Cryptography and network Security

Unit-1

Key Principles of Security

The classification of security services are as follows:

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of a message. Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

Authentication: Authentication mechanism help establish proof of identities. Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: When the content of a message are changed after the sender sends it but before it reaches the intended recipient, we say that integrity of a the message is lost. Ensures that only authorized parties are able to modify computer system assets and transmitted information.

Non repudiation: Non- repudiation does not allow the sender of a message to refute the claim of not sending that message. Non-repudiation requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: The principles of access control determines who should be able to access what.

Availability: The principle of availability states that resources should be available to authorized parties at all times. Availability requires that computer system assets be available to authorized parties when needed.

Cryptographic Attacks

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks do not involve any modifications to the content of an original message.

Passive attacks are of two types:

1. **Release of message contents:** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

2. **Traffic analysis:** If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

   Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Active attacks

These attacks involve some modification of the data stream or the creation of a false stream. In active attacks, the contents of the original message are modified in some way.

These attacks can be classified in to four categories:

1. **Masquerade** – Trying to pose as another entity involves masquerade attacks. One entity pretends to be a different entity.

2. **Modification**- Modification attacks can be classified further in to **replay attacks** and **alteration of messages.**

   Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

   Alteration of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

3. **Denial of service** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

   It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

The Practical side of Attacks

The attacks discussed earlier can come in a number of forms in real life. They can be classified into two broad categories: application- level attacks and network-level attacks.

Application- level attacks: These attacks happen at an application level in the sense that the attacker attempt to access, modify, or prevent access to information of a particular application or the application itself.

Network-level attacks: These attacks generally aim at reducing the capabilities of network by a number of possible means. These attacks generally make an attempt to either slow down, or completely bring to halt a computer network.

Security attacks can happen at the application level or the network level.

Symmetric and Asymmetric key cryptography

Symmetric and public key algorithms Encryption/Decryption methods fall into two categories.

1. Symmetric key: In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

2. Asymmetric key: there are two keys one is public key and other is private key. Public key is announce to the public and used for encryption but the private key is use for decryption

BLOCK CIPHER PRINCIPLES

Virtually, all symmetric block encryption algorithms in current use are based on a structure referred to as Fiestel block cipher. For that reason, it is important to examine the design principles of the Fiestel cipher. We begin with a comparison of stream cipher with block cipher.

- A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. E.g, vigenere cipher. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically a block size of 64 or 128 bits is used

Block cipher principles

- most symmetric block ciphers are based on a Feistel Cipher Structure needed since must be able to decrypt ciphertext to recover messages efficiently. block ciphers look like an extremely large substitution
- would need table of 264 entries for a 64-bit block
- Instead create from smaller building blocks
- using idea of a product cipher in 1949 Claude Shannon introduced idea of substitution-permutation (S-P) networks called modern substitution-transposition product cipher these form the basis of modern block ciphers
- S-P networks are based on the two primitive cryptographic operations we have seen before:
- substitution (S-box)
- permutation (P-box)
- provide confusion and diffusion of message
- diffusion – dissipates statistical structure of plaintext over bulk of ciphertext
- confusion – makes relationship between ciphertext and key as complex as possible