Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Review of Role of SSL in Cyber Security

Er. Prabhjot Kaur
Research Scholar, Department of CSE
SBBSU, Padhiana
narwalprabhjot@gmail.com

Er. Gurjeet Kaur
Assistant Professor, Department of CSE
SBBSU, Padhiana
gurjeetminhas@gmail.com

***Abstract*- The world is becoming more interconnected with the arrival of the Internet and new networking technology. The number of internet users increasing day by day; there is increase in online transactions. As more number of websites are coming up with easy facility of transmitting information it has been seen that it has lead to substantial increase in fraud. A wide spectrum of e-commerce (B2B/B2C), banking, financial trading and other business applications require the exchange of data to be highly secure. The Secure Sockets Layer (SSL) protocol is the most popular protocol used in the Internet for facilitating secure communications through authentication, encryption, and decryption.**

***Keywords*- Cyber security, SSL, SSL to secure transaction, SSL Certificate**

INTRODUCTION

A. Security Concepts : -

As internet has become a part of our daily life, the need of cyber security has also increased. As more and more users connect to the internet it attracts a lot of criminals. Cyber security/ Internet security refers to protecting the website domains or servers from various forms of attacks by criminals. Cyber security is very useful in every field of today's world such as military, government and even in our daily lives. [1] Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of cyber security. Billions of dollars of transactions happens every hour over the internet, this need to be protected. Even a small unnoticed vulnerability in a network can cause serious damage. In every field of Internet, whether it is financial, personal or business everyone wants to know whom they are communicating with, ensuring that their data can be sent securely, and whether it has reached the destination correctly. Cyber security is the continuing effort to protect electronic data and computer systems from unwanted intrusions. Transmission of data over a network implies a possible loss of confidentiality, message integrity or endpoint authentication. [2]

There are mainly three major aspects that have to be considered when speaking about data security:-

1) Confidentiality: - Confidentiality is a set of rules that limits access to information. We can say that confidentiality is equivalent to privacy.

2) Message Integrity: - The user wants integrity of its data that is what is received is what is sent. It is basically the assurance that the information is trustworthy and accurate. [3]

3) Endpoint Authentication: - The user wants to be sure that he is communicating to the right person. Authentication provide this surety to the user that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

4) *Encryption:*- Encryption *is* the process of encoding a message or information in such a way that only authorized parties can access it that is unauthorized access are prevented. Information or message referred as plaintext in encryption can be encrypted using an encryption algorithms, these encryption algorithm generates cipher text that can only be read by the authorized person by using decryption algorithms. The scheme of using the same key for encryption and decryption is often referred to as Secret Key Cryptography (SKC).

5) Symmetric key: - In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties that wants to transfer data must have the same key before they can achieve a secure communication.

6) Public key: - In public-key encryption schemes, the encryption key are published for anyone to use and encrypt messages. But, only the receiving party has access to the decryption key that enables messages to be read. [4]

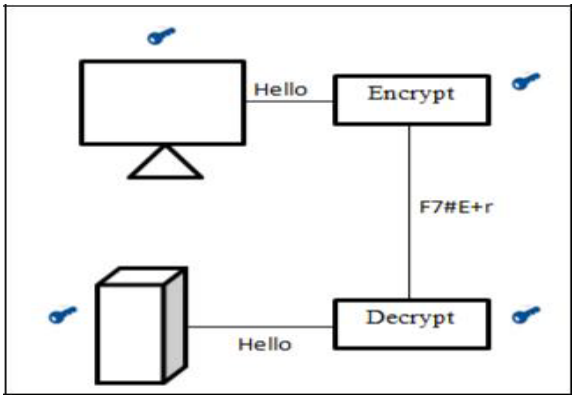

Figure 1: - Secret key cryptography

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

B. Overview of SSL

One of the most important components of online business is creating such an environment where potential customers feel confident in making purchases. The SSL (Secure Socket Layer) protocol is used for this purpose. It was developed by Netscape Communications in the 1990s. The company wanted to encrypt data in transit between its flagship Netscape Navigator browser and Web servers on the Internet to ensure that sensitive data/information, such as credit card numbers, social security numbers, and login credentials were protected**.** Thus, Secure Socket Layer is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server for communication, so that any information exchanged is protected within the secured tunnel. It uses s TCP to provide end –to-end secure services. [5]

II. HOW SSL SECURE A TRANSACTION

SSL protocol uses a combination of public-key and symmetric-key encryption to secure a connection between two machines that can be a Web or mail server and a client machine, communicating over the Internet or an internal network.

