# 4 Threats to Network Communication:

- Interception - unauthorized viewing
- Interruption - preventing authorized access
- Modification - unauthorized changing
- Fabrication - unauthorized creation

A **network perimeter** is a boundary between the private and locally managed side of the network.

**A perimeter includes**

- Border Routers: They serve as traffic signs for allowing data to flow inside and outside the network, it is the final checkpoint before data connects to untrusted networks like the internet.
- Firewall: It is a device that has a set of rules on which type of traffic to allow or deny to get access to the network.
- Intrusion detection system: It is a single device or collection of sensors placed in the networks to detect and alert admin of any suspicious activity in the network.
- Intrusion Prevention System: Automatically defends the network from attacks without admin intervention
- DMZ/Screened Subsets: They are small networks that contain public facing services and are blocked off from the rest of the network using firewalls

## Interception

Vulnerabilities that lead to interception in networks are:

1. Anonymity: Attackers can make thousands of attempt anonymously from far away
2. Many points of attack - Large network allow attackers access to many entry points for attack
3. Sharing - Networked Systems allow access to multiple users which increases risk
4. System complexity - Networks contain multiple systems each with their own software, protocols, OS, etc. making it difficult to protect all.
5. **Unknown Perimeter -** The network continuously grows and shrinks in size so it is hard to tell which devices belong to the network and which ones are outside it.
6. **Unknown Path -** There may be many paths including untrustworthy ones from one host to another which is a security risk.

Two common interception network attacks are:

**Eavesdropping** is the unauthorized interception of private communication, such as data, voice, or messages, during transmission. This can occur over networks when attackers "listen in" to unencrypted traffic between users, often using packet sniffers or compromised routers. Eavesdropping threatens the confidentiality of data and can be used to steal sensitive information like passwords, financial details, or personal messages.

**Wiretapping** is a form of eavesdropping specifically involving the monitoring of telephone or network communications, often through physical access to cables or tapping into communication lines. It can be legal (when done by law enforcement with proper authorization) or illegal (when done by hackers or malicious actors). Wiretapping can capture conversations, call metadata, or even digital data if done on VoIP systems.

## Interruption

**Loss of service:**
Occurs because of

Routing: Routing is complicated and misconfiguration of one router may cause the poisoning of data of many other routers in the network, causing packets to not reach the intended destination.

Excessive Demand: Network Capacity is finite and can get exhausted, an attacker may generate enough demand to overload a critical part of the network.

Component Failure: Component Failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for.

**Port Scanning:**

**Port scanning** is a technique used to identify open ports and services available on a target device or network. It's commonly used by network administrators to check for vulnerabilities or unauthorized services, but attackers also use it to find entry points for exploitation.

By sending requests to various ports and analyzing the responses, a port scan can reveal which ports are open, closed, or filtered by a firewall. This helps determine what services (like HTTP, FTP, or SSH) are running and if any might be misconfigured or vulnerable to attack.

# Wireless Networks

## Vulnerabilities:

**Confidentiality**: Since every message on wifi is broadcast, attackers who are connected to the network and within range can intercept and read all unencrypted messages.

**Integrity**: When WiFi receives two requests claiming to be the same computer, they accept the one with the greater signal strength as legitimate. This can allow attackers to take over and spoof user sessions using signal boosters

**Availability:** Attacks such as session hijacking, forced disassociation and jamming of signals can take place which threaten availability of connectivity.

**Unauthorised Wifi Access**

**Picking Up the Beacon -** Hidden SSIDs can be obtained by monitoring client requests for SSIDs in absence of beacons from access points

# WEP

Wired Equivalent Privacy or WEP is an early protocol that was developed to secure communications over WiFi. Many weaknesses were discovered in the protocol subsequently, allowing it to be cracked very easily, thus it is no longer in use.

**How it works:**

- Client and Access Point (AP) have a pre-shared key.
- AP sends a random number to the client which the client encrypts using the key and sends to AP.
- AP decrypts the number using the key and sees if it is the same number sent.
- Once the client is authenticated they communicate using messages encrypted with the same key.

