ISSN:0975-9646

Comparison between SSL and SSH in Network and Transport Layer

Trivedi Anjali[1], Shah Krishna[2], Zatakiya Poonam[3]

[1,2,3] *BabuMadhav Institute of Information Technology, UkaTarsadia University, Bardolimhavua Road Tarsadi, Dist: Surat - 394 350 Gujarat (INDIA)*

Abstract- In this paper, we discuss about the Secure Socket Layer. Secure Socket Layer is developed by Netscape. SSL is working between the Transport Layer and Application Layer. Secure Socket Layer protocol: Handshake protocol, Record protocol and Alert protocol, Change Cipher suite. Secure shell is transport layer security. SSH sub protocol for establishing the connection. This sub protocol, SSH ensure authentication of the server and confidentiality and integrity of the communication. SSH has two sub protocol SSH Authentication protocol, SSH connection protocol. We were discuss on SSL Structure and how to SSL work, Attack on the SSL, Implementing of the SSL, purpose of the certificate authority and step of the SSL.

Keywords: Secure Socket Layer (SSL), Secure shell (SSH) Transport Layer Security (TLS), Man-In-The Middle (MITM) attack, Internet Engineering Task Force (IETF), Massage authentication code (MAC), Addressresolutionprotocol (ARP) .

1. INTRODUCTION

SSL is known as Secure Socket Layer. Secure Socket is developed by Netscape. Secure Socket Layer provide security between client and server authentication. A Secure Socket Layer method is provided for web based application. Secure Socket Layer is worked between the Application layer and Transport Layer. The Secure Socket Layer purpose is to message integrity and confidentiality.

There are different types of protocol of Secure Socket layer. Which are the handshake protocol, Record protocol, change cipher suite and Alert protocol. They have their own basic definition.

. SSH sub protocol for establishing the connection. This sub protocol, SSH ensure authentication of the server and confidentiality and integrity of the communication. SSH has two sub protocol SSH Authentication protocol, SSH connection protocol.

Secure Socket Layer is a work between Transport layer and Application Layer. Secure Socket layer fetches the data from the Transport Layer and that data send to the Application layer.

Implementing the SSL. we discuss the purpose of the certificate authority and configuration of the SSL. Certification Authorities (CA) are responsible for managing certificate requests and issuing certificates Participating IPSec network devices. Configuring Secure Socket Layer is used by a by application such as HTTP servers.

There is a different type of attacks on Secure Socket Layer: Man-In-The-Middle (MITM) attack, ARP poisoning attack, Rollback Attacks, Cipher Suite Rollback Attack, Compelled Certificate Creation Attacks, SSLstrip etc... The main problems that are dealing with are: ARP Poisoning; and Fake Certificate Attack.

2 . SECURE SOCKET LAYER (SSL)

SSL is stand for Secure Socket Layer. Secure Socket Layer is developed by Netscape. In 1994 Secure Socket Layer protocol is later renamed to Transport Layer Security. Secure Socket Layer main purpose is to message integrity and confidentiality.

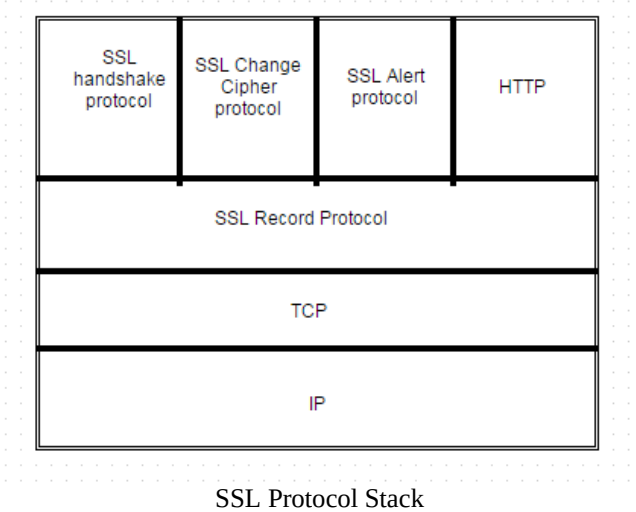
SSL version (1.0) was never released. SSL version(2.0) was released in February 1995. SSL version(3.0) was released in 1996 by Internet Engineering Task Force (IETF). In 1990 upgrade SSL protocol was released that called Transport Layer Security.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are used for securing Internet transactions such as banking, e-mail and e-commerce.

SSL provides identifies via trusted certificate and private communicatin via an encryption. When we use SSL there have must be buy the SSL certificate. After Buy the SSL certificate we can use the SSL.

2.1 SSL protocol

Secure Socket Layer has their four protocols: Handshake Protocol [1], Record protocol [2], Alert protocol [3], Change Cipher Suite protocol [4].



SSL Protocol Stack

Handshake Protocol

Handshake protocol is used to secure communication between the Client and Server. Handshake includes Certificate exchange.

