CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Information Security

Module:

- Introduction to Information Security
    - By the end of this module you will be able to:
        - Differentiate between Confidentiality, Integrity, and Availability
        - Understand technical areas that must underpin any effective security strategy
        - Differentiate between threats, attacks and assets

The NIST Internal/Interagency Report NISTIR 7298 defines the term *computer security* as follows:

“ Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.”

NIST: National Institute of Standards and Technology (www.nist.gov)

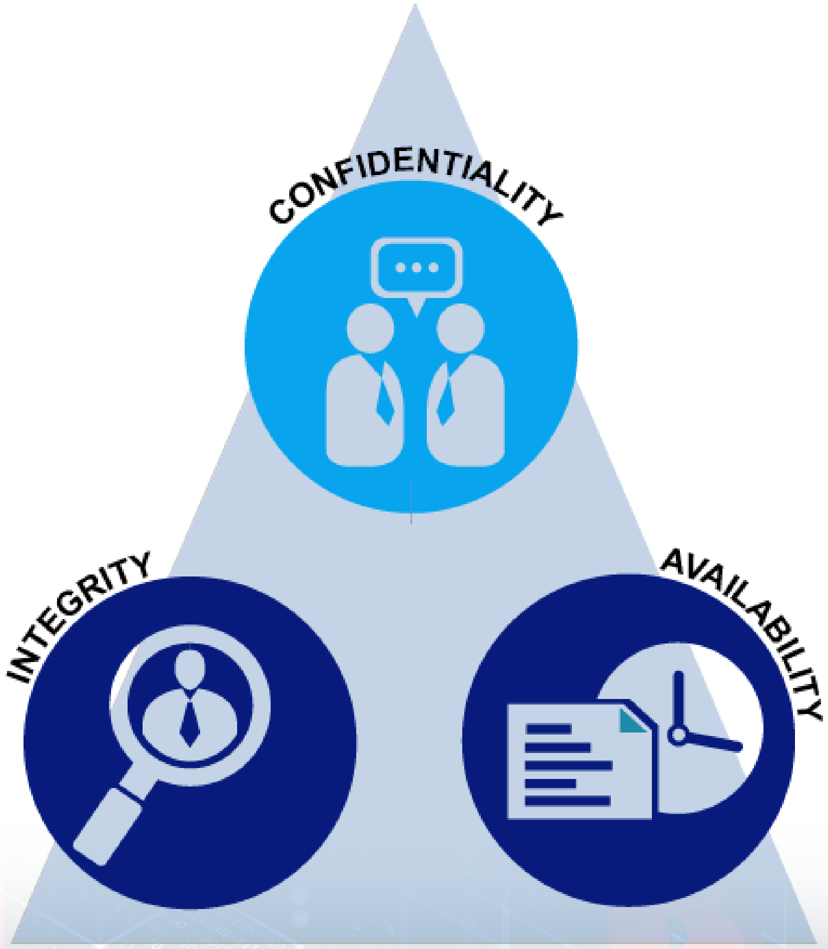
Key Security Objectives

- Confidentiality
  - Data confidentiality: assure confidential information not made available to unauthorized individuals
  - Privacy: assure individuals can control what information related to them is collected, stored, distributed

- Integrity
  - Data integrity: assure information and programs are changed only in a authorized manner
  - System integrity: assure system performs intended function

- Availability
  - Assure that systems work promptly and service is not denied to authorized users

