Computer Network Security

Unit – 01: Attacks on computers and computer security

- Computer security, need for security, approaches, principles,
- Attacks on computers and types of attacks,
- Operational model of network security,
- Cryptography concepts and techniques,
- substitution transposition,
- encryption and decryption,
- symmetric, Asymmetric key cryptography,
- key range size,

Questions to be discussed:

1. What is computer security?
2. Explain need of information security.
3. Discuss different types of attacks.
4. What is cryptography? Explain types of cryptography.
5. Differentiate between substitution and transposition cipher techniques.

What is Computer Security?

- Computer security is the protection of computer systems and information from harm, theft, and unauthorized use.
- It is the process of preventing and detecting unauthorized use of your computer system.
- Computer security is also called cyber security, digital security or IT security.
- August Kerckhoffs is known as the father of computer security.

Types of computer security:

Computer security can be classified into four types:

1. Cyber Security
2. Information Security
3. Application Security
4. Network Security

Cyber Security:

- It is defined as protecting computer systems, which communicate over the computer networks
- Cyber attacks are those attacks that happen when our system is connected to the Internet.

Information Security:

- Information security is securing information from unauthorized access, modification & deletion
- It has mainly three objectives: confidentiality, integrity, and availability of information(CIA).

Application Security:

- Application security means securing our applications and data so that they don't get hacked and also the databases of the applications remain safe and private to the owner itself so that user's data remains confidential.

Network Security:

- Network Security is by securing both the software and hardware technologies.
- Network security means securing a network and protecting the user's information about who is connected through that network.

Need of information security:

- It is essential for protecting sensitive and valuable data from unauthorized access.
- The need of information security is essential because:
  1. Protecting Confidential Information.
  2. Maintaining Business Continuity.
  3. Protecting Customer Trust.
  4. Preventing Cyber-attacks.
  5. Protecting Employee Information.

Types of cyber attack:

1. Denial of service attack or DOS.
2. Backdoor
3. Eavesdropping
4. Phishing
5. Spoofing
6. Malware
7. Social engineering
8. Polymorphic Attacks

Denial of service attack or DOS:

- A denial of service attack is a kind of cyber attack in which the attackers disrupt the services of the particular network by sending infinite requests.

Backdoor:

- In a backdoor attack, malware, trojan horse or virus gets installed in our system and start affecting it's security along with the main file.

Eavesdropping:

- Eavesdropping refers to secretly listening to someone's talk without their permission or knowledge.
- Attackers try to steal, manipulate, modify, hack information or systems by passively listening to network communication, knowing passwords etc.

Phishing:

- Similarly, in phishing, a user is tricked by the attacker who gains the trust of the user or acts as if he is a genuine person and then steals the information by ditching.
- Not only attackers but some certain websites that seem to be genuine, but actually they are fraud sites.

Spoofing:

- Spoofing is the act of masquerading as a valid entity through falsification of data(such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain.
- Spoofing is of several types- email spoofing, IP address spoofing, biometric spoofing etc.

Malware:

- Malware is made up of two terms: Malicious + Software = Malware.
- Malware intrudes into the system and is designed to damage our computers.
- Different types of malware are adware, spyware, ransomware, Trojan horse, etc.

Social engineering:

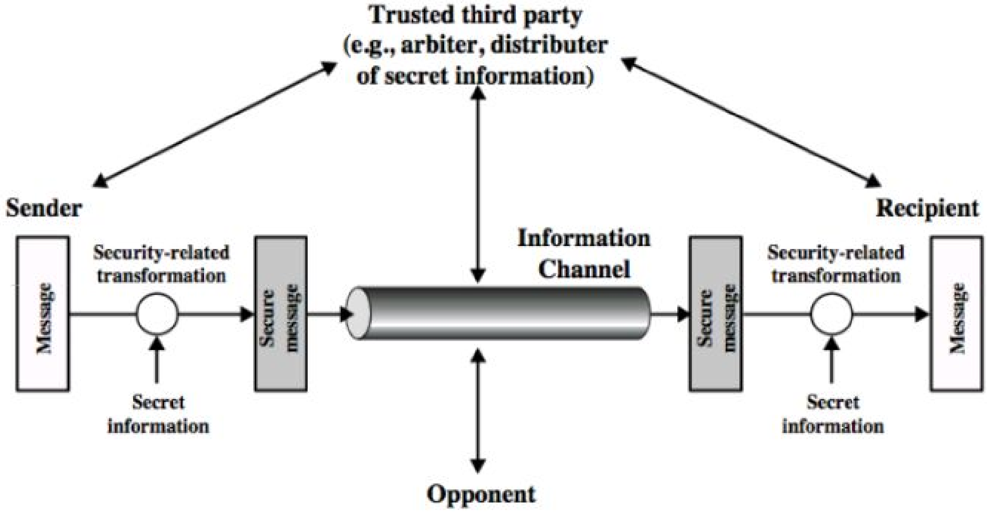
- Social engineering attack involves manipulating users psychologically and extracting confidential or sensitive data from them by gaining their trust.

