Unit-4

Transport Level Security

Website Security Consideration

- Websites are always to prone to security risks. **Cyber crime** impacts your business by hacking your website. Your website is then used for hacking that install malicious software or malware on your computer.

1. Updated Software

   It is mandatory to keep you software updated. It plays vital role in keeping your website secure.

2. SQL Injection

It is an attempt by the hackers to manipulate your database. It is easy to insert rogue code into your query that can be used to manipulate your database such as change tables, get information or delete data.

3. Cross Site Scripting (XSS)

It allows the attackers to inject client side script into web pages. Therefore, while creating a form It is good to endure that you check the data being submitted and encode or strip out any HTML.

4. Error Messages

   You need to be careful about how much information to be given in the error messages. For example, if the user fails to log in the error message should not let the user know which field is incorrect: username or password.

5. Validation of Data

   The validation should be performed on both server side and client side.

6.Passwords

- It is good to enforce password requirements such as of minimum of eight characters, including upper case, lower case and special character. It will help to protect user’s information in long run.

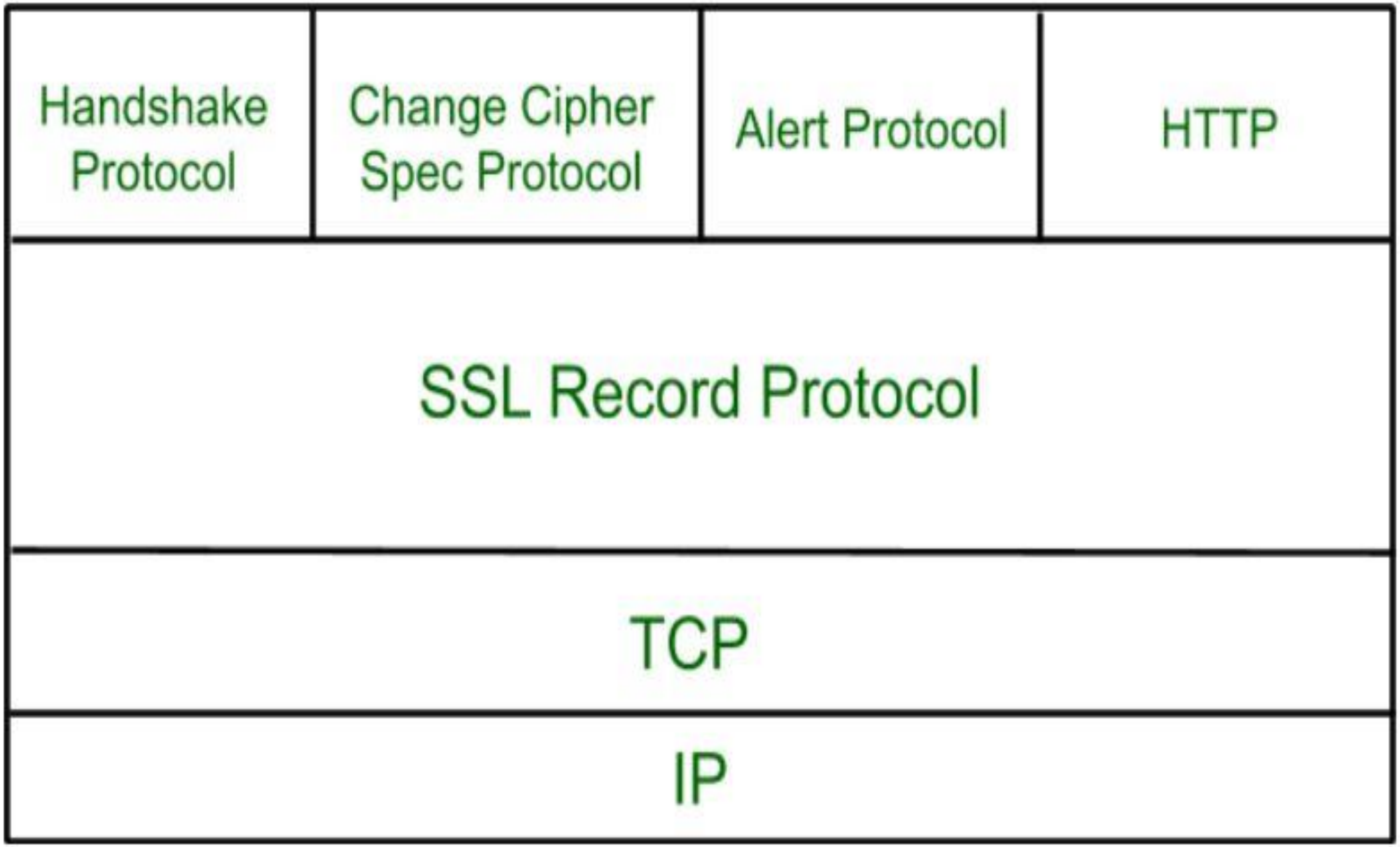
Secure Socket Layer (SSL)