Handshake protocol communication between the client and server. When Client and server are communicate with each other,

The client sends a Hello message to the server, server Send the response with the certificate. Then Client sends the client key exchange and change cipher spec and also send

the finish message to the server. Server will encrypt plaintext then send to the client. Then Server response to the client and send Change cipher spec message and also send finish message to the client. The server also sends the application data to the client. The client send application data to the server.

Record protocol:

Record protocol is used to encrypt the data and sent to the network using the key that have been establishing the handshake protocol. The SSL Record protocol provides the confidentiality and Message Integrity (using the message authentication code.

Alert protocol

In record layer data are transfer, If any error generated in transferring data then alert protocol will be initiated.

Change Cipher Suit protocol

Change Cipher suit protocol is used to signal that further message should encrypt to the last cipher suite.

3. SECURE SHELL (SSH)

SSH is particularly defined in five RFCs,

Where the first two describes the notations and architecture.

[SSH-NUMBERS], summaries the numbers and symbolic names used in the protocol such as for message numbers, error messages, etc

[SSH-ARCH], describes the architecture of the protocol.

And, the other three RFCs describes the sub-protocols, i.e; Transport Layer ,Authentication and SSH Connection Protocol respectively.

[SSH-TRANS] is used to establish a connection. Also establishes session keys, authenticates the server and finishes with the beginning of data exchange.

[SSH-USERAUTH] is used to authenticate the user who is going to login with the use of SSH.

[SSH-CONNECT] is used to build different communication channel within an SSH session

3.1 SSH protocol

SSH has two sub protocol: SSH Authentication protocol [1], SSH connection protocol [2].

SSH Authentication protocol:

SSH Authentication protocol is the sub protocol to establish the authenticity of the user with the use of SSH.

SSH Connection protocol:

SSH connection protocol is the sub protocol to establish different communication channel with SSH.

3.2 Comparison SSL and SSH:

SSL	SSH
secure socket layer	secure shell
SSL implement in presentation layer.	SSH has its own transport protocol independent from ssl.
SSL use a PKI via signed certificate.	In SSH you have to exchange the key fingerprints manually.
SSL uses port 443.	SSH uses port 22.
SSL is used predominantly for securely transmitting critical information like in credit cards and banking.	SSH is for securely executing commands across the internet.

4 HOW SSL WORK

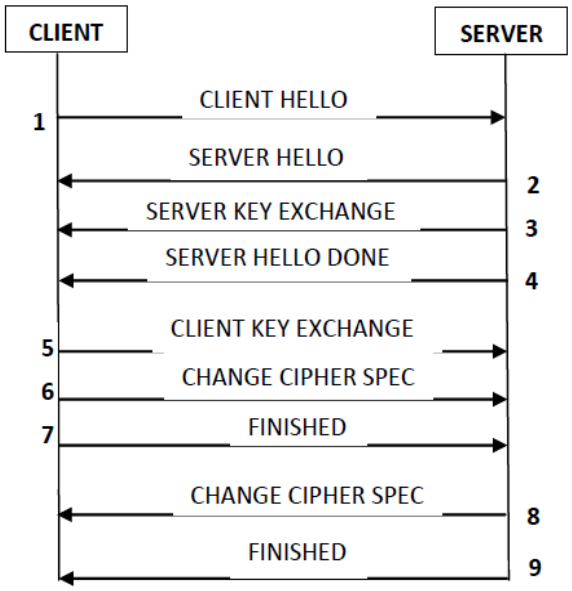


Fig: SSL handshake

4.1 Attacks on SSL

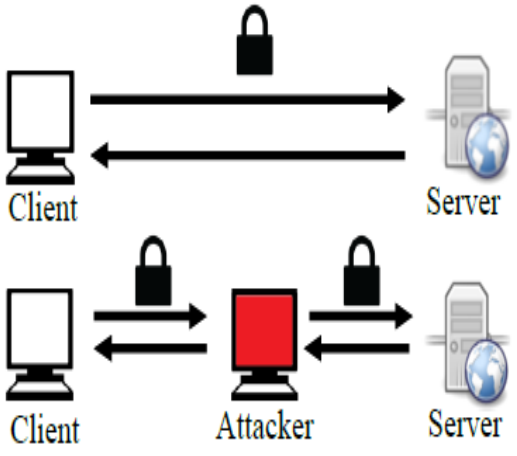
The type of attack on SSL is Man in the Middle attack (MITM), ARP poisoning attack, Rollback Attacks, Cipher Suite Rollback Attack, Compelled Certificate Creation Attacks, SSLstrip, Poodle attack etc...

Fake Certificate Attack

Phishing is attack in which fake website is forcefully made by user. This looks similar to authentic website that makes easier to share their information. But in a sophisticated manner, an attacker can hijack the session between the client and the server.

