

# Introduction and Basic Concepts

System Security (CM0625, CM0631) 2026-27  
Università Ca' Foscari Venezia

Riccardo Focardi

<https://www.unive.it/people/focardi>  
[segroup.dais.unive.it](https://segroup.dais.unive.it)



Università  
Ca' Foscari  
Venezia

# Course Overview

# Objectives

System Security  
(CM0625, CM0631)

<https://www.unive.it/data/course/733828/programma>

This course aims at providing:

- basic **concepts** and **techniques** for the development of secure systems
- **skills** and **tools** for evaluating and increasing the security of applications, systems and devices

# Programme

System Security  
(CM0625, CM0631)

<https://www.unive.it/data/course/733828/programma>

- **Build secure foundations:** Design principles and cryptography
- **Manage identities and permissions:** Authentication and access control
- **Understand and detect attacks:** Malware, DoS, intrusion detection
- **Protect code and data:** Software and database security
- **Secure the platform:** OS security and trusted computing
- **Analyze security mechanisms:** Security APIs and formal methods
- **Uncover hidden leaks:** Side-channel attacks

*Hands-on labs and security challenges*

# Material

System Security  
(CM0625, CM0631)

<https://www.unive.it/data/course/733828/programma>

- **Book:** William Stallings, Lawrie Brown. *Computer Security Principles and Practice (Fourth Edition)*. Pearson Edu. 2018
- *Blended* course of the Ca' Foscari e-learning program:
  - traditional classroom
  - on-line classes
  - hands-on challenges
- **Slides** and extra material are available in moodle

# Assessment

System Security  
(CM0625, CM0631)

<https://www.unive.it/data/course/733828/programma>

- **Written test** (base mark)
- Non-mandatory **assignments** (extra score)
  - *Challenges* on attacking and securing IT systems and applications
  - Bonus score with respect to the the mark of the written test

# Basic Concepts

# Why is Computer Security so relevant?

Information systems are **pervasive** and extremely **connected**.

## Examples:

- IoT
- Industry 4.0
- Critical infrastructures
- Government services
- Financial services (e.g. Banks)
- ...

Attacking information systems is more and more **harmful**!

# What is Computer Security?

The National Institute of Standards and Technology (NIST) defines **Computer Security** as:

*“Measures and controls that ensure **confidentiality, integrity, and availability** of the **information** processed, stored (and communicated) by a computer”*

The so-called “CIA” triad: Confidentiality, Integrity, Availability

**NOTE:** information system assets including **hardware, software, firmware** are all involved.

Reference: [https://csrc.nist.gov/glossary/term/computer\\_security](https://csrc.nist.gov/glossary/term/computer_security)

# Confidentiality

## Definition:

1. **Data confidentiality:** confidential information is not disclosed to unauthorized individuals
2. **Privacy:** individuals control what information related to them may be collected and stored and by/to whom that information may be disclosed

## Examples:

- Sensitive data in a database
- On-line payments (e.g. by credit card)
- Personal privacy while browsing the Web

# Integrity

## Definition:

1. **Data integrity:** information and programs are changed only in a specified and authorized manner
2. **System integrity:** a system performs its intended function, free from unauthorized manipulation

## Examples:

- Bank accounts
- Bank transfers
- IoT device firmware should not be altered

# Availability

## Definition:

- Systems work promptly and services are not denied to authorized users

## Examples:

- Cloud services
- E-voting
- Electrical grids (Cyber-physical)
- Remote surgery (QoS)

# More properties: Authenticity

## Definition:

1. **Identification:** The possibility of correctly identifying an entity
2. **Message Authentication:**  
Confidence in the validity of a transmission, a message, or message originator/receiver

## Examples:

- User login
- ATM PINs
- Verified email messages (origin and destination)
- PEC (Posta Elettronica Certificata): message integrity and authenticity of sender/receiver emails

# More properties: Accountability

## Definition:

- The possibility of **tracing** an event to a unique entity
- ⇒ allows for tracing a **security breach** to a responsible party

## Examples:

- Digital signature
- Activity logs
- Forensic analysis

What happens when security  
is violated?

