SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit I- NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

Topic : SSL & TLS PROTOCOL

SSL PROTOCOL

- SSL or Secure Sockets Layer, is an Internet security protocol that encrypts data to keep it safe. It was created by Netscape in 1995 to ensure privacy, authentication, and data integrity in online communications.

Working of SSL

Encryption: SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.

Authentication: SSL starts an authentication process called a handshake between two devices to confirm their identities.

Data Integrity: SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data received is exactly what was sent by the sender.

IMPORTANCE OF SSL

The data on the web was transmitted in plaintext, making it easy for anyone who intercepted the message to read it.

For example, if someone logged into their email account, their username and password would travel across the Internet unprotected.

SSL was created to solve this problem and protect user privacy.

By encrypting data between a user and a web server, SSL ensures that anyone who intercepts the data sees only a scrambled mess of characters.

This keeps the user’s login credentials safe, visible only to the email service.
Additionally, SSL helps prevent cyber attacks by:

Authenticating Web Servers: Ensuring that users are connecting to the legitimate website, not a fake one set up by attackers.

Preventing Data Tampering: Acting like a tamper-proof seal, SSL ensures that the data sent and received hasn’t been altered during transit.

TLS PROTOCOL

Transport Layer Security (TLS) is the most widely used protocol for implementing cryptography on the web.

TLS uses a combination of cryptographic processes to provide secure communication over a network.

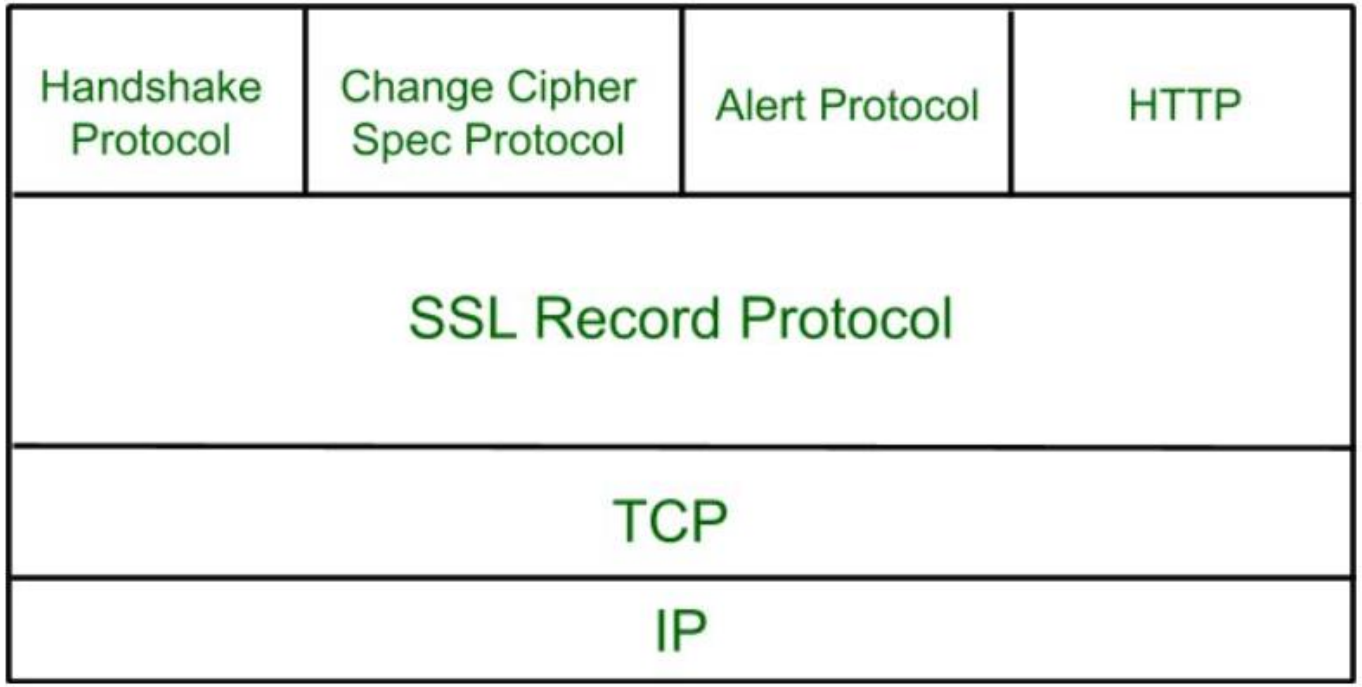
TLS provides a secure enhancement to the standard TCP/IP sockets protocol used for Internet communications.

