Network Security Theory

🔥 Special thanks to **VJ Cyber**, my heaviest project and biggest breakthrough so far.

Intro to Network Security

What is Network Security?

Network Security → The shield that protects the CIA of information and resources in a network.

CIA Triad

1. Confidentiality → Ensuring only authorized users can access sensitive information within a network using encryption and access controls.
2. Integrity → Ensuring data within a network is accurate and has not been tampered with using intrusion detection systems.
3. Availability → Ensures that authorized users can access the information and resources they need whenever they require them using firewalls and network redundancy strategies.

Threats

Malware

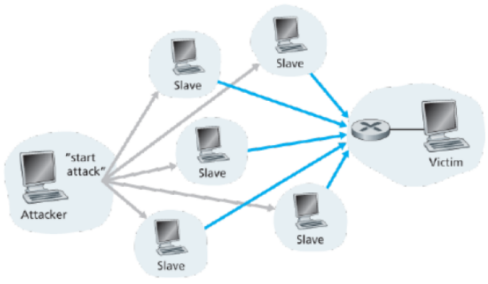
Malware → Software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system.

Name	Description
Ransomware	Blocks access to a computer system until a ransom is paid
Scareware	Frightens victims into providing financial information or downloading viruses

Name	Description
Spyware	Secretly collects personal information about users and sends it to attacker
Adware	Pushes unwanted advertisements at users
Fileless Malware	Operates in computer’s memory, hiding in a trusted application or tool
Cookies	Small piece of data on websites that stores users’ personal information
Pharming	Intercepts requests going to a website and redirects it to a fake website
Phishing	Using fake emails and websites that appear to be from reputable companies
Spamming	Mass distribution of unwanted messages to emails gained from mailing lists
Trojan Horse	Pretends to be a harmless file or useful application until run
Virus	Attaches itself to a harmless program and modifies it, and spreads to other programs when the infected program is run
Worm	Runs automatically and tries to spread copies of itself across a network, consuming bandwidth and harming the host server

Denial of Service

- Denial of Service → An attempt to overload a website or network with requests with the aim of degrading its performance or rendering it inaccessible to users.
- Distributed Denial of Service → An attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target with internet traffic using multiple compromised computer systems as weapons.
- DDoS Botnet



A distributed denial-of-service attack

Protection

Firewalls

- What is a Firewall
  - Firewall → Filter that monitors access between an organization's internal network and the internet, allowing some packets to pass and blocking others.
- Types of Firewalls
  - Hardware Firewall → Physical, connects the network and gateway through wires
  - Software Firewall → Internal, works using port numbers and applications
  - Cloud-based Firewall → Firewalls can grow with the organization and do well with perimeter security
  - Host Based Firewall → Installed on an individual computer to protect it from activity occurring on its network
  - Network Based Firewall → May be installed at the perimeter of a network to protect corporations from hosts on the internet, cannot protect internally
- Functionality of Firewalls
  - Traffic Control → All communication must pass through the firewall. Using a single firewall helps ensure this, but bigger organizations may enforce multiple layers

