SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMKUR

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

—

Project 5 : SECURE SOCKET LAYER PROTOCOL

Team

Kushala R	1SI18CS049
A M Siri	1SI18CS139
Prerana R Shetty	1SI18CS077
Sinchana P	1SI18CS109

Under the guidance of

Mrs.Shwetha A N
Assistant Professor
Dept of CSE, SIT

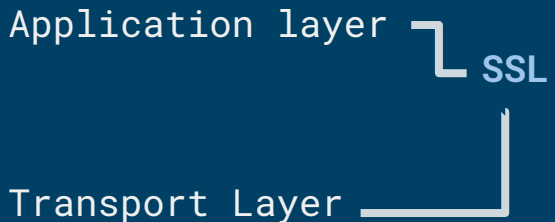
PROBLEM STATEMENT

Visualize different state transitions that happen as part of SSL protocol and how handshake is completed along with various parameters that are exchanged.
Input: Packet Capture of SSL.

What is SSL?

- Secure Socket Layer
- Security to data that is transferred between web browser and server.
- Encrypts the link to ensure privacy and security from data breaches and attacks

Where is SSL?



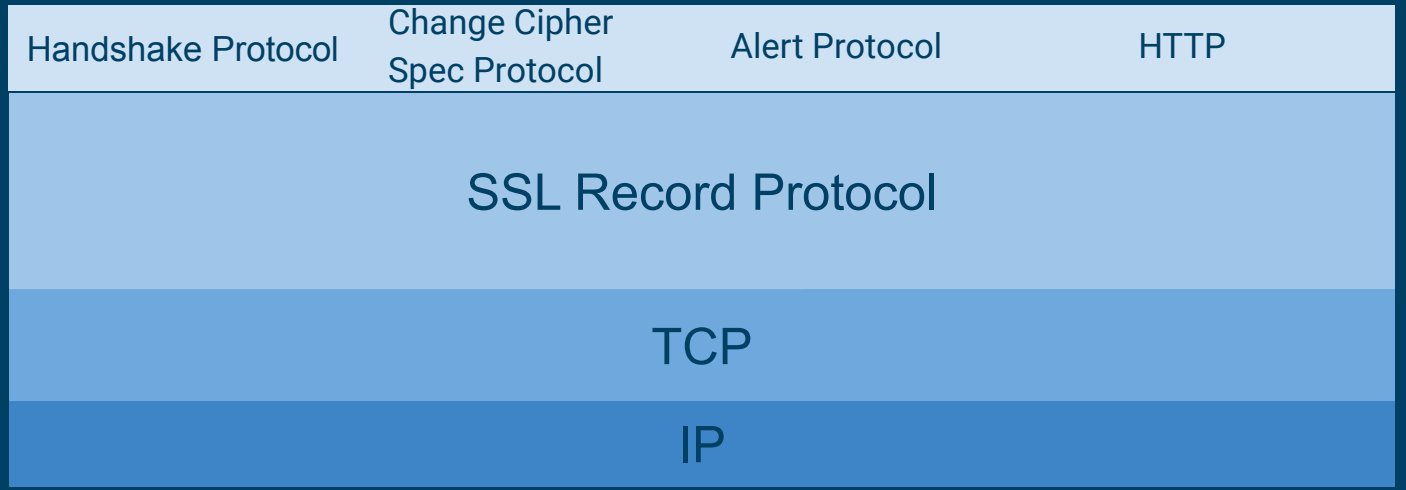
KEY RESPONSIBILITIES

Integrity

Authentication

Confidentiality

SSL PROTOCOL STACK



HANDSHAKE

- Establish sessions
- Authentication (Client - Server)

