**Transport Layer Security (TLS)**

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.

There are several benefits of TLS:

* **Encryption:**   
  TLS/SSL can help to secure transmitted data using encryption.
* **Interoperability:**   
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
* **Algorithm flexibility:**   
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
* **Ease of Deployment:**   
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
* **Ease of Use:**   
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

**Working of TLS:**   
The client connect to server (using [TCP](https://www.geeksforgeeks.org/tcp-ip-model/)), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.

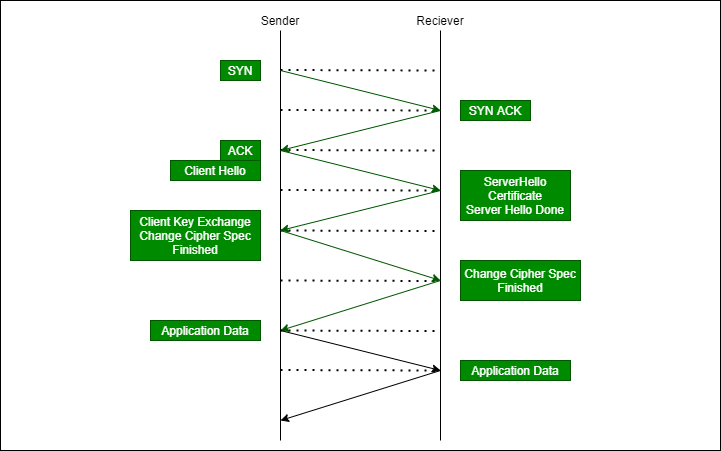
Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

**Transport Layer Security (TLS) Handshake**

TLS is a data privacy and security protocol implemented for secure communication over internet. It usually encrypts communication between server and clients. TLS is a successor to Secure Socket Layer (SSL) protocol. SSL v3.0 and TLS v1.0 were very similar but it was replaced with TLS. You can also refer to Transport Layer Security (TLS).

A Transport Layer Security (TLS) connection is established via handshake.

**TLS Handshake in action :**



**Figure –** TLS Handshake

1. With a TLS enabled service, a sender sends a ClientHello (as referred in protocol). This includes information about Client.
2. Then server responds with ServerHello message (selecting highest version of TLS supported by Client) and then chooses a cipher suite from list in ClientHello message. The server also transmits its Digital certificate and a final ServerHelloDone message.
3. Client validates certificate. Client then sends ClientKeyExchange message. Here client chooses a key exchange mechanism to securely establish a shared secret with server. Client also needs to send ChangeCipherSpec indicating that it is switching to secure communication now, which is finally followed by Finished message for indicating a successful handshake.
4. Server replies with ChangeCipherSpec and an encrypted Finished message once shared secret is received.

Session key is Shared Symmetric Encryption Key used in TLS sessions to encrypt data being sent back and forth.

**Difference between Secure Socket Layer (SSL) and Transport Layer Security (TLS)**

SSL stands for Secure Socket Layer while TLS stands for Transport Layer Security. Both Secure Socket Layer and Transport Layer Security are the protocols used to provide security between web browsers and web servers. The main difference between Secure Socket Layer and Transport Layer Security is that, in SSL (Secure Socket Layer), the Message digest is used to create a master secret and It provides the basic security services which are **Authentication** and **confidentiality**. while In TLS (Transport Layer Security), a Pseudo-random function is used to create a master secret.

There are some differences between SSL and TLS which are given below:

| **SSL** | **TLS** |
| --- | --- |
| SSL stands for Secure Socket Layer. | TLS stands for Transport Layer Security. |
| SSL (Secure Socket Layer) supports the **Fortezza** algorithm. | TLS (Transport Layer Security) does not support the **Fortezza** algorithm. |
| SSL (Secure Socket Layer) is the 3.0 version. | TLS (Transport Layer Security) is the 1.0 version. |
| In SSL( Secure Socket Layer), the Message digest is used to create a master secret. | In TLS(Transport Layer Security), a Pseudo-random function is used to create a master secret. |
| In SSL( Secure Socket Layer), the Message Authentication Code protocol is used. | In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used. |
| SSL (Secure Socket Layer) is more complex than TLS(Transport Layer Security). | TLS (Transport Layer Security) is simple. |
| SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security). | TLS (Transport Layer Security) provides high security. |
| SSL is less reliable and slower. | TLS is highly reliable and upgraded. It provides less latency. |
| SSL has been depreciated. | TLS is still widely used. |
| SSL uses port to set up explicit connection. | TLS uses protocol to set up implicit connection. |

35