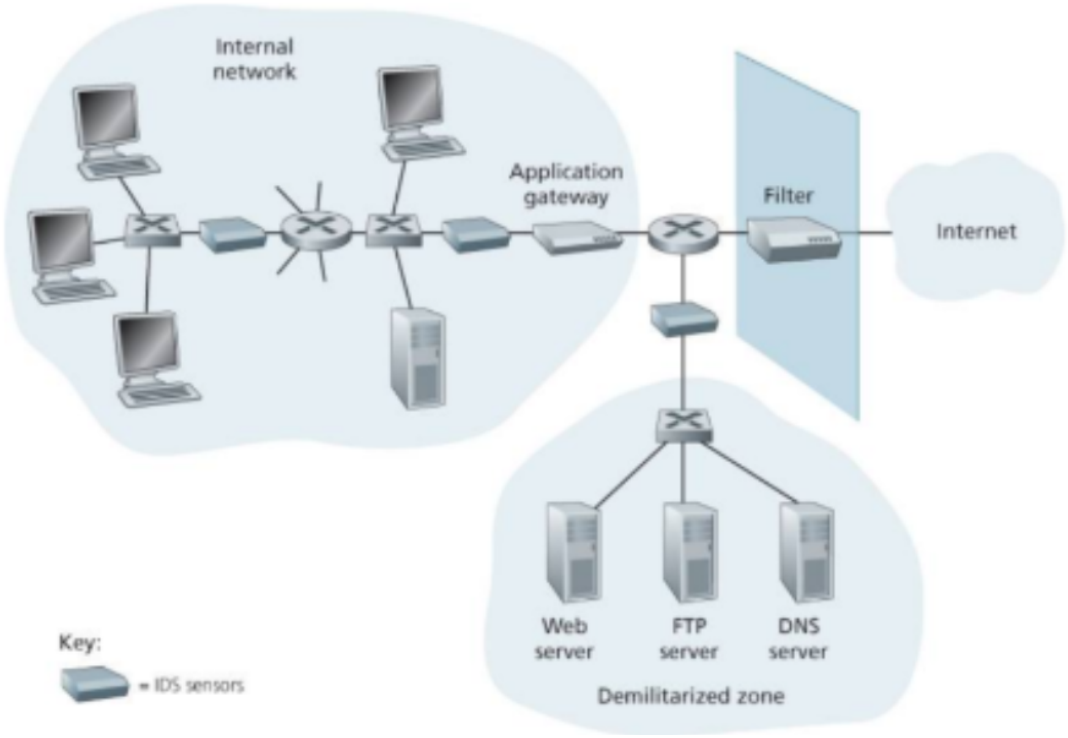
    - Authorized Traffic → Only authorized traffic will be allowed to pass, and the rest are blocked
    - Maintaining Security → While connected to the network itself the firewall is meant to be resistant to attacks
- Applications of Firewalls
    - Packet Filters → Occur at gateway routers that connect internal networks to ISPs. The admins can specify what's allowed and what is not.
    - Stateful Packet Filters → Track TCP connections and use this information to make filtering decisions
    - Application Gateways → Application specific servers through which all app data must pass. They look beyond just IP TCP UDP Headers and make the decisions based on the app data.
- Limitations of Firewalls
    - Cannot protect against attacks from a source if a user has explicitly allowed it to bypass the firewall
    - Cannot protect against internal threats as the malicious traffic may not need to pass through the firewall
    - If the firewall goes down, everything becomes vulnerable (single point of failure)

Intrusion Systems

- What are IDSs?
    - Intrusion Detection Systems IDS → Device that generates alerts when it observed potentially malicious traffic
    - Intrusion Prevention Systems IPS → Device that filters out suspicious traffic
- IDS Use Cases
    - Detect a wide range of attacks including network mapping, port scans, TCP stack scans, DoS bandwidth flooding attacks, worms, viruses, OS vulnerability attacks and app vulnerability attacks

    - Usually more than one is deployed in an organizational network, and they work in concert to send all suspicious activity to a central IDS, which does the IDS alerting process

- How IDS Works
    - Organizational Diagram



    - Network is divided into high-security region and DMZ
    - High-security region protected by packet filter and application gateway
    - DMZ includes public web server and DNS server, protected by packet filter
    - IDS sensors monitor both regions
    - IDS performs deep packet inspection and signature comparison
    - Placing IDS sensors downstream reduces traffic load per sensor
    - Signature-based IDS uses a database of attack signatures
    - Signatures are created by network security engineers and can be customized

    - IDS inspects each packet and generates alerts for matches
    - Alerts are sent to administrators, management systems, or logged
- Signature Based IDS
    - Requires previous knowledge of attacks to generate accurate signatures
    - Blind to new, undocumented attacks
    - Can produce false alarms even if a signature is matched
    - Every packet must be compared with an extensive collection of signatures
    - Can become overwhelmed and fail to detect many malicious packets
- Anomaly Based IDS
    - Creates a traffic profile based on normal operation
    - Detects statistically unusual packet streams (e.g., high percentage of ICMP packets, exponential growth in port scans and ping sweeps)
    - Can detect new, undocumented attacks
    - Challenging to distinguish between normal and unusual traffic
    - Most IDS deployments are primarily signature-based, with some including anomaly-based features

