

5.2 Lesson: Secure Communication Protocols (HTTPS, SSH, SFTP)

Secure Communication Protocols play a crucial role in ensuring the safety and integrity of data transmitted over networks. Among these, HTTPS (Hypertext Transfer Protocol Secure) is widely used for secure communication on the internet, encrypting data between web browsers and servers to protect sensitive information such as login credentials and personal details from interception by malicious actors.

SSH (Secure Shell) is another vital protocol that provides a secure channel over an unsecured network. It enables secure remote logins and command execution on networked devices. SSH employs strong encryption methods to safeguard against eavesdropping, connection hijacking, and other attacks while ensuring the authenticity of both users and devices involved in the communication.

SFTP (Secure File Transfer Protocol), closely related to SSH, facilitates safe file transfers over a secure connection. Unlike its predecessor FTP (File Transfer Protocol), which transmits data in plaintext, SFTP encapsulates file transfer sessions within a secure shell session. This ensures that files transferred between clients and servers are encrypted, offering protection against tampering and unauthorised access during transit.

Collectively, these protocols form the backbone of secure online activities by providing mechanisms for encrypted communication, safeguarding sensitive information from cyber threats, and enhancing overall trust in digital interactions.