Trusting SSL for Unsecure Internet

Poonam Ashok Kakade,
Student(BE), Department of Computer Science& Engineering,
Shri Sant Gadge Baba college of engineering, Bhusawal,
North Maharashtra University, Maharashtra, India.

Abstract: Secure socket layer is a security protocol, that provides privacy between the protocol that provides a secure channel between a client and a server at the transport communicating parties over the internet.SSL protocol is designed to authenticate the server and the client and allow Transport Layer Security (TLS) is a connection-oriented layer of the network. This practical serves to explain the Secure Sockets Layer (SSL). This paper particularly serves as a resource to those who are new to the in sequence guarantee field, and provides an insight to two common protocols used in Internet security. Though SSL and TLS are not the only safe protocol currently in use, they are very common for sites dealing with transactions that could involve sensitive data (ie: passwords, personal and financial information, etc.).

Keywords: HTTP, IP, MAC, SSL, TCP.

I. INTRODUCTION

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. We can implement SSL in either 40 bit or 128 bit encryption (here 40 bit and 128 bit refers to the range of assembly key). As we know, a session key

is shared between client and server. SSL is widely used in 40-bit strength and domestically used in 128-bit strength. SSL/TLS are widely viewed as robust means of providing confidentiality, integrity and server authentication.

A. What is SSL?

SSL is the ubiquitous security procedure used in not quite 100% of secure Internet transactions, SSL transform a typical consistent transport set of rules (such as TCP) into a protected communications feed suitable for conducting sensitive transactions.

B. Why SSL Is Used Over The Internet

There were two security issues for communication over the internet:

1. You are not confident that you are relating to the accurate attendant.

2. You don't recognize that your information is secure or not from interfering eyes during the transmission.

To solve these two problems to huge scale, now a large amount internet services maintain apply 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.

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.

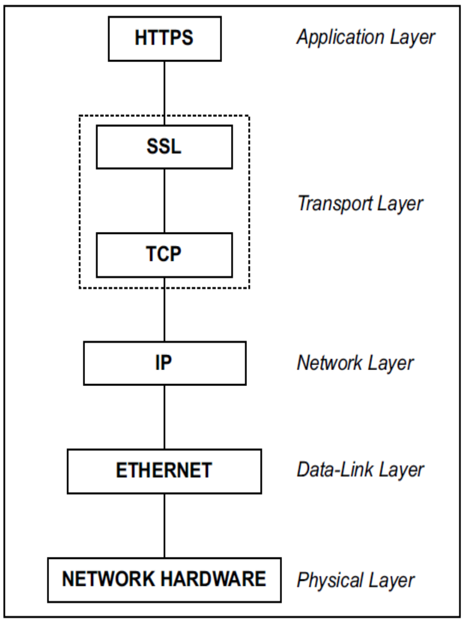

Figure 1 References model

II. HISTORY

Netscape developed the original version of SSL in 1994. A few months after it released SSLV1.0, Netscape unrestricted an keep posted to the specification as SSLV2.0.In November 1995, Netscape made the specification for SSLV3.0 public. Since 1995, SSLV3.0 has developed in recognition and become a regular. 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,

III .SSL SESSIONS AND CONNECTIONS

A. Handshake between Client and Server-

When client go with HTTPS based URL, in its browser, the browser begin a TCP connection to HTTPS default port number 443 at server. Once the connection is successful, browser and server exchange some information like uppermost protocol version, ciphers used, compression method, and some random data. Following that, SSL client's sends MAC to the server, which is computed on all the handshake messages exchanged between both of them. Then, server also replies by similar MAC to the browser. Thus, browser and server can make sure that none of the messages had been tampered/ altered during transit if the MAC values are same. Mismatch in the value of authentication codes may terminate the SSL connection. Popular algorithms used in MAC computation are MD-5, SHA-1, HMAC, etc.

B. Exchange of Encrypted Message-

Subsequently, browser breeds a symmetric secret key for this SSL session, encrypts it with public key of server, and transmits over server. This encrypted symmetric key can be uniquely decrypted by private key of server. Consequently, both the browser and server possess the same secret key, and now they can exchange data encrypted by this key during entire session. The foremost weakness with symmetric key cryptography is in key distribution especially when they do not trust each other. Thus, SSL uses asymmetric key cryptography, to exchange symmetric key between both the parties. Then there is no use of asymmetric key pair for that session Symmetric key is preferred to employ for the entire session over asymmetric key, because it require very less computations.

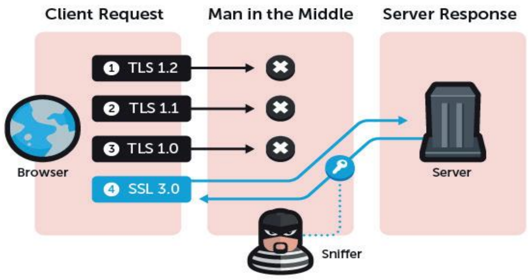

Figure 2 Renegotiation and downgrading of protocol

IV. SSL BENEFITS

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

1. For network application developers as it is as trouble-free as implement unsecured socket.

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.

V. 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.

VI. FUTURE OF SSL

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

ACKNOWLEDGMENT

I feel great pleasure in submitting this Paper on "Trusting SSL for unsecure internet"**.** I wish to express true sense of gratitude towards my my Principal Dr. R. P. Singh and my H.O.D., **Prof. D. D. Patil. I also wish to thank my teacher Prof. R. R. Singh** who at very separate step in training of this Paper contribute his valuable management and facilitate to solve every difficulty that arise. Also, With all respect and appreciation, I would like to show gratitude all the people, who have helped me directly or indirectly. I be obligated my all achievement to them.

CONCLUSION

SSL is fundamental to Web security. It provides a burly intelligence of privacy, message integrity, and identity authentication to users. The industry of e-business is joined personally to consumer confidence in the identity assurance aspect of SSL certificate crossways the web.

As a result, in the future SSL certificates will evolve to offer more security and uniqueness assurance. The encryption of key lengths, secret message suites and new guidelines for SSL certificates will also evolve to ensure a consistent level of identity verification during online transactions. This way, e-commerce will be able to persist to cultivate as users raise more secure in shopping and banking online.

REFERENCES

[1] B Möller, A Langley: "TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks", Internet Draft draftietftlsdowngradescsv00, 2014.
[2] POODLE – An SSL 3.0 Vulnerability (CVE-2014-3566) https://securityblog.redhat. Com/2014/10/15/poodle-a-ssl3- vulnerability-cve-2014-3566/
[3] Prince, Matthew (14 Oct 2014). "SSLv3 Support Disabled By Default
Due to POODLE Vulnerability", https://blog.cloudflare.com/sslv3- support-disabled-by-default-due-to vulnerability/. [4] Bodo Möller, Thai Duong, Krzysztof
Kotowicz," This POODLE Bites: Exploiting The SSL 3.0 Fallback"
Google September 2014.
[5] Attack of the week: RC4 is kind of broken in TLS, http:// blog. Cryptography engineering. com/2013/03/attack-of-week-rc4- is-kind-of-broken-in.html