Computer Network Security

TE - IT

Lecture -6
21/07/2022

Session: 3:30 - 4:30 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-1

✓ Contents

1. Security Services
2. Security Mechanisms

Security Services

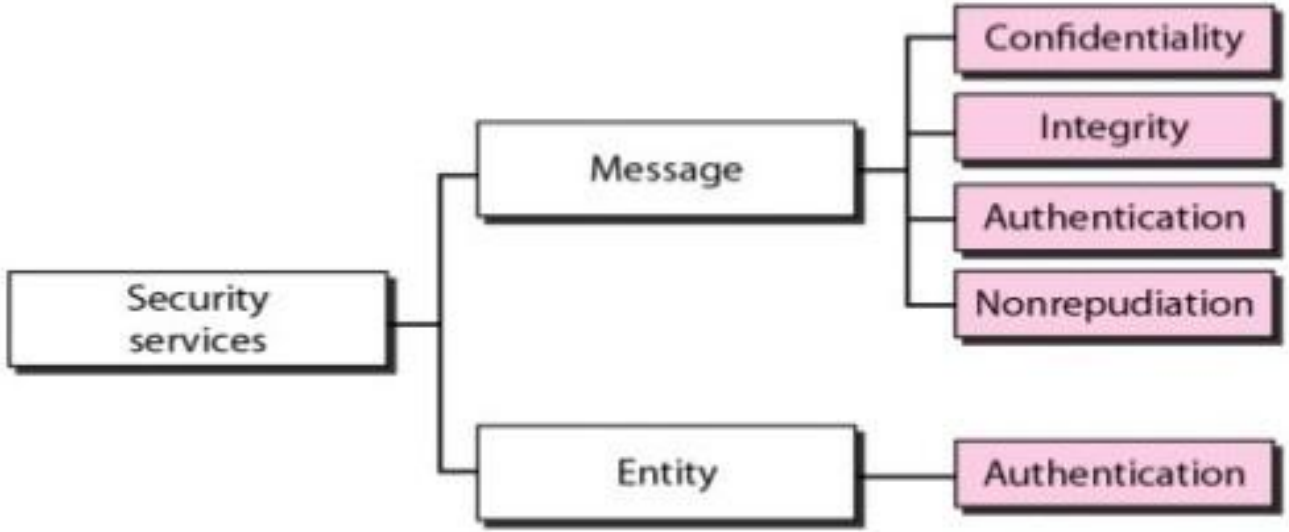
X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers

RFC 2828 defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 defines it in 5 major categories

Security Services (X.800)

Authentication - assurance that the communicating entity is the one claimed
Access Control - prevention of the unauthorized use of a resource
Data Confidentiality –protection of data from unauthorized disclosure
Data Integrity - assurance that data received is as sent by an authorized entity
Non-Repudiation - protection against denial by one of the parties in a communication


Security services
Message
Confidentiality
Integrity
Authentication
Nonrepudiation
Entity
Authentication

Message Confidentiality

The confidentiality or privacy make sense when the transmitted message must make sense to only the intended/expected receiver. The message must be garbage to all others. To achieve such privacy, the sender must encrypt/ encode the message and the only receiver should decrypt/ decode it. Such privacy can be provided using two ways: Symmetric-key cryptography & Asymmetric-key cryptography.

Symmetric-key Cryptography: To provide security with symmetric-key cryptography, the sender and receiver need to share a secret key. The secret key is shared through session key. A session key is such a key that is used only for the duration of one session. Session key itself is exchanged using symmetric key cryptography. The nature of symmetric key allows the communication to be carried on in both directions although this is not recommended today. Using two different keys is more secure because if one key is compromised, the communication is still confidential in other direction. Symmetric key cryptography is still dominating for a long message because of its efficiency to provide confidentiality.

Asymmetric-key Cryptography: In this method of message confidentiality, there is no key sharing. There is a public announcement instead. The receiver creates two keys: public key & private key. The public key is publicly announced and the private key is kept secret for decryption. The public key is used for encryption only and the private key is used for decryption only. While using asymmetric-key cryptography, there arise two problems:

The message is inefficient for long messages because of long mathematical calculations using long keys.

The sender of the message still needs to be certain about the public key of the receiver. A system of trust is needed here.

Message Integrity

The concept of integrity of message says that the data must arrive at the receiver exactly as they were sent. There must be no alteration during the transmission neither accidentally nor intentionally. Encryption and Decryption of message may provide secrecy, privacy or confidentially but it is not able to provide integrity. Message Integrity is more important than privacy. Instead of hiding message from other, it is more important to keep it safe from any tampering. Message integrity can be provided using the following methods:

Document & Fingerprint: Fingerprint is a way to preserve the integrity of a document. If one needs to be sure that the contents of her document will not be illegally changed, she can put her fingerprint at the bottom of the document. To preserve the integrity of a document, both the Fingerprint & the Document are needed.

Message & Message Digest: Message & Message Digest is the electronic equivalent of Document & Fingerprint. Here, the message is passed through the Hash algorithm for integrity preservation of the message. The hash function creates a compressed image of the message that can be used as a fingerprint.

Message Authentication

Message authentication ensures the receiver about the sender's identity. It makes the receiver sure that an imposter hasn't sent the message. A Hash function can guarantee the integrity of the message but it does not authenticate the sender of the message. To provide message authentication, the sender needs to provide proof that he is sending the message and he is not an imposter. We can add authenticity of the message in the network by the following ways:

Message Authentication Code (MAC): we need to change MDC (Modification Detection Code) provide by Hash function to MAC (Message Authentication Code) to provide message authentication. MDC uses keyless hash function while MAC has keyed hash function. Keyed hash function includes the symmetric key at the time of digest creation between sender and receiver.

Hashed Message Authentication Code (HMAC): Hashed MAC or HMAC uses any keyless hash function such as SHA-1. HMAC creates a nested MAC by applying a keyless hash function to the concentration of the message and a symmetric key.

Message Non-repudiation

Message Non-repudiation means that a sender must not be able to deny sending a message that he/she did send in fact. The burden of proof falls on the receiver. Let us take an example of a bank transaction. When a customer sends a message to withdraw money from his account, the bank must have proof that the customer actually requested this transaction. MAC can provide message authenticity & integrity but there is a problem of sharing a symmetric key between sender and receiver. This can be resolved by Digital signature. Nonrepudiation can be provided using a trusted party.

Digital Signature: Digital Signature is an electronic signature that can prove the authenticity of the sender to receiver. Digital Signature is a proof to the recipient that the message is coming from the authenticated person. It can use a pair of asymmetric keys: a private and a public key. The digital signature can be achieved in two ways:

Signing the document: It is easier but less efficient way. Encrypting a document with the private key of the sender and decrypt with the public key of the sender.

Signing the digest of the document: the digest of the message is signed instead of signing the original message. The sender can sign the message digest and receiver can verify the message digest. The effect is the same.

THANK YOU