INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY PROTOCOLS FOR INTERNET: A REVIEW

ER. AMRINDER KAUR

Assistant Professor, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra

Accepted Date: 27/01/2016; Published Date: 01/02/2016

Abstract: - Today computer and Internet is ubiquitous. Due to invent of new applications everyone is trying to be up to date with technology and every individual, organizations and institutes are sharing their sensitive information on the internet. Securing all this information is very tedious task. Internet services like email, electronic commerce, online stock trading etc. have various security measures. Many organizations secure themselves with the help of firewalls and authentication methods. But internet is not fully secure and reliable, for the security of information various protocols like Secure Socket Layer (SSL) later known as Transport Layer Security (TLS) protocol, for electronic payment system; Secure Electronic Transaction (SET) protocol is available. This paper will explain how internet works, working of SSL/TLS and SET and their comparison.

Keywords: Internet, TCP/IP protocol, SSL/TLS protocol, SET protocol.

Corresponding Author: ER. AMRINDER KAUR

Access Online On:

www.ijpret.com

How to Cite This Article:

Er. Amrinder Kaur, IJPRET, 2016; Volume 4 (6): 64-73

PAPER-QR CODE

1. INTRODUCTION

Internet is network of different networks i.e. LAN, MAN, WAN, public networks, private networks etc. Each system on the network have different hardware and software configurations and when there is need of computer to computer communication then some universal translator must be present, who facilitate the communications between different computers and the answer to this need is Internet protocol, which define the abstract model of communication. In daily schedule, web is used by almost every individual to perform activities like online shopping, online payments, cash transfer etc. and input to these transactions are highly confidential.

1.1. Basic concepts for working of Internet:

Main content in internet communication is client (web browser) and server (web server). Communication between client and server is possible with the help of hypertext transfer protocol i.e. HTTP. Client or web browser sends http request to the web server and then server respond back with http response. Basic element of communication is web pages. Web pages are categorized into static web pages, dynamic web pages and active web pages.

Static web pages are those whose content are unchanged or constant. These pages are created by application developer and then stored on the web server. When a client requested for a page, server send back the page without performing any additional processing. Contents on web pages never changed they remain always same. Dynamic pages are those whose content are changing or lively. Content of these pages vary continuously depending on the parameters. For example online stock prices, weather forecasting etc. Dynamic pages are complex as compared to static web pages and it involves server side programming. Active web pages are similar to other web pages but it contains a small program which execu**tes** on client computer inside its web browser. For example java applets, which is a client side program and is used to perform variety of tasks like painting of charts, graphs, images and other drawing objects on client side.

1.2. Transmission Control Protocol/ Internet Protocol (TCP/IP)

As internet is collection of computer and network. Computer and network in internet have different hardware and software configuration. For facilitate communication between different system there must be universal translator that is able to hide the entire configuration. Protocol defines an abstract model for communication and it is independent of all physical characteristics of computer and network.

The most popular software translator is TCP/IP. It is blend of numerous protocols and enables communication among computers on network. TCP/IP supports different applications like email, file transfer, remote login etc. It also state how browser identify a server, how server will respond to client request and so on. TCP/IP protocol suite consists of five layers i.e. physical layer (PL), data link layer (DLL), internet layer (IL), transport layer (TL) and application layer (AL) which are responsible for communication between networks. Each layer is responsible for perfoming some specific task. For example all application programs like email, http, smtp, telnet etc are part of application layer.

For communicating a message, initially application layer on sender machine interact with transport layer which interact with network layer on the same machine, which in turn interacts with data link layer and finally data link layer interacts with physical layer. Physical layer is responsible for physical transmission of messages. On receiver side reverse process of sender side take place. Intermediate node is only responsible for forwarding information between sender and destination as shown below in figure 1.