TLS is the successor to **SSL (Secure Sockets Layer)**. While they are often used interchangeably, **TLS is more secure** and efficient than SSL.

TLS uses public-key cryptography to provide authentication, and secret-key cryptography with hash functions to provide for privacy and data integrity

SSL / TLS PROTOCOLS

- SSL Record Protocol
- Handshake Protocol
- Change-Cipher Spec Protocol
- Alert Protocol



Handshake Protocol | Change Cipher Spec Protocol | Alert Protocol | HTTP

SSL Record Protocol

TCP

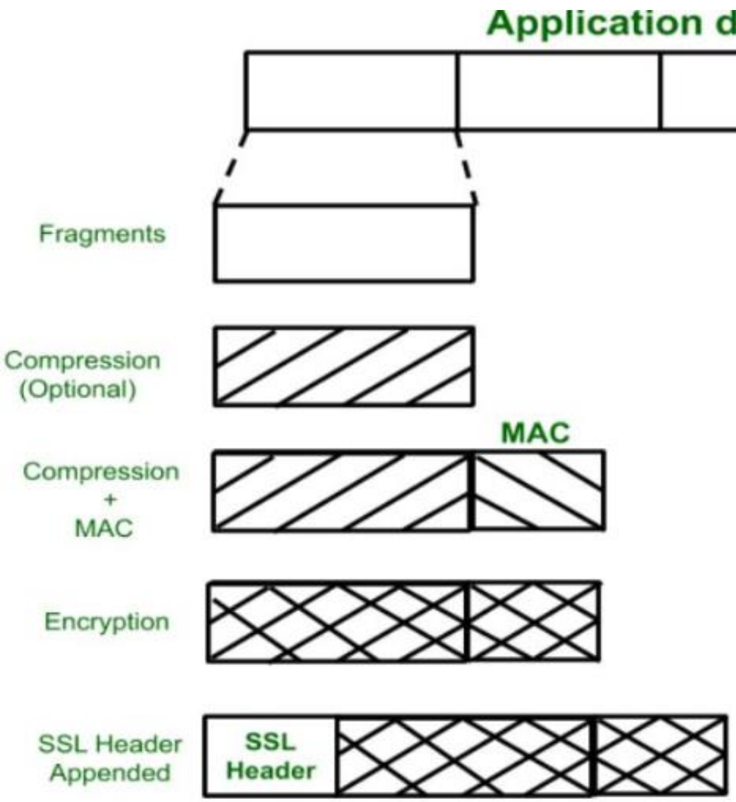
IP

SSL / TLS Record Protocol

