Jamia Millia Islamia

Dept. Of Computer Science

Cryptography

Submitted By: Wasit Shafi

Roll no: 18MCA054

Submitted To: Dr. Rafat parveen

Q1.Define the three security goals.

Sol: The Three Security Goals Are Confidentiality, Integrity, and Availability. All information security measures try to address at least one of three goals:

1. Protect the confidentiality of data
2. Preserve the integrity of data
3. Promote the availability of data for authorized use

1. Confidentiality: Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content. It prevents essential information from reaching the wrong people while making sure that the right people can get it. Data encryption is a good example to ensure confidentiality.

Tools for Confidentiality

- Encryption.
- Access Control.
- Authentication.
- Authorization.
- Physical Security.

Encryption

Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key)

Access control

Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information.

Authentication

An authentication is a process that ensures and confirms a user's identity or role that someone has. It can be done in a number of different ways, but it is usually based on a combination of-

- something the person has (like a smart card or a radio key for storing secret keys),
- something the person knows (like a password),
- something the person is (like a human with a fingerprint).

Authorization

Authorization is a security mechanism which gives permission to do or have something. It is used to determine a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features.

Physical Security

Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other properties from damage.

2. Integrity: **Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.**

Tools for Confidentiality

- Encryption.
- Access Control.
- Authentication.
- Authorization.
- Physical Security.

Backups

Backup is the periodic archiving of data. It is a process of making copies of data or data files to use in the event when the original data or data files are lost or destroyed. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy.

Checksums

A checksum is a numerical value used to verify the integrity of a file or a data transfer. In other words, it is the computation of a function that maps the contents of a file to a numerical value. They are typically used to compare two sets of data to make sure that they are the same. A checksum function depends on the entire contents of a file.

Data Correcting Codes

It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

3. Availability

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools for Availability

- Physical Protections
- Computational Redundancies

Physical Protections

Physical safeguard means to keep information available even in the event of physical challenges. It ensure sensitive information and critical information technology are housed in secure areas.

Computational redundancies

It is applied as fault tolerant against accidental faults. It protects computers and storage devices that serve as fallbacks in the case of failures.

Q2. Distinguish between passive and active security attacks .Name some passive and active security attacks.

Sol:

Sr. No.	Key	Active Attack	Passive Attack
1	Modification	In Active Attack, information is modified.	In Passive Attack, information remain unchanged.
2	Dangerous For	Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
3	Attention	Attention is to be paid on detection.	Attention is to be paid on prevention.
4	Impact on System	In Active Attack, system is damaged.	In Passive Attack, system has no impact.

Sr. No.	Key	Active Attack	Passive Attack
5	Victim	Victim gets informed in active attack.	Victim does not get informed in passive attack.
6	System Resources	System Resources can be changed in active attack.	System Resources are not changed in passive attack.

Active and Passive attacks

Active Attack –

Masquerade

Modification of messages –

Repudiation –

Replay –

Denial of Service –

Passive attacks

The release of message content –

Traffic analysis –

Q3. What is the OSI security architecture? Explain.

Sol: OSI SECURITY ARCHITECTURE

To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The OSI security architecture was developed in the context of the OSI protocol architecture. However, for our purposes in this chapter, an understanding of the OSI protocol architecture is not required.

For our purposes, the OSI security architecture provides a useful, if abstract, overview of many of the concepts. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks, Services And Mechanisms

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

- ***Security attack*** *– Any action that compromises the security of information owned by an organization.*

- ***Security mechanism*** *– A mechanism that is designed to detect, prevent or recover from a security attack.*

- ***Security service*** *– A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.*

SECURITY SERVICES

The classification of security services are as follows:

Confidentiality: *Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. Eg., printing, displaying and other forms of disclosure.*

Authentication: *Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.*

Integrity: *Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.*

Non repudiation*: Requires that neither the sender nor the receiver of a message be able to deny the transmission.*

Access control*: Requires that access to information resources may be controlled by or the target system.*

Availability*: Requires that computer system assets be available to authorized parties when needed.*

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality

The protection of all user data on a connection.

Connectionless Confidentiality

The protection of all user data in a single data block

Selective-Field Confidentiality

AUTHENTICATION

The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic Flow Confidentiality

The protection of the information that might be derived from observation of traffic flows.

Connection Integrity with Recovery

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery

As above, but provides only detection without recovery.

Selective-Field Connection Integrity

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin

Proof that the message was sent by the specified party.

Nonrepudiation, Destination

Proof that the message was received by the specified party.

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are

Encipherment

Digital Signature

Access Control

SECURITY ATTACKS

There are four general categories of attack which are listed below.