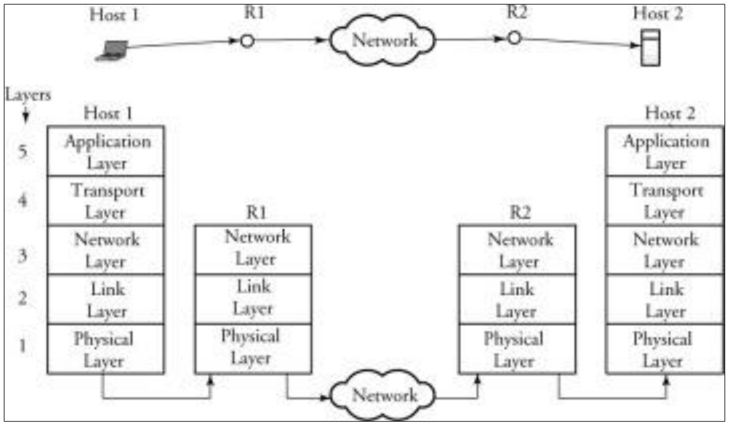

Figure 1: TCP/IP communication model using intermediate nodes

2. SSL (Secure Socket Layer) and TLS (Transport Layer Security)

Secure Socket Layer was developed by Netscape Corporation in 1994. It is most popular web security mechanism. SSL is supported by almost every web browser. SSL comes in three version in which version 3 is most popular and it was released in 1995. In TCP/IP protocol suite, SSL layer is positioned amid transport layer (TL) and application layer (AL). TLS is an IETF standardization initiative. It provides authentication service. Netscape goal is to standardize SSL and handed protocol over to IETF.

SSL provide end to end reliable communication by using TCP. SSL perform encryption on the data which is received from application layer and add its own header i.e. SSL header to the encrypted data. [1][2]

2.1. Working of SSL

SSL is two layer protocols as shown in figure 2 below. SSL record protocol is responsible to provide security services to higher layer. Specifically Hyper Text Transmission Protocol (HTTP) operates on the peak of SSL and its responsibility is to provide transfer services for web client/ server interaction

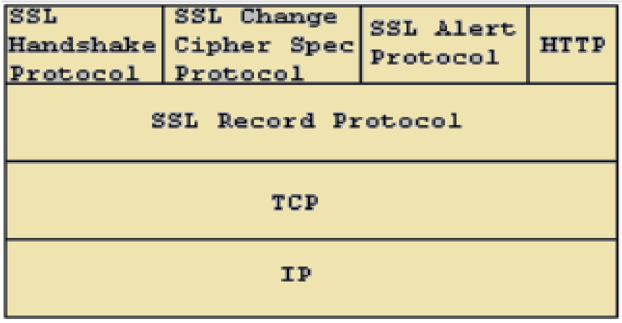

Figure 2: SSL Protocol Stack

SSL consists of three higher layer protocols namely the Handshake Protocol, the Change Cipher Spec Protocol, and the Alert Protocol. But two important concepts are SSL session and SSL connection. Connection provides a suitable type of service for transport. SSL connections are transient and have node to node relationship. Whereas session is created by handshake protocol and it is an association between client and server.

