📘 Unit 5 : Communication Security & System Security

Communication Security

Communication security refers to the protection of data transmitted over a communication network. It involves various techniques and protocols to ensure the following:

- **Confidentiality**: Ensuring data is only accessible to authorized users.
- **Integrity**: Ensuring data is not altered during transmission.
- **Availability**: Ensuring data is available to authorized users when needed.

HTTPS - Hypertext Transfer Protocol Secure

HTTPS is a secure version of HTTP that uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt data transmitted between a web server and a web browser.

Key Features:

- **Encryption**: HTTPS encrypts data using cryptographic algorithms to protect it from eavesdropping.
- **Authentication**: HTTPS verifies the identity of the web server and client, preventing man-in-the-middle attacks.
- **Integrity**: HTTPS ensures that data transmitted between the server and client has not been tampered with.

Additional Details:

- **HTTPS (HTTP over SSL)**: A combination of HTTP and SSL/TLS to secure communications between the browser and the server.
- **Documented in**: RFC 2818
- **No fundamental changes**: Whether using SSL or TLS, the mechanism remains largely the same.
- **Uses**: `https://` instead of `http://` and port **443** instead of port **80**.

Data Encrypted:

- URL, document contents, form data, cookies, HTTP headers

Data Not Encrypted:

- IP address of the server
- IP address of the client (Network layer)
- Hostname (in cases of virtual hosting: multiple domain names on a single server)

SSH - Secure Shell

SSH is a protocol for secure network communications, designed to be both simple and inexpensive.

SSH1:

- Provides a secure remote login facility, replacing TELNET and other insecure schemes.
- Offers general client/server capabilities.

SSH2:

- Fixes a number of security flaws found in SSH1.
- Documented in RFCs 4250 through 4254.

Key Use:

- **SSH clients and servers** are widely available and provide secure remote login and X tunneling services.

Wireless Security and Its Threats

Wireless security refers to the protection of data transmitted over wireless networks, such as Wi-Fi.

Common Threats:

- **Eavesdropping**: Unauthorized interception of data transmitted over the wireless network.

- **Man-in-the-middle attacks**: An attacker positions themselves between a client and a server to intercept and manipulate data.
- **Rogue access points**: Unauthorized access points set up within a network to intercept traffic.
- **Denial of Service (DoS) attacks**: Overwhelming a wireless network with traffic to disrupt its normal operation.

IPsec

IPsec is a suite of protocols that provides security for IP networks. It offers authentication, encryption, and key management services.

Key Features:

- **Authentication Header (AH)**: Provides authentication, integrity, and anti-replay protection for IP packets.
- **Encapsulating Security Payload (ESP)**: Provides encryption, authentication, and anti-replay protection for IP packets.
- **Key Management Protocol (IKE)**: Negotiates security associations and manages cryptographic keys.

IPsec Modes

IPsec operates in two primary modes to achieve its security goals:

- **Tunnel Mode**: Provides comprehensive protection for entire IP packets and is often used for network-level security.
- **Transport Mode**: Focuses on protecting the data within IP packets, typically used for individual computer-level security.

Virtual Private Networks (VPNs)

A **VPN** creates a secure, private network connection over a public network, such as the internet. It encrypts data and hides the user's IP address.

Types of VPNs:

- **Site-to-site VPN**: Connects two or more networks over a public network.

- **Remote access VPN**: Allows individual users to connect to a private network remotely.
- **SSL/TLS VPN**: Uses SSL/TLS encryption to create a secure connection between a client and a server.

System Security

System security is the practice of protecting information systems from unauthorized access, modification, or destruction. System security measures help organizations protect sensitive data and prevent cyber threats.

Key Concepts:

- **Malicious software (Malware)**: Software programs designed to exploit vulnerabilities in computing systems.
- **Malicious software**: Software intentionally inserted into a system for harmful purposes.

Categories of Malware

1. **Viruses:** Self-replicating programs that attach themselves to other files and execute when the host file is run.
2. **Worms:** Self-replicating programs that spread independently through networks, often exploiting vulnerabilities.
3. **Logic Bombs:** Malicious code embedded in a program that triggers when a specific condition is met, often a date or event.
4. **Trojan Horses:** Malicious programs disguised as legitimate software, often used to gain unauthorized access to systems.
5. **Backdoors (Trapdoors):** Hidden methods of accessing a computer system, often installed by malware to bypass security measures.
6. **Mobile Code:** Malicious code designed to run on mobile devices, often exploiting vulnerabilities in mobile operating systems.
7. **Exploits:** Programs that take advantage of vulnerabilities in software or hardware to gain unauthorized access or execute malicious code.
8. **Downloaders:** Malware that downloads and installs other malicious software onto a compromised system.

9. **Auto-rooters:** Malware that attempts to gain root or administrator-level access to a system, often on mobile devices.
10. **Kits (Virus Generators):** Tools used to create new malware variants, often sold on the dark web.
11. **Spammer Programs:** Programs that send unsolicited email messages, often used to spread malware or promote scams.
12. **Flooders:** Programs that generate excessive network traffic, often used to disrupt services or overwhelm systems.
13. **Rootkits:** Malware that installs itself at a low level of the operating system to hide its presence and gain control.
14. **Zombie Bots:** Infected computers controlled remotely by a malicious actor, often used to form botnets for various attacks.
15. **Spyware:** Malware that collects information about a user's activities without their knowledge or consent.
16. **Adware:** Malware that displays unwanted advertisements, often without the user's consent

---

Introduction to Firewalls

A **firewall** is any device or software used to filter or control the flow of traffic. Firewalls are typically implemented on the network perimeter and function by defining trusted and untrusted zones.

Zones:

- **Trusted zone**: Most firewalls permit traffic from the trusted zone to the untrusted zone without explicit configuration.
- **Untrusted zone**: Traffic from the untrusted zone to the trusted zone must be explicitly permitted. Any traffic not explicitly permitted from the untrusted to trusted zone is implicitly denied (by default in most firewall systems).
- **Multiple zones**: Firewalls can have multiple 'less trusted' zones, often referred to as **Demilitarized Zones (DMZs)**.

Firewall Services

Firewalls perform several key services:

- **Packet Filtering**
- **Stateful Packet Inspection**
- **Proxying**
- **Network Address Translation (NAT)**

Packet Filtering

Packet Filtering is a core service provided by firewalls. Packets can be filtered (permitted or denied) based on a wide range of criteria:

- Source address
- Destination address
- Protocol Type (IP, TCP, UDP, ICMP, ESP, etc.)
- Source Port
- Destination Port

Stateful Packet Inspection

Stateful packet inspection goes beyond simple packet filtering by tracking TCP or UDP sessions between devices.

Key Features:

- **Session Tracking**: Tracks connections originating from the trusted network. The session information is stored in a state session table, allowing temporary holes to be opened in the firewall for return traffic that would otherwise be denied.
- **DoS Attack Prevention**: Connections from the untrusted network to the trusted network are monitored to prevent Denial of Service (DoS) attacks. If a large number of half-open sessions are detected, the firewall can drop the session, block the source, or send an alert message.

Half-open Sessions:

- **Half-open TCP session**: Indicates the three-way handshake has not yet been completed.

- **Half-open UDP session**: Indicates no return UDP traffic has been detected. A large number of half-open sessions can consume resources and prevent legitimate connections from being established.