**Weaknesses:**

- Weak Encryption Key: The key was only 64 or 128 bits long with 24 (thus making it 40 and 104 bits) reserved for Initialisation Vector, thus making brute force possible. Keys were alphanumeric or hex phrases typed by users, thus making dictionary attacks possible
- Static Key: The value of the key remained the same for many months of communication.
- Weak Encryption Process: The 40 bit key could be brute forced easily and because of vulnerabilities in the encryption algorithm, the104 bit key could also be brute forced.

- Weak Encryption Algorithm: The RC4 algorithm was used in a weird way that allowed attackers to decrypt large portions of any message.
- Faulty Integrity Check: WEP included checksum to detect transmission errors, but failed to include one that addressed malicious modification.
- No Authentication: Any client that knows AP's SSID and MAC address is treated as legitimate.

## WPA

WPA/WPA2 (WiFi Protected Access) was designed as a replacement for WEP and is still used today.

**Strengths:**

- Non Static Keys: Uses a hierarchy of new keys for every new session, thus ensuring confidentiality and integrity. New encryption key is generated for each packet.
- Authentication: It performs authentication by certificates, tokens or password.
- Uses AES as its encryption algorithm which is secure.
- Integrity Protection: It includes a 64 bit integrity check
- Session Initiation: It begins with a 4 way handshake that results in separate keys for encryption and integrity on both ends.

| Feature | WEP (Wired Equivalent Privacy) | WPA (Wi-Fi Protected Access) |
|---|---|---|
| **Introduced** | 1997 | 2003 |
| **Security Level** | Weak | Stronger than WEP |
| **Encryption Algorithm** | RC4 with static key | TKIP (WPA), AES (WPA2/WPA3) |
| **Key Management** | Manual/static keys | Dynamic key generation |
| **Integrity Check** | CRC-32 (vulnerable to tampering) | MIC (Message Integrity Check) |

| | | |
|---|---|---|
| **Vulnerability** | Easily cracked with tools | Much harder to break, especially WPA2/3 |
| **Status** | Obsolete, insecure | WPA2 is standard; WPA3 is the latest |
| **Recommended Use** | Not recommended | Use WPA2 or WPA3 for secure connections |

# Attacks on Availability - DoS and DDoS

**Denial of Service (DoS)** attacks are attempts to disrupt a system's **availability** by overwhelming it through various methods, such as **volumetric attacks**, **application-level exploits**, **disabled communications**, or even **hardware/software failures**.

**Distributed Denial of Service (DDoS)** attacks are a type of DoS attack that uses a **botnet**—a large network of compromised computers—to **simultaneously flood a target** (like a website or server) with traffic. Attackers create these botnets by installing **Command and Control (C2) software** via **malware or unpatched vulnerabilities**, making the attack highly effective and hard to block.

**Types of DDoS attacks:**

**Application Layer Attacks**: They aim to exhaust the resources of the target service and make it incapable of responding to requests. The botnet sends the server a complicated request that takes up resources like database writes or a large download. This brings the server to a crawl or completely stops it. An example is the HTTP Flood attack where the server is overwhelmed with millions of fast HTTP requests.

**Protocol Attacks:** Protocol DDoS attacks target the network layer of the target systems. They try to overwhelm the tablespaces, firewalls or load balancers. These network services on the concept of FIFO. There are a limited number of slots in the queue and the attack aims to fil the queue up with requests while the service struggles to process them. A SYN Flood attack is an example. It makes use of the 3 way handshake of the TCP/IP protocol suite. The attackers send SYN packets with fake IP addresses. The server tries to send an ACK to these fake IPs and waits for the responses to time out which exhausts the resources to deal with the other processes.

**Types of DoS Attacks:**

**Ping Flood**:
This is a basic DoS attack where the attacker sends an overwhelming number of ICMP "echo request" (ping) packets to the target system. The target uses resources to process and reply to each request, which can exhaust its bandwidth or CPU, making it slow or unresponsive.

**Smurf Attack**:
In a Smurf attack, the attacker sends ICMP requests to a network's broadcast address, spoofing the source IP to be the victim's address. All devices on the network reply to the victim, flooding it with traffic and causing a denial of service.

