UNIT-1V

TRANSPORT LEVEL SECURITY AND WIR ELESS NETWORK SECURITY

1. Transport Layer Security (TLS)

Introduction

Transport Layer Security (TLS) is a cryptographic protocol used to secure communication over computer networks. It provides:

- Confidentiality (Privacy)
- Integrity (Data protection)
- Authentication (Identity verification)

TLS is the successor of SSL (Secure Socket Layer).

TLS Services – Detailed Description

1. Authentication:

Authentication is the process of verifying the identity of communicating parties. In TLS, authentication ensures that the client is communicating with the legitimate server and not with an attacker pretending to be the server.

TLS Provides Authentication

- The server sends a **Digital Certificate** issued by a trusted **Certificate Authority (CA)**.
- The client verifies the certificate before establishing the connection.
- This confirms the server's identity.

Example

When you access an online banking website using HTTPS, TLS verifies that the website actually belongs to the bank and not a fraudulent website.

Benefits

- Prevents impersonation attacks.
- Protects users from fake websites.
- Builds trust between client and server.

2. Confidentiality

Confidentiality ensures that information exchanged between the client and server remains private and cannot be read by unauthorized parties.

TLS Provides Confidentiality

- TLS encrypts data using symmetric encryption algorithms such as **AES**.
- Even if attackers intercept the transmitted data, they cannot understand it without the decryption key.

Example

When a user enters a credit card number on an e-commerce website, TLS encrypts the information before transmission.

Benefits

- Protects sensitive information.
- Prevents eavesdropping.
- Ensures privacy during communication.

3. Data Integrity

Data Integrity ensures that the transmitted data is not altered, modified, or tampered with during transmission.

TLS Provides Data Integrity

- TLS uses cryptographic hash functions such as **SHA-256**.
- A Message Authentication Code (MAC) or authentication tag is generated.
- The receiver verifies the integrity of the received message.

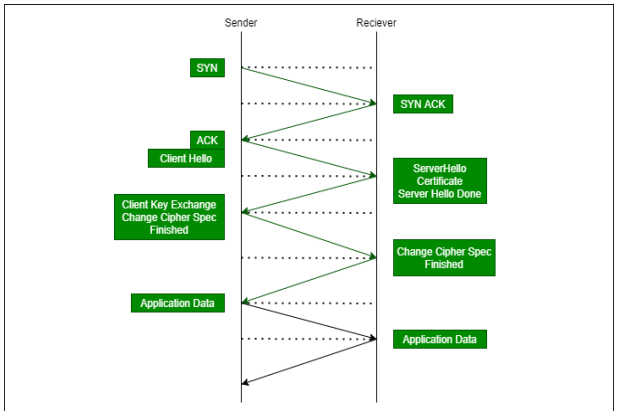
Example

If an attacker attempts to change the amount in an online banking transaction, TLS detects the modification and rejects the altered data.

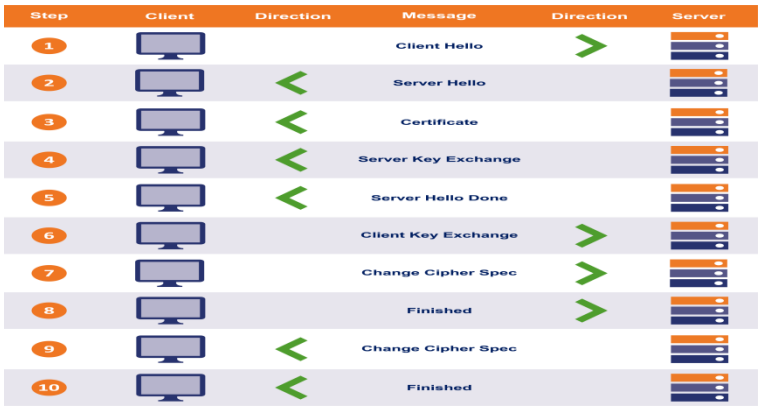
Benefits

- Detects unauthorized changes.
- Prevents data tampering.
- Ensures accurate communication.

TLS Architecture



TLS Handshake Process



TLS Working

The TLS (Transport Layer Security) Handshake is the process used to establish a secure communication channel between a client and a server.

Steps in TLS Handshake

1. Client Requests Connection

- The client (browser) sends a **Client Hello** message to the server.
- It includes:

- TLS version supported
- List of supported cipher suites
- Random number (Client Random)

2. Server Sends Certificate

- The server responds with a **Server Hello** message.
- The server sends its **Digital Certificate** containing its public key.
- The certificate is issued by a trusted Certificate Authority (CA).

