Security Attacks

Security Objectives (Torra, 2018)

- The identification of security objectives is the first step you can take to help ensure the security of your application.
- **Security objectives** are goals and constraints that affect the confidentiality, integrity, and availability of your data and application.
- Although the use of the CIA triad to define security objectives is well established, many in the security field feel that additional concepts are needed to present a complete picture, as illustrated in *Figure 1.*

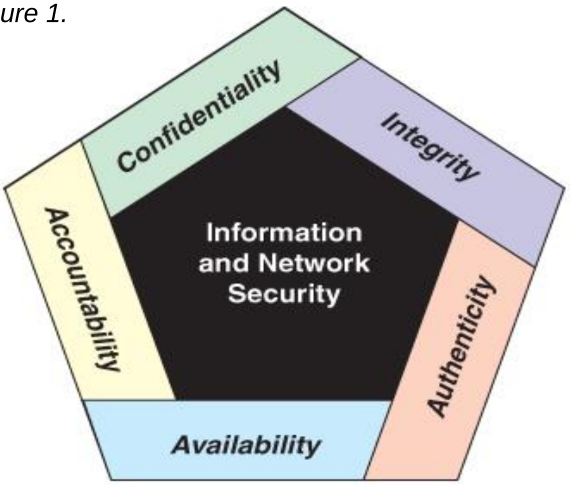


Figure 1. Security Objectives

- **Confidentiality:** Also known as data confidentiality, this property means that information is not made available or disclosed to unauthorized individuals, entities, or processes. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** This term covers two (2) related concepts:
    - **Data integrity** ensures that data (both stored and is transmitted packets) and programs are changed only in a specified and authorized manner. A loss of data integrity is the unauthorized modification or destruction of information.
    - **System integrity** ensures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability** ensures that systems work promptly and the service is not denied to authorized users. A loss of availability is the disruption of access to or use of information or an information system.
- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or a message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, it must be possible to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

OSI Security Architecture (Torra, 2018)

- The security architecture for Open Systems Interconnection (OSI) defines a general security architecture that is useful to managers as a way of organizing the task of providing security
- This standardized architecture defines security requirements. The key concepts that are covered in these sections are summarized in *Figures 2-3.*
    - **Security attacks** are any action that compromises the security of information owned by an organization.
    - Security attacks attempt to gain unauthorized access to information resources or services, or cause harm or damage to information systems.

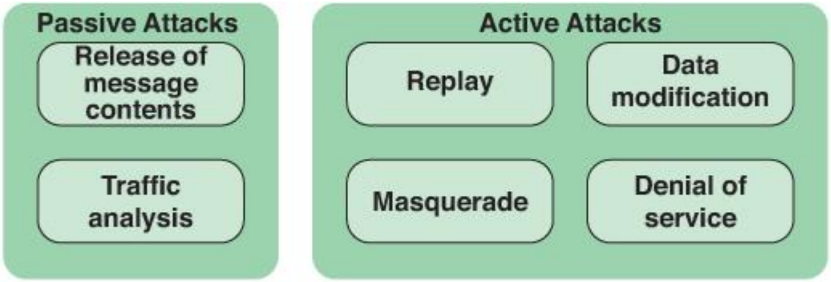


Figure 2. Attacks

- ○ **Security mechanisms** are technical tools and techniques that are used to implement security services
- ○ A process that is designed to detect, prevent, or recover from a security attack.
- ○ **Security service** is a processing or communication service that enhances the security of the data processing systems, and the information transfers of an organization. Security services are intended to counter security attacks, and they make use of security mechanisms to provide the services.

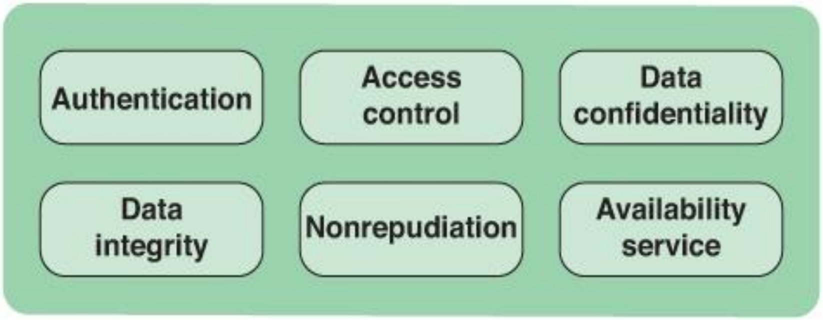


Figure 3. Services

Passive Attack (Torra, 2018)

