Data and Network Security - Jaish Khan

1. Basics

> **Network Security** → Practices, technologies, policies, and procedures to protect the integrity, confidentiality, and availability of computer networks and data.

Involves safeguarding the network infrastructure from **unauthorized access, misuse, destruction, modification, or disclosure**.

> **Cybersecurity** → Protecting systems, data, devices, and software from cyber threats.
> Network Security is a subset of cybersecurity.

1.1. The CIA Triad

These are the 3 main objectives of Computer Security.

1. **Confidentiality** → Assures that private or confidential information is not made available or disclosed to *unauthorized individuals*. **Privacy** is also included which is that people must have control over what information related to them may be collected, stored, and disclosed, and by whom.
2. **Integrity** → Assures that information and programs are changed only in a *specified and authorized manner*. This also includes **System Integrity** (a system performs its intended function in an *unimpaired manner*, free from deliberate or inadvertent unauthorized manipulation).
3. **Availability** → Assures that systems work promptly and service is not denied to *authorized users*.

Other Possible Objectives → *Authenticity* (Verifying that users are who they say they are) and *Accountability* (Actions can be traced uniquely to an entity).

1.2. Security Attacks

A **Security Attack** is any action that *compromises the security of information* owned by an organization. A **Security Mechanism** is then a process made to *detect, prevent, or recover* from a security attack and a **Security Service** is a service that *improves the security* of data processing systems and information transfers.

Security Attacks can be divided into Passive Attacks or Active Attacks.

> ⚠ **Passive Attacks**
>
> Attempts to learn or make use of information from the system but do not affect system resources. They are difficult to identify and prevent because the attacker is not changing anything.

- Goal → obtain transmitted information.
- **Types**
  - *Release of message contents*: Eavesdropping on or monitoring transmissions.
  - *Traffic analysis*: Monitoring transmissions to obtain information about the traffic flow (source, destination, frequency, length).

ϟ **Active Attacks**

Attempts to change/alter system resources or affect their operation. They involve some modification of the data stream or the creation of a false stream.

- Goal → detect attacks and recover from any disruption or delays.
- **Types**
  - *Masquerade*: Takes place when one entity pretends to be a different entity. Usually includes another form of active attack.
  - *Replay*: Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
  - *Modification of messages*: Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect.
  - *Denial of service*: Prevents or inhibits the normal use or management of communications facilities.

1.3. Security Mechanisms

1. **Authentication** → Makes sure that a communication is authentic and verifying the identities of involved users.
2. **Access Control** → Limit the access to host systems and applications.
3. **Data Confidentiality** → Protecting transmitted data from passive attacks.
4. **Data Integrity** → Makes sure that the information is changed only in an authorized manner.
5. **Nonrepudiation** → Prevents either sender or receiver from denying a transmitted message.
6. **Availability** → Makes sure that systems work properly and service is not denied to users.

2. Cryptography

> The use of mathematical algorithms to transform data into a form that is not understandable and then recover that data (depends on the algorithm).

These algorithms are divided based on the:

1. Performed Operation → Substitution (replace) vs Transposition (shuffle).
2. Way of Processing → Stream (one bit at a time) vs Block (entire chunks at a time).
3. Keys for Encryption/Decryption → Symmetric (same key) vs Asymmetric (different keys).

Cryptanalysis → Process of attempting to discover the plaintext or key.

ⓘ Computationally Secure Cipher

A cipher is considered **computationally secure**, If the ciphertext generated by it meets one or both of these criteria:

- The *cost* of breaking the cipher exceeds the value of the encrypted information.
- The *time* required to break the cipher exceeds the useful lifetime of the information.

A **brute-force approach** of trying every possible key is often considered:

- `56-bit` key (used by DES) takes about 10 hours to crack.
- `128-bit` key (used by AES) take over 10^{18} years to crack.

This difference suggests that a 128-bit key algorithm is unbreakable by brute force.

2.1. Ciphers

1. **Substitution Ciphers** → Mapping individual letters of a plaintext alphabet to a particular letter of the ciphertext alphabet.
    - *Caesar Cipher* → More secure than Atbash but still easy to break (e.g., shift of 3).
    - *Vigenère Cipher* → A polyalphabetic cipher that uses a keyword repeated to form a keystream. Encryption and decryption use a "tabula recta" based on plaintext/ciphertext and keystream letters.
2. **Transposition Ciphers** → Shuffles the letters in the plaintext around to make the ciphertext. Examples:

    - *Rail Fence Cipher* → Writes message on alternate lines (zigzag) and reads off each line. Key is the number of rows. Encryption and Decryption processes described.
    - *Columnar Cipher* → Encryption involves writing plaintext in a grid based on a keyword, then reading columns based on the alphabetical order of the keyword. Decryption reconstructs the grid.

Block Ciphers (not important) → Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) , Counter (CTR)

2.2. Encryption

2.2.1 Symmetric Encryption

Also known as conventional, secret-key, or single-key encryption

> Uses the same key for both encryption and decryption.

Involves an encryption algorithm, a secret key shared by the sender and receiver, and the plaintext and ciphertext.
Examples → *AES*, *DES* and *Triple DES* algorithms.

2.2.2. Asymmetric Encryption

Also known public-key cryptography

> Uses different keys for encryption and decryption.

Involves an encryption algorithm, a secret unique key that is not shared (private key), a secret key that is shared across the network (public key), and the plaintext and ciphertext.

- Depending on the application, the sender uses either their private key, the recipient's public key, or both to perform cryptographic functions.
- They are used computationally expensive and hence are used only for small amounts of data like encrypting symmetric encryption keys for transfer and digital signatures.
  Examples → *RSA*, *Diffie-Hellman* and *ECC* algorithms.