**Teardrop Attack**:
This attack exploits vulnerabilities in how some operating systems handle fragmented IP packets. The attacker sends overlapping packet fragments, which the system fails to

reassemble properly, leading to crashes, freezes, or reboots.

**DNS Spoofing (Cache Poisoning)**:
DNS spoofing involves injecting false DNS records into a DNS server's cache. When users attempt to visit legitimate websites, they are redirected to fake or malicious ones, which can lead to further attacks or data theft. It can also disrupt services if critical domain names are affected.

**Rerouting Routing**:
Routers constantly exchange information about the best paths to reach different network destinations. In a rerouting attack, an attacker sends false routing updates, tricking routers into redirecting traffic through inefficient or non-existent paths. They can lead to dropped packets, network congestion, or service unavailability.

**Session Hijacking**:
Session hijacking occurs when an attacker takes over an established communication session between two systems, often by stealing session tokens or injecting malicious packets.The attacker resets the senders connection while it continues to communicate with reciever.

## Link Encryption

In this encryption mechanism the data is only encrypted before it is placed on the physical communications link, and decrypted just when they arrive at the destination system. I.e at level 1 of the OSI layer.

If there is an intermediate node, the data might be decrypted, and then encrypted for the next link. It is used when transmission lines are the greatest point of vulnerability like wireless networks.

## End to End Encryption

In end to end encryption data is encrypted all the way from layer 7 the application layer. Decryption also occurs at the application layer of the receiver. The important thing is that the intermediate nodes cannot decrypt the data. It is appropriate when sending sensitive data through untrustworthy nodes, eg. over the internet.

| **Link Encryption** | **End-to-End Encryption** |
|---|---|
| **Security within hosts** | |
| Data partially exposed in sending host | Data protected in sending host |
| Data partially exposed in intermediate nodes | Data protected through intermediate nodes |
| **Role of user** | |
| Applied by sending host | Applied by user application |
| Invisible to user | User application encrypts |
| Host administrators select encryption | User selects algorithm |
| One facility for all users | Each user selects |
| Can be done in software or hardware | Usually software implementation; occasionally performed by user add-on hardware |
| All or no data encrypted | User can selectively encrypt individual data items |
| **Implementation considerations** | |
| Requires one key per pair of hosts | Requires one key per pair of users |
| Provides node authentication | Provides user authentication |

## SSL and TLS

SSL (Secure Sockets Layer) is a protocol to protect communication between browser and server. It was later updated and renamed to TLS. (Transport Layer Security)

It is implemented at OSI Layer 4 (Transport Layer) and provides client authentication, server authentication and encrypted communication.

At the start of the communication the client and the server negotiate the cipher suite, a set of encryption algorithms. The server sends a list of cipher suite options and the client chooses from that list. A cipher suite contains

- A digital signature algorithm for authenticity
- An encryption algorithm for Confidentiality
- A hashing algorithm for integrity.

This cipher suite negotiation step is most prone to attacks as servers offer a wide range of suites in the interest of compatibility but a man in the middle attack can choose a weak suite that can then be broken.

Used in HTTPS to protect and secure web communication and allow browsers to authenticate websites.

## Onion Routing

**Onion Routing** is a technique used to ensure **anonymous communication** over a network by encrypting messages in multiple layers, like the layers of an onion.

Here's how it works:

- A message is **wrapped in multiple layers of encryption**, each meant for a different node (or relay) in the network.
- As the message travels through the **onion network**, each node decrypts only its own layer to reveal the next destination.
- No single node knows both the source and the final destination, preserving **anonymity**.
- The final node decrypts the innermost layer and forwards the original message to the intended recipient.

Onion routing is the core technology behind **Tor (The Onion Router)**, widely used for private browsing and bypassing censorship.

## Virtual Private Network (VPN)

A **Virtual Private Network (VPN)** is a service that allows users to securely connect to another network over the internet by creating an **encrypted tunnel** between the user's device and a remote VPN server. It is commonly used to **protect privacy**, **secure communications**, and **bypass geo-restrictions or censorship**.

