**Topic: HTTP and HTTPS**

Reading Time: 15 mins

**·        Note\* Highlight important/core points while reading**

·        Read the content and write the answers given in the document in your words, to get the solid grip on topic.

**HTTP and HTTPS**

HTTP (**Hypertext Transfer Protocol**) and HTTPS (**Hypertext Transfer Protocol Secure**) are the two main protocols used for communication between web browsers and web servers on the **World Wide Web (WWW)**.

**1. HTTP (Hypertext Transfer Protocol) - Working Mechanism**

HTTP is a **stateless** communication protocol used for transmitting web pages and other resources over the Internet. It follows a **request-response model**, meaning:

1. The user enters a URL in the web browser.
2. The browser sends an **HTTP request** to the web server.
3. The web server processes the request and sends back the requested web page as an **HTTP response**.
4. The browser receives the response and displays the web page to the user.

**Key Features of HTTP:**

* **Stateless** → Each request is independent, meaning the server does not remember previous interactions.
* **Unsecured** → Data is transmitted in **plain text**, making it vulnerable to hackers.
* **Uses Port 80** → Default port for HTTP communication.
* **Faster than HTTPS** → Since it does not involve encryption.

**Example of an HTTP URL:**

http://www.example.com

**2. HTTPS (Hypertext Transfer Protocol Secure)**

HTTPS is a **secure** version of HTTP that encrypts the data transmitted between the web browser and the web server using **SSL (Secure Sockets Layer) or TLS (Transport Layer Security)** encryption.

**How HTTPS Works:**

1. The user enters a URL that starts with https://.
2. The browser requests a **digital certificate (SSL/TLS certificate)** from the web server.
3. The web server provides the certificate, which contains a **public key** for encryption.
4. The browser verifies the certificate’s authenticity (issued by a **Certificate Authority (CA)**).
5. If the certificate is valid, an **encrypted connection** is established between the browser and the server.
6. The browser and server exchange encrypted data, ensuring **secure communication**.

**Key Features of HTTPS:**

* **Encrypted Communication** → Protects user data from hackers.
* **Authentication** → Ensures that the website is genuine and not a fake/phishing site.
* **Uses Port 443** → Default port for HTTPS communication.
* **Slightly Slower than HTTP** → Due to encryption processes.

**Example of an HTTPS URL:**

<https://www.secure-website.com>

**Differences Between HTTP and HTTPS**

|  |  |  |
| --- | --- | --- |
| **Feature** | **HTTP** | **HTTPS** |
| **Security** | Not secure | Secure (encrypted using SSL/TLS) |
| **Data Transmission** | In plain text | Encrypted |
| **Port Used** | 80 | 443 |
| **Speed** | Faster | Slightly slower due to encryption |
| **Authentication** | No authentication | Uses SSL/TLS certificate to verify identity |
| **Usage** | Used for non-sensitive data | Used for secure transactions like online banking, shopping, etc. |

**A-Rated Questions/Answers By Examiner**

**Q1: What is HTTP, and how does it work?**

**Answer:**HTTP (**Hypertext Transfer Protocol**) is a communication protocol used for transmitting web pages and resources over the Internet. It follows a **request-response model**, where:

1. A browser sends an **HTTP request** to a web server.
2. The web server processes the request and responds with the requested web page as an **HTTP response**.
3. The browser then displays the web page to the user.

**Q2: What is the main difference between HTTP and HTTPS?**

**Answer:**The main difference is **security**:

* **HTTP** sends data in plain text and is **not secure**.
* **HTTPS** encrypts data using **SSL/TLS**, making it **secure** against cyber threats like hacking and eavesdropping.

**Q3: Why is HTTPS important for websites handling sensitive data?**

**Answer:**HTTPS is important because it:

1. **Encrypts data** to protect user information (e.g., passwords, credit card details).
2. **Prevents hacking and eavesdropping** by securing communication.
3. **Provides authentication**, ensuring users interact with the genuine website and not a fake or phishing site.

**Q4: What is an SSL/TLS certificate, and what is its role in HTTPS?**

**Answer:**An **SSL/TLS certificate** is a digital certificate issued by a **Certificate Authority (CA)** to secure communication between web browsers and servers. It:

* Provides **encryption** for secure data transfer.
* **Authenticates** the identity of the website.
* Prevents cyber-attacks such as **man-in-the-middle (MITM) attacks**.

**Q5: What are the default ports used for HTTP and HTTPS communication?**

**Answer:**

* HTTP uses **Port 80**.
* HTTPS uses **Port 443**.

### Write your Answers on your Notebook and Verify it on Next Screen

**Q6: How does HTTPS improve user trust and website credibility?**

**Q7: What is a Certificate Authority (CA), and why is it important in HTTPS?**

**Q8: What are some common cyber threats that HTTPS helps protect against?**

**Q9: Why is HTTP still used despite its security risks?**

**Q10: How can a website transition from HTTP to HTTPS?**

**6. Answer:**

1. HTTPS displays a padlock icon in the browser address bar, indicating a secure connection.
2. Websites with HTTPS are less likely to be flagged as "Not Secure" by browsers.
3. Users feel more confident sharing personal and financial information on HTTPS-enabled sites.
4. Search engines like Google prioritize HTTPS websites, improving their ranking in search results.

**7. Answer:**

1. A Certificate Authority (CA) is an entity that issues SSL/TLS certificates to verify website authenticity.
2. CAs ensure that the website is legitimate and not operated by hackers.
3. Popular CAs include Let’s Encrypt, DigiCert, and GlobalSign.
4. Browsers trust HTTPS websites only if their certificates are issued by a recognized CA.

**8. Answer:**

1. **Man-in-the-Middle (MITM) Attacks** – Prevents attackers from intercepting and altering data.
2. **Phishing Attacks** – Ensures users are connecting to legitimate websites, reducing fake site scams.
3. **Data Eavesdropping** – Encrypts communication, preventing hackers from stealing sensitive information.
4. **Data Tampering** – Ensures that data exchanged between the browser and server is not altered.

**9. Answer:**

1. HTTP is faster since it does not require encryption, making it useful for non-sensitive content.
2. Some legacy systems and internal networks still rely on HTTP.
3. HTTPS requires an SSL/TLS certificate, which may be costly for some website owners.
4. Websites that do not handle user data, such as informational blogs, may not prioritize HTTPS.

**10. Answer:**

1. Obtain an SSL/TLS certificate from a trusted Certificate Authority (CA).
2. Install and configure the certificate on the web server.
3. Update internal links and ensure all resources (images, scripts) load over HTTPS.
4. Redirect HTTP traffic to HTTPS using server settings (e.g., 301 redirects in .htaccess).
5. Test and verify the HTTPS implementation to ensure security and performance.