CIA Triad



Extended CIA Triad

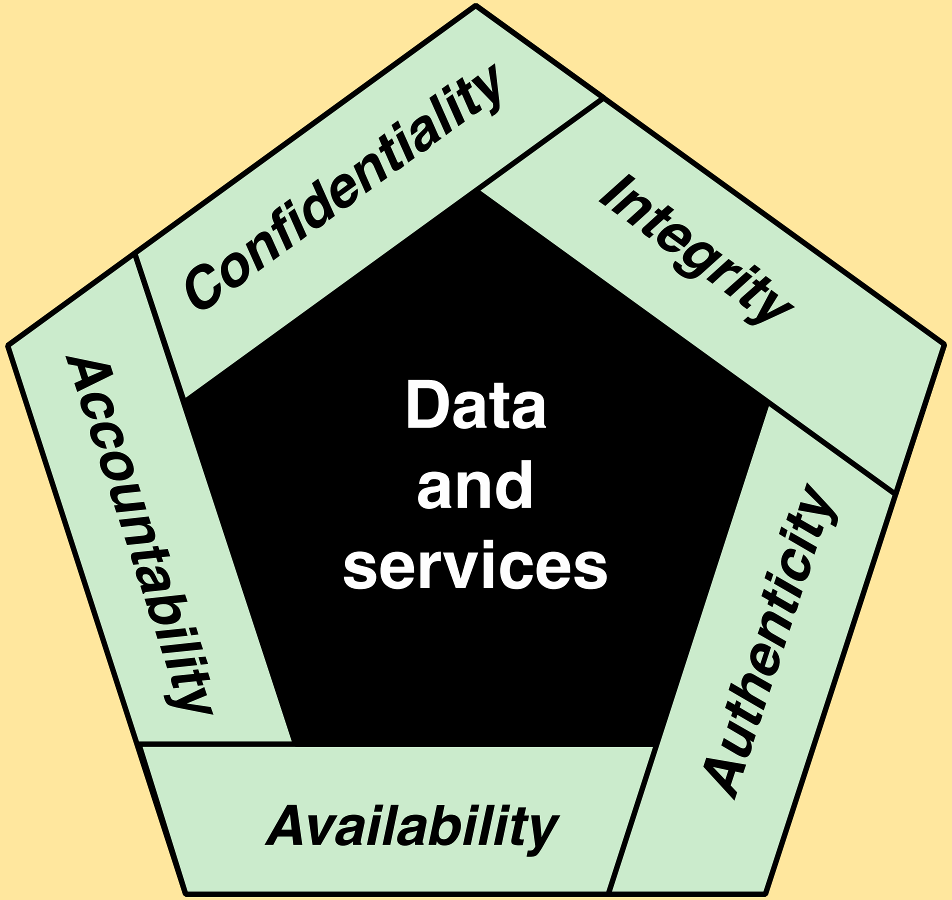


Figure 1.1 Essential Network and Computer Security Requirements

Extended CIA Triad

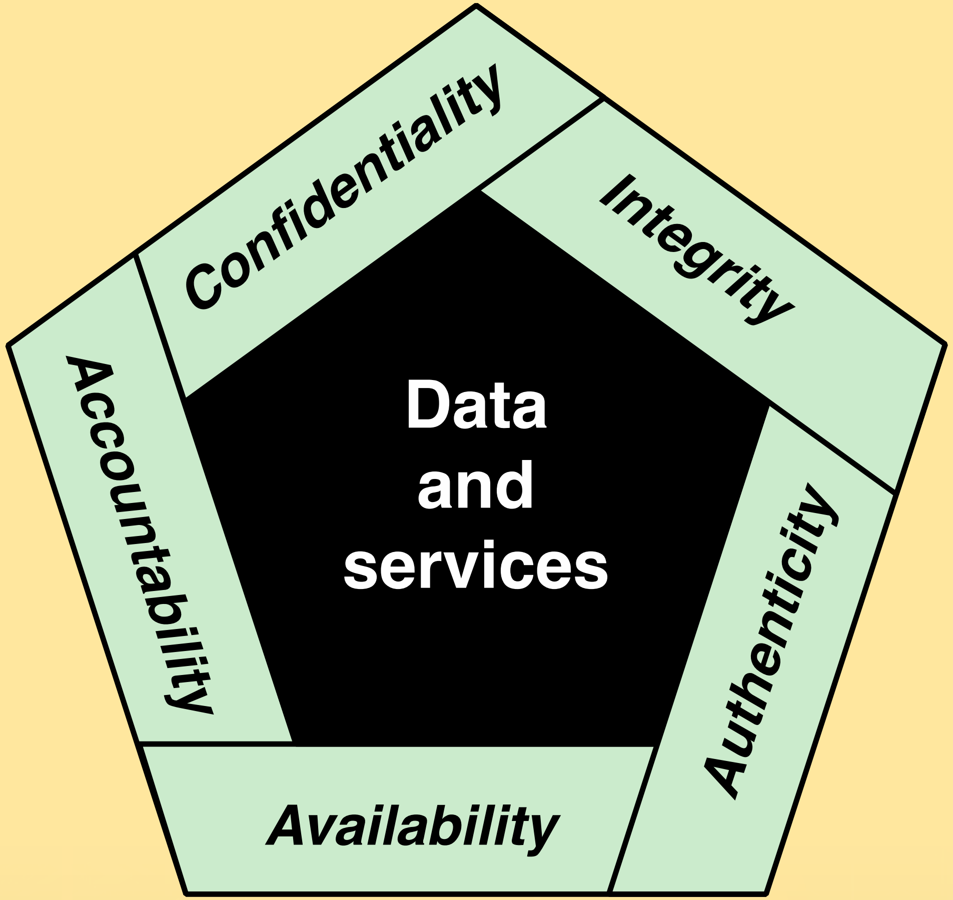


Figure 1.1 Essential Network and Computer Security Requirements

Extended CIA Triad

- Authenticity
  - Users and system inputs are genuine and can be verified and trusted
    - Data authentication
    - Source authentication

- Accountability
  - Actions of an entity can be traced uniquely to that entity
    - Supports: non-repudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery

Key Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

Levels of Impact

- We use three levels of impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

- These levels are defined in FIPS 199:
  - Low
  - Moderate
  - High

FIPS: Federal Information Processing Standards (part of NIST)

Levels of Impact

Low

The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

High

The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Computer Security Challenges

1. Computer security is not as simple as it might first appear to the novice

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features

3. Procedures used to provide particular services are often counterintuitive

4. Physical and logical placement of security mechanisms needs to be determined

5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information

6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security

7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process

8. Security requires regular and constant monitoring

9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

10. Many users and even security administrators view strong security as an obstacle to efficient and user-friendly operation of an information system or use of information

Module:

- Introduction to Information Security
  - By the end of this module you will be able to:
    - Differentiate between Confidentiality, Integrity, and Availability
    - Understand technical areas that must underpin any effective security strategy
    - Differentiate between threats, attacks and assets