## How it works:

- When a VPN is activated, all data from the user's device is **encrypted** before being sent over the internet.
- This encrypted data is first routed to a **VPN server**, which then decrypts it and forwards it to the intended destination (e.g., a website or service).
- The response from that destination is sent back to the VPN server, encrypted again, and delivered securely to the user.
- Because of this, the user's **IP address and location are masked**, and external parties (like ISPs, hackers, or government surveillance) **cannot view the actual content** or the true destination of the traffic.

VPNs are especially useful when using **public Wi-Fi** networks, as they prevent unauthorized access to sensitive data. They are also widely used in corporate settings to enable **secure remote access** to internal systems.

# Firewalls

Firewalls are devices that filter all traffic between a protected internal network and a less secure external network. It is implemented as a separate device because it is easier to fix bugs and improve performance.
Firewalls have a policy or a set of rules to determine which traffic can or cannot enter the network. It must have three characteristics:

- It cannot be circumvented and is always invoked
- It is tamper proof
- It is small enough to analyse rigorously.

Types of Firewalls:

- Packet filtering gateways or screening routers
- Stateful inspection gateways
- Application level gateways or proxies
- Circuit level gateways
- Guards
- Personal or host-based firewalls

## Packet Filtering Gateways

The packet filtering gateway controls access to the network on the basis of Source IP Address and specific transport protocol type/ Port Number (Example HTTP/Telnet). It does not maintain state information and handles packets 1 at a time.

## Stateful Inspection Gateways

They maintain state information from one packet to the next. They inspect not only headers but also state of the connection making sure the packets are of a valid session. They are more secure than regular packet filtering gateways

## Application Level Gateways/ Proxies

An application proxy simulates the behaviour of the real application on OSI Layer 7, the application layer, ensuring only legitimate secure requests are received by the real application. It can be used to filter dangerous requests, log requests made to the application, cache results to save bandwidth.

## Circuit Level Gateways

They operate at OSI Layer 5 the Session Layer. It allows one network to act as an extension of the other. It is used to implement VPNs.

## Guards

Highly secure firewalls often used in military or government settings. They perform strict filtering and validation of content, possibly using custom code or security policies to enforce specific rules.