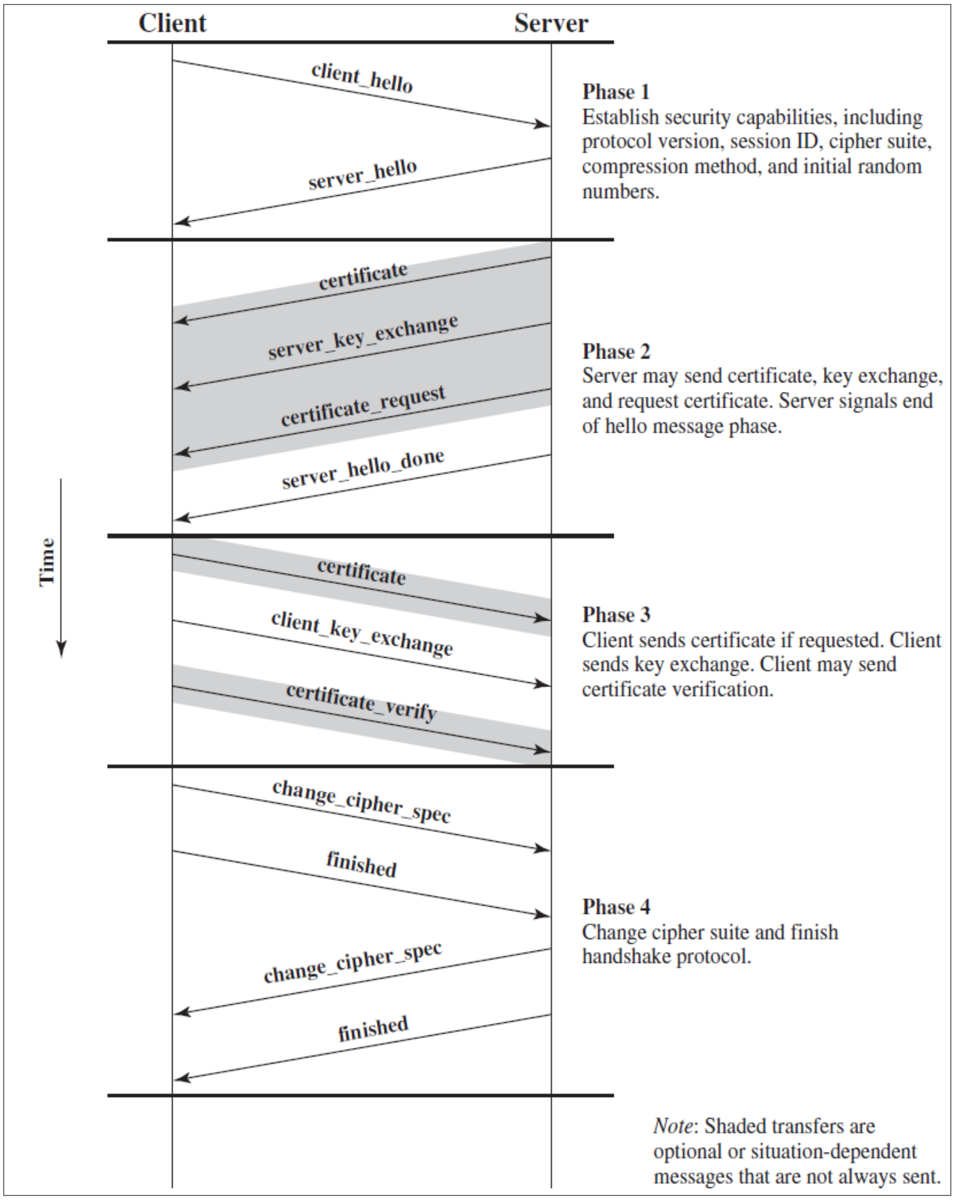
Client
Server
client_hello
server_hello
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Phase 4
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Figure 3: Handshake Protocol

Handshake is the first sub protocol used by server and client for communication using SSL enabled connection. In this, initially authentication of one another is done by server and client and then settlement on an encryption algorithm, MAC algorithms and cryptographic keys. Then decided keys are used to protect data sent in an SSL record. Handshake protocol is made up of four phases i.e. establish security capabilities, server authentication & key exchange, Client authentication and key exchange and finish and messages exchanged while establishing a connection is shown in figure 3 above.

2.1.1. The Record Protocol

After successful handshake between client and server, record protocol comes into picture. Record protocol offers two security services i.e. confidentiality and integrity of messages. Confidentiality of message is guaranteed by using encryption key decided in handshake protocol. Whereas message integrity is guaranteed by shared secret key and this key is used to generate a message authentication code (MAC).There is one more protocol change cipher spec protocol that uses SSL record protocol. This protocol uses single byte with the value 1 in single message. The purpose of this message is to copy the pending state into current state, which is responsible to update cipher suite used for the connection.

