International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 2 ǁ February. 2013 ǁ PP.40-44

Review of Secure Socket Layer

Ritika Saroha, Sarika Choudhary

(M.Tech (Network Security) School Of Engg. And Sci. /B.P.S.M.V Khanpur Kalan Sonepat, India)
(M.Tech (Network Security) School Of Engg. And Sci. /B.P.S.M.V Khanpur Kalan Sonepat, India)

ABSTRACT : *Secure socket layer is a security protocol, that provides privacy between the communicating parties over the internet.SSL protocol is designed to authenticate the server and the client and allow client/server application to communicate in a way that can't be eavesdropped.*

Keywords —*HTTP, IP, MAC, SSL, TCP.*

I. INTRODUCTION

The SSL was originated by Netscape in 1994.It's goal was to create an encrypted link/data path between client and server(regardless of the platform/OS being used).Netscape also designed SSL to take advantage of new encryption schemes as they become available such as recent adoption of AES, which replaced the DES.

For the purpose of providing a secure communication between client and server, it allows mutual authentication, and uses digital signature for integrity and encryption for privacy.

Now a days, SSL becomes an industry standard, as it is used by millions of websites in the protection of their online transactions with their customers.SSL protocol can negotiate an encryption algo. and session key as well as authenticate a server before the application protocol transmit or receive it's first byte of data. We can implement SSL in either 40 bit or 128 bit encryption (here 40 bit and 128 bit refers to the size of session keys). As we know, a session key is shared between client and server. For the encryption of every SSL session, these session keys are used because as longer the session key, it becomes harder to break the encryption of SSL session and to read the transmitted data. Internationally, SSL is widely used in 40-bit strength and domestically used in 128-bit strength.

II. WHY SSL IS USED OVER THE INTERNET

Earlier, there were two security issues for communication over the internet:

1. You are not sure that you are connecting to the right server.
2. You don't know that your data is safe or not from prying eyes during the transmission.

To solve these two problems to large degree, now most internet services support use of SSL as a mechanism for securing communication.

Hence SSL is a security protocol that is used to secure web transactions and e-commerce. For data transmission and reception it requires a reliable connection-oriented transport protocol like TCP/IP. SSL is a protocol layer may be placed between TCP/IP and application layer protocol like HTTP.

APPLICATION DATA
SECURE SOCKET LAYER (SSL)
TCP
IP

Fig 1: Overall SSL packet format.

SSL works at the transport and session layer of the OSI (Open System Interconnection) model to support the application layer, where both the web server and browser interoperate.

III. SSL PROTOCOL VERSIONS

Netscape developed the original version of SSL in 1994. A few months after it released SSLV1.0, Netscape released an update to the specification as SSLV2.0.In November 1995, Netscape made the specification for SSLV3.0 public. Since 1995, SSLV3.0 has grown in popularity and become a standard. SSLV3.0 is the version that most web servers support today.

VERSION	SOURCE	DESCRIPTION
SSL V1.0	**Netscape corporation**	**This version was not released by Netscape**
SSL V2.0	**Netscape corporation**	**First SSL protocol for which implementation exists.**
SSL V3.0	**Netscape corporation**	**Revision to prevent specific security attacks**
TLS V1.0	**IETF**	**Revision of SSLV3.0 to update the MAC layer to HMAC, msg. order standardization, more alert msg.**

IV. SSL ARCHITECTURE

SSL is not a single protocol but rather two layers of protocols:

1. SSL Record Protocol: It provides basic security to various higher-layer protocols.
2. HTTP: It provides transfer services for web client/server interaction & can operate on top of SSL
   The higher-layer protocols are:-
1. Handshake Protocol
2. Change Cipher Specification Protocol
3. Alert Protocol

<table>
<tr><td><b>SSL HANDSHAKE PROTOCOL</b></td><td><b>SSL CIPHER CHANGE PROTOCOL</b></td><td><b>SSL ALERT PROTOCOL</b></td><td><b>HTTP</b></td></tr>
<tr><td colspan="4"><b>SSL RECORD PROTOCOL</b></td></tr>
<tr><td colspan="4"><b>TCP</b></td></tr>
<tr><td colspan="4"><b>IP</b></td></tr>
</table>

Fig 2 SSL Protocol Stack

a. SSL RECORD PROTOCOL

It doesn't deal with records as it's name indicate but rather it is an encapsulation method for the Handshake protocol and Alert protocol. It is used to transfer application and SSL control data between client and server. It fragment the data into smaller units or combining multiple higher level protocol data messages into single units. It may compress, attach MAC and then encrypt these units before transmitting them using underlying reliable transport protocol.

