Unit 1

Introduction: Security Concepts, Challenges, Security architecture, Security attacks, security services, security mechanisms

Introduction: Security Concepts, Challenges, Security architecture, Security attacks, security services, security mechanisms

Unit 2

Error detecting/correction: Block Codes, Generator Matrix, Parity Check Matrix, Minimum distance of a Code, Error detection and correction, Standard Array and syndrome decoding, Hamming Codes

Unit 3

Cryptography: Encryption, Decryption, Substitution and Transposition, Confusion and diffusion, Symmetric and Asymmetric encryption, Stream and Block ciphers, DES, cryptanalysis.

Public-key cryptography, Diffie-Hellman key exchange, man-in-the-middle attack

Digital signature, Steganography, Watermarking.

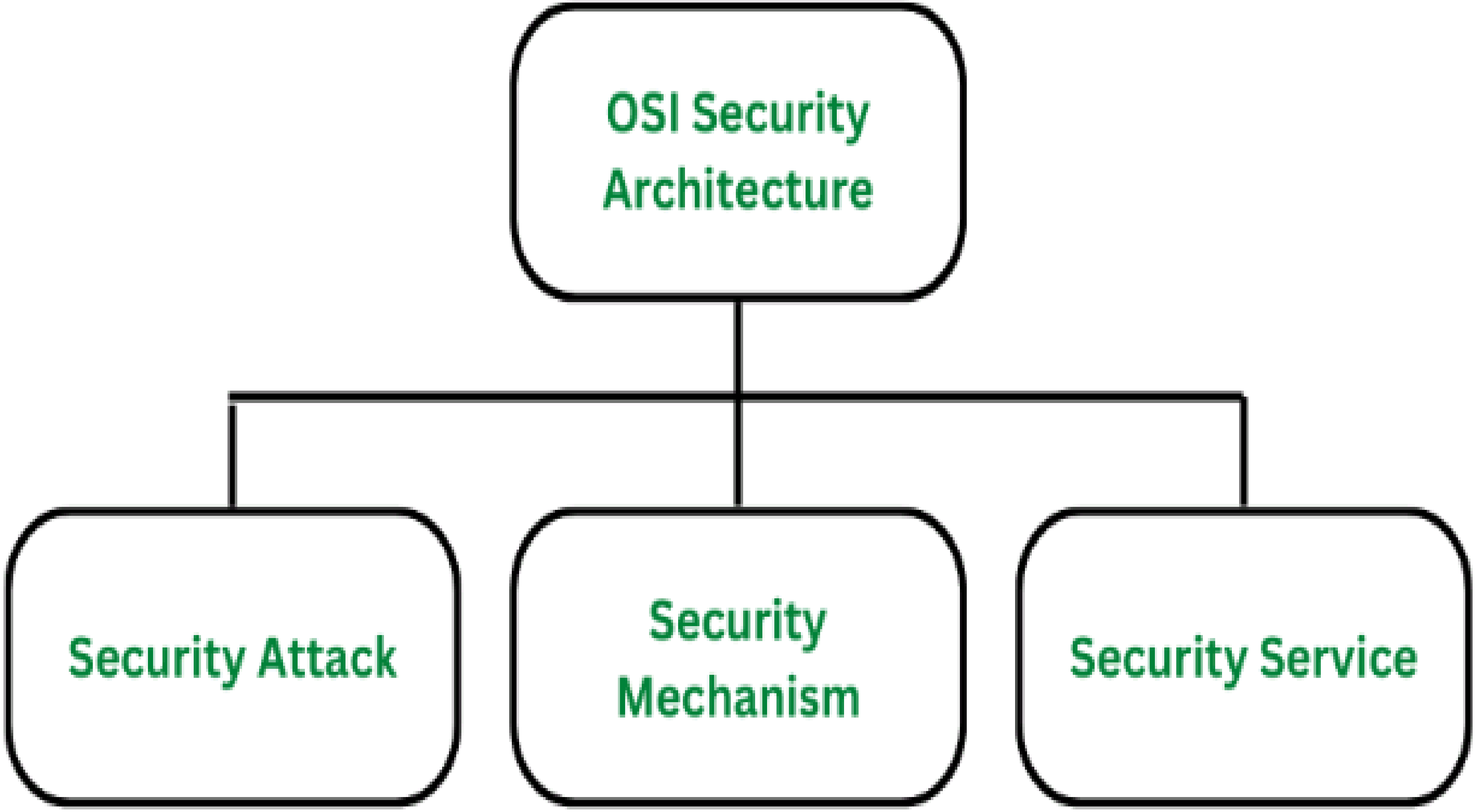
Unit 4

Malicious software's: Types of malwares (viruses, worms, trojan horse, rootkits, bots), Memory exploits - Buffer overflow, Integer overflow

Unit 5

Security in Internet-of-Things: Security implications, Mobile device security - threats and strategies

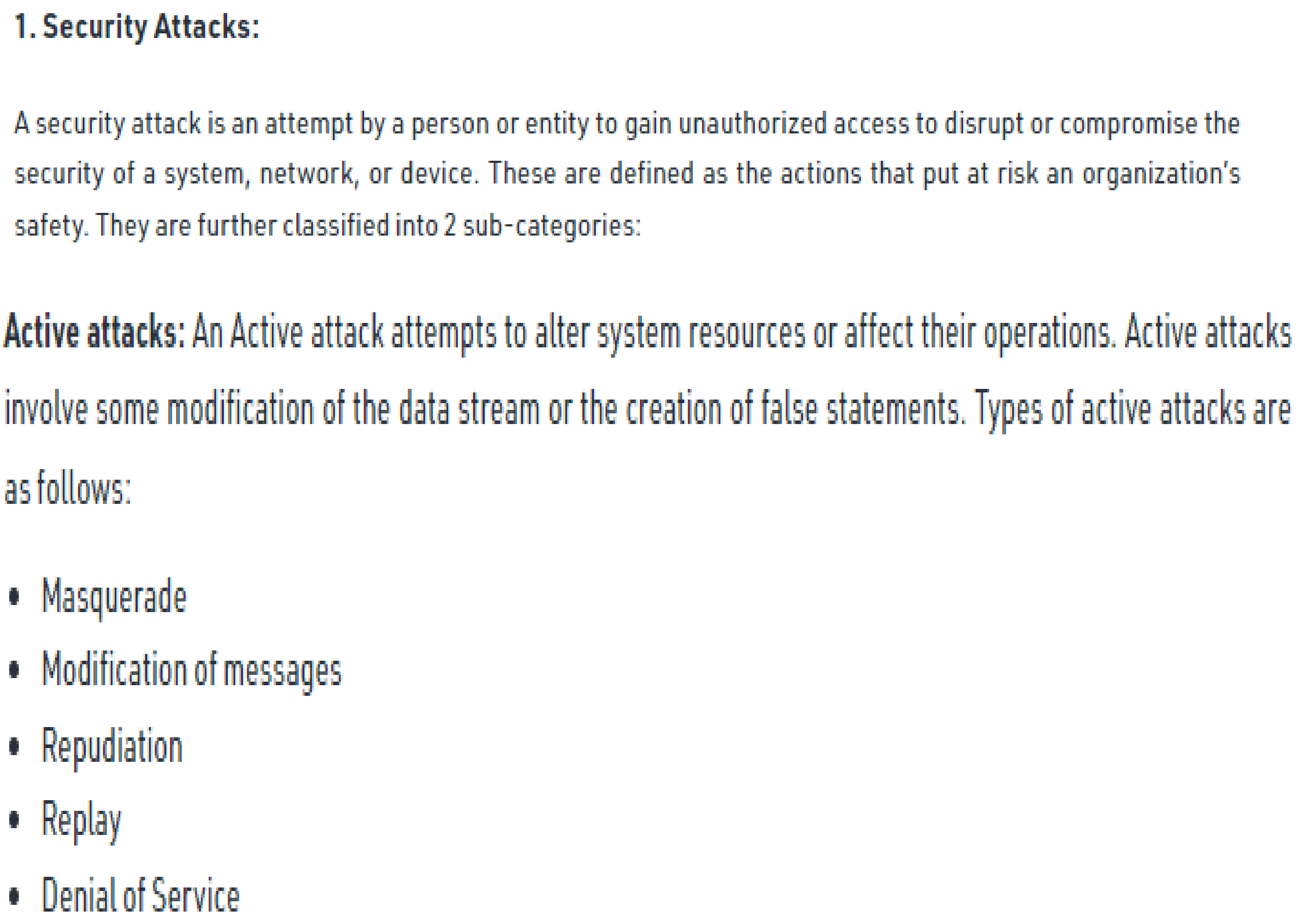
Classification of OSI Security Architecture



