Name : Divesh Jadhwani
Institution : Pimpri Chinchwad University

Communication and Web Technology

- **Introduction:** Understanding how communication protocols and web technologies impact cyber security.
- **Objective:** Learn about secure communication practices and the regulation of cyberspace.
- **Real-life Context:** Importance of secure communication in everyday internet use, such as online banking and messaging apps.

2: Overview of Communication Protocols

- **Definition:** Communication protocols are rules that define how data is transmitted and received over a network.
- **Examples:** HTTP, HTTPS, TCP/IP, FTP, SMTP.
- **Importance:** Ensures reliable and secure data exchange between devices.
- **Real-life Example:** HTTPS used in secure online transactions.

HTTP (HyperText Transfer Protocol)

- **Definition:** HTTP is the foundation of data communication on the web. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands.

- **Function:** When you enter a URL in your browser, HTTP is used to fetch and display the web page.
- **Example:** When you visit a website like `http://example.com`, your browser uses HTTP to request the web page from the server, which then sends the page back to your browser.
- **Real-life Example:** Every time you click on a link or enter a web address, HTTP is being used to retrieve the information and display it to you.

HTTPS (HyperText Transfer Protocol Secure)

- **Definition:** HTTPS is the secure version of HTTP. It uses encryption to secure data being transferred between your browser and the web server.

- **Function:** It ensures that data, such as personal information and passwords, is encrypted and secure from hackers.
- **Example:** When you visit a secure website like `https://bank.com`, HTTPS ensures that your connection is encrypted and secure.
- **Real-life Example:** Online banking, shopping, and any website where you enter sensitive information use HTTPS to protect your data.

TCP/IP (Transmission Control Protocol/Internet Protocol)

- **Definition:** TCP/IP is the basic communication language or protocol of the internet. It allows different devices to communicate over a network.
- **Components:**

    - **TCP (Transmission Control Protocol):** Manages the sending and receiving of all your data as packets.
    - **IP (Internet Protocol):** Handles the address part of each packet so that it gets to the right destination.
- **Function:** Ensures reliable and orderly communication between computers.
- **Example:** When you send an email, TCP/IP is used to break the email into packets, send them, and then reassemble them at the recipient's end.
- **Real-life Example:** Every time you access the internet, whether it's browsing, emailing, or streaming, TCP/IP is working behind the scenes.

FTP (File Transfer Protocol)

- **Definition:** FTP is a standard network protocol used to transfer files from one host to

another over a TCP-based network, such as the internet.

- **Function:** Used for transferring files between computers on a network.
- **Example:** When you download software from a website, FTP might be used to transfer the file from the server to your computer.
- **Real-life Example:** Web developers often use FTP to upload files from their computer to a web server.

SMTP (Simple Mail Transfer Protocol)

- **Definition:** SMTP is a protocol for sending email messages between servers. Most email systems that send mail over the internet use SMTP to send messages from one server to another.
- **Function:** Handles the sending of email messages.

- **Example:** When you send an email from your email client (like Outlook or Gmail), SMTP is used to send your message to the mail server, and then to the recipient's mail server.
- **Real-life Example:** Every email you send, whether for work or personal use, travels via SMTP to reach its destination.

3: Role of Web Technologies in Cyber Security

- **Definition:** Web technologies include web browsers, web servers, and various protocols that enable the functioning of the web.
- **Importance:** Plays a crucial role in data transmission, user authentication, and secure communications.
- **Examples:** SSL (Secure Sockets Layer) and TLS (Transport Layer Security) for

secure communication, firewalls for protection, secure coding practices.

- **Security of SSL and TLS:**

  SSL had several security vulnerabilities that led to the development of TLS.

  TLS includes enhancements and fixes over SSL, providing better security and performance.

  How TLS is better :

  - **SSL:** Uses the Message Authentication Code (MAC) after encrypting the data.
  - **TLS:** Uses the HMAC (Hash-based Message Authentication Code) before encrypting the data, enhancing security.
  - **Real-life Example:** Use of SSL/TLS to secure e-commerce transactions.