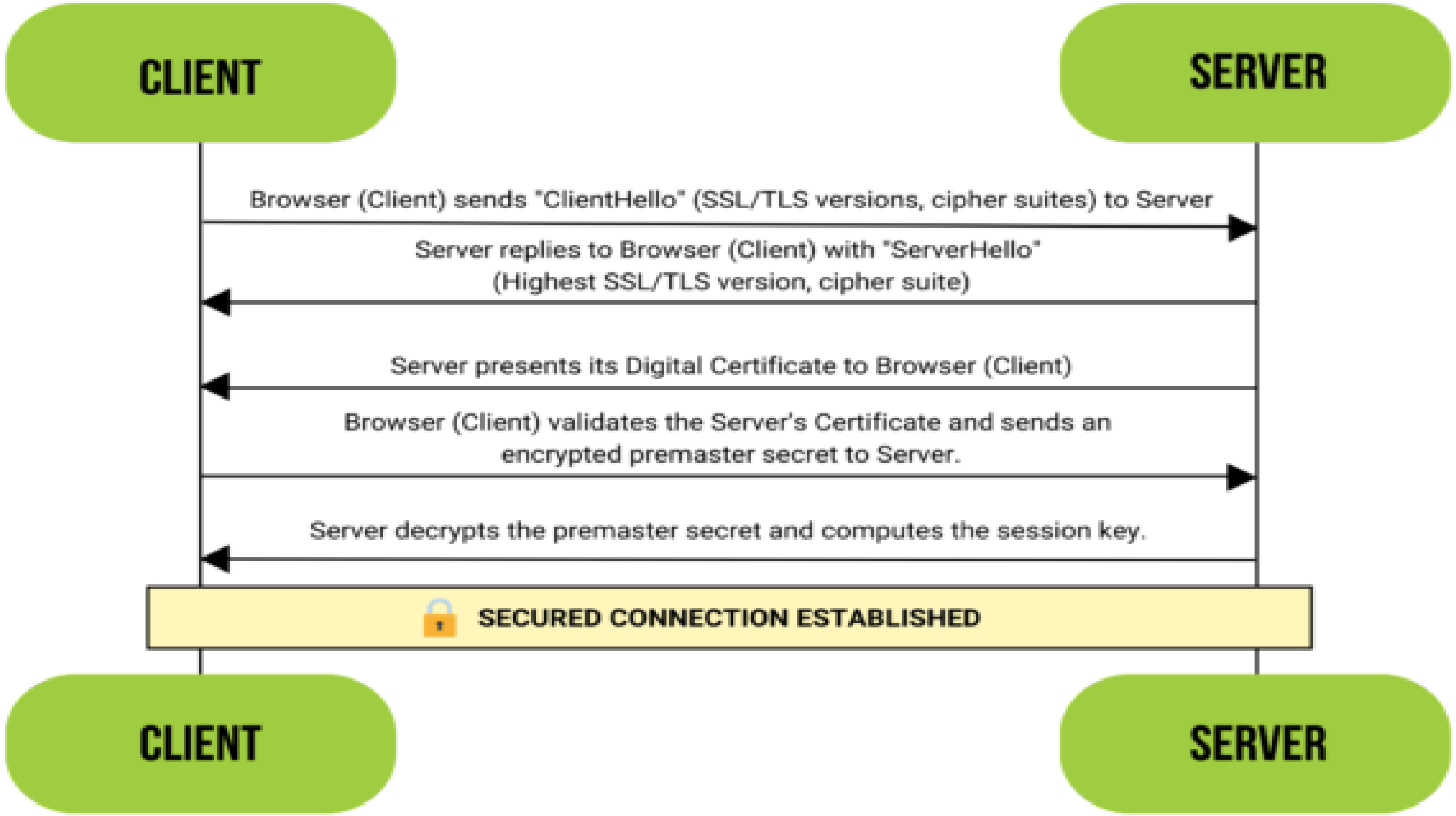
SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest). After that encryption of the data is done and in last SSL header is appended to the data.



SSL/TLS HANDSHAKE



CLIENT

SERVER

Browser (Client) sends "ClientHello" (SSL/TLS versions, cipher suites) to Server

Server replies to Browser (Client) with "ServerHello"
(Highest SSL/TLS version, cipher suite)

Server presents its Digital Certificate to Browser (Client)

Browser (Client) validates the Server's Certificate and sends an encrypted premaster secret to Server.