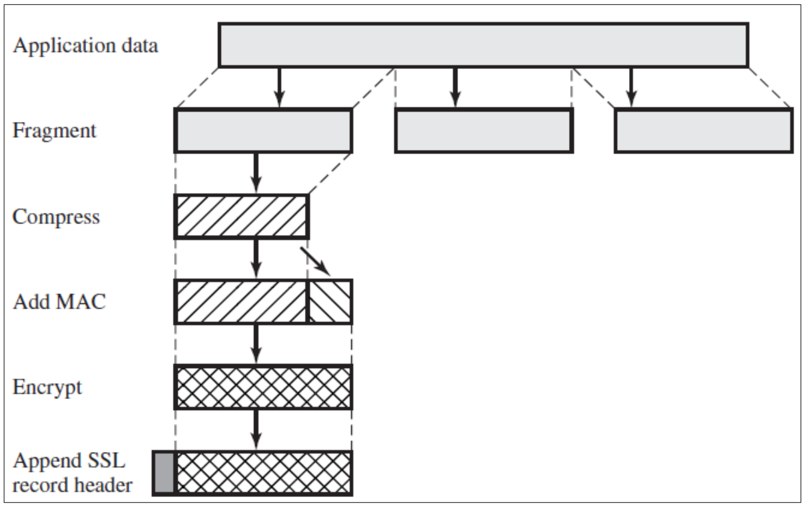

Figure 4: SSL Record Protocol

Application message is act as input in record protocol. This application data is first divided into fragments of size 2^{14} bytes or less. Next step is compression which is optional and if compression is done then it should be lossless i.e. originality of data is preserved. Then message authentication code of each block is calculated which is done with the help of shared secret key. Next step in record protocol is encryption which is done using symmetric key, decided during handshake protocol. Last step in record protocol is addition of SSL record header to the encrypted data. This header contains content types, different versions, compressed length etc.

Resulting unit is then transmitted using TCP segment and reverse process will be performed on receiver side as shown in figure 4 above.

2.1.2. Alert Protocol

Alert messages are either communicated by client or by server. When some error is detected by either peer then detecting party send alert message to other party. If the detected error is fatal then both parties immediately close the SSL connection and before closing the connection session identifier, keys and secrets associated with the connection is destroyed. If the detected error is not severe then parties handles the error and continue with their communication.

In alert protocol there is alert message which consists of 2 bytes. First byte defines the type of error and second byte specifies the actual error. If first byte contains 1 then it is a warning and if it contains 2 then the error is fatal. Fatal errors can be unexpected message, bad record MAC, decompression failure, handshake failure, illegal parameters and certificate expired etc.[1][2][3][5]

3. Secure Electronic Transaction Protocol

E-commerce is geared up by the popularity of the internet. SSL is effective and accepted as online payment standard but it requires client and merchant to trust each other. Whereas Master & Visa card and other 11 companies want some standard for internet transactions.

Secure electronic transaction protocol is most widely used on internet for protecting the electronic transactions like credit card payments on the internet. It is not a payment system rather it is a set of security protocols that enables the user to use the existing payment system in a secure manner on the internet. SET provides authentication by the use of digital certificates. It also ensures confidentiality, because information is only available to the parties which are involved in the transaction.

SET participants are cardholder, merchant, issuer, payment gateway, certification authority. Card holder is an authorized holder for payment card such as credit card, visa card & master card. Merchant is an individual or an organization who wants to sell products and services. Issuer is the financial authority like banks that provide the payment card to card holder. Payment gateway processes the message of payment and it act as an interface between SET and existing payment gateway and the duty of certificate authority is to provide public key certificates to all those participants which are involved in the transaction like cardholder, merchant, payment gateway etc.[6][7]