Secure Access Methods

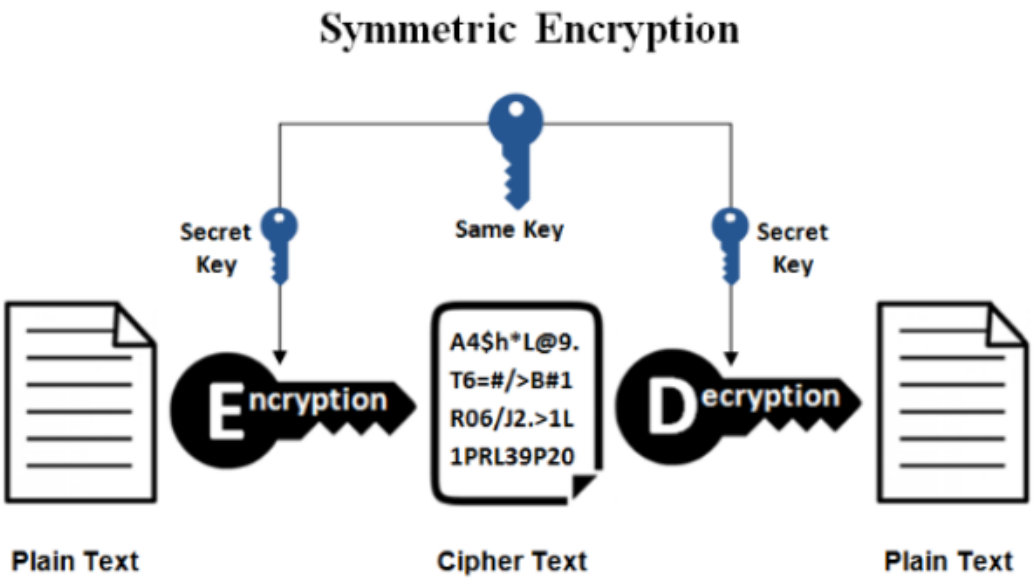
Encryption

- Encryption → Process that uses an algorithm to code a message written in plaintext into ciphertext
- Decryption → Decoding the ciphertext back into the original plaintext using a decryption algorithm and key
- Used to protect data from unauthorized access by only allowing authorized users to have the secret key.
- Non-repudiation → Assurance that someone cannot deny the validity of something

- Cryptography is used for confidentiality, authentication, message integrity and non-repudiation

Symmetric Key Encryption

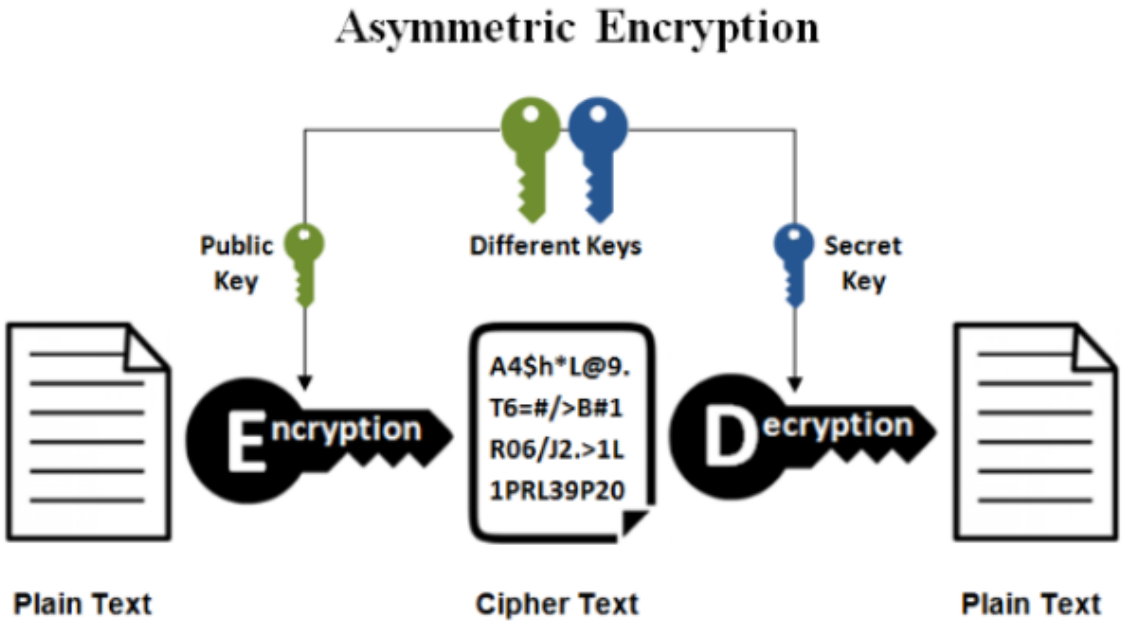
- Symmetric Encryption Diagram



- There is only one key, shared by sender and receiver, to use the algorithms to encrypt and decrypt, and it must be very secretly and carefully delivered
- Some SKEs are Caesar, Monoalphabetic and Polyalphabetic