4: Secure Communication Practices

- **Definition:** Methods to ensure that data sent over the internet is protected from unauthorized access and tampering.
- **Practices:** Encryption, secure protocols (HTTPS, Secure File Transfer Protocol (SFTP)), VPNs, two-factor authentication (2FA).
- **Importance:** Protects sensitive information like personal data and financial transactions.
- **Real-life Example:** Use of VPNs to secure remote work communications.

5: Case Study: The Importance of HTTPS

- **Overview:** Google's push for HTTPS adoption to improve web security.
- **Details:** Non-HTTPS sites marked as "Not Secure" in Chrome, leading to a significant increase in HTTPS adoption , first ranking , and Let's Encrypt scheme,

which provides free SSL/TLS certificates, making it easier and more affordable for website owners to implement HTTPS.

- **Impact:** Improved data security, increased user trust.
- **Lessons Learned:** The importance of secure protocols in protecting user data.

6: Legal and Ethical Considerations in Cyber Security

- **Overview:** Understanding the legal and ethical responsibilities in cyber security.
- **Legal Aspects:** Compliance with laws such as GDPR, CCPA, HIPAA.

  GDPR (General Data Protection Regulation

  ): A law in Europe to protect personal data and privacy for people in the European Union (EU).

- Companies must get permission before collecting personal data.
- They must be clear about what data is being collected and why.
- People have control over their data and can ask for it to be deleted.

INDIA’s - Personal Data Protection Bill, 2019 (PDPB) India's Information should only be with indians.

CCPA (California Consumer Privacy Act

): A law in California, USA, to protect personal information of California residents.

- Companies must tell people what data they collect about them.
- People can see what data is collected and request it to be deleted.
- People can stop companies from selling their data.

HIPAA (Health Insurance Portability and Accountability Act

): A U.S. law to protect sensitive patient health information.

Healthcare providers must keep patient information private and secure.

They must inform patients if there is a breach (unauthorized access) of their information

- **Ethical Aspects:** Responsible disclosure of vulnerabilities, ethical hacking, protecting user privacy.
- **Real-life Example:** GDPR enforcement and its impact on global data protection practices.

7: International Cyber Security Regulations

- **Overview:** Different countries have various regulations to protect data and privacy.
- **Examples:** GDPR in Europe, CCPA in California, Cybersecurity Law in China.
- **Importance:** Ensures a standard level of protection across borders, helps in international cooperation against cyber threats.
- **Real-life Example:** Cross-border data transfer requirements under GDPR.

8: Compliance and Enforcement Challenges

- **Challenges:** Diverse regulatory environments, rapid technological changes, resource constraints.
- **Strategies:** Regular audits, staying updated with regulations, investing in compliance tools.

- **Real-life Example:** Challenges faced by multinational corporations in complying with varying data protection laws.

9: Case Study: Facebook and GDPR Compliance

- **Overview:** Facebook's efforts to comply with GDPR.
- **Details:** Implementation of data protection measures, updates to privacy policies, and user consent mechanisms.
- **Impact:** Increased transparency and user control over data.

Clear History Tool

Increased Privacy Controls

- **Lessons Learned:** The importance of proactive compliance with data protection regulations.

10: Future Trends in Cyber Security and Regulation

- **Emerging Trends:** Increased focus on AI and machine learning, zero trust security models, stricter regulations.
- **Importance:** Staying ahead of evolving threats and regulatory requirements.
- **Real-life Example:** Adoption of AI for threat detection and response.

Quiz s

11: Quiz - Communication Protocols

- **Question:** What is the primary purpose of communication protocols?
  - **Options:**
    - A) To create web pages

        - B) To define rules for data transmission
        - C) To store data
        - D) To monitor network traffic

12: Quiz - Secure Communication Practices

- **Question:** Which of the following is a secure communication practice?
    - **Options:**
        - A) Using HTTP
        - B) Sharing passwords via email
        - C) Using two-factor authentication (2FA)
        - D) Disabling firewalls

13: Quiz - International Cyber Security Regulations

- **Question:** Which regulation is known for its strict data protection rules in Europe?

- **Options:**
  - A) HIPAA
  - B) CCPA
  - C) GDPR
  - D) Cybersecurity Law of China