SSL vs. TLS – What are differences?

Phew! Internet security is jargon-filled world. For a newbie like me it is a nightmare to make sense of these terms and how they work together.

It takes a lot of prodding to understand how they work and how they are different from one another.

If you have been reading about SSL recently, you would have stumbled across TLS as well.

SSL refers to Secure Sockets Layer whereas TLS refers to Transport Layer Security. Basically, they are one and the same, but, entirely different.

How similar both are? SSL and TLS are cryptographic protocols that authenticate data transfer between servers, systems, applications and users. For example, a cryptographic protocol encrypts the data that is exchanged between a web server and a user.

SSL was a first of its kind of cryptographic protocol. TLS on the other hand, was a recent upgraded version of SSL.

Why do you need an SSL/TLS certificate?

Cyber security has become a serious threat that is spreading across all sections of the internet. From schools to enterprises and individuals, it puts user data of all types and sizes at risk. The risk is especially higher when there is exchange of information through client and server systems.

There is a need for secure system that encrypt data flow from either side. An SSL/TLS certificate helps with that. It acts as an endpoint encryption system that encrypt data preventing unauthorized access by hackers.

In the present day, SSL has also gained importance as a serious ranking signal due to Google's announcement. Websites with SSL certificates gain better search ranking traction, have better user experience and do not pose any security concerns — even during eCommerce transactions.

A brief about SSL

Netscape developed SSL in the year 1994. It was envisioned as a system that will ensure secure communication between client and server systems on the web. Gradually, the IETF (the Internet Engineering Task Force) picked up the protocol and standardized it as a protocol. Two versions of SSL followed that ironed out the vulnerabilities found in version 1. The current SSL version is SSL 3.0. If we look at below history, we can assume that IETF seriously attempted to secure online data with robust security at its best.

SSL 1.0	Due to security flaw, SSL 1.0 was not released.
SSL 2.0	SSL v2.0 was the first public release of SSL by Netscape. It was released in February 1995 but there were design flaws that compelled Netscape to release SSL v.3. However, SSL v.2.0 was deprecated in 2011.
SSL 3.0	SSL v3 was an upgrade version of earlier version SSL v2.0 that fixed few security design flaws of SSL v2.0 However, SSL v3.0 deemed insecure in 2004 due to the POODLE attack.

A brief about TLS

TLS means Transport Layer Security, which is a cryptographic protocol successor of SSL 3.0, which was released in 1999.

TLS 1.0	TLS 1.0 which was upgrade of SSL v.3.0 released in January 1999 but it allows connection downgrade to SSL v.3.0.
TLS 1.1	After that, TLS v1.1 was released in April 2006, which was an update of TLS 1.0 version. It added protection against CBC (Cipher Block Chaining) attacks. In March 2020, Google, Apple, Mozilla and Microsoft has announced for deprecation of TLS 1.0 and 1.1 versions.
TLS 1.2	TLS v1.2 was released in 2008 that allows to specification of hash and algorithm used by the client and server. It allows authenticated encryption, which was added more support with extra data modes. TLS 1.2 was able to verify length of data based on cipher suite.
TLS 1.3	TLS v1.3 was released in August 2018 and had major features that differentiate it with its earlier version TLS v1.2 like removal of MD5 and SHA-224 support, require digital signature when earlier configuration used, compulsory use of Perfect forward secrecy in case of public-key based key exchange, handshake messages will now be encrypted after “Server Hello”.

Differences between SSL and TLS

However, the differences between SSL and TLS are very minor. In fact, only a technical person will be able to spot the differences. The notable differences include:

Cipher suites

SSL protocol offers support for Fortezza cipher suite. TLS does not offer support. TLS follows a better standardization process that makes defining of new cipher suites easier like RC4, Triple DES, AES, IDEA, etc.

Alert messages

SSL has the “No certificate” alert message. TLS protocol removes the alert message and replaces it with several other alert messages.

Record Protocol

SSL uses Message Authentication Code (MAC) after encrypting each message while TLS on the other hand uses HMAC — a hash-based message authentication code after each message encryption.

Handshake process

In SSL, the hash calculation also comprises the master secret and pad while in TLS, the hashes are calculated over handshake message.

Message Authentication

SSL message authentication adjoins the key details and application data in ad-hoc way while TLS version relies on HMAC Hash-based Message Authentication Code.

These are the essentially differences between an SSL and TLS certificate. Like I mentioned before, it takes a trained eye to understand the differences.

> ***In nutshell, SSL is obsolete and TLS is new name of older SSL protocol as modern encryption standard using by everybody. Technically, TLS is more accurate, but everyone knows SSL.***

Few considerations of TLS protocol

- It prevents intruders from tampering the communication passes between the server and the user.
- It also prevents intruders from listening to server communication.
- TLS adds latency to site traffic.
- TLS uses asymmetric encryption for connection establishment then, it allows symmetric encryption for the client and the server for faster connection.
- With the addition of HTTP/2, TLS makes connection faster.

At Last, do you need an SSL/TLS certificate?

If you look at SSL versus TLS certificate, both perform the same task of encrypting data exchange. TLS was an update and secure version of SSL. Nevertheless, SSL certificates that are abundantly available on the Internet serve the same purpose of securing your website. In fact, they both offer websites the same HTTPS address bar that have come to be recognized as the hallmark symbol of online security.