Hello friends, in this video, you will learn about the SSL and TLS protocols used for securing Transport layer data.

SSL or TLS are designed to provide security at the transport layer. SSL which stands for Secure Socket Layer, was the predecessor of TLS (Transport layer Security) protocol, currently being used.

Here is a brief timeline about SSL and TLS. SSL was introduced in the year 1994 and went up to version 3.0 in 1995. later in the year 1996, TLS1.0 came which was equivalent to SSL version 3.1, and became an IETF standard. In 2006 TLS version 1.1 came and in 2008 TLS version 1.2 was released. The latest version of TLS, TLS 1.3, came in the year 2018, being used by most of the applications today.

TLS protocol, working on transport layer, protects the data coming from Application layer. This is the reason why you see https in your URL, when TLS is implemented. Similarly, SSL/TLS is used to protect email and File Transfer Protocol(FTP) also.

To provide protection to the data, SSL/TLS uses a set of protocols starting from handshake protocol to Record protocol, as shown in the figure. Handshake protocol, Change Cipher Spec protocol and Alert protocols work to provide input and support to Record protocol. Let's understand these protocols.

In Handshake protocol, the sender and receiver, get ready for the communication by creating and exchanging keys and authenticating each other. Change Cipher Specification protocol, indicates the readiness and the alert protocol is used in case of errors.

The record protocol is the main operating protocol in SSL/TLS. It provides fragmentation for more manageability, compression, authentication, and encryption of the data received on the transport layer for the maximum level of security. An SSL header is also added to the data.

For implementing SSL protocol for any website i.e. to use HTTPS in place of HTTP, in the URL, it is necessary to get an SSL/TLS certificate.
An SSL certificate contains the website's public key, the domain name it's issued for, the issuing certificate authority's digital signature, and other important information. When a client wants to communicate with a server, it needs an SSL certificate containing the public key of the server. The browser cache of the client has most of the keys available. If the key is not available in cache, server sends its SSL certificate, which is verified by the client and used for sending the encrypted secret key to the server, to be used for encryption and decryption.

As TLS is the upgraded SSL protocol, definitely, it has some differences from SSL. The TLS protocol does not support

Fortezza /DMS cipher suites while SSL supports Fortezza. Also, the TLS standardization process makes it much easier to define new cipher suites. The SSL record protocol adds MAC (Message Authentication Code) after compressing each block and encrypts it. As against, TLS record protocol uses HMAC (Hash-based Message Authentication Code). The “No certificate” alert message is included in SSL. On the other hand, TLS removes alert description (No certificate) and adds a dozen other values.

Thank You.