Cryptography and Network Security Principles

Muaaz Shoaib
Fa20-BCS-074

Agenda

- Cryptography Introduction
- Two types of attacks in cryptography
- The Principles of Security

Cryptography Introduction

- Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries.
- Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary.
- In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

Two types of attacks in cryptography

- Passive attacks are those that retrieve information from the system without affecting the system resources.
- Active attacks are those that retrieve system information and make changes to the system resources and their operations.

The Principles of Security are:

- Confidentiality
- Authentication
- Integrity
- Non-Repudiation
- Access control
- Availability
- Issues of ethics and law

Confidentiality

- The degree of confidentiality determines the secrecy of the information.
- The principle specifies that only the sender and receiver will be able to access the information shared between them.
- Confidentiality compromises if an unauthorized person is able to access a message.

Authentication

- Authentication is the mechanism to identify the user or system or the entity.
- It ensures the identity of the person trying to access the information.
- The authentication is mostly secured by using username and password.
- The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

Integrity

- Integrity gives the assurance that the information received is exact and accurate.
- If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

Non-Repudiation

- Non-repudiation is a mechanism that prevents the denial of the message content sent through a network.
- In some cases, the sender sends the message and later denies it.
- But the non-repudiation does not allow the sender to refuse the receiver.

Access control

- The principle of access control is determined by role management and rule management.
- Role management determines who should access the data while rule management determines up to what extent one can access the data.
- The information displayed is dependent on the person who is accessing it.

Availability

- The principle of availability states that the resources will be available to always authorize party.
- Information will not be useful if it is not available to be accessed.
- Systems should have sufficient availability of information to satisfy the user request.

Issues of ethics and law

- The following categories are used to categorize ethical dilemmas in the security system.
- Individuals' right to access personal information is referred to as privacy.
- Property: It is concerned with the information's owner.
- Accessibility is concerned with an organization's right to collect information.
- Accuracy: It is concerned with the obligation of information authenticity, fidelity, and accuracy.

Thank You

- If you have any questions, please ask.