes

i) Verifying that client browser is communicating to the authenticated server .
ii) Ensuring that only server is able to read client's data and only client is able to read data sent by server.

So main function of SSL is to encrypt data between the server and client. If in case anyone is able to intercept data, he is still not able to read actual data [8].

Picture given below shows content of a packet captured by wireshark when the communication is taking place with HTTPS protocol

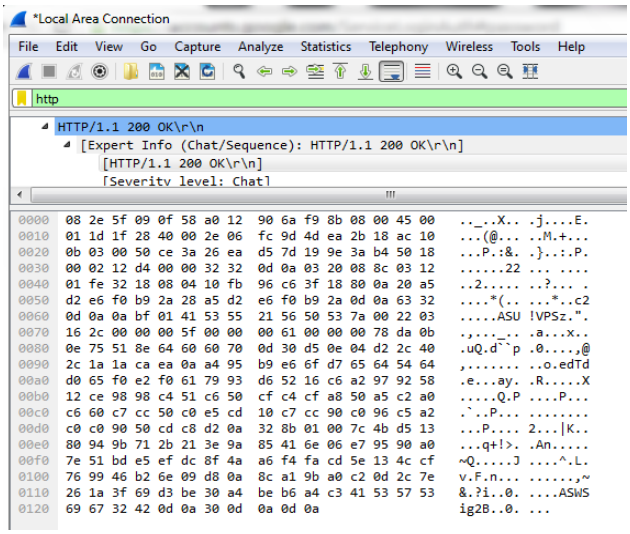

Figure 4 content of a packet

Connection between a client and server is set by a handshake which ensures that

i) client is talking to the right server and server is talking to the right client.
ii) to make an agreement on the encryption algorithm client and server will use to exchange the data
iii) an agreement on the necessary keys that will be used by this algorithm [8] .

Main steps which are followed during https connection are given below:

i) client request a secure page by typing https:// in the browser.
ii) server then sends public key, and its certificate.
iii) browser verify the certificate: checks that it is not expired and it is issued by a trusted party
iv) browser then creates a Symmetric key and send to server.
v) server decrypt this key with its private key
vi) server then sends the requested page to the client encrypted with symmetric key
vii) browser then decrypt the received page with the symmetric key and display the result to user [6].

V. NEED OF CERTIFICATE

When client and server are connected with HTTP protocol then data is transmitted across the network in plain text and it can be read by any hacker if he is able to sniff data. So if a user is sending his personal information across the network then it is not secured. When the client and server are using HTTPS protocol then all the communication across the network is encrypted. So even in case an attacker is able to sniff data he/she has to decrypt it first [9].

A picture of certificate for website facebook is shown below:

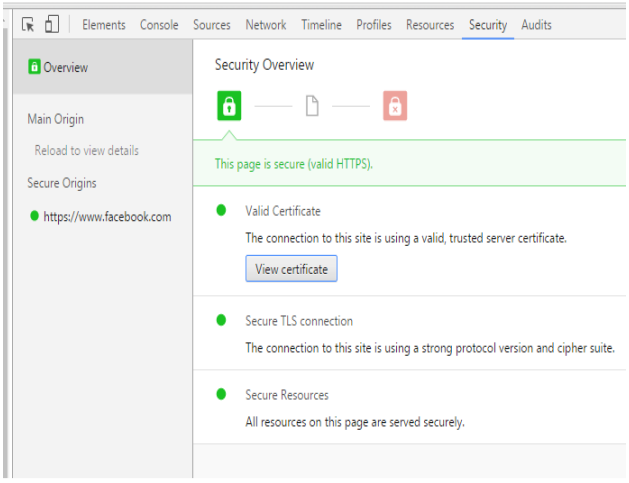

Figure 5 Viewing HTTPS certificate

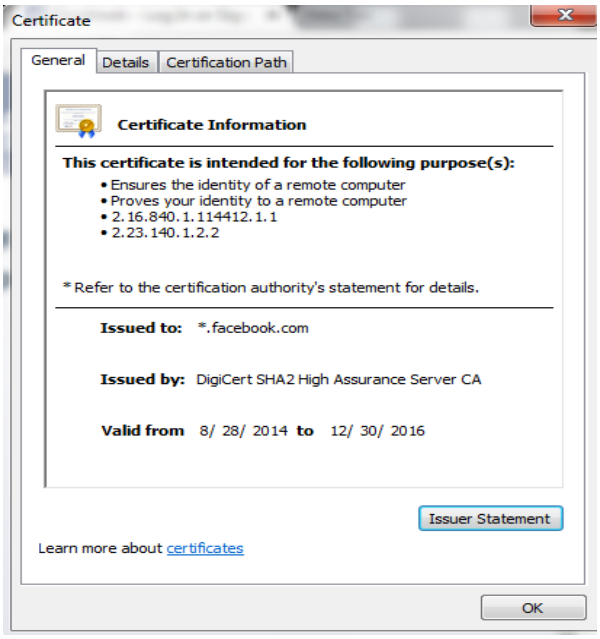

Figure 6 facebook certificate

VI. DIFFERENCES BETWEEN HTTP AND HTTPS

a) HTTP protocol use port 80 for communication. HTTPS uses port 443 for communication.
b) In case of HTTP URL starts with http:// whereas in case of HTTPS URL starts with the https://
c) HTTP is unsecured whereas HTTPS is secured.
d) In case of HTTP no certificates are used but in case of HTTPS certificates are used.
e) In case of HTTP information is passed as a plain text across the network but in case of HTTPS data is encrypted.

VII. CONCLUSIONS

HTTP is useful when user is only intended to access the information from a given website. But it is not safe for the user to transfer his personal information using HTTP. HTTPS protocol is helpful for the users when users want to send their personal information across the internet. HTTPS is not unbreakable but it is still a robust way to send personal information across the internet.

REFERENCES

[1] http://www.thewindowsclub.com/difference-http-https
[2] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[3] http://www.jmarshall.com/easy/http/
[4] http://www.tutorialspoint.com/http/http_overview.htm
[5] http://www.brighthub.com/internet/web-development/articles/105799.aspx
[6] http://www.tutorialspoint.com/security_testing/https_protocol_basics.htm
[7] http://code.tutsplus.com/tutorials/http-the-protocol-every-web-developer-must-know-part-2--net-31155
[8] http://robertheaton.com/2014/03/27/how-does-https-actually-work/
[9] https://www.instantssl.com/ssl-certificate-products/https.html
[10] Naylor, David, et al. "The cost of the S in HTTPS." Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. ACM, 2014.
[11] Berners-Lee, Tim, Roy Fielding, and Henrik Frystyk. "Hypertext transfer protocol--HTTP/1.0." (1996).
[12] Yannakopoulos, John. "Hypertext Transfer Protocol: A short Course." University of Crete. August (2003).