Classification of OSI Security Architecture

Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information.
- **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 data processing systems and information transfers. A security service makes use of one or more security mechanisms.



1. Security Attacks:

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety. They are further classified into 2 sub-categories:

Active attacks: An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements. Types of active attacks are as follows:

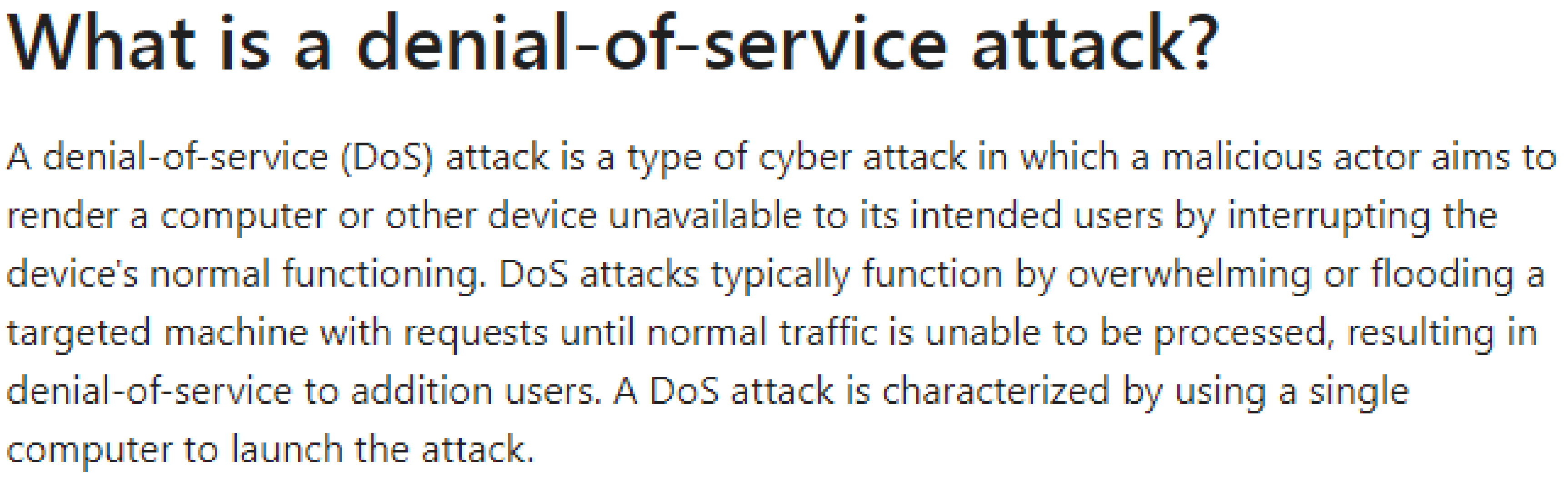
- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

- **Masquerade attack** refers to **an attack that uses a fake identity, to gain unauthorized access to personal computer information through legitimate access identification**.