SSL runs on the transport layer and the network layer. These layers are responsible for the transportation of data between the processes and the routing of network traffic between the processes and the routing of network traffic. SSL basically consists of two phases: handshake phase and data transfer phase. [6]

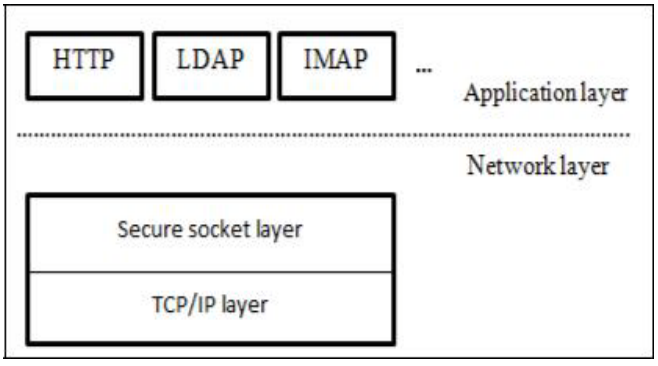

Figure 2: - Location of Secure Socket Layer

Both the client and server use a public key encryption algorithm to determine secret-key parameters during the handshake phase. In the second phase that is transfer phase, however, clients and server use secret key to encrypt and decrypt successive data transmissions. [7]

The client will initiate the SSL handshake connection by first sending a Hello message. The hello message contains a list of the secret-key algorithms, called as cipher specs, which the client will support. On the other side of the connection, the server will respond with a similar Hello message, selecting its own preferred cipher spec.

Following the Hello message, the server sends a certificate that will contain its public key. A certificate is simply a set of data that validates the server's identity. The certificate contains information such as server's ID, its public key, and several other parameters. Certificate authority generates (CA) generates the certificate and verifies its authenticity. In order to obtain a certificate, a server must use secure channels to send its public key to a CA. After the CA generates the certificate, which contains its own ID, the server's ID, and the server's public key and other information, it uses a message digest algorithm to create a certificate fingerprint. The message digest takes a given stream of data and produces a deterministic, fixed-length output. Then, CA encrypts fingerprint with its private key to create the certificate signature. In order to validate the server's certificate, the CA's public key must first decipher the signature and read the pre-calculated fingerprint. Then the client independently computes the certificate's fingerprint. If the two fingerprints don't match, the certificate has been tampered with.

The client should maintain a list of trusted CAs and their public keys. This will ensure that whenever the client receives a server's certificate, it verifies that the CA signing the certificate belongs to its list of trusted CAs. As soon as the client authenticated the server, both of them can use public-key algorithm to determine secret-key information. In order to complete the handshake phase with finished messages, and the connection enters the data transfer phase, both client and server need to indicate their readiness to begin using the secret key. [8]

There may be some overhead during transaction that is only due to the SSL handshakes. Handshakes are lengthy and drastically increase the number of round-trips required for a HTTPS session over a HTTP one. Hence, cause some overhead.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

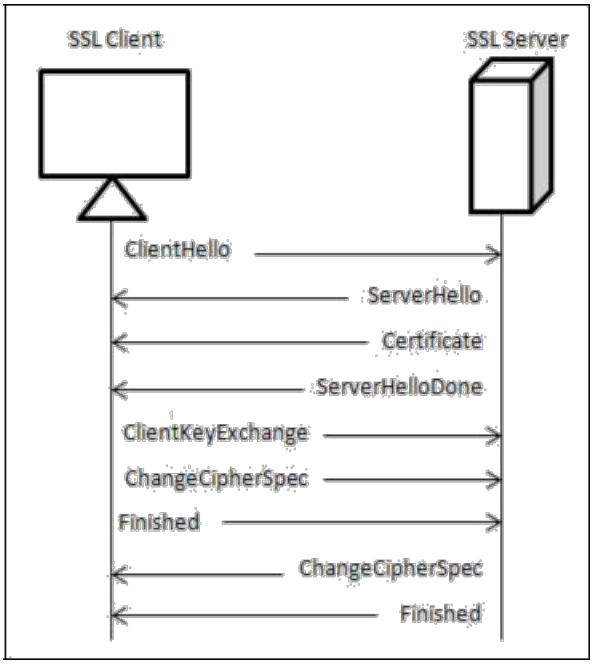

Figure 3:- Handshake and data transfer phases.

III. SSL CERTIFICATE

SSL Certificates basically are small data files that digitally bind a cryptographic key to an organization's details that can be individual or organization that uses them. It provides the individual or organization's name, location, email address, server name and the dates during which the certificate is valid. However, it is relatively easy for an organization to create a certificate with seemingly authenticate information, regardless of their true identity. To overcome this, Certificate Authorities (CA) were created. In order to certify a certificate, the certificate Authorities will investigate the identity of the requester and, if satisfied, "sign" the SSL certificate. [9]

SSL Certificates bind together: - A domain name, server name or hostname for which the certificate was issued and an organizational identity (i.e. company name) and location. It also contains the validity dates of the certificate.