- **Secure Socket Layer (SSL)** provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

- **SSL Protocol Stack:**



Handshake Protocol

Change Cipher Spec Protocol

Alert Protocol

HTTP

SSL Record Protocol

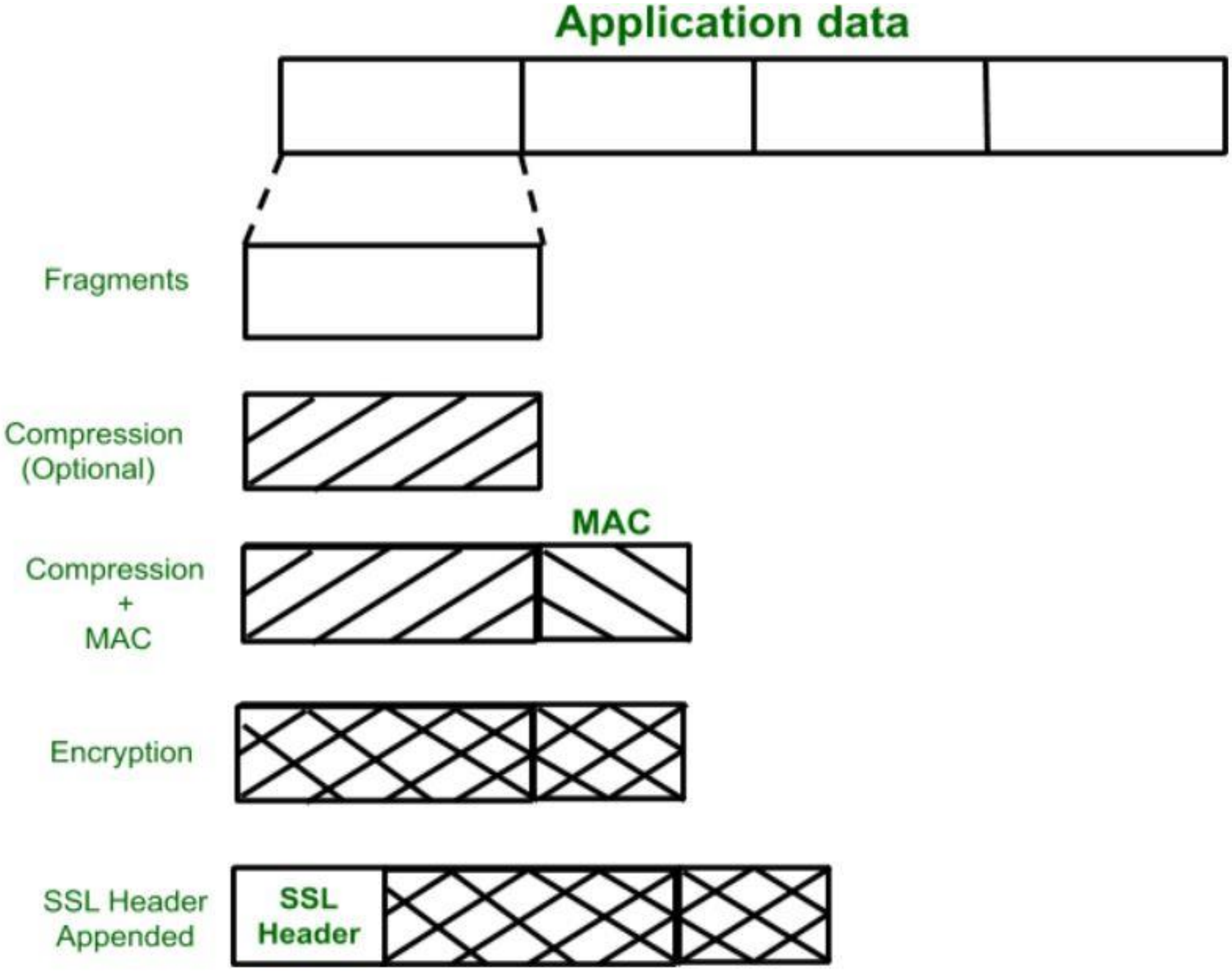
TCP

IP

- **SSL Record Protocol:**

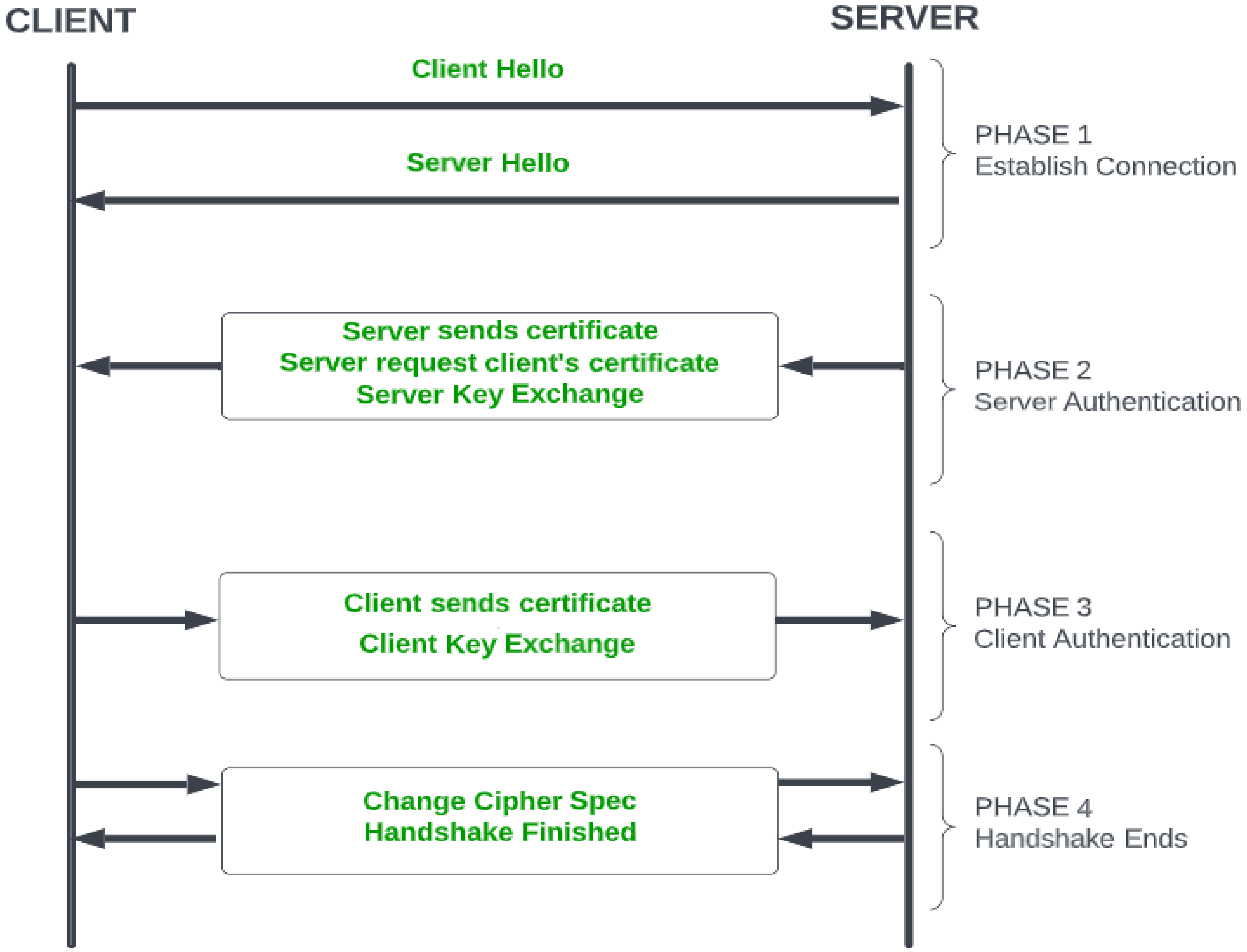
SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity


Application data
Fragments
Compression
(Optional)
MAC
Compression
+
MAC
Encryption
SSL Header
Appended
SSL
Header

- **Handshake Protocol:**

  Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.



SSL HANDSHAKE 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:

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

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.

HTTPS

- **HTTPS** stands for **Hyper Text Transfer Protocol Secure**. HTTP Secure (HTTPS), could be a combination of the Hypertext Transfer Protocol with the SSL/TLS.
- It is an additional layer of security which is provided by TLS/SSL.
- Ex: Website starting with(https:\\)
- It is more secured compared to http.
- Why it is more secure because in http the

data is in the form of plain text only.

- In http-the client sends data in PT.
- The server again sent it in PT only.
- In https-data is in the form of PT and CT.
- Here encryption and decryption takes place.
- Https belongs to Transport Layer Protocol.
- It runs on Port Number 443 of server.
- The server will have different ports.
- It uses a Certificate Authority(CA).

- It works on Asymmetric PKI and uses 2 different keys.
- Usage: Banking websites, Login Credentials.