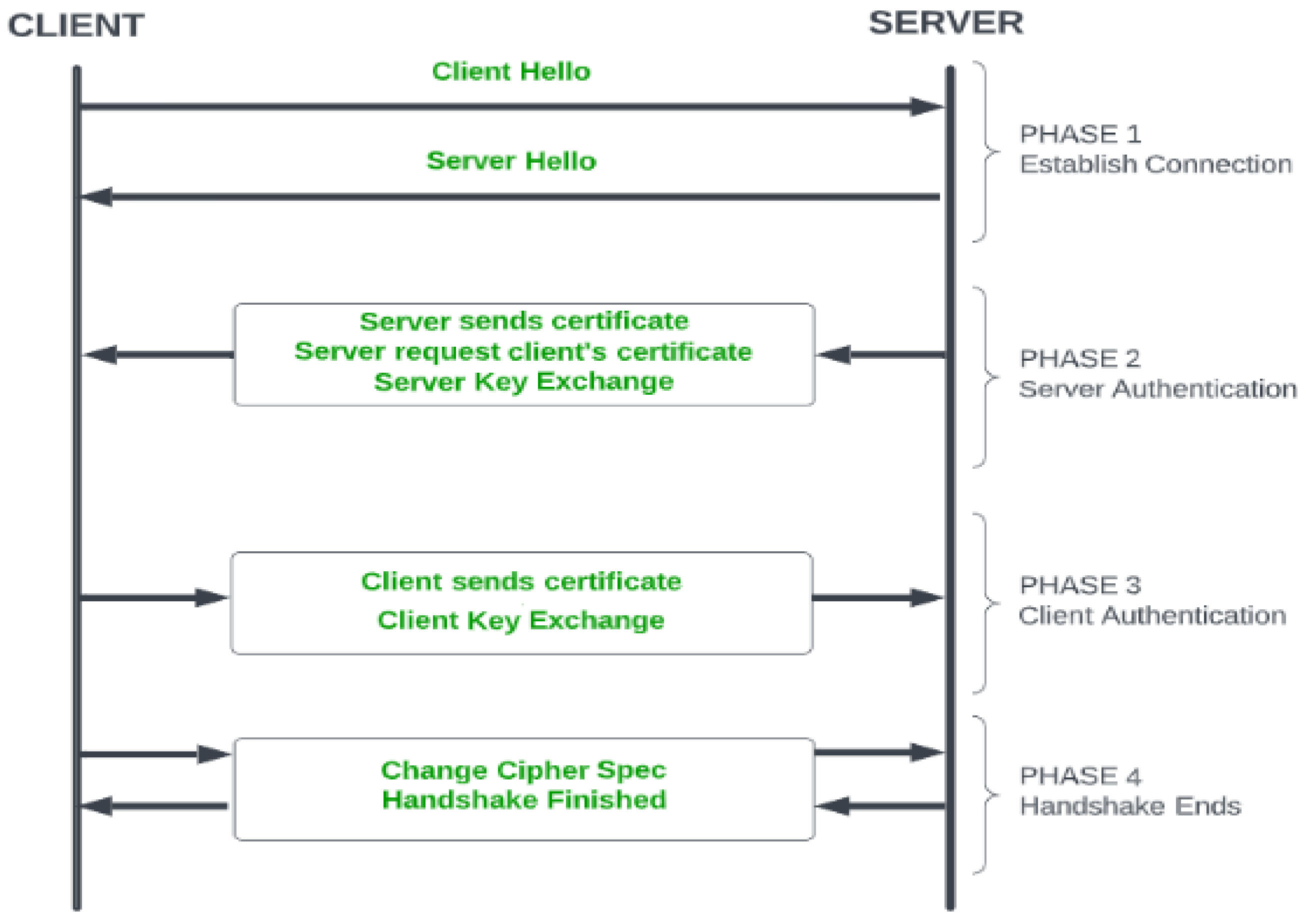
Server decrypts the premaster secret and computes the session key.

🔒 SECURED CONNECTION ESTABLISHED

CLIENT

SERVER

Handshake Protocol



SSL HANDSHAKE PROTOCOL

SSL/TLS HANDSHAKE

1.Introduction (ClientHello): Your browser sends a **“ClientHello”** message to the server when you request a secure website. This message contains essential information, including the SSL/TLS versions it supports and the cipher suites it can use.