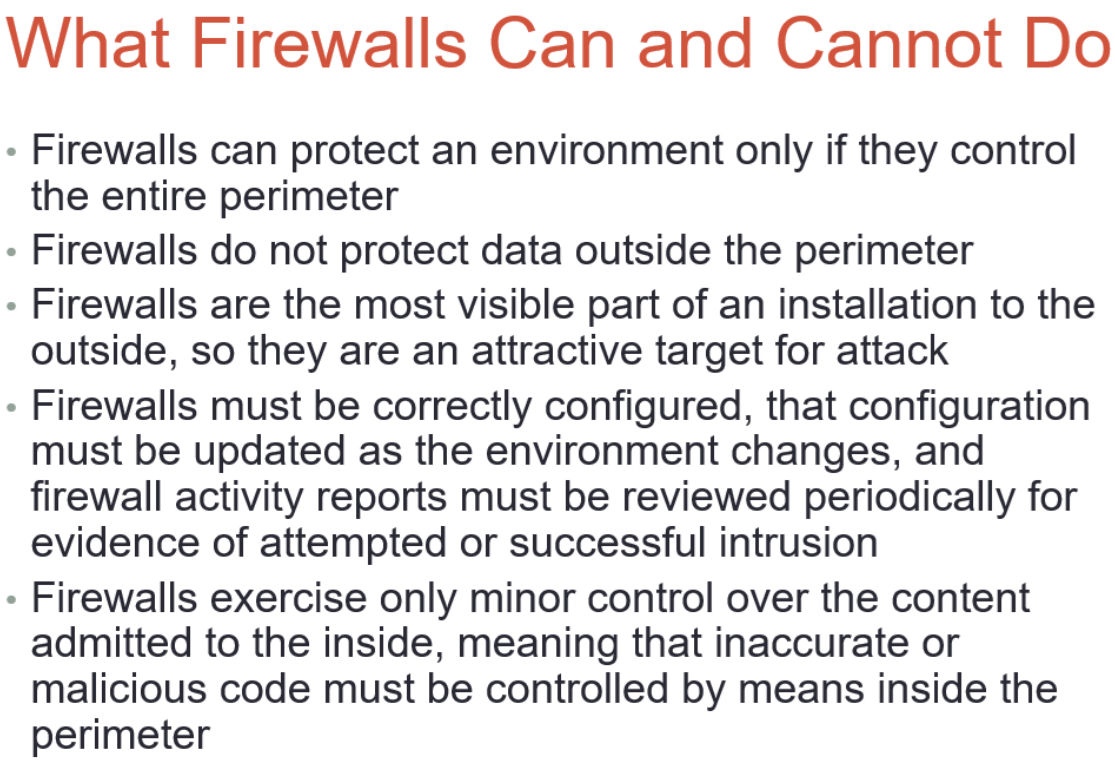
## Personal Firewall

A personal firewall runs on the workstation or computer of the individual and can implement traffic filtering policies just like other firewalls. They monitor incoming and outgoing traffic of a single device.

| Packet Filter | Stateful Inspection | Application Proxy | Circuit Gateway | Guard | Personal Firewall |
|---|---|---|---|---|---|
| Simplest decision-making rules, packet by packet | Correlates data across packets | Simulates effect of an application program | Joins two subnetworks | Implements any conditions that can be programmed | Similar to packet filter, but getting more complex |
| Sees only addresses and service protocol type | Can see addresses and data | Sees and analyzes full data portion of pack | Sees addresses and data | Sees and analyzes full content of data | Can see full data portion |
| Auditing limited because of speed limitations | Auditing possible | Auditing likely | Auditing likely | Auditing likely | Auditing likely |
| Screens based on connection rules | Screens based on information across multiple packets—in either headers or data | Screens based on behavior of application | Screens based on address | Screens based on interpretation of content | Typically, screens based on content of each packet individually, based on address or content |
| Complex addressing rules can make configuration tricky | Usually preconfigured to detect certain attack signatures | Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior | Relatively simple addressing rules; make configuration straightforward | Complex guard functionality; can be difficult to define and program accurately | Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise |

## Demilitarized Zones (DMZs)

It is a small network consisting of public facing services like web, email and ftp servers that should be somewhat accessible from the outside network. They are isolated from the rest of the network using a firewall thus protecting the rest of the network from being accessible from the internet.




## Network Address Translation

With NAT, the source firewall converts the source address in the packet into the firewall's own address. The firewall also makes an entry in a translation table showing the destination address, the source port & the original source address to be able to forward any replies to the original source address. The firewall then converts the address back on any return packets.

This has the effect of concealing the true address of the internal host and prevents the internal host from being reached directly.