This can be visible through handshake protocol, whenever the server sends public key information and this isn't secured. So the attacker captures this message and change the detail in the certificate.

Secured connection is securely connected to the victim computer and the server, this disadvantage of the PKI model that the SSL supports. This helps user giving warning being forced and gives the user to accept the certificate or reject the connection.



Poodle Attack

Poodle attack (Padding Oracle And Downgraded Legacy Encryption). First handshake offers the highest protocol version supported by the client, if it gets failing get the earlier version with retry to legacy server many TLS clients acknowledge, So this triggered by network glitches TLS 1.0 readily conifer to SSL.3.

This SSL 3.0 either user RC4 stream cipher or block this cipher in CBC mode. SSL3 use CBC encryption to show attacker can modify network transmission between the client and server. SSL to achieve secure encryption SSL3.0 must be avoided.

The most problem of CBC SSL3.0 is that it block cipher padding and not cover by MAC. So the integrityof padding cannot be fully verified.

This SSL.3.0 weakness can be encrypted by man in the middle attack to server HTTP cookies usingtechniques from the beast attack.

Arp poisoning attack

Arp (Address resolution protocol) is a protocol methods detect the MAC address. I.e. logical address of the destination node. The destination node sends broadcast packet asking the MAC address of known IP address. SO it detects the device in the network and stores this MAP in it's up cache.

Sometime ARP poisoning may occur in this attacker first of all tries to capture packet where the device is connected to it, or to get knowledge which is the gateway. When finds victim and the gateway IPaddress, this sends ARP reply to victim to state the gateway MAC address, then it's changed to that of attacker's MAC.

With this attacker can hijack a session even if it is secured by SSSL/TLS. An attacker can get all packets that travel through a network and see all data.

5 IMPLEMENTING THE SSL

SSL is an application level protocol. It is provided secure communication between client and server by allowing mutual communication. As for integrity, and encryption for privacy. SSL and TLS are certificated by Public Key and private key.

Certificates are same as to the digital ID card. Prove the identity to server to client. Certificated issued by certified authorities.

Public and private key are used to encrypt and decrypt the information. Public and private key are working together. Data are encrypted with the public key and can be decrypted with the only private key. Certificates are included name of the authority. Time stamps indicates the certificate's expiration date.

To implement the SSL must need some things like..Purpose of Certificate authority, How to implement SSL Step

5.1 Purpose Of Certificate Authority

Certification Authorities (CA) are responsible for handling certificate requests and issuing certificates. These service provides centralized key management for the devices that are participating in the system.

CA simplifies the management of IPSec network devices. Usage of CA can be done with a network containing multiple IPSec-compliant devices, such as routers.

Digital signatures provide a way of digitally authenticating devices and individual users.

5.2 How to Implement SSL step

Configuring Secure Socket Layer is used by a by application such as HTTP servers.

Implementing the SSL there is the step to Configuration the SSL setup and the Example of the SSL Implement

How to configure SSL Step: Summary

1. **Crypto key generate RSA** [**usage-keys** | **general-keys**] [*keypair-label*
2. **Configure**
3. **domain ipv4 host host-name [v4address1 [v4address2...v4address8] [unicast | multicast]**
4. **Crypto ca trustpoint *ca-name***
5. **Enrolment url CA-URL**
6. Use one of these commands:

• **end**

• **commit**

7. RP/0/RSP0/CPU0: router **crypto ca authenticate** *ca-name*
8. **Crypto ca enroll** *ca-name*
9. Show crypto ca certificates

6 CONCLUSION

World has been emerging with many technologies and with the advancement with technology, many things have gone online. One of the trending thing is online transaction. And providing security in this purpose is much more important. Low security leads to many problems and issues like data theft, un-necessary money transfer, etc. Hence, Security Socket Layer provides you security over the online transactions and the transfers.

REFERENCES

[1] Guide to T102: SSL Security Threats Veronika Heimsbakk André Boganskij Amundsen May 14, 20120

[2] Guide to Analysis on Man in the Middle Attack on SSL INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS IN TECHNOLOGY · MAY 2012 2 AUTHORS:Pushpendra Kumar Pateriya Srijith S Kumar

[3] This POODLE Bites: Exploiting The SSL 3.0 Fallback Bodo Möller, Thai Duong, Krzysztof Kotowicz Google September 2014

[4] Network-based HTTPS Client Identification Using SSL/TLS Fingerprinting Martin Husa´k, Milan C˘ erma´k, Toma´s˘ Jirs´ık, Pavel C˘ eleda Institute of Computer Science, Masaryk University, Brno, Czech Republic fhusakm, cermak, jirsik, celedag@ics.muni.cz (June 2012)

[5] Man-in-the-browser _ IMT4122 Software Security Trends _ Spring 2013

[6] Rigorous specifications of the SSH Transport Layer Erik Poll1 and Aleksy Schubert2