3. Firewalls

> A software or hardware device that monitors/manages/blocks the data entering (inbound) and exiting (outbound) the network.

- Defines a single choke point where security, audit, monitoring and logging can be done.
- Stops unauthorized programs/users from entering/exiting/accessing the network/computer.
- Inserted between the premises network and the Internet to establish a controlled link and act as a security gateway.

> All traffic from inside to outside, and vice versa, must pass through the firewall and Only authorized traffic, as defined by the local security policy, will be allowed to pass.

Limitations of a Firewall → It cannot protect against:

1. Attacks bypassing it like trusted organizations and trusted services (SSL/SSH).
2. Internal threats (malicious employees).
3. Viruses and Trojans from reaching the machine via email, file sharing, or direct download nor their transfer.

Positives of a Firewall	Negatives of a Firewall
User authentication (Require user login, allowing control and tracking).	**Traffic bottlenecks** (Forcing all traffic through can cause congestion).
Auditing and logging (Can keep and analyze activity information).	**Single point of failure** (Incorrect configuration or unavailability can block all traffic).
Anti-Spoofing (Detecting when the source of network traffic is being "spoofed").	**Increased management responsibilities** (Adds complexity to network management and troubleshooting).

3.1. Techniques to Enforce Security by Firewall

1. **Service control** → Which Internet services can be accessed?
2. **Direction control** → Which direction, a particular service requests can be accessed?
3. **User control** → Which user is attempting to access what service?.
4. **Behavior control** → How a particular service is being used?.

3.2. Firewall Types

Hardware vs Software Firewall

- **Hardware Firewalls** → Protect an entire network, implemented on the router level, usually more expensive, harder to configure.
- **Software Firewalls** → Protect a single computer, usually less expensive, easier to configure.

Based on how the firewall works, we can divide them in these categories:

3.2.1 Packet Filtering Firewall

> Applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. Filters in both directions.

Filtering Rules → Based on Source and Destination IP address, Source and destination transport-level address (port number) and Interface.

- A rule has two parts: **Selection Criteria**, **Action Field**.
- If there is a match, the rule decides to forward or discard.
- Default Policies
  - **Default = discard** (prohibited unless permitted)
  - **Default = forward** (permitted unless prohibited).
- They make decisions on an individual packet basis without higher layer context.

3.2.1.1. Stateful Inspection Packet Filter

> Creates a directory of outbound TCP connections and allows related inbound traffic to high-numbered ports..

Also called a **network layer firewall** (OSI layer 3/4). It is faster, can be implemented transparently, typically less expensive BUT is difficult and lacks authentication.

3.2.2. Application-Level Gateway (or Proxy)

> Works as a relay of application-level (OSI Layer 7) traffic.

When a user tries to access a service the gateway intercepts the request and asks for the name of the remote host and, upon receiving valid user ID and authentication information, contacts the application on the remote host. The gateway then relays TCP segments containing the application data between the two endpoints.

It has full access to protocol and is wayyyy more secure BUT adds a lot processing overhead.

3.2.3. Circuit-Level Gateway

> Operates at the transport layer (OSI Layer 4) and session layer (OSI Layer 5).

- It monitors TCP or UDP sessions, instead of individual packets.
- Validates sessions before opening a connection and Leaves the port open for other packets in that session until termination.
- Maintains a virtual circuit table.

It is more secure than packet filter firewalls, **faster than application level firewalls**.

3. Malicious Software

> **Malware** → Software that tries to intentionally harm a system, steal data or block it from accessing.

Spread through email (attachments), infected floppy disks, downloading/exchanging corrupted files or computer games. There are many categories of malicious software:

3.1. Virus

> A piece of self-replicating code attached to some other code(host). It spreads and infects other programs as well by changing their code(payload).

May cause random damage to files or attempt to destroy files and disks. Can cause significant damage by occupying disk space and/or main memory, and by using up CPU processing time. They are **hard to detect, destroy or deactivate** and easy to **spread**.

Types of Viruses → Boot-Sector virus, File virus and Email virus.

There are 3 phases of a virus **Dormant** (Waiting), **Triggering** (By an Event to execute code), **Execution** (Running code), **Propagation** (Spreading).

3.2. Worm

> Program that spreads copies of itself through a Network. It spreads but doesn't infect a program and can cause irrecoverable damage.

3.3. Trapdoor

> Secret entry point into a program allowing bypass of usual security procedures (authentication).

Some undocumented vulnerability, usually used by administrators for troubleshooting, but can be exploited. It is a major threat when left in production programs and is very hard to block in OS.

3.4. Logic Bomb

> Code embedded inside in a program that activates when some conditions are met (like the presence/absence of file, date/time, user). When triggered, typically damages the system (modify/delete files/disks).

3.5. Trojan Horse

> Program with hidden side-effects. It enters the system, often disguised as something attractive. It allows attacker to indirectly gain access and It doesn't spread or clone itself..

Types of Trojan Horse
1. *Remote-access* Trojan (Takes full control)
2. *Data-sending* Trojan (Sends data back to the hacker),
3. *Destructive* Trojan (Destroys or Deletes files)
4. *Denial-of-service* Trojan (Launches attack on another system from the infected one).

3.6. Hoax

> False alerts of spreading viruses which can flood network resources, causing bandwidth wastage and may block systems.

3.7. Spyware

> Programs that find information in a system and send it to a specified address.

Used for investigation or attack preparation. It is a serious threat that can steal data, monitor communications, or even install other malware.