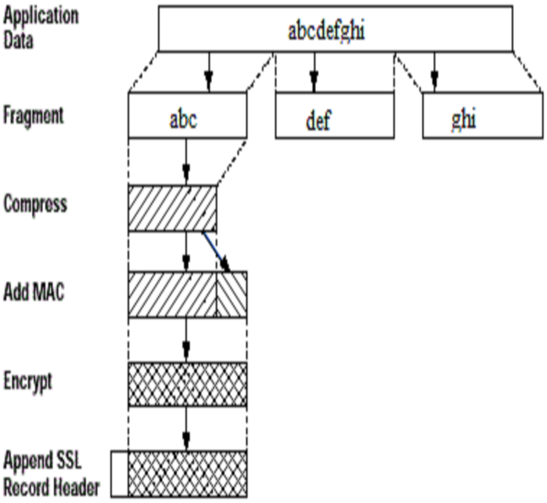

Fig 3 SSL Record Protocol Operation

The final step of SSL Record Protocol is to append a header having following fields:

1. Content Type
2. Major Version
3. Minor Version
4. Compressed Length

The Content Types are defined as Change cipher specification, alert, handshake, application data.

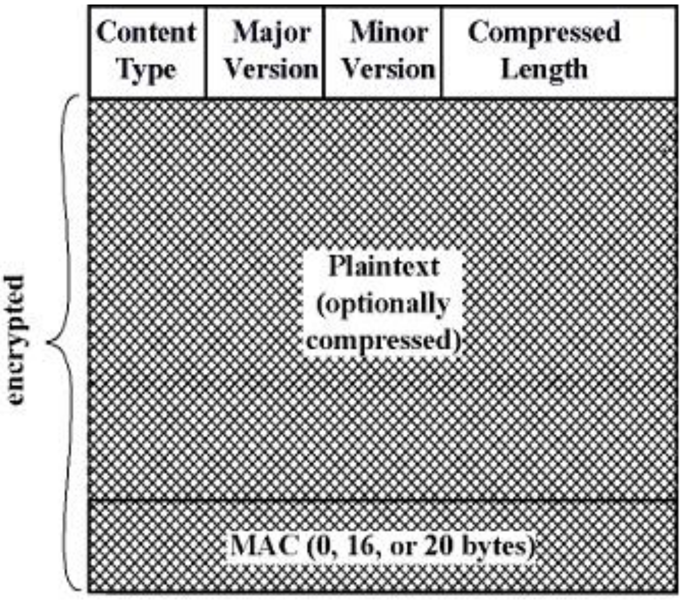

Fig 4. SSL Record Format

4.2 SSL CHANGE CIPHER SPEC. PROTOCOL

It is the simplest protocol of Secure Socket Layer, which indicates the transition of cipher suits to be used on connection between the client and server. This protocol consists of a single message, containing a single byte with value 1.This message is encrypted and compressed with current cipher suite. The main purpose of this message is to copy the pending state to the current state, which updates the cipher suite. This signal is used as coordination signal. The client must send it to the server and server must send it to the client. After each side has received it, all of the following messages are sent using the agreed-upon ciphers and keys.

4.3 SSL ALERT PROTOCOL

SSL Alert protocol is used to report errors like: unexpected messages, bad record MAC, decompression failure, illegal parameters, handshake failure etc. It is also used for following purpose:

1. To notify closure of the connection.
2. To notify the absence of certificate (When requested).
3. To notify that a bad or unknown certificate was received.
4. To notify that a certificate is revoked or has expired.

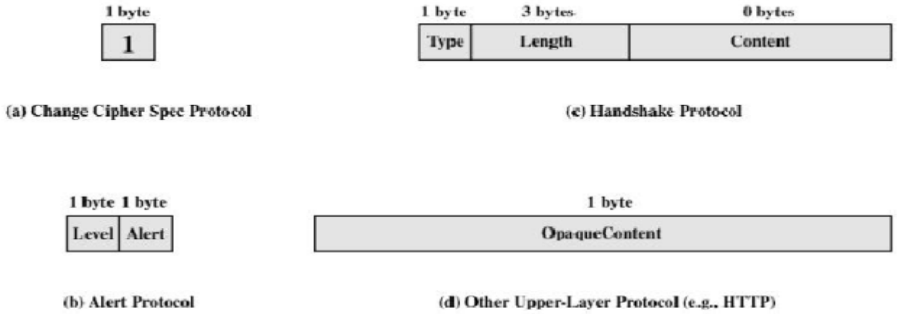

Fig 5. SSL Record Protocol Payload

4.4 SSL HANDSHAKE PROTOCOL

This is the most complex part of SSL, that operate on the top of SSL record protocol layer. It performs the following operations:

1. It allows the client and server to authenticate each other.
2. It negotiates the encryption, MAC algorithm, and cryptographic keys.
3. Used before any application data is transmitted.