- In a **message modification attack**, **an intruder alters packet header addresses to direct a message to a different destination or to modify the data on a target machine**. Message modification attacks are commonly email-based attacks.

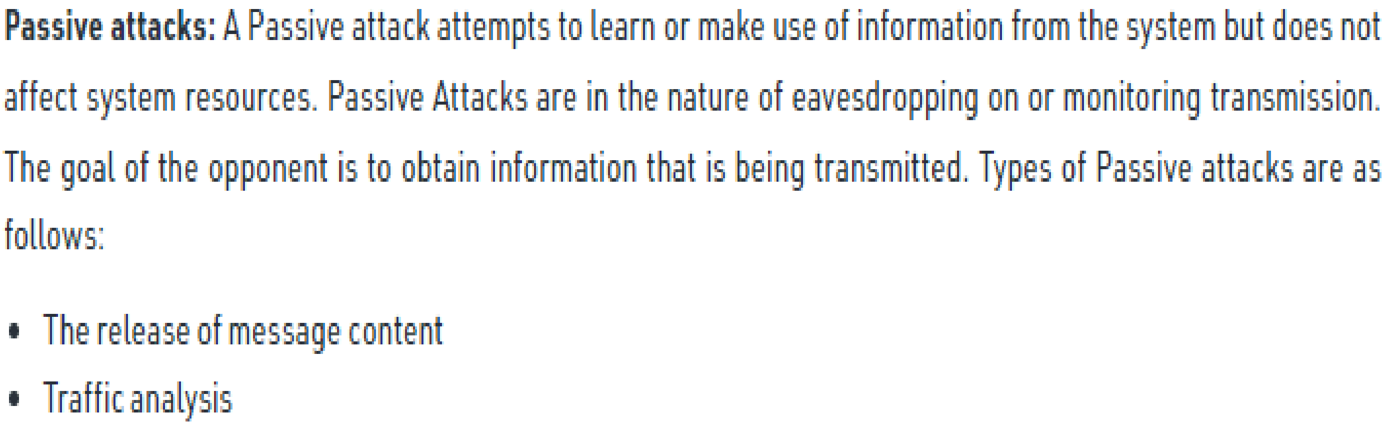
- A **repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions**, thus permitting malicious manipulation or forging the identification of new actions.

- A **replay attack** that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.



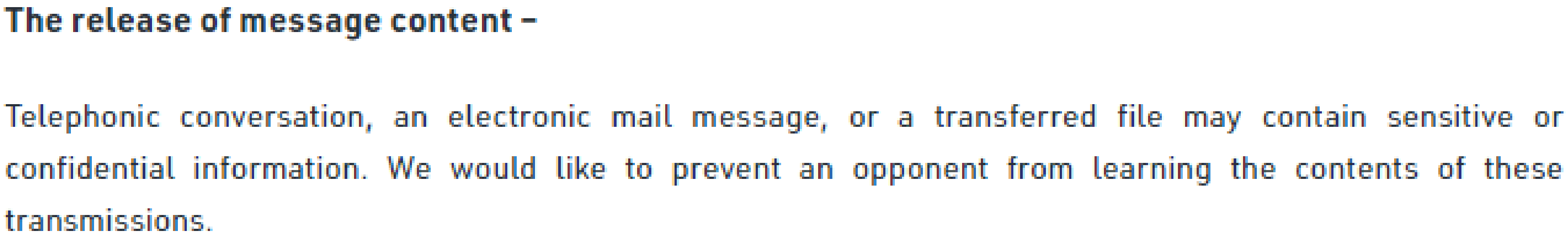
What is a denial-of-service attack?

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.



Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as follows:

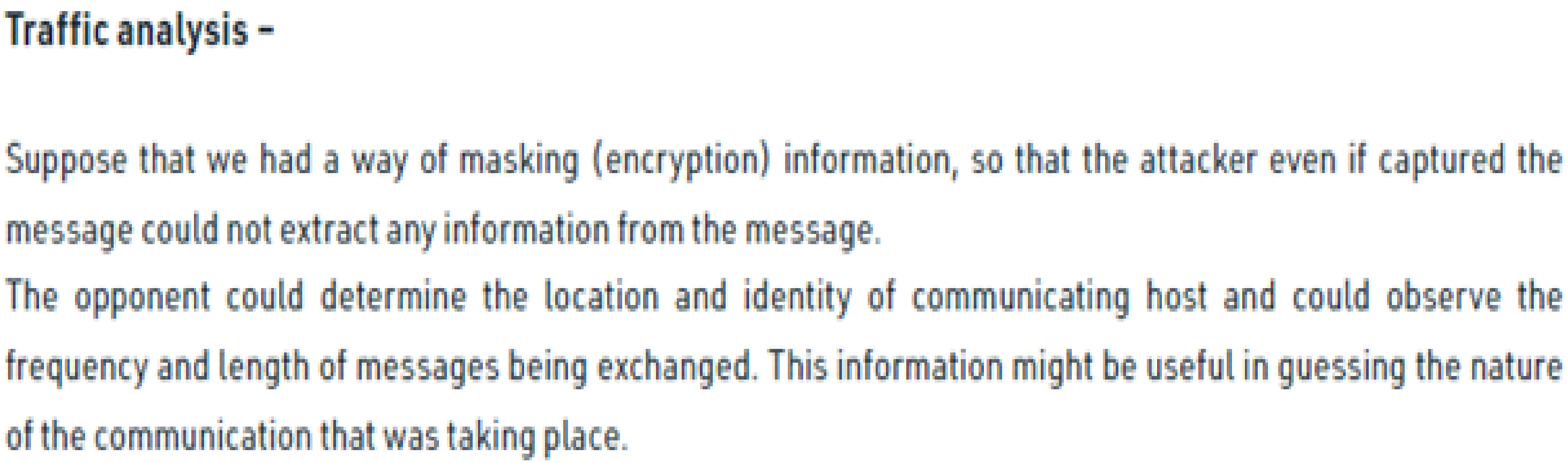
- The release of message content
- Traffic analysis



The release of message content –

Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

The release of message contents is **a type of attack that analyzes and read the message delivered between senders to receiver.**

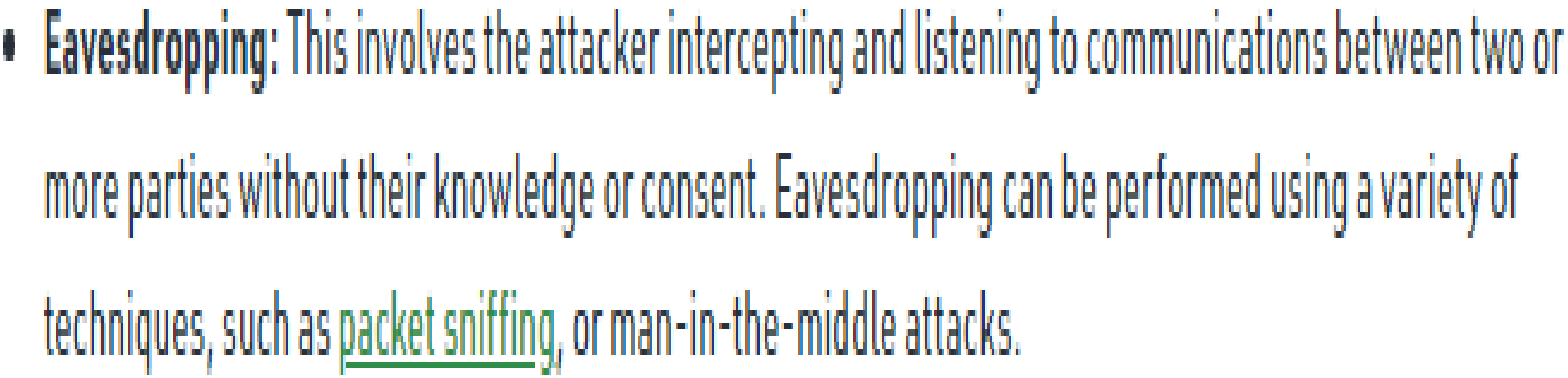


Traffic analysis -

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

The traffic analysis attacker simply listens to the network communication to perform traffic analysis to determine the location of key nodes, the routing structure, and even application behavior patterns



- **Eavesdropping:** This involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.

