Basic Security Concepts:

1. Firewall

A Firewall is a system (or group of systems) that enforces a security policy between a secure internal network and an untrusted network such as the Internet. A firewall is a security system intended to protect an organization's network against external threats such as hackers coming from another network.

A firewall is a combination of hardware and software that isolates an organization's internal network from the internet allowing specific connections to pass and blocking others.

Organizations employ firewalls for the following reasons.

- To prevent intruders from interfering with the daily operation of the internal network, denial of service attack, SYN FIN Attack.
- To prevent intruders from deleting or modifying information stored within the internal network
- To prevent intruders from obtaining secret information.
- Allow only authorized access to the inside network.
- Prevent illegal modification/access of internal data: e.g., attacker replaces official homepage with something else.

Types of Firewalls:

A firewall is usually classified as a packet-filter firewall and a proxy-based firewall/ application-level gateway firewall.

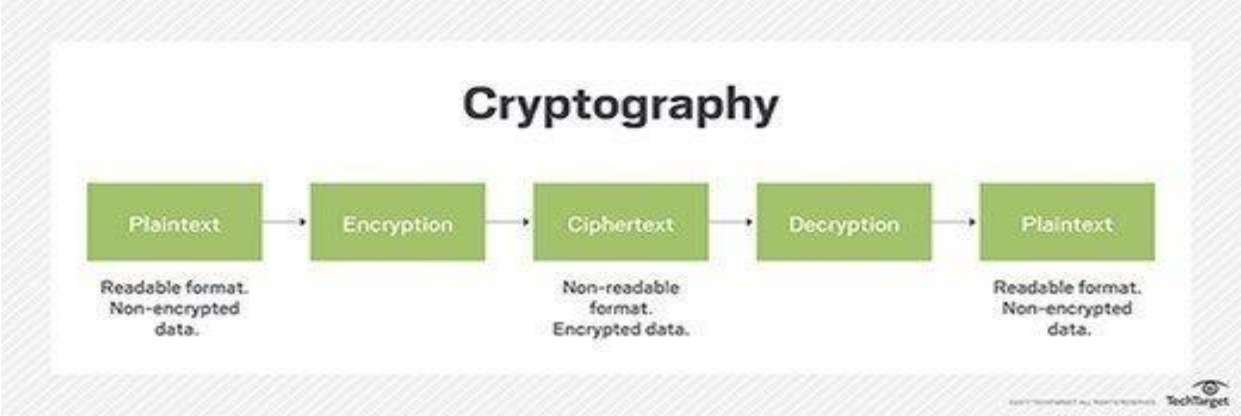
a. Packet-Filter Firewall
   Packet filter is the first generation firewall which is essentially a router that has been programmed to filter out certain IP addresses or TCP port numbers. These routers perform a static examination of the IP addresses and TCP port numbers, then either deny a transaction or allow it to pass based on
   information stored in their tables.
b. Application-Level Gateway
   It is not possible to control the data with packet filters because they are not capable of understanding the contents of a particular service. For this purpose, an application-level control is required.
   An application-level gateway is often referred to as a proxy. An application-level gateway provides higher-level control of the traffic between two networks in that the contents of a particular service can be monitored and filtered according to the network security policy. Therefore for any desired application, the corresponding proxy code must be installed on the gateway in order to manage the specific service passing through the gateway.

2. Cryptography

Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. Cryptography plays a vital role in private communication through public networks. Some important terminologies used in cryptography are:

- Plain text/Clear text: Original message produced by sender.Data before transmission
- Cipher(code) text: Plain text transformed into ciphertext through encryption. Encrypted form
- Key: It is secret information to encrypt or decrypt data which is a value or a number. The cipher as an algorithm operates on the key.
- Ciphers: The encryption and decryption algorithms together are referred to as ciphers. This term is also used to refer to different categories of algorithms in cryptography.

Cryptography software and/or hardware devices use mathematical formulas(algorithms) to change text from one form to another. It is the technique of protecting the integrity or secrecy of electronic messages by converting them into unreadable (cipher text) forms. The encryption and decryption algorithms are public and anyone can use them but the encryption and decryption keys are secret. It's widely used to protect sensitive information, such as passwords, personal data, and communications.



Types of Cryptography Algorithm:

a. Symmetric key system (Secret key)
b. Asymmetric key system(Public key)

Symmetric key system (Secret key)	Asymmetric key system(Public key)
Sender and receiver both users share a pair key	The sender uses the public key of the receiver to encrypt and the receiver decrypts the message using the private key.
It is more efficient.	It is less efficient.
It is useful for encryption and decryption of long messages.	It is used for encryption and decryption of short messages.
A large number of keys are required.	The number of keys is less.

3. Secure Network Configurations

- **Changed Default Router Passwords:** Default router passwords are often weak and publicly known, making them a prime target for attackers. Changing these to strong, unique passwords enhances security.
- **Enabled WPA2/WPA3 Encryption:** WPA3 provides stronger security for wireless networks compared to WPA/WEP, protecting against brute-force attacks and improving encryption strength.
- **Disabled Unnecessary Network Services:** Many routers and devices come with default services enabled (such as remote management, UPnP, and Telnet), which can introduce vulnerabilities. Disabling unnecessary services minimizes attack surfaces.
- **Implemented MAC Address Filtering:** Restricting network access to known MAC addresses helps prevent unauthorized devices from connecting to the network.

- **Enabled Network Segmentation:** Dividing the network into segments using VLANs reduces the impact of a security breach, preventing unauthorized lateral movement between different network areas.
- **Deployed Network Address Translation (NAT):** NAT hides internal IP addresses, making it more difficult for attackers to target specific devices within the network.
- **Configured DNS Security Features:** Using secure DNS providers and enabling DNS filtering helps prevent access to malicious websites and phishing domains.
- **Regular Security Audits and Updates:** Periodically reviewing network configurations and applying firmware updates ensures protection against newly discovered vulnerabilities.