3.1. SET Process:

Secure electronic transaction protocol have various steps while purchasing some goods and services. The very first step is customer opens a credit card account with the bank and this account supports online payment mechanisms. After opening an account customer get a digital certificate from certificate authority by verifying their identity. Identity can be verified by passport, voter id, business documents etc. Similarly merchant of products and services also possesses digital certificate from certificate authority. After this customer browse the list of available item to search the required item, after that select one or more item from the available list and then places the order. After that an order form is returned back to customer who contains details of no. of items, quantity, price, total bill etc. for the record of customer. Simultaneously merchant also sends its digital certificate to the customer which authenticates the merchant. Now customer confirms the order by sending the order and payment details to the merchant. Along with these documents customer also send his/ her digital certificate to the merchant. The payment contains credit card details in encrypted form and this information is not available to merchant. This payment information is forwarded by merchant to payment gateway and requests the gateway to verify the payment by ensuring the credit card is valid. After getting the detail of credit card, the payment gateway verifies the detail of customer with the help of issuer. If details are correct then payment is authorized otherwise the payment is rejected. After confirmation from payment gateway, merchant sends a confirmation of the order to the customer. After all formalities goods are packed and shipped to customer address as per the order of customer.[6][7]

4. Comparison between SSL and TLS, SSL and SET:

The comparison of SSL & TLS, SSL & SET is shown in table below [3][4]:

Property	SSL	TLS
Protocol Version	3.0	1.0
Number of Alert protocol Message Type	12	23
Message Authentication	MAC	HMAC
Key Material Generation	To create key material RSA, Diffie Hellman, fortezza	TLS uses HMAC and its pseudorandom function (PRF)

	output is used	output to create key
Certificate Verify	Requires complex procedure of messages.	All verified information is contained in handshake messages.
Finished	Either Client or server create finish message.	The process of generating finish message is same as key material is generated
Baseline Cipher Suite	SSL support RSA, Diffie Hellman and fortezza algorithm	TLS does not support fortezza algorithm

Comparison of SSL & SET

Issues	**SSL**	**SET**
Purpose	Encrypted data is exchange	Conducting safe electronic commerce
Authentication Mechanism	Not very strong	Strong mechanism
Fraud by Merchant	Probable because consumer provide monetary data to merchant	Not possible, as customer provides economic data to payment gateway.
Fraud by Customer	Possible because customer refuses to pay later and no method exist for this.	Payment instructions are digitally signed by customer
Certification	Certificate exchange between two parties	Third party certify all involved parties
Action Against	Legal action is against merchant	Legal action is against

Customer Fraud		payment gateway
Usage	Very high	Low as compared to SSL
No of messages in establishment of secure connection	Six Messages	Three Messages
Encryption	Encrypt whole information	Encrypt only sensitive data

CONCLUSION:

Today internet is mostly used by every individuals, every organization for different purpose. Internet can be used for data transfer, shopping, online transaction etc. Many organizations still not connected to internet due to security issues on the internet. For securing the internet transaction and data transfer SET, SSL/TLS protocols are discussed in this paper. SSL provide tunnel between sender and receiver and proved as best protocol for online security whereas SET provides authentication of users by digital certificates. Both protocols have their own domain for usage and their own encryption procedure. With the help of this paper one can able to understand about SSL/TLS and SET protocols.

REFERENCES:

1. Neetu Kawatra etal.,*" Analysis of E-Commerce Security Protocols SSL and SET",* National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC), 2011.

2. Jateen Gadhiya etal., *" Analysis of Security threats over TLS/SSL",* IJARCSSE, Volume 4, Issue 1, January 2014.

3. *Anssi Mattila "SET & SSL: Is there a comparison for a good night sleep",*IJECBS, Volume 2 Issue 2 July 2012.

4. Holly Lynne McKinley, *"SANS Institute InfoSec Reading Room",* 2003.

5. Homin K. Lee etal. , *"Cryptographic Strength of SSL/TLS Servers: Current and RecentPractices",* IMC'07, October 24-26, 2007, USA, 2007.

6. Houssam El Ismaili etal. , *"A Secure Electronic Transaction Payment Protocol Design and Implementation"*, IJACSA, Volume 5, No. 5, 2014.

7. Ajeet Singh etal. , *"A Review: Secure Payment System for Electronic Transaction"*, IJARCSSE, Volume 2, Issue 3, March, 2012.