CHANGE CYPHER SPEC

- Pending state to be copied to current state
- Change Encryption

SSL RECORD

- Confidentiality
- Message Integrity

ALERT

- SSL related Alerts to peer entity

HANDSHAKE PROTOCOL

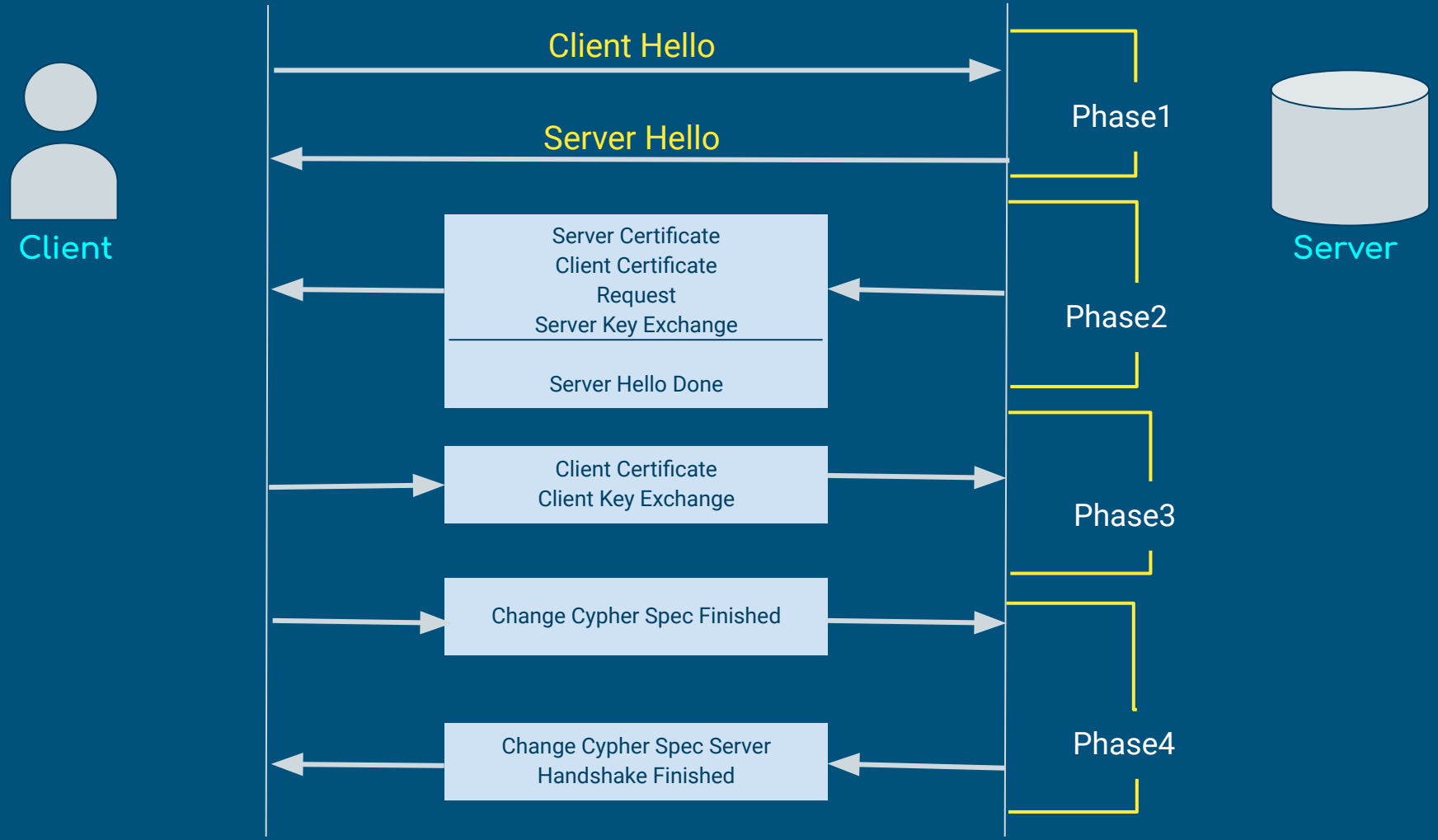
- Used to establish **sessions.**
- Allows client and server to **authenticate** with each other by sending a series of messages to each other.

Phase-1:
- Both Client and Server send **hello-packets** to each other.
- In this IP session, cipher suite and protocol version are exchanged for security purpose.

Phase-2:
- Server sends its certificate and **Server-key-exchange.**
- Server ends the phase-2 by sending Server-hello-end packet.

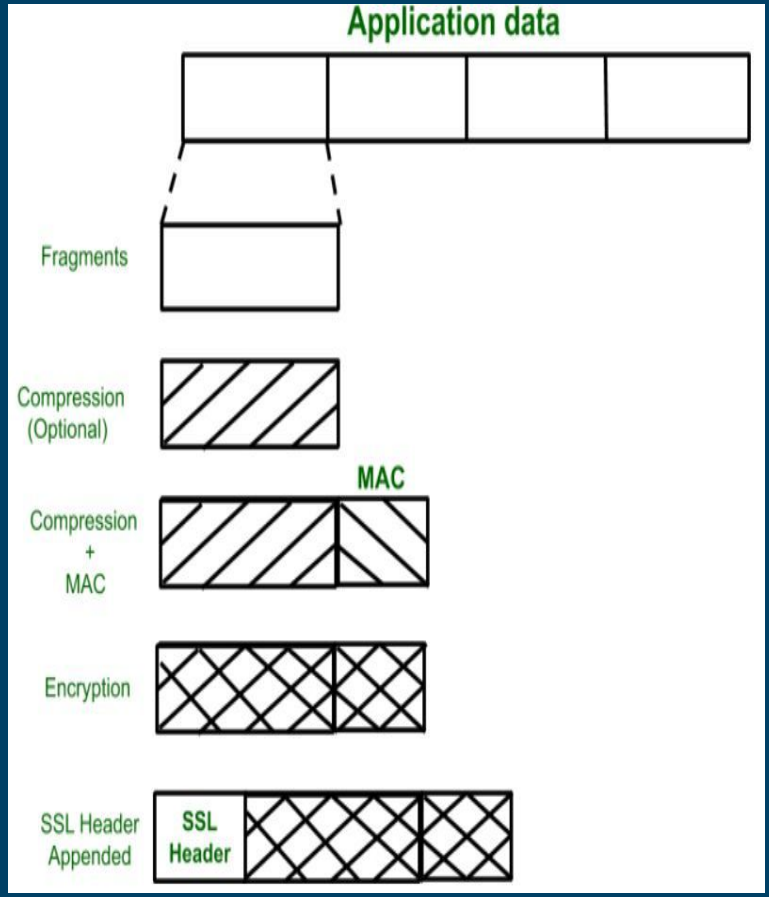
Phase-3:
- In this phase Client replies to the server by sending its certificate and **Client-exchange-key**.

Phase-4:
- Change-cipher suite occurs
- Handshake Protocol ends.


Client
Client Hello
Server Hello
Server Certificate
Client Certificate
Request
Server Key Exchange
Server Hello Done
Client Certificate
Client Key Exchange
Change Cypher Spec Finished
Change Cypher Spec Server
Handshake Finished
Phase1
Phase2
Phase3
Phase4
Server

SSL RECORD PROTOCOL

- Application data is **divided into fragments.**
- The fragment is compressed and encrypted MAC (Message Authentication Code) is generated by algorithms like SHA .
- MD5 is appended.
- Later, encryption of the data is done
- Atlast SSL header is appended to the data.



Onto Analysis