Public Key Encryption

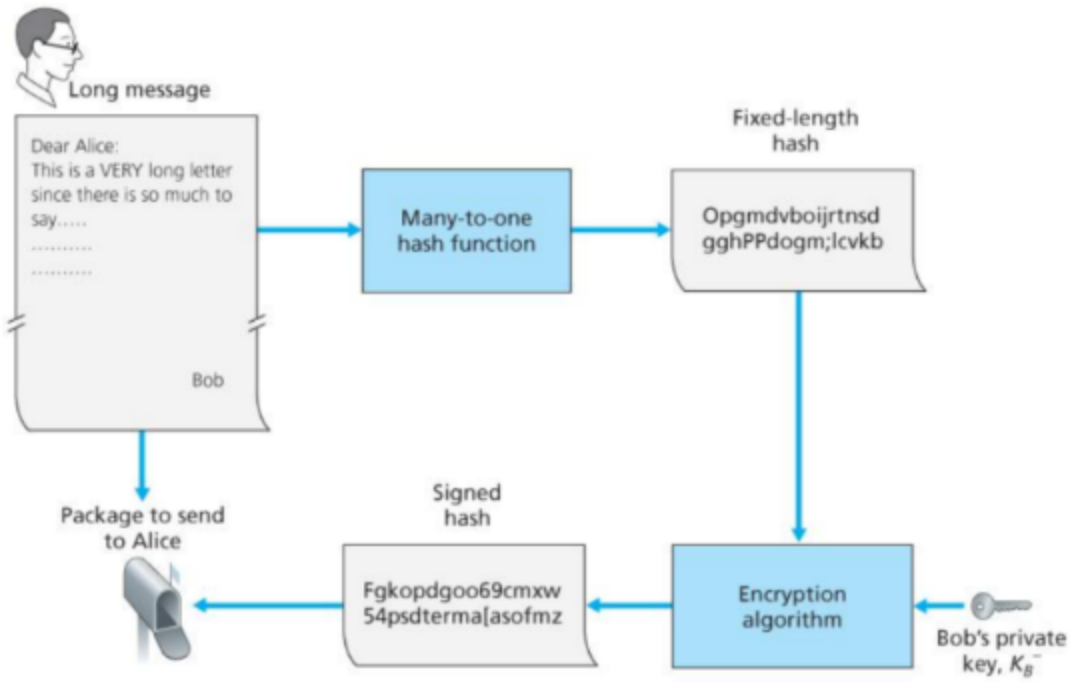
- Public Key Encryption Diagram



- Eliminates the need to share the key carefully and secretly as there are different keys
- Some PKEs are RSA, ECC and Diffie-Hellman

Digital Signature

- Authenticates the sender, indicates the owner or creator of a resource or a document's content
- Made possible using PKEs, which can identify authenticity of the data
- When used in reverse, the message will not be confidential but the sender can be verified
- However, this is computationally very expensive
- Alternative Digital Signature



- An alternative is for the sender to use a public cryptographic one-way hash function which creates a fixed-length hash that is uniquely defined for the particular message, called a 'digest'. The private key is used to encrypt the digest. The encrypted digest is the digital signature.
- The message can be transmitted as plaintext together with the encrypted digest as a separate file. As the digest is much smaller than the whole message, the encryption and the transmission are faster processes than if the whole message were encrypted.
- At the receiver end, the same public one-way hash function is used to create a digest from the received message. The encrypted version of the original digest is decrypted using the public key. If the two digests are identical, the receiver can be confident that the message is authentic and has been transmitted unaltered.
- Public key certification helps identify that a public key belongs to a certain entity like IP sec and SSL

Authentication

- End point authentication → Process of one entity proving its identity to another entity over a computer network
- Usually, network elements must authenticate each other. Here, authentication must be done soley on the basis of messages and data exchanged.
- Common authentication methods include passwords, biometrics, token values and 2FA