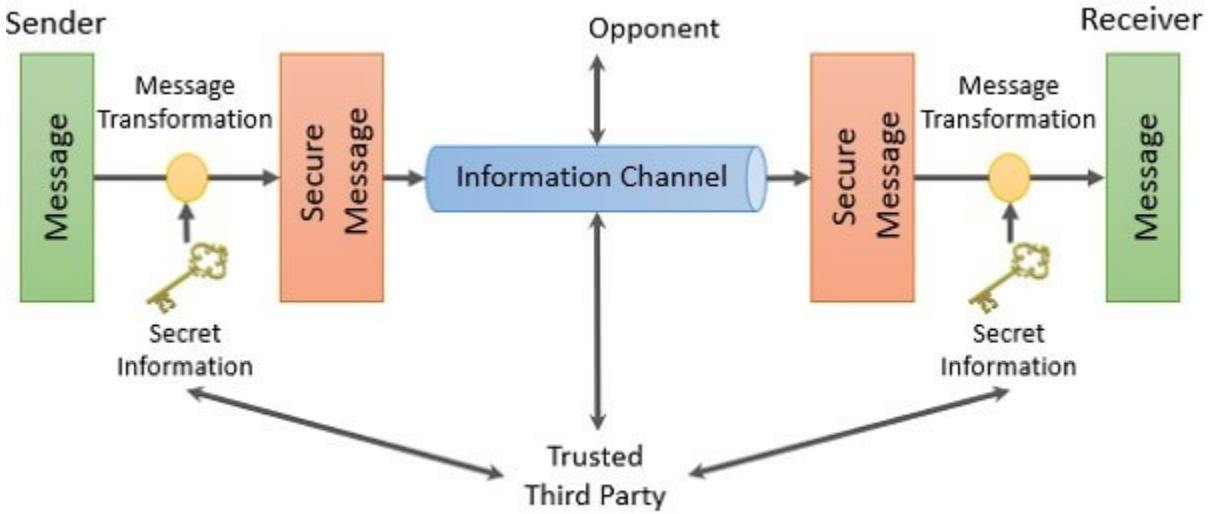
Network Security

What is Network Security?

- Network security is the security designed to protect the integrity of the network from unauthorized access and threats. The network administrators are responsible for adopting various defensive measures to guard their networks from possible security risks.

A Model of Network Security

- A network security model in computer networks refers to the structured defensive mechanisms and protocols implemented to protect the integrity, confidentiality and availability of data transmitted between devices over an interconnected system of networks.



Network Security Model contd....

- Its core purpose in computer network security (CNS) is to transform plain text data into encrypted ciphertext before sending it over the vulnerable network channel so that potential attackers cannot decipher or make sense of the information.
- This is achieved by applying a cryptographic algorithm powered by a secret key known only to the communicating parties in the network security model in CNS. The encrypted data gets transmitted and later decrypted at the receiving end with the same secret key.

Principle of Cryptography

- **Confidentiality**
- Confidentiality agreements have rules and guidelines to keep the information secure and private. Confidentiality must be protected using techniques like encryption. It ensures that only authorized people can access the information at certain places — and it restricts access to other unauthorized parties.
- **Authentication**
- The process of confirming that the person who sent a specific message is the sender of that message. This principle ensures the receiver receives the message from a sender who is permitted to do so. Two common authentication mechanisms are:
- Access tokens
- Auth signatures

- **Encryption**
- Encryption is the process of transforming information into an unreadable format using an encryption algorithm to protect the privacy of the information. Only the receiver can read them using the decryption key.
- **Data integrity**
- The data should be consistent and accurate without any alterations while in transit from the sender to the receiver. Data integrity ensures that no manipulation has been done to the data during its lifecycle using techniques like cryptographic hashing.
- **Non-repudiation**
- The non-repudiation principle ensures that the message sender cannot repudiate the authenticity of his signature using techniques like digital signatures.

Symmetric cryptography

- Symmetric-key cryptography involves encrypting and decrypting using the same cryptographic keys. Here, the sender and all receivers share a common secret key. The plaintext messages are transformed into cipher text using a particular encryption key. The receiver can use the same encryption key to decrypt the message using the shared secret key.
- Examples of symmetric-key encryption algorithms include:
  - Advanced Encryption Standard (AES)
  - Data Encryption Standard (DES)
  - Triple Data Encryption Standard (Triple DES)
  - International Data Encryption Algorithm (IDEA)
  - TLS/SSL protocol

Public Key Cryptography (Asymmetric Key Cryptography)

- This type of cryptography, known as "public-key cryptography," uses different cryptographic keys for the encryption and decryption processes. The sender and the receiver have a private key and a public key:
- The public key is shared with all the parties that must communicate with the sender.
- The private key is kept secret from each

Public Key Algorithm- RSA

- The RSA (Rivest-Shamir-Adleman) algorithm is an asymmetric encryption algorithm invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. It is used to encrypt data and communications over the internet and for email encryption.
- However, there are still several exploitable vulnerabilities in the RSA. For example, researchers were able to crack a key 768-bit RSA algorithm. It is recommended to use 2048 bits as the key length.

Digital Signature Algorithm

- Digital signatures are one of the applications of public key cryptography that provide authenticity and data integrity. The sender generates a unique signature using the private key and attaches it to the document, which needs to be verified using the public key.

DSA contd..

- The Digital Signature Algorithm, or DSA, is a Federal Information Processing Standard for digital signatures. It facilitates the authentication of digital messages or documents by ensuring that signatures are valid and unaltered. Leveraging a pair of keys in its operation—one private, which is kept secret by the message sender, and one public, which is available to message recipients—DSA enables the secure verification of the sender's identity and the integrity of the message sent, effectively safeguarding against unauthorized modifications and impersonation in digital communications.

Communication Security

- Ipsec
- Internet Protocol Security (IPsec) is a suite of protocols and services that provide security for IP networks. It is a widely used virtual private network (VPN)technology. IP packets lack effective security mechanisms and may be forged, stolen, or tampered with when being transmitted on a public network, such as the Internet. To solve this problem, the communicating parties establish an IPsec tunnel for encrypted transmission of IP packets. This ensures secure transmission of IP packets on an insecure network, such as the Internet.
- VPN
- Virtual Private Networks (VPNs) enable secure remote connections for teleworkers and road warriors and connect distributed sites. VPNs create encrypted tunnels across public networks to ensure data confidentiality and integrity.

Firewalls

- Firewalls monitor all incoming and outgoing network traffic and stop viruses, hackers and DDoS assaults depending on security standards. Firewalls provide perimeter security through traffic filtering and block unauthorised access attempts.

Wireless Security

- Wireless security is, in essence, preventing unwanted users from accessing a particular Wi-Fi network. More so, wireless security, also known as Wi-Fi security, aims to ensure that your data remains only accessible to users you authorize.

How Does Wireless Security Work?

- Wireless Security Protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the authentication security protocols created by the Wireless Alliance used to ensure wireless security. There are four wireless security protocols currently available.
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)
- Wi-Fi Protected Access 3 (WPA 3)