Polymorphic Attacks:

- Poly means "many" and morph means "form", polymorphic attacks are those in which attacker adopts multiple forms and changes them so that they are not recognized easily.
- These kinds of attacks are difficult to detect due to their changing forms.

Operational model of network security:

- A Network Security Model exhibits how the security service has been designed over the network.
- It prevent the opponent from causing a threat to the confidentiality of the information that is being transmitted through the network.
- When we send our data from source side to destination side we have to use some transfer method like the internet or any other communication channel by which we are able to send our message.



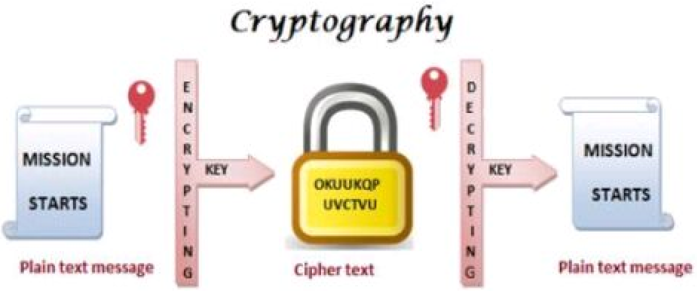
Cryptography:

- It is a technique of sending information from sender to receiver using codes.
- It securing information through use of codes so that only intended person can understand & process it.
- Cryptography is used to preventing unauthorized access of information.
- The prefix "crypt" means "hidden" and suffix "graphy" means "writing".
- Claude E. Shannon is considered to be the father of mathematical cryptography.

Components used in cryptograph:

There are various components of cryptography:

1. Plaintext and
2. Ciphertext
3. Key



Plaintext and Ciphertext:

- The original message, before being transformed, is called plaintext.
- After the message is transformed, it is called ciphertext.
- The process of conversion of plain text to cipher text this is known as Encryption.
- The process of conversion of cipher text to plain text this is known as decryption.
- The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

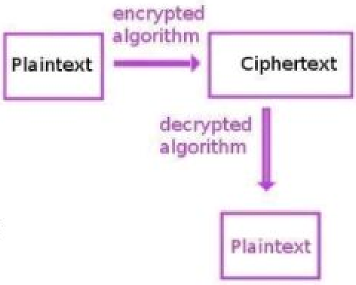
Key:

- In cryptography, a key is a string of characters used within an encryption algorithm for altering data so that it appears random.
- Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

Types of Cryptography:

In general there are three types Of cryptography:

1. Symmetric Key Cryptography:
2. Asymmetric Key Cryptography:



Symmetric Key Cryptography:

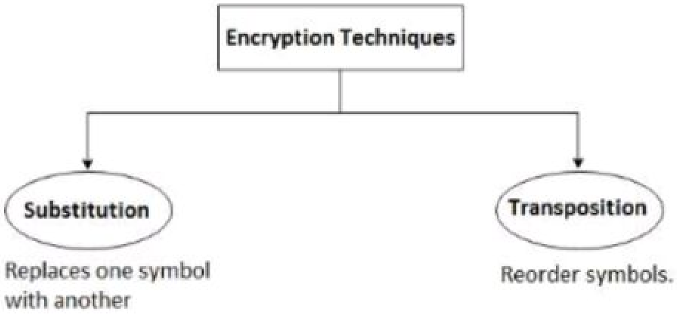
- It is an encryption system where the sender and receiver of message use encrypt and decrypt messages.
- Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner.
- The most popular symmetric key cryptography system are
  1. Data Encryption System(DES) and
  2. Advanced Encryption System(AES).

Asymmetric Key Cryptography:

- Under this system a pair of keys is used to encrypt and decrypt information.
- A receiver's public key is used for encryption and a receiver's private key is used for decryption.
- Public key and Private Key are different.
- Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key.
- The most popular asymmetric key cryptography algorithm is
    - RSA algorithm.

What is encryption?

- In cryptography, encryption is the process of encoding information.
- This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
- Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.
- Substitution and transposition ciphers are two common types of symmetric encryption, which means that the same key is used to encrypt and decrypt the message.
- They are often used in combination to increase the security of the communication.



Substitution cipher:

- A substitution cipher replaces each letter or symbol in the plaintext with another one, according to a fixed rule or a key.
- The key is the number of shifts, and it can be changed periodically to avoid repetition.
- Substitution ciphers are easy to implement and understand.
- But in this an attacker can guess the key by looking at the most common patterns in the ciphertext.

Transposition cipher:

- A transposition cipher rearranges the order of the letters or symbols in the plaintext, according to a certain pattern.
- Transposition ciphers are more difficult to break than substitution ciphers, but they can still be attacked, which means that an attacker can try to find words or phrases that fit the ciphertext.

Difference between Substitution Cipher and Transposition Cipher Technique:

Substitution Cipher Technique	Transposition Cipher Technique
In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
In substitution Cipher Technique, The letter with low frequency can detect plain text.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.