HTTP & HTTPS — Technical Summary

Basics of Web Communication Protocols

Prepared by: Selena Gómez
Date: 2025

HTTP & HTTPS — Educational Document
Holberton School

1. Differences between HTTP and HTTPS

HTTP (Hypertext Transfer Protocol) is the base protocol that allows communication between browsers and servers. It does not encrypt information, making it vulnerable to espionage and manipulation.

HTTPS (Hypertext Transfer Protocol Secure) adds a layer of security using SSL/TLS, which encrypts data to protect it during transmission.

Key differences:

- HTTP transmits data unencrypted; HTTPS uses encryption.

- HTTPS ensures confidentiality, integrity and authenticity.

- HTTPS is essential for sites with sensitive data.

2. Structure of an HTTP Request and Response

HTTP Request Example

GET /index.html HTTP/1.1
Host: example.com
User-Agent: Chrome/120
Accept: text/html

Components:

- Method: GET

- Path: /index.html

- Version: HTTP/1.1

- Headers: information sent by the client

- Body: usually empty in GET requests

HTTP Response Example

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 512

Components:

- Status code (200 OK)

- Headers sent by the server

- Body: returned content

Diagram — Simplified HTTP Flow

CLIENT ----------> SERVER
HTTP Request

CLIENT <---------- SERVER
HTTP Response

3. Common HTTP Methods

- GET: Gets data from the server. Example: load a web page.

- POST: Send data to the server. Example: submit a form.

- PUT: Updates or completely replaces an existing resource.

- DELETE: Deletes a resource from the server.

4. Common HTTP Status Codes

- 200 OK: The request was successful.
- 301 Moved Permanently: The resource has been moved permanently.
- 400 Bad Request: The client's request is invalid or poorly formed.
- 403 Forbidden: The client does not have permissions to access the resource.
- 404 Not Found: The requested resource does not exist.
- 500 Internal Server Error: Internal error on the server.