Introduction

Table of Contents

[CIA Triad 2](#_Toc133106199)

[Security Attacks 2](#_Toc133106200)

[Security Services 4](#_Toc133106201)

[Security Mechanisms 5](#_Toc133106202)

[Security Techniques 6](#_Toc133106203)

## CIA Triad

The **CIA Triad** refers to the three fundamental security goals that must be achieved to keep information secure:

* **Confidentiality** – This applies to the storage and transmission of information. The information must be concealed from those who are unauthorized from accessing it.
* **Integrity** – Unauthorized changes to the information at any point of time must be prevented.
* **Availability** – The information must be accessible to authorized entities whenever they want.

## Security Attacks

**Security Attacks** can be divided into two forms depending on whether we are looking at them from the perspective of the security goals or from the perspective of their effect on the system.

When looking at the attacks from the perspective of the **security goals**, we have separate types of attacks that affect each of the goals.

**Confidentiality** is affected by attacks such as:

* **Snooping** which refers to the unauthorized interception of data while it is in transit, e.g., packet sniffing
* **Traffic Analysis** which is a little more roundabout, such as IP tracing, where the routes taken by packets are analyzed to determine the activity of a user

**Integrity** is threatened by:

* **Modification**, which simply means that the data was modified
* **Masquerading**, also called spoofing, which refers to situations where the attacker sends some data to a receiver pretending to be the sender
* **Replaying**, where a legitimate message is intercepted and is sent again later on
* **Repudiation**, where the sender or receiver denies having sent or receiver a particular message

**Availability** is threatened by **Denial of Service** (DOS) attacks, where a user sends repeated requests to a server with the explicit intent of overloading it and making it crash. It can also take other forms, such as intercepting messages from real clients and sending them repeatedly to the server (which makes use of replaying), or even just intercepting the server’s responses to clients, making clients believe the server is down.

Based on their **effect on the system**, security attacks can be of two types, passive and active. **Passive attacks** do not directly harm the system. They simply gain access to information they should not be able to. This might end up harming the client, but regardless, the system is unaffected. The confidentiality attacks are passive attacks. **Active attacks** harm the system or clients. The integrity and availability attacks are active attacks. These tend to be easier to detect than to prevent, simply because there are so many ways in which they can be done.

## Security Services

The **International Telecommunication Union-Telecommunication Standardization Sector** (ITU-T) has defined some services that deal with the security goals and preventing the attacks:

* **Data Confidentiality** – This deals with preventing unauthorized access to data. It includes prevention of both snooping and traffic analysis.
* **Data Integrity** – This includes anti-change and anti-replay mechanisms.
* **Authentication** – This includes peer-entity authentication (verifying both sender and receiver) in the case of connection-oriented communication and data origin authentication (only verifying the sender) in the case of connectionless communication.
* **Non-Repudiation** – This service provides proof of origin to the receiver, so that the sender cannot deny sending the data, as well as proof of delivery to the sender, so that the receiver cannot deny receiving the data.
* **Access Control** – This service prevents unauthorized access to data.