It establish a session, which defines a set of cryptographic parameters to be used. The Handshake protocol consists of a series of messages exchanged between the client and server, by four phases:

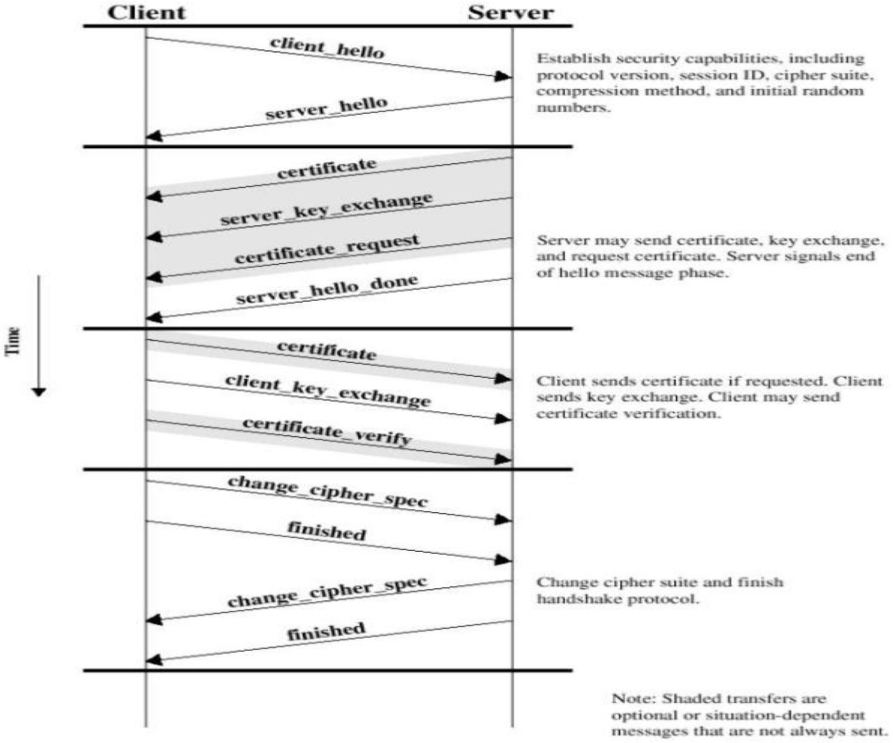
Client
Server
client_hello
server_hello
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Server may send certificate, key exchange, and request certificate.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

Fig 6. SSL Handshake Protocol Action

Phase 1: Establish security capabilities.
Phase 2: Server authentication and key exchange.
Phase 3: Client authentication and key exchange.
Phase 4:Finish.

V. SERVICES TO BE PROTECTED WITH SSL

Almost any Internet service can be protected with SSL. Common ones include WebMail and other secure web sites such as banking sites and corporate sites, POP, IMAP, and SMTP.

VI. SSL BENEFITS

The benefit of SSL is that it provides ease of implementation:

1. For network application developers as it is as easy as implementing unsecured sockets.
2. For network implementation developers as they have to add simply a layer to established network protocol stacks.
3. For users as they only need to authorize the certificate.

VII. SSL DRAWBACKS

The drawbacks of the Secure Socket Layer are:

1. It needs more bandwidth.
2. It is slow.
3. Needs a dedicated port like 443 for HTTPS.

VIII. FUTURE OF SSL

SSL 3.0 has evolved into the Internet Engineering Task Force (IETF) Transport Layer Security (TLS) 1.0 protocol, sometimes referred to as SSL V3.1.

REFERENCES

[1]. Alan O. Freier, Philip Karlton, Paul C. Kocher, The SSL Protocol Version 3.0, 1996.
[2]. http://www.netscape.com/eng/ssl3/draft302.txt.
[3]. Kipp E.B. Hickman, The SSL Protocol, 1995. See http://www.netscape.com/eng/security/SSL_2.html
[4]. “SecureSocketsLayer.” Netscape Network. http://wp.netscape.com/security/techbriefs/ssl.html
[5]. ftp://ftp.ietf.org/internet-drafts/draft-ietf-tls-protocol-05.txt
[6]. ftp://ftp.ietf.org/internet-drafts/draft-ietf-tls-https-01.txt
[7]. **BOOKS:**
[8]. Network Security by William Stalling.
[9]. Security In Computing by Charles P. Pfleger