Assignment 1 19UCS122

Q1. What are the examples of Security Attacks?

→

The Open Systems Interconnection (OSI) security architecture provides a systematic framework for defining security attacks, mechanisms, and services.

◆ Security attacks are classified as either passive attacks, which include the unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service.

◆ A security mechanism is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.

◆ Security services include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability

19UCS122

Q2. Explain x-800 Security Services

->

1. X. 800 defines it in 5 major categories
2. Authentication - assurance that the communicating entity is the one claimed
3. Access Control - prevention of the unauthorized use of a resource
4. Data Confidentiality - protection of data from unauthorized disclosure
5. Data Integrity - assurance that data received is as sent by an authorized entity
6. Non-Repudiation - protection against denial by one of the parties in a communication

Security Mechanisms (X. 800) Cont

Divided into

1. specific security mechanisms:
2. pervasive security mechanisms

19UCS122

Q3

1. specific security mechanisms:
2. May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
3. encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
4. pervasive security mechanisms:
5. Mechanisms that are not specific to any particular OSI security service or protocol layer.
6. trusted functionality, security labels, event detection, security audit trails, security recovery

X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms.

A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted.

q.5 What is the difference betn Symmetric and asymmetric Cryptographic System?

Symmetric Cryptography	Asymmetric Cryptography
Same key is used for encryption & decryption.	One key is used for encryption & another key is used for decryption.
Very fast speed of encryption / decryption.	Slower speed of encryption or decryption.
Size of resulting encrypted text is usually same as or less than the original plaintext size.	Size of resulting encrypted text is more than the original plaintext size.
Both parties should known the key is symmetric key encryption	One of the keys is known by the two parties in public key encryption.
Usage - Confidentiality	Confidentiality, Digital Signature

19UCS122

Q4. Explain model for Network Security

->

Model for Network Security Cont. All the techniques for providing security have two components:

1 A security-related transformation on the information to be sent. Examples include the encryption of the message and the addition of a code to verify the identity of the sender

2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used

using this model requires us to:

1 design a suitable algorithm for the security transformation

2 generate the secret information (keys) used by the algorithm

3. develop methods to distribute and share the secret information