2.Server’s Response (ServerHello): The server replies with a **“ServerHello”** message, including the highest SSL/TLS version and cipher suite both parties support.

3.Server’s Credentials: The server presents its digital certificate, verified by a Certificate Authority (CA) such as www.SSL.com, like an ID card providing its authenticity.

4.Client’s Verification and Key Generation: Your browser validates the server’s certificate. Once verified, it uses the server’s public key to encrypt a ‘**premaster secret**,’ a unique session key, and sends it back to the server.

5.Establishing a Secure Connection: The server decrypts the premaster secret with its private key. The server and client then compute the session key, which will be used for symmetric encryption of all communication.

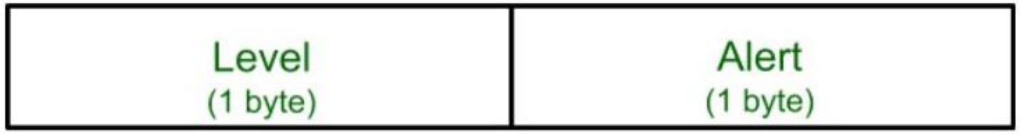
Change –Cipher Protocol

Change-Cipher Protocol
This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state.
Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol

Alert Protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



Level (1 byte)	Alert (1 byte)

The level is further classified into two parts:

Warning (level = 1)

This Alert has no impact on the connection between sender and receiver. Some of them are:

Bad Certificate: When the received certificate is corrupt.

No Certificate: When an appropriate certificate is not available.

Certificate Expired: When a certificate has expired.

Certificate Unknown: When some other unspecified issue arose in processing the certificate, rendering it unacceptable.

Close Notify: It notifies that the sender will no longer send any messages in the connection.

Alert Protocol Cont.,

Unsupported Certificate: The type of certificate received is not supported.

Certificate Revoked: The certificate received is in revocation list.

Fatal Error (level = 2):
This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are :

Handshake Failure: When the sender is unable to negotiate an acceptable set of security parameters given the options available.

Decompression Failure: When the decompression function receives improper input.

Illegal Parameters: When a field is out of range or inconsistent with other fields.

Bad Record MAC: When an incorrect MAC was received.

Unexpected Message: When an inappropriate message is received.
The second byte in the Alert protocol describes the error.

