**INFORMATION SECURITY CONCEPTS**

**INTRODUCTION:-**

**INFORMATION:-**

**SECURITY:-**



 *Fig:Information Security goals*

**Confidentiality**

It covers two related concepts to ensure:

**Data confidentiality:**

**1. Privacy**

**2. Integrity**

**(i) Data integrity**

**(ii) System integrity**

**3. Availability**

**Security Attacks:**



 *Fig: Taxonomy of attacks with relation to security goals*

**Attacks on Confidentiality:**

**Snooping**refers to unauthorized access to or interception of data.

**Traffic analysis** refers to obtaining some other type of information by monitoring

Online traffic.

 **Attacks on Integrity**

**Modification** means that the attacker intercepts the message and changes it.

**Masquerading *or spoofing*** happens when the attacker impersonates somebody

else.

**Replaying** means the attacker obtains a copy of a message sent by a user and later

tries to replay it.

**Repudiation** means that sender of the message might later deny that she has sent

the message; the receiver of the message might later deny that he has received the

Message.

 **Attacks on Availability**

Denial of Service (DoS) is a very common attack. It may slow down or totally

Interrupt the service of a system***.***

**Passive Attacks:**

A passive attack attempts to learn or make use of information from the system but

does not affect system resources.

 A passive attack is difficult to detect and isolate.

These do not involve any modification to the contents. So the approach should be to

prevent a passive attack rather than detection and corrective actions on it. Passive

attacks are of two types:

1. **Release of message contents**
2. **Traffic Analysis**

**Active Attacks:**

**Masquerade**

**Replay**

**Modification of messages**

**denial of service(Dos)**

**Passive versus Active Attacks:**

|  |  |  |
| --- | --- | --- |
| Attacks | Active/passive | Threatening |
| Snooping traffic analysis | Passive | confidentiality |
| Masquerading,replay,modification,reproduction | Active | Integrity |
| Denial of services | Active | availabilty |

**Category of security services:**



 *Fig: Categories of Security Services*

**Authentication**

**Peer entity authentication**

**Data origin authentication**

**Access Control**

**Data Confidentiality**

**Availability Services**

**Specific Security Mechanisms**

**Encipherment :**

The use of mathematical algorithms to transform data into a form that is not readily

intelligible. The transformation and subsequent recovery of the data depend on an

algorithm and zero or moreencryption keys.

**Digital Signature :**

Data appended to, or a cryptographic transformation of, a data unit that allows a

recipient of the data unitto prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

**Access Control :**

A variety of mechanisms that enforce access rights to resources.

**Data Integrity:**

A variety of mechanisms used to assure the integrity of a data unit or stream of data

units.

**Authentication Exchange:**

A mechanism intended to ensure the identity of an entity by means of information

exchange.

**Traffic Padding:**

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

**Routing Control:**

Enables selection of particular physically secure routes for certain data and allows

routing changes, especially when a breach of security is suspected.

**Security Management :**



**Table: Relationship between Security Services and Mechanisms:**

|  |  |
| --- | --- |
| Security Services | Security Services and Mechanisms |
| Data confidentiality | Encipherment and routing control |
| Data Integrity | Encipherment, Digital Signature, Data integrity |
| Authentication | Encipherment, Digital Signature, Authentication exchanges |
| Non repudiation | Digital Signature, Data integrity and notarization |
| Access Control | Access control mechanism |

· **Computer Security** is concerned with protecting the assets of the computer

System; information and services they provide.

· **Network Security** is the measures to protect data during their transmission.

· **Internet Security** is the measures to protect data during their transmission

over a collection of interconnected networks called Internet.

· **Information Security** is about to prevent attacks or failing that to detect

attacks on information based schemes/systems.

· **Security attack** means any action that compromises the security of

information owned by an organization.

· **Security mechanism** is a mechanism that is designed to detect, prevent or

recover from a security attack.

· **Security service** means 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.

**ASSESSMENT QUESTIONS-**

1. What are the three goals of Information Security?
2. Identify different categories of active attacks
3. Identify different categories of passive attacks.
4. What is the difference between passive and active attacks?
5. Name the security attacks on confidentiality.
6. Name the security attacks on integrity
7. Name the security attacks on availability.
8. What are the key challenges of Information Security?
9. What are Passive Attacks**?** Why are they difficult to detect?
10. List and define categories of security services.