Eavesdropping attacks in the cyber security world are **when the perpetrator “listens” to and records data that is transmitted between two devices**. In simple terms, the hacker reads messages sent via, for example, an open and unsecured network.

2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats. Security mechanisms can be implemented at various levels within a system or network and can be used to provide different types of security, such as confidentiality, integrity, or availability.

Some examples of security mechanisms include:

- **Encipherment (Encryption)** involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.
- **Digital signature** is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

3. Security Services:

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Security mechanism

- **Encipherment** – This is **the procedure of using numerical algorithms to change data into a form that is not freely intelligible.**

- **Access control identifies users by verifying various login credentials, which can include usernames and passwords, PINs, biometric scans, and security tokens**.

- **Notarization** : **This security mechanism involves use of trusted third party in communication**. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

- **Data integrity** is **the overall accuracy, completeness, and consistency of data**.

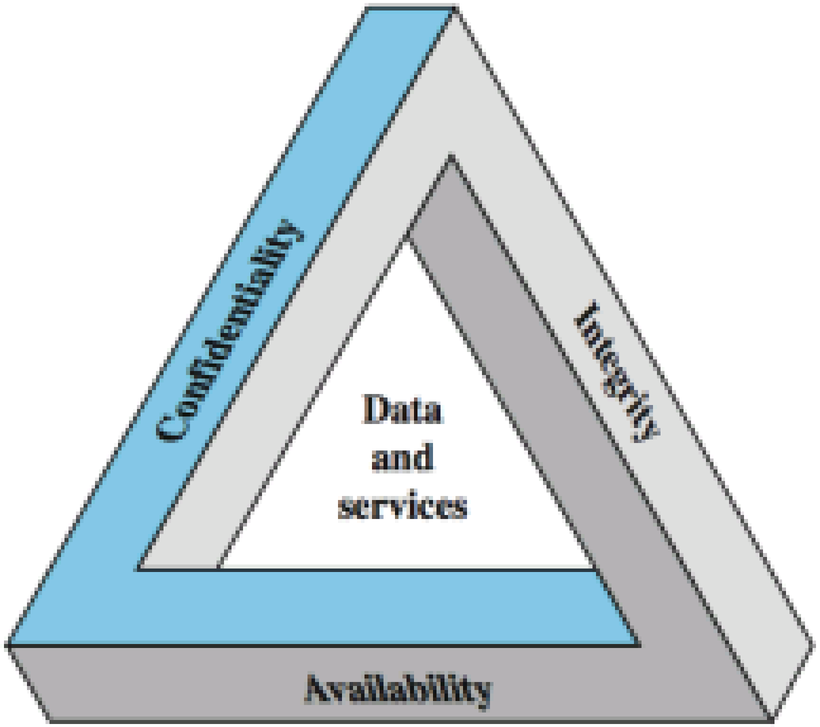
- **Authentication Exchange** − This is **a structure intended to provide the integrity of an entity by means of information exchange**.
- Traffic Padding − The insertion of bits into gaps in an information flow is known as traffic padding.

- **Bit stuffing** is a security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

- A digital signature is **an electronic, encrypted, stamp of authentication on digital information such as email messages or electronic documents**. A signature confirms that the information originated from the signer and has not been altered.

The **CIA Triad**

- **The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems.**


Confidentiality
Integrity
Data and services
Availability