Network Security

Madiba Hudson-Quansah

Contents

Chapter 1

Introduction

1.1 Networks

Definition 1.1.1: Computer Network

A collection of interconnected devices that communicate to share data, resources and services. Examples:

- LAN (Local Area Network)
- WAN (Wide Area Network)
- WLAN (Wireless Local Area Network)

A network consists of:

Devices - Computers, services, routers, and switches.

Transmission Medium -

- Physical (Ethernet cables, fiber optics)
- Wireless (Wi-Fi, Bluetooth)

Data and Protocols - Standardized methods for data transmission ensuring communication

1.1.1 Terms

Definition 1.1.2: Data Packet

A subdivision of data formatted for transmission over a network. Packets contain a portion of the original data and necessary metadata for routing and reassembly.

Definition 1.1.3: Routing

Directing data packets from source to destination across networks.

Definition 1.1.4: MAC Address

Unique identifier of a Network Interface Card (NIC), that connects a computer and a network

Definition 1.1.5: Port

A number associated with an application program that serves or monitors for a network service

Definition 1.1.6: Daemon

A service program that runs in the background and receives and passes data to the associated program.

1.2 Networking Models

Networking models standardize communications between computers, enabling different systems to communicate. There are two main models:

- OSI Model (Open Systems Interconnection)
- TCP/IP Model (Transmission Control Protocol/Internet Protocol)

1.2.1 OSI Model

Consists of seven layers:

Physical - Hardware, cables, and signals

Data Link - Frames, MAC addresses, switches

Network - IP addresses, routers, routing

Transport - TCP/UDP, ports, data transfers

Session - Establishes, manages and terminates connections

Presentation - Data translation, encryption, compression

Application - User Interfaces, email, web browsers

1.2.2 TCP/IP Model

Consists of four layers:

Link - Combination of physical and data link layers, hardware and LAN

Internet - IP addressing and routing

Transport - TCP/UDP, manages end-to-end data transmission

Application - Combines application, presentation and session layers. Handles high-level protocols.

1.3 Domain Name System (DNS)

DNS translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 154.158.23.4) that computers use to identify each other on the network.

Chapter 2

Network Security Concepts

Involves policies, practices, and tools designed to protect data and infrastructure from unauthorized access, misuse, or harm. It's goal is to ensure the integrity, confidentiality, and availability of network resources.

2.1 Common Threats

Interception - Eavesdropping and Wiretapping (Confidentiality loss)

Modification - Data Corruption (Integrity loss)

- Sequencing
- Substitution
- Insertion
- Replay
- Physical replay

Interruption - Denial of Service (Availability loss)

Definition 2.1.1: Security Perimeter

A virtual boundary that separates a trusted internal network, i.e a protected zone containing a set of computing resources, and an untrusted external network, i.e the internet.

2.1.1 Eavesdropping and Wiretapping

Definition 2.1.2: Wiretapping

Covert and unauthorized data interception during transmission.

The things that make a network vulnerable to eavesdropping and wiretapping include:

Anonymity - Attackers can hide their identity

Multiple points of access - Data may pass through many hosts to get to the user

Shared resources - Networks enable resource and workload sharing giving potential access to more attack vectors

Complexity - More complex systems have more vulnerabilities, as users have no idea of all the processes active in the background

No obvious perimeter - One host may be a node on two different networks.

Some countermeasures include:

- Encryption
- Physical security
- Dedicated lines
- Controlled routing, i.e. ensuring that communication travels only along certain paths

2.1.2 Data Corruption / Modification

This is caused by:

Modification - Change of data en route

Insertion - Addition of extra data

Replay - Repeating a previous communication

2.1.2.1 Sequencing

Definition 2.1.3: Sequencing

A sequencing attack permutes the order of data packets. This can lead to misinterpretation of data, as the receiving system may not be able to correctly reassemble the original message.

Network protocols such as TCP/IP include features to check for and correct transmission errors. However application programs do not always detect or correct sequencing problems.

2.1.2.2 Substitution

Definition 2.1.4: Substitution

A substitution attack is the replacement of one piece of a data stream with another.

2.1.2.3 Insertion

Definition 2.1.5: Insertion

An insertion attack involves the insertion of new data values into a communication stream without replacing or removing the existing data. The attacker doesn't even need to break the encryption scheme as long as they know precisely where to insert the new data.

Countermeasures for both insertion and substitution include:

- Encryption
- Integrity checks (e.g. checksums, hash functions)

2.1.2.4 Replay

Definition 2.1.6: Replay

A replay attack involves the reuse of legitimate data transmissions.

Countermeasures include:

- Sequencing
- Timestamps

2.1.3 Interruption / Denial of Service (DoS)

Definition 2.1.7: Denial of Service (DoS)

An attack that aims to make a network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.

2.2 Basic Network Security Measures

Firewalls - Act as a barrier between a network and external threats, monitoring and controlling incoming and outgoing traffic.

Encryption - Encrypts all data transmissions, making intercepted data unreadable without the correct decryption key.

Antivirus and Anti-malware Software - Detects and removes malicious software that could compromise network security.

Chapter 3

Practical Network Security

3.1 Firewalls

Definition 3.1.1: Firewall

A combination of hardware and software that filters or prevents specific types of information from moving between an untrusted network, like the internet and a trusted network, like a private LAN. Firewalls may be a separate computer system, a software service running on an existing router, or server or a separate network that contains several supporting devices.

Firewalls can be categorized based on processing modes:

- Packet Filtering
- Application layer proxy
- Media access control layer
- Hybrid

3.1.1 Packet Filtering Firewalls

Examines the header information of data packets that come into a network. When installed on a TCP/IP based network, it functions at the IP layer and denies/drops or allows/forwards the packets to the next network connection based on the rules programmed into the firewall.

Restrictions can be based on:

- IP source and destination addresses
- Direction, i.e. incoming or outgoing
- Protocol type (TCP, UDP, ICMP)
- Port number

Packet filtering firewalls can further be classified into:

Static packet filtering

- Filters based on rules developed and installed with the firewall
- Rules are created and changed by the firewall administrator
- Common in network routers and gateways

Dynamic packet filtering -

Firewall reacts positively or negatively to traffic patterns

More secure than static filtering

Stateful Packet Inspection (SPI) -

- Keeps track of each network connection between internal and external systems using a state table

3.2 Virtual Private Networks (VPNs)

Definition 3.2.1: Virtual Private Network (VPN)

A private, secure network operated over a public and insecure network, implemented using cryptographic technology by means of a tunnelling protocol coupled with security procedures.

A VPN keeps the contents of the network messages hidden from observers who have access to public traffic and is used to securely connect remote users to a private network. VPNs often use protocols like IPSec to encrypt traffic.