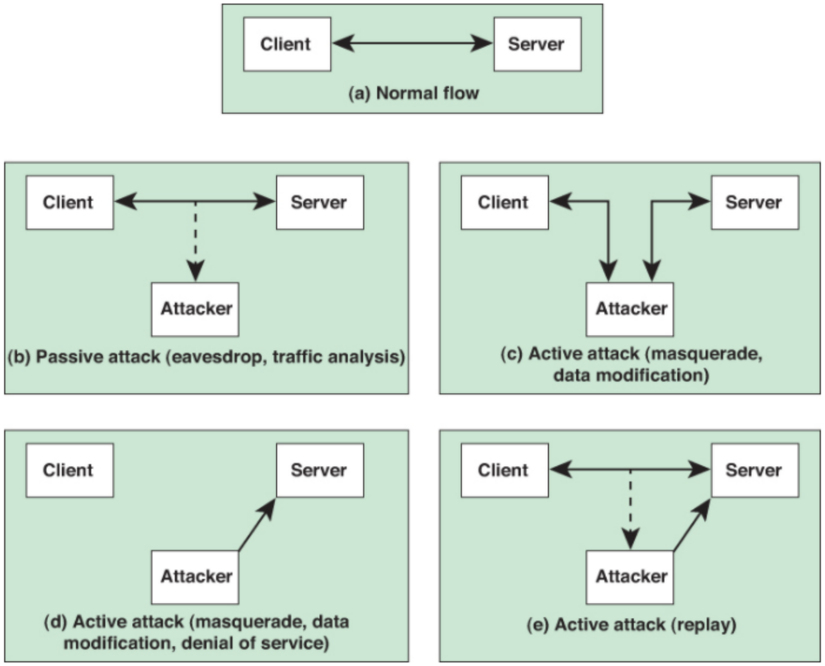
- **Passive attacks** are like eavesdropping or monitoring transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis:
  - ○ **Release of message contents:** In this type, an attacker will monitor an unprotected communication medium like unencrypted email or telephone call and intercept it for sensitive information.
  - ○ **Traffic analysis:** In this type, an attacker monitors communication channels to collect a range of information, including human and machine identities, locations of these identities, and types of encryption used, if applicable.
- Passive attacks are very difficult to detect because they do not involve any alteration of the data.
- The message traffic is sent and received in a normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern.
- The best way to prevent a passive attack is by using strong network encryption methods. This means that the original message should be well encrypted into an unintelligible language at the sender's end and should be decoded into an understandable language at the receiver's end.

Active Attack (Torra, 2018)

- **Active attacks** involve some modification of stored or transmitted data or the creation of false data. There are four categories of active attacks: replay, masquerade, modification of messages, and denial of service.
  - ○ A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
  - ○ **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
  - ○ **Data modification** simply means that some portion of a legitimate message is altered or that messages are delayed or reordered to produce an unauthorized effect. For example, a message stating "Allow Kit Estrada to read confidential file,

Accounts" might be modified to say, "Allow Fred Brown to read confidential file, Accounts."

- A **denial-of-service attack** prevents or inhibits the normal use or management of communication facilities. Such an attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages to degrade performance.



(a) Normal flow

(b) Passive attack (eavesdrop, traffic analysis)

(c) Active attack (masquerade, data modification)

(d) Active attack (masquerade, data modification, denial of service)

(e) Active attack (replay)

Figure 4. Types of attacks in the context of a client/server interaction.

Security Services (Torra, 2018)

- **Authentication** service is concerned with ensuring that communication is authentic. In the case of a single message, such as a warning or an alarm signal, the function of the authentication service is to ensure the recipient that the message is from the source that it claims to be from.
- **Access control** is the ability to limit and control access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified or authenticated so that access rights can be tailored to the individual.
- **Data confidentiality** is the protection of transmitted data from passive attacks. Concerning the content of data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period. For example, when a logical network connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the connection.
- **Data integrity** ensures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays
- Data integrity ensures that information is modified only in appropriate ways by persons authorized to change it.
- **Nonrepudiation** prevents either a sender or a receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver received the message.
- **Availability service** means that a system or a system resource is accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; that is, a system is available if it provides services according to the system design whenever users request them.

References:

Kumar, G., Saini, DK., Huy Cuong, NH. (2020). *Cyber defense mechanisms: Security, privacy, and challenges.* CRC Press.
Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technologies, and regulations.* Assison-Wesley Professional. Torra, V. (2018). *Data privacy: foundations, new developments, and the big data challenge.* Springer International Publishing.