Network Security Notes

1 Introduction

Key Idea

The Internet was **not originally designed with much security in mind**. Original vision: "a group of mutually trusting users attached to a transparent network" ☺. Today, Internet protocol designers are constantly playing **catch-up** to include security considerations at all layers.

1.1 Focus Areas in Network Security

We now need to think about:

- How attackers can compromise computer networks.
- How to defend networks against attacks.
- How to design architectures that are immune to attacks.

2 Types of Attacks

2.1 Packet Interception

Packet Sniffing

Packet sniffing occurs when a network interface in **promiscuous mode** reads and records all packets passing through the network, including sensitive information like passwords. **Examples:**

- Broadcast media such as shared Ethernet or wireless.
- Tools like **Wireshark** (free packet-sniffer used in labs).

2.2 Fake Identity

IP Spoofing

Attackers inject packets with a **false source address** to impersonate another host.

2.3 Denial of Service (DoS)

DoS Attack

An attack that makes a network resource (server or bandwidth) unavailable to legitimate users by overwhelming it with bogus traffic. **Typical Steps:**

1. Select the target.
2. Compromise hosts around the network (e.g., via a **botnet**).
3. Send massive packets to the target from compromised hosts.

3 Lines of Defense

3.1 Authentication

- Verifying your identity before granting access.
- Example: Cellular networks use **SIM cards** to provide hardware-based identity.

3.2 Confidentiality

- Achieved using **encryption** to prevent eavesdropping.

3.3 Integrity Checks

- Ensure data is not tampered with using **digital signatures**.

3.4 Access Restrictions

- Examples: password-protected VPNs.

3.5 Firewalls

Firewall

A specialized **middlebox** deployed in access or core networks to filter incoming/outgoing traffic. **Note:** Typically off-by-default, requiring configuration.

3.6 Detection and Response to DoS

- Specialized systems detect abnormal traffic patterns.
- Mitigation techniques include filtering traffic or rate-limiting requests.

Security Principle

Security in networking requires a multi-layered approach: authentication, confidentiality, integrity, access control, monitoring, and timely response to attacks.