Topic: HTTP & HTTPs

The Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) are foundational technologies of the World Wide Web, enabling the communication between web browsers and servers.

HTTP (Hypertext Transfer Protocol)

- Purpose: HTTP is a protocol used for transferring hypertext requests and information on the internet. It defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands. Essentially, it facilitates the retrieval of web-based data and resources, such as HTML documents, images, and videos, making them accessible in a web browser.
- Operation:
  - Client-Server Communication: When a user enters a URL in their web browser or clicks a link, the browser sends an HTTP request to the server where the website is hosted. This request includes a method, such as GET (to retrieve data) or POST (to submit data).
  - Stateless Protocol: HTTP is stateless, meaning it doesn't remember previous interactions. Each request from a client to server is treated as new, with no memory of past sessions. This is where cookies come into play, allowing servers to remember users and their activities.
  - Response: The server processes the request and sends back a response, which includes a status code indicating whether the request was successful (e.g., 200 OK) and the requested content if available. The browser then displays the content to the user.

HTTPS (Hypertext Transfer Protocol Secure)

- Purpose: HTTPS is the secure version of HTTP, designed to protect the integrity and confidentiality of data exchanged between the user's browser and the website. It aims to prevent eavesdropping, tampering, and message forgery by encrypting the data in transit.
- Operation:
  - Encryption: HTTPS uses Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL), to encrypt the data. This means that any information sent from the browser to the server and vice versa is encrypted, making it difficult for hackers to intercept and understand.
  - Certificate and Handshake Process :When a browser connects to an HTTPS server, the server presents a certificate to the browser, verifying that the server is legitimate and that the session is secure. This is part of the SSL/TLS handshake process, which also involves the browser and server agreeing on the encryption algorithms they will use to secure the data.
  - Secure Indicators: Browsers typically indicate an HTTPS connection with a padlock icon or similar in the address bar, reassuring users that their connection is secure.

Topic: HTTP & HTTPs

In summary, while HTTP is essential for the basic retrieval and display of web content, HTTPS adds a layer of security by encrypting the data in transit, protecting against eavesdroppers and ensuring that data sent and received is not tampered with. The move towards a more secure web means that HTTPS is becoming the standard for all web traffic.