An organization needs to install the SSL Certificate onto its web server to initiate secure sessions with the browsers. Once installed, it is possible to connect to the website over the domain as this tells the server to establish a secure connection with the browser. When SSL Certificate is installed on any of the web server, it activates the padlock and the https protocol and allows secure connections between web server and a web browser. [10]

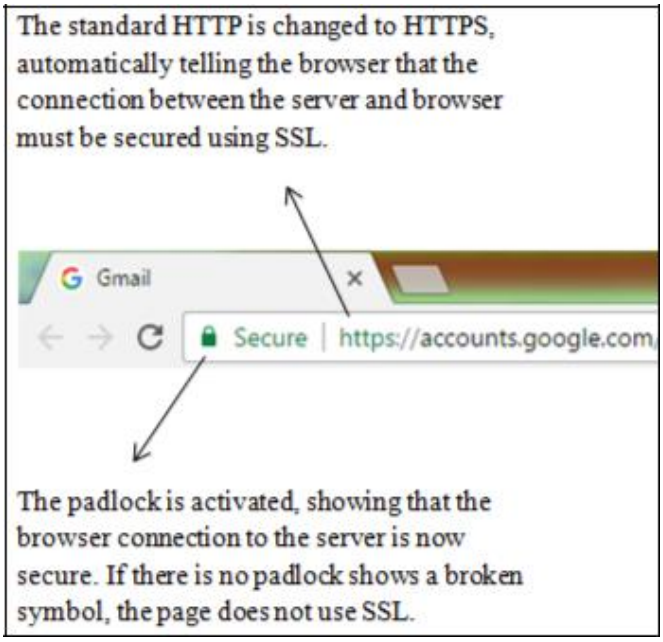

Figure 4:-SSL Certificate.

Installing a digital certificate on the web server lets you:

1) Authenticate your site: -. A digital certificate on your server automatically provides your site's authenticity to visitors' web browsers, confirming that the visitor is actually communicating with you, and not with a fraudulent site stealing credit card numbers or personal information.

2) *Keep private communications private*: - A digital certificate encrypt the data in such a way, that the visitor's exchange with your site is safe from interception using SSL technology, the industry standard method for protecting web communications. [11].

Once a secure connection is established between web server and a web browser, all web traffic between the web server and the web browser will be safe. Certificate lets you securely exchange your sensitive information online and increase your business by giving your customers confidence that their transactions are safe.

IV. CONCLUSION

In this paper, we focus on SSL because it can secure millions of peoples' data every second, during online transactions or when transmitting confidential information over Internet. With the data encryption up to 256-bits, SSL protocol converts data into virtually incomprehensible code that is safe from hackers and identity thieves and increases the confidence of users during transactions. It also provides confidence in the integrity and security in online business and network infrastructure. Thus, we can say that SSL is the backbone of secure Internet.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

REFERENCE

[1] Kartikey Agarwal and Dr. Sanjay Kumar Dubey, " Network Security : Attacks and Defence."

[2] Mr. Pradeep Kumar Panwar and Mr. Devendra Kumar," Security through SSL ." in International Journal of Advanced Research in *Computer Science and Software Engineering Volume 2, Issue 12, December 2012.*

[3] Confidentiality integrity and availability CIA http://whatis.techtarget.com/definition.

[4] Encryption and secret key cryptography cryptography/www.wikipedia.org.

[5] Network Security: History, Importance, and Future by University of Florida Department of Electrical and Computer Engineering Bhavya Daya.

[6] Mohammed A. Alnatheer , " Secure Socket Layer (SSL) Impact on Web Server Performance ." in *Journal of Advances in Computer Networks, Vol. 2, No. 3, Sept 2014.*

[7] K. Kant, R. Iyer, and P. Mohapatra, "Architectural impact of secure socket layer on internet servers: A Retrospect" in *Proc. International Conference on Computer Design*.

[8] K. Kant, R. Iyer, and P. Mohapatra "Architectural impact of secure socket layer on internet servers" in Int. Conf. on Computer Design, pp. 7-14, 2000.

[9] SSL Certificate Explained by Scion Solutions Ltd.

[10] SSL Information Center/What is an SSL Certificate- https://www.globalsign.com/en-in.

[11] MS.Bhiogade Patni Computer Services, Secure Socket Layer InSITE - "*Where Parallels Intersect*" June 2002.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)