Interruption

Interception

Modification

Fabrication

Passive attack

Release of message contents

Traffic analysis.

Active attacks

Masquerade –
Replay –.
Modification of messages –.
Denial of service –

Q4. What are the essential ingredients of a symmetric cipher?

Sol:

A symmetric encryption scheme has five ingredients:

1. Plaintext

2. Encryption algorithm

3. Secret Key

4. Cipher text

5. Decryption algorithm:

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret Key: The secret key is also input to the encryption algorithm. The key is the value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the key.

Decryption algorithm: This is essentially the encryption algorithm in reverse. It takes the cipher text and the secret key and produces the original plaintext.

Q5. What are the two basic functions used in encryption algorithms? Explain.

Sol:

All the encryption algorithms are based on two general principles:

Substitution: In which each element in the plaintext(bit, letter, group of bits or letters) is mapped into another element.

Transposition: In which elements in the plaintext are rearranged.

The fundamental requirement is that no information be lost(that is ,that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

Q6. Differentiate between block cipher and stream cipher ?

Sol:

BASIS OF COMPARISON	STREAM CIPHER	BLOCK CIPHER
Description	A stream cipher is a symmetric key cipher (method of encryption) where plaintext digits are combined with a pseudorandom cipher digit stream.	A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text.
Key Use	Stream Cipher uses a different key for each byte.	Block cipher uses the same key to encrypt each block.
Integrity	Stream ciphers do not provide integrity protection or authentication.	Some block ciphers (depending on the mode) can provide integrity protection, in addition to confidentiality.
XOR Function	Stream cipher uses XOR function for converting the plain text into cipher text that is the reason why it is easy to reverse the XORed bits.	Block cipher do not use XOR function.
Plaintext Encryption	Stream cipher uses confusion to encrypt plaint text.	Block ciphers use both confusion and diffusion to encrypt plaintext into ciphertext.
Speed	1 byte (8 bits) at a time is converted in the stream cipher, this makes the process faster.	Block ciphers, the normal size of the block could be 64 or 128 bits in the block cipher and this makes block cipher slower than stream cipher.
Implementation	Stream ciphers are more difficult to implement correctly, and are prone to weaknesses based on usage.	Relatively easy to implement.

Algorithm Modes	Stream cipher uses CFB (Cipher Feedback) and OFB (Output Feedback).	Block cipher uses ECB (Electronic Code Book) and CBC (Cipher Block Chaining).

Q7. What are the two general approaches to attack a cipher?

Sol: The general two approaches for attacking a cipher

1. **Cryptanalysis**

2. **Brute-force attack**

Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some samples plaintext-cipher text pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with the key are compromised.

Brute-force attack: The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Q8. A cipher text has been generated with an affine cipher. The most frequent letter of the ciphertext is 'F' , and the second most frequent letter of the ciphertext is 'C' . Break this code.

Sol: let us assume the most freq. plaintext letter is 'e' & Second most frequent letter is 't'.

We know C = (a * p + b) mod n.

Here C = 'F'(5) and 'C'(2).

$$\Rightarrow 5 = (4a + b) \bmod 26 \qquad \text{eq(1)}$$
$$\Rightarrow 2 = (19a + b) \bmod 26 \qquad \text{eq(2)}$$

On solving eq. 2 and 3, we get

$$-3 = (15a) \bmod 26 \qquad \text{eq(3)}$$

As LHS can't be negative, so we add n(26) to it

⇨ 15a mod 26 = 23

By hit & trial method, we get value of a = 5

On putting the value of a in eq(1), we get b = 11

Therefore a = 5 & b= 11

Q9. A small private club has only 100 members . Answer the following questions:

a. How many secret keys are needed if all members of the club need to send secret messages to each other?

b. How many secret keys are needed if everyone trusts the president of the club? If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member.

c. How many secret keys are needed if the president decides that the two members who need to communicate should contact him first. The president then creates a temporary key to be used between the two. The temporary key is encrypted and send to both members.

Sol:

(a) The number of keys = n × (n − 1) / 2 = (100 × 99) / 2 = 4950

(b) Just 100 keys are required. One secret key will be shared between the president and each member.

(c) Only 100 keys are needed: This can be established using session key. Member A sends a request to president to talk to B. The president creates a session key and encrypts using secret key shared between him and A. He also encrypts the session key by secret key between him and B. This A will be delivering to B. After the session key is established, the two members can use the one-time session key.

Q10.Some archeologists found a new script written in an unknown language. The archeologists later found a small tablet at the same place that contains a sentence in the same language with the translation in Greek. Using the tablet, they were able to read the original script. What type of attack did the archeologists use?

Sol: Known-plain-text attack is used by the archeologists.