SSL / TLS

Prof Brijendra Singh
Department of Computer Science,
Lucknow University, Lucknow

SSL and TLS are both cryptographic protocols that provide authentication and data encryption between servers, machines, and applications operating over a network (e.g. a client connecting to a web server).

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details.

SSL can transfer any data between users and sites, or between two systems, which is impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.

Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information.

TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term, but when you are buying SSL from Symantec you are actually buying the most up to date TLS certificates with the option of RSA or DSA encryption.

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.

When? connections between a client and a server secured by TLS should have one or more of the following properties:

1.The connection is *private* (or *secure*) because symmetric cryptography is used to encrypt the data transmitted.

2.The identity of the communicating parties can be *authenticated* using public-key cryptography.

3.The connection is *reliable* because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

TLS supports many different methods for exchanging keys, encrypting data, and authenticating message integrity. As a result, secure configuration of TLS involves many configurable parameters.