3. Certificate is Verified

- The client verifies:
  - Certificate validity
  - Certificate Authority signature
  - Domain name matching
- If verification fails, the connection is terminated.

4. Session Key is generated

- The client generates a **Pre-Master Secret**.
- Using key exchange algorithms (RSA, Diffie-Hellman, ECDHE), both client and server derive the same **Session Key**.
- This key is used for encryption during the session.

5. Data is Encrypted Using Symmetric Encryption

- After the session key is established:
  - Client and server use symmetric encryption (AES, ChaCha20, etc.).
  - Symmetric encryption is faster than public-key encryption.

6. Secure Communication Begins

- Both parties exchange encrypted messages.
- Confidentiality, Integrity, and Authentication are ensured.
- Data transmitted cannot be read or modified by attackers.

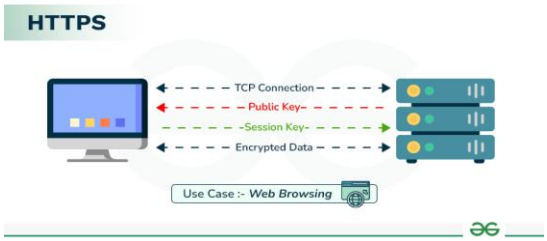
Advantages

- Strong encryption
- Secure authentication
- Data integrity
- Protection against eavesdropping

2. HTTPS (Hyper Text Transfer Protocol Secure)

HTTPS is the secure version of HTTP that uses TLS/SSL to protect web communication.

HTTPS Architecture



Features

- Encrypts web traffic
- Prevents data theft
- Provides authentication
- Ensures integrity

HTTPS Process

User Request
|
TLS Handshake
|
Encrypted Communication
|
Secure Web Page

Benefits

- Secure online banking
- Secure e-commerce
- Protection from hackers

3. Secure Shell (SSH)

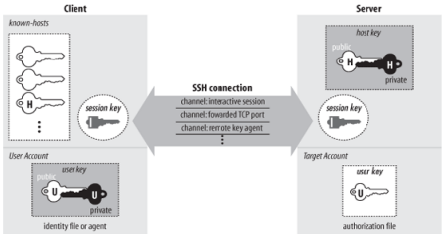
Introduction

SSH is a protocol used for secure remote login and secure file transfer.

SSH Services

- Remote Login
- Secure Command Execution
- File Transfer
- Port Forwarding

SSH Architecture



SSH Authentication Methods

1. Password Authentication

2. Public Key Authentication

SSH Working

Client Request
|
Key Exchange
|
Authentication
|
Secure Session

Advantages

- Strong security
- Remote administration
- Secure file transfer

4. Wireless Network Security

Wireless security protects wireless networks from unauthorized access.

Security Threats

- Eavesdropping
- Unauthorized Access
- Rogue Access Points
- Denial of Service Attacks

Wireless Security Model

User Device
|
Wi-Fi
|
Access Point
|
Internet

5. Mobile Device Security

Objectives

- Protect data
- Secure applications
- Prevent malware attacks

1. Malware

Definition

Malware (Malicious Software) is any software intentionally designed to damage, disrupt, steal data, or gain unauthorized access to a mobile device or computer system.

Types of Malwares

- **Virus** – Attaches itself to files and spreads when executed.
- **Worm** – Self-replicates and spreads across networks.
- **Trojan Horse** – Appears legitimate but performs malicious activities.

- **Spyware** – Secretly collects user information.
- **Ransomware** – Encrypts data and demands payment for recovery.

Effects of Malware

- Theft of personal information
- Data corruption or deletion
- Unauthorized access to accounts
- Device performance degradation

Prevention

- Install antivirus software
- Download apps only from trusted sources
- Regularly update operating systems
- Avoid suspicious links and attachments

2. Phishing

Phishing is a cyberattack in which attackers trick users into revealing sensitive information such as passwords, banking details, or personal data by pretending to be a trusted entity.

Phishing Works

1. Attacker sends a fake email, SMS, or website link.
2. User believes it is legitimate.
3. User enters confidential information.
4. Attacker steals the information.

Common Types

- Email Phishing
- SMS Phishing (Smishing)
- Voice Phishing (Vishing)
- Website Phishing

Effects

- Identity theft
- Financial loss
- Unauthorized account access
- Data breaches

Prevention

- Verify sender information
- Avoid clicking unknown links
- Enable two-factor authentication

3. Device Theft:Device theft refers to the physical loss or stealing of a mobile phone, tablet, or laptop containing sensitive information.

