Module 7: Network Security – Elaborated Class Notes

---

1. Network Security Architecture

✅ What is Network Security Architecture?

It is the **overall design and framework** that protects an organization's network from unauthorized access, threats, and attacks.
It includes **hardware, software, policies, and procedures**.

Key Components

1. Perimeter Security

- The first boundary of protection.
- Includes:
  - **Firewalls** (filter incoming/outgoing traffic)
  - **Routers with access control**
  - **Gateway security**

Example:
Firewall blocks unknown IPs from entering the company network.

2. Network Segmentation

- Dividing the network into smaller sections (subnets).
- Limits the spread of an attack.

Example;
HR network, Finance network, Student WiFi, Staff WiFi all separated.

---

3. Access Control

Controls **who** can access **what**.

Two types:

3. Access Control

Controls **who** can access **what**.

Two types:

- **Authentication:** Confirming identity (username/password, biometrics, OTP).
- **Authorization:** What the user is allowed to do (read/write/modify).

- Converts data into unreadable format.
- Protects data in:
  - **Transit** (while moving)
  - **Rest** (while stored)

Example:
HTTPS encrypts data between browser and server.

---

5. Monitoring and Logging

- Tracks network activity.
- Helps detect suspicious behaviour.

Example:
Tracking login attempts, failed logins, unusual file downloads.

---

6. Security Policies

Rules and guidelines for employees.

Includes:

- Password rules
- Acceptable use policy
- Incident response procedure

2. Intrusion Detection Systems (IDS)

✅ What is IDS?

IDS is a **monitoring system** that **detects suspicious activity** inside a network.

It does NOT block attacks — it only alerts.

⬘ Types of IDS

1. Network-Based IDS (NIDS)

- Placed on network segments.
- Monitors traffic flowing across the network.

Example:
Detects abnormal traffic from a hacker scanning all computers.

---

2. Host-Based IDS (HIDS)

- Installed on individual systems (laptops/servers).
- Monitors files, logs, system activities.

Example:
Alerts when an important file is changed unexpectedly.

IDS Detection Methods

1. Signature-Based Detection

- Matches traffic with known attack signatures.
- Works like antivirus.

Example:
Detects known malware patterns.

Limitation: Cannot detect new attacks.

---

2. Anomaly-Based Detection

- Uses machine learning / behaviour analysis.
- Detects unusual behaviour.

Example:
User normally downloads 5 files per day → suddenly downloads 500.

🔹 IDS Alerts

- **True Positive:** Attack is correctly detected.
- **False Positive:** Normal traffic marked as attack.
- **False Negative:** IDS misses the attack.

---

3. Intrusion Prevention Systems (IPS)

✅ What is IPS?

IPS not only **detects** threats but also **blocks/prevents** them.

Think: **IDS + Action**

⬘ Functions of IPS

1. Blocking Malicious Traffic

Stops harmful packets automatically.

2. Resetting Connections

Breaks a suspicious network session.

3. Reconfiguring Firewall

Adds blocking rules when threats are detected.

🔷 Types of IPS

1. Network-Based IPS (NIPS)

Placed at key network points to stop threats in real-time.

2. Host-Based IPS (HIPS)

Installed on individual machines to protect them.

🔷 IPS Detection Techniques

- Signature-Based
- Anomaly-Based
- Policy-Based (violations of defined rules)

⭐ IDS vs IPS – Easy Comparison

Feature	IDS	IPS
Purpose	Detect attacks	Detect + Prevent attacks
Action	Sends alerts	Blocks or stops threats
Placement	Monitors traffic	Inline between source and destination
Impact	Passive	Active

---

4. Real-World Examples

✓ Firewall + IDS + IPS combination

A company uses:

- Firewall → Filters traffic
- IDS → Alerts if any suspicious event happens
- IPS → Automatically blocks the suspicious traffic

---

2. Wireless Network Security (WPA, WPA2, WPA3)

⭑ Why Wireless Security Is Important?

Wi-Fi signals travel through air →
Hackers can capture signals if Wi-Fi is not protected.

So wireless security standards are used.

◆ 1. WPA (Wi-Fi Protected Access)

Introduced to replace weak WEP.
Provides:

- Better encryption
- Basic protection

But still vulnerable today.

🔷 2. WPA2

Most commonly used standard for many years.

Features:

- Uses **AES encryption** (very strong)
- Good protection for home and office networks

Weakness:

- Vulnerable to "KRACK Attack"
- Still widely used but not the safest now

🔷 3. WPA3 (Latest and Strongest)

Improvements:

- Stronger encryption

- Better protection even with weak passwords
- Protection against dictionary attacks
- Enhanced security for public Wi-Fi (open networks)

WPA3 Features:

- **SAE (Simultaneous Authentication of Equals)** → prevents password guessing
- **Individualized Data Encryption** → each user gets separate encryption key

Example:
In a café Wi-Fi, even if 50 people connect, each user's data is separately encrypted.

⭐ Comparison Table

Feature	WPA	WPA2	WPA3
Security Level	Medium	Strong	Very Strong
Encryption	TKIP	AES	AES + SAE
Password Protection	Low	Good	Excellent
Public Wi-Fi Protection	No	No	Yes

3. Virtual Private Networks (VPNs) & Remote Access Security

🔹 What is a VPN?

A VPN creates a **secure, encrypted tunnel** between a user and the internet or a company network.

This protects:

- Data confidentiality
- IP address and location
- Online activity

⭐ Why VPN is Used?

1. Secure Remote Access