## Data Loss Prevention

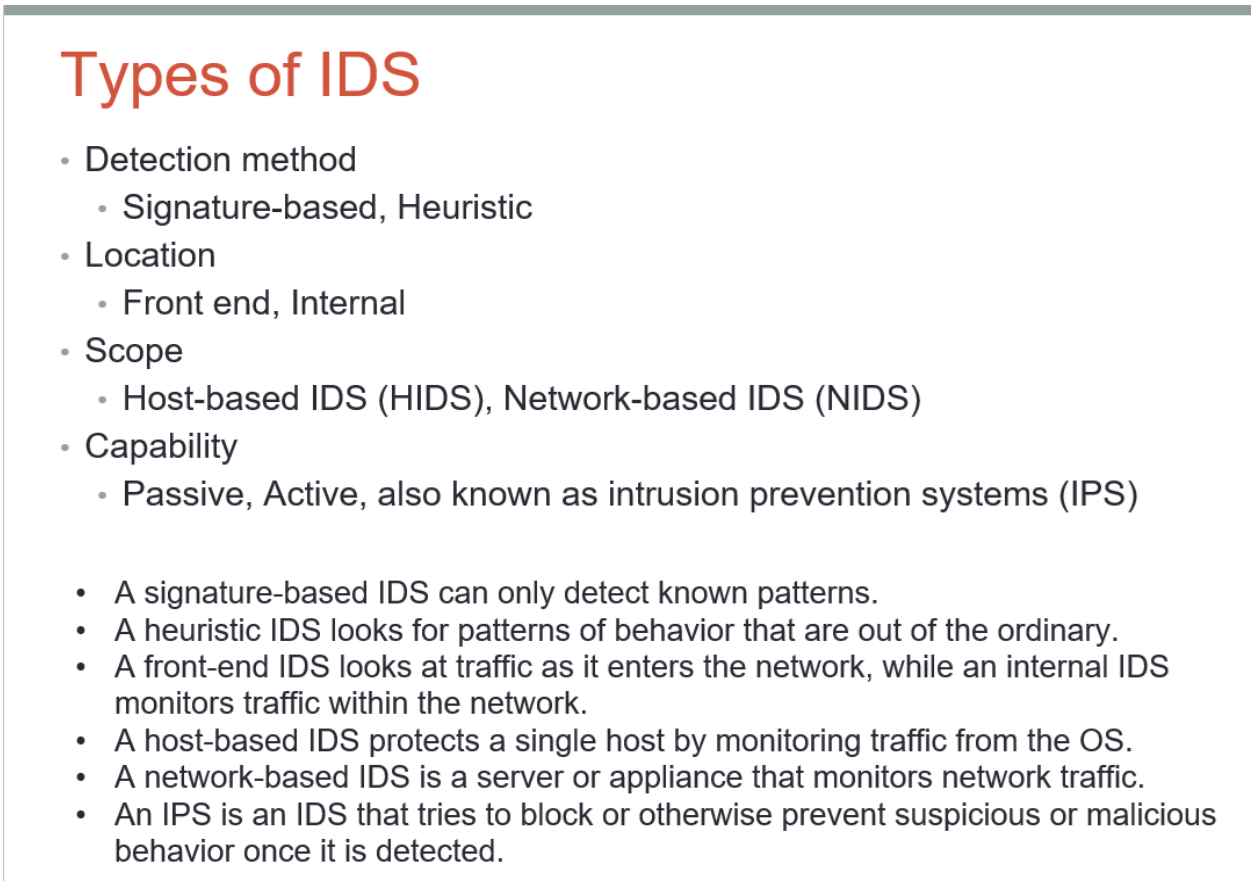
DLP is a set of technologies that detect and prevent attempts to send data where it should not

be going. Can be implemented as a guard or an agent in the OS rootkit. It is best for preventing accidents as attackers will find ways to circumvent it.

### Intrusion Detection Systems

IDSs complement preventative controls as a next line of defense. IDSs monitor activity to identify malicious or suspicious events. IDSs may:

- Monitor user and system activity
- Audit system configurations for vulnerabilities and misconfigurations
- Assess integrity of critical system and data files
- Recognize known attack patterns in system activity




### Security Information and Event Management

SIEMs are software systems that collect security-relevant data—usually audit logs—from a variety of hardware and software products to create a unified security dashboard for security operations center personnel.

## Honeypot

A **honeypot** is a cybersecurity tool designed to **lure attackers** by mimicking vulnerable systems, with the goal of **detecting**, **distracting**, and **studying** unauthorized access attempts. It's a trap set up to detect, deflect, or study attempts at unauthorized use of information systems. Honeypots can be software-based, such as emulated servers or networks, or hardware-based, such as physical devices that appear to be part of a network

### Purpose

- **Detect Intrusions:** Monitor malicious activity in a controlled environment.
- **Distract Attackers:** Divert threats from real systems.
- **Gather Intelligence:** Learn about attacker techniques and tools.
- **Study Threats:** Analyze emerging threats and test defenses.

### Strengths

- **Early Threat Detection**
- **Insight into Attacker Behavior**
- **Deception & Misdirection**
- **Threat Intelligence Generation**
- **Support for Research & Development**

### Weaknesses

- **Resource Intensive** to maintain and analyze.
- **False Positives** if misconfigured.
- **Legal/Ethical Issues** related to privacy and consent.
- **Limited Real-World Relevance** compared to actual environments.
- **Risk of Compromise** if attackers exploit the honeypot.