Risks Associated with Device Theft

- Unauthorized access to personal data
- Exposure of passwords and financial information
- Identity theft
- Corporate data leakage

Consequences

- Loss of confidential files
- Unauthorized transactions
- Privacy violations
- Misuse of stored credentials

Prevention

- Use strong passwords or PINs
- Enable biometric authentication
- Encrypt device storage
- Activate remote tracking and wiping features
- Regularly back up important data

4. Data Leakage

Definition

Data leakage is the unauthorized transmission, exposure, or disclosure of sensitive information to external parties.

Causes of Data Leakage

- Insecure applications
- Weak security settings
- Malware infections
- Lost or stolen devices
- Human errors

Examples

- Sharing confidential documents accidentally
- Uploading sensitive data to unsecured cloud storage
- Sending information to the wrong recipient

Effects

- Financial losses
- Reputation damage
- Legal penalties
- Loss of customer trust

Prevention

- Use encryption
- Implement access controls
- Regular security audits
- Employee awareness training

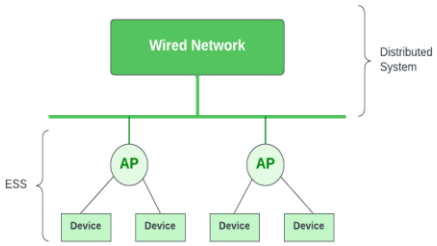
- Secure data backup systems

Security Measures

6. IEEE 802.11 Wireless LAN

IEEE 802.11 is the standard for Wi-Fi networks.

Components



Services

1. Association

Definition

Association is the process by which a wireless device (station) establishes a connection with a Wireless Access Point (AP).

Purpose

- Allows a device to join a wireless network.
- Enables communication between the device and the access point.

Working

1. The device scans for available Access Points.
2. The user selects a Wi-Fi network.
3. The device sends an association request.
4. The Access Point accepts the request and assigns resources.

Example

When a smartphone connects to a home Wi-Fi network, it first performs the association process.

2. Authentication

Definition

Authentication is the process of verifying the identity of a wireless device before allowing it to access the network.

Purpose

- Prevent unauthorized access.
- Ensure only legitimate users connect to the network.

Working

1. Device requests network access.
2. Access Point verifies credentials.
3. Authentication succeeds or fails.
4. Access is granted only to authorized users.

Example

Entering a Wi-Fi password to connect to a secured wireless network.

Authentication Methods

- Open System Authentication
- Shared Key Authentication
- WPA/WPA2 Authentication

3. Roaming

Roaming is the ability of a wireless device to move from one Access Point to another without losing network connectivity.

Purpose

- Provides uninterrupted communication.
- Supports user mobility within a wireless network.

Working

1. Device moves away from the current AP.
2. Signal strength decreases.
3. Device detects a stronger AP.
4. Connection is transferred automatically to the new AP.

Example

A student walking across a college campus remains connected to Wi-Fi while moving between different access points.

Advantages

- Continuous connectivity
- Improved user experience
- Mobility support

4. Data Delivery

Data Delivery is the service responsible for transmitting data packets between wireless devices and the network.

Purpose

- Ensure reliable communication.
- Deliver data from sender to receiver.

Working

1. Device sends data frames.
2. Access Point receives the frames.

3. Frames are forwarded through the network.
4. Destination device receives the data.

Example

Sending an email or browsing a website through a Wi-Fi network.

Advantages

- Reliable communication
- Efficient data transfer
- Supports various network applications

Advantages

- Mobility
- Easy Installation
- Scalability

7. IEEE 802.11i Wireless LAN Security

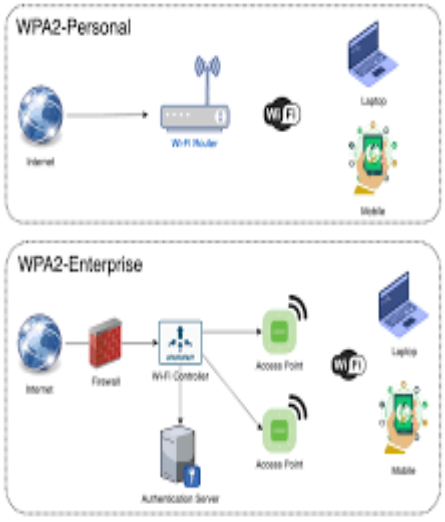
Introduction

IEEE 802.11i improves WLAN security using WPA2.

Security Features

- AES Encryption
- Authentication
- Key Management

WPA2 Architecture



Benefits

- Strong encryption
- Better authentication
- Protection against attacks