## Security Mechanisms

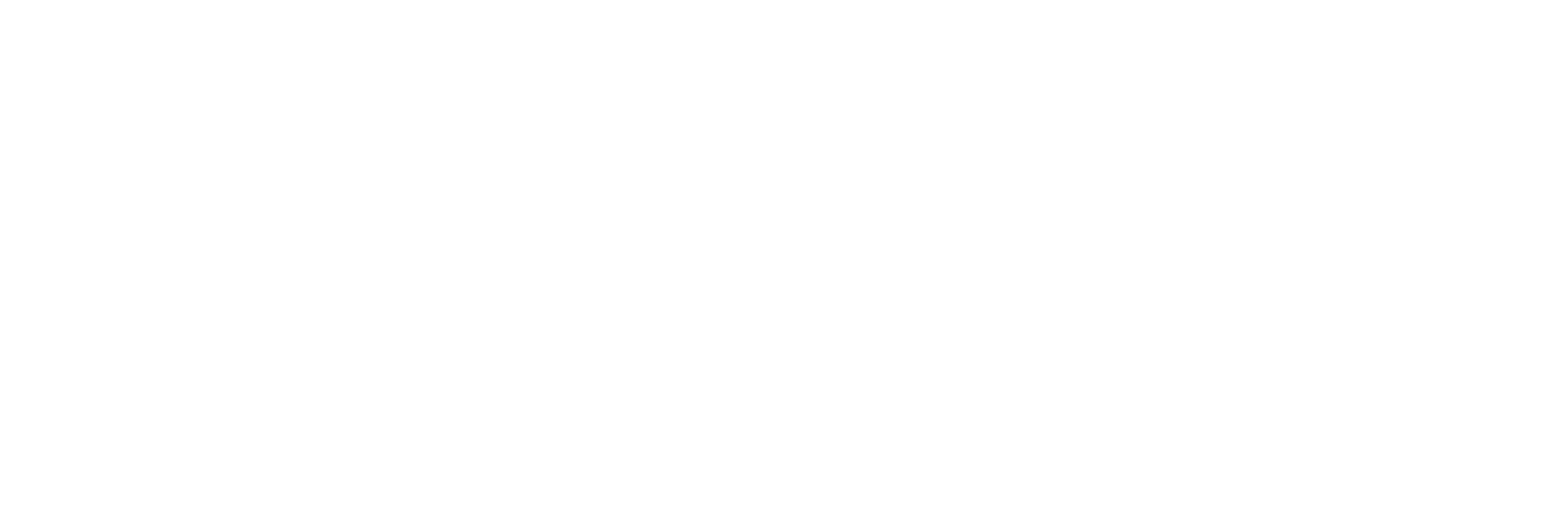
The security services are provided by a variety of **security mechanisms**. Each mechanism may server one or more security services.

* **Encipherment** – The data is hidden using cryptography or steganography.
* **Data Integrity** – A checksum is created by the sender and sent along with the data. The receiver recalculates the checksum from the data and verifies that the values match to be assured that the data was unchanged in transit.
* **Digital Signature** – The sender signs the data with a private key. The public key of the sender is used by the receiver to verify that the data is genuinely signed by that sender.
* **Authentication Exchange** – The two parties exchange some information to prove their identities, e.g., some secret that only that party should know.
* **Traffic Padding** – Random data is inserted into data traffic to thwart traffic analysis.
* **Routing Control** – Data is transmitted through a variety of routes, changing the route being used frequently, thus preventing snooping on a specific route.
* **Notarization** – A third party controls the communication between two parties to prevent repudiation.
* **Access Control** – Methods are used to verify that a client has the right to access some data, such as a password.

|  |  |
| --- | --- |
| **Security Mechanism** | **Security Service** |
| Encipherment | Data Confidentiality, Data Integrity, Authentication |
| Data Integrity | Data Integrity, Non-Repudiation |
| Digital Signature | Data Integrity, Authentication, Non-Repudiation |
| Authentication Exchange | Authentication |
| Traffic Padding | - |
| Routing Control | Data Confidentiality |
| Notarization | Non-Repudiation |
| Access Control | Access Control |

## Security Techniques

Security goals are implemented with two techniques, cryptography and steganography.



**Cryptography** transformers the message to make it more secure and immune to attacks. It is of three types:

* **Symmetric key encipherment**, which uses a single key to encrypt and decrypt the message.
* **Asymmetric key encipherment**, which uses one key to encrypt the message and a different one to decrypt it.
* **Hashing**, which creates a much smaller, fixed length digest. This can be used to verify that the message is unchanged.

**Steganography** refers to covered writing, meaning the message is hidden but not encrypted. Historically it was used as:

* War messages being written on silk and rolled into small balls to be swallowed by the messenger
* Messages carved into wood and covered in wax
* Messages written in invisible inks which could be exposed by heating the paper.

Modern uses include:

* Text cover, where single spaces and double spaces are placed between words in some random text to represent 0s and 1s and hide the true message



* Image Cover, where the last bit of the pixel values of an image is set as 0 or 1 to send the message secretly. The image itself does not noticeable change. This method is called Least Significant Bit (LSB).

|  |  |  |
| --- | --- | --- |
| 0101001**1** | 1011110**0** | 0101010**1** |
| 0101111**0** | 1011110**0** | 0110010**1** |
| 0111111**0** | 0100101**0** | 0001010**1** |

* Other covers, including covering under audio or video or even embedding the data during compression.