SSL CERTIFICATIONS

Types of SSL Certificates

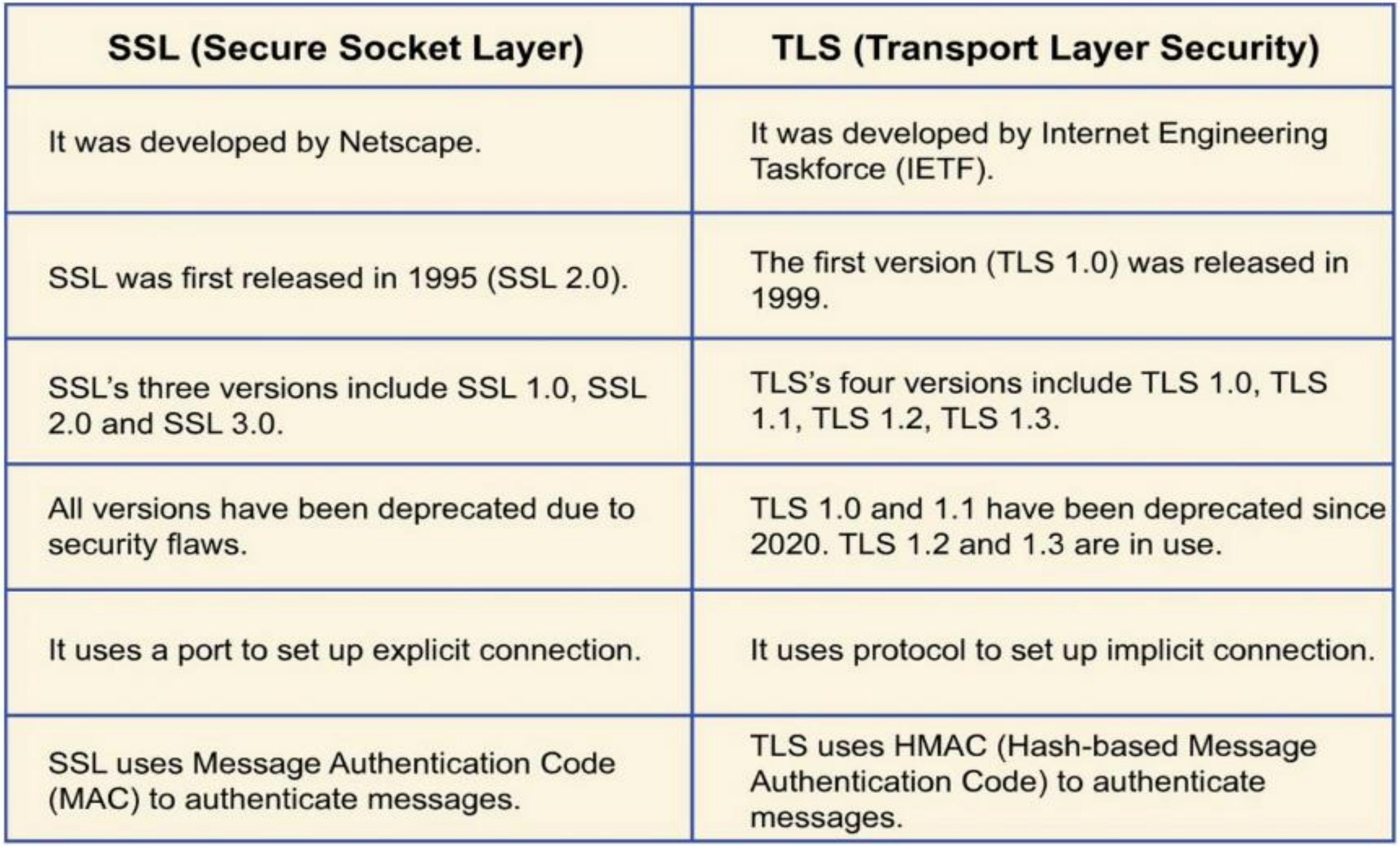
There are different types of SSL certificates, each suited for different needs:

Single-Domain SSL Certificate: This type covers only one specific domain. A domain is the name of a website, like www.geeksforgeeks.org. For instance, if you have a single-domain SSL certificate for www.geeksforgeeks.org, it won’t cover any other domains or subdomains.

Wildcard SSL Certificate: Similar to a single-domain certificate, but it also covers all subdomains of a single domain. For example, if you have a wildcard certificate for *.geeksforgeeks.org, it would cover www.geeksforgeeks.org, blog.www.geeksforgeeks.org, and any other subdomain under example.com.

Multi-Domain SSL Certificate: This type can secure multiple unrelated domains within a single certificate.

Difference between SSL & TSL



SSL (Secure Socket Layer)	TLS (Transport Layer Security)
It was developed by Netscape.	It was developed by Internet Engineering Taskforce (IETF).
SSL was first released in 1995 (SSL 2.0).	The first version (TLS 1.0) was released in 1999.
SSL's three versions include SSL 1.0, SSL 2.0 and SSL 3.0.	TLS's four versions include TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
All versions have been deprecated due to security flaws.	TLS 1.0 and 1.1 have been deprecated since 2020. TLS 1.2 and 1.3 are in use.
It uses a port to set up explicit connection.	It uses protocol to set up implicit connection.
SSL uses Message Authentication Code (MAC) to authenticate messages.	TLS uses HMAC (Hash-based Message Authentication Code) to authenticate messages.

Any Query????

Thank you……