# Impact (cf. FIPS 199)

## Low

- i. effectiveness of primary functions is **noticeably** reduced
- ii. **minor** damage to organizational assets
- iii. **minor** financial loss
- iv. **minor** harm to individuals

## Medium

- i. effectiveness of primary functions is **significantly** reduced
- ii. **significant** damage to organizational assets
- iii. **significant** financial loss
- iv. **significant** harm to individuals

## High

- i. **unable** to perform one or more primary functions
- ii. **major** damage to organizational assets
- iii. **major** financial loss
- iv. **severe** or **catastrophic** harm to individuals (e.g. loss of life)

# Examples

Integrity of patient allergy information:

Inaccurate information could result in **severe harm or death** to a patient, and expose the hospital to massive liability

⇒ **high** requirement of **integrity**

Availability of a university website:

Not a critical component of the university's information system, but its unavailability would cause **significant troubles** to students and professors

⇒ **medium** requirement of **availability**

# Key security concepts

**Asset:** Anything valuable that needs protection: data, systems, equipment, or people

**Security Policy:** Rules defining allowed and required activities to protect assets

**Threat:** A circumstance or event that could harm an asset

**Vulnerability:** A weakness that can be exploited or triggered to cause harm

**Adversary (threat agent):** An individual or group that carries out harmful activities

**Attack:** A threat deliberately put into action, often by exploiting a vulnerability

**Countermeasure:** A tool, technique, or procedure that reduces the likelihood or impact of an attack

**Risk:** A measure of potential harm, based on its likelihood and impact

# Classifying Attacks: What Effect? Where From?

What does the attack do?

**Passive attack:** Observes or collects information without altering resources.

**Active attack:** Alters resources or disrupts operations

Where does the attack originate?

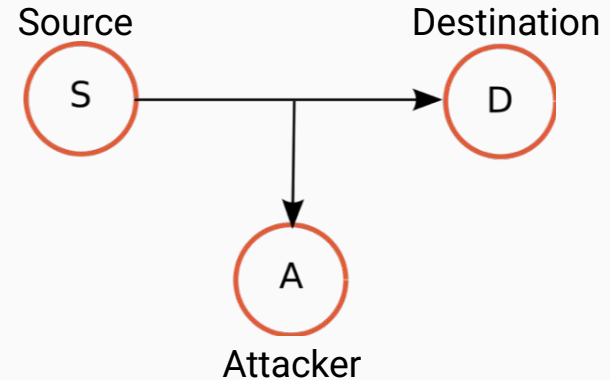
**Outside attack:** Originates outside the security perimeter, often attempting to bypass access restrictions

**Inside attack:** Originates within the security perimeter, often abusing trusted access or privileges

# Example 1: Interception

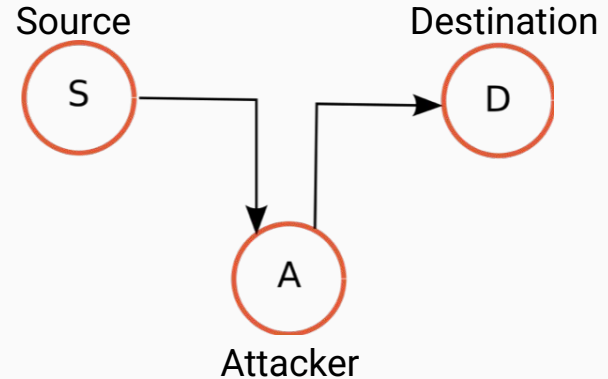
- Attacker gets **unauthorized access** to information
- Breaks **data confidentiality**
- **Passive attack**
- **Example:**
  - S sends a credit card number to D “in the clear”

⇒ Threat consequence:  
*Unauthorized disclosure*



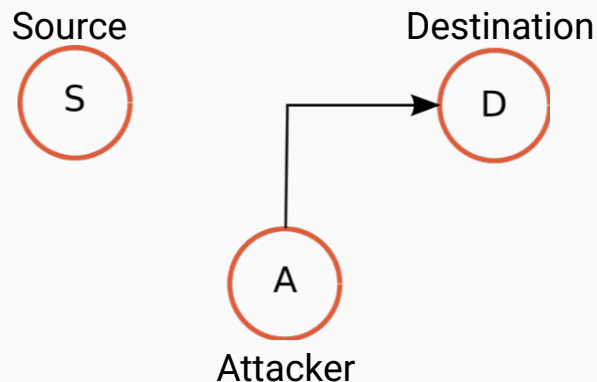
# Example 2: Modification

- Attacker **maliciously modifies** information
- Breaks **integrity** and possibly **authenticity, accountability**.
- **Active attack**
- **Example:**
  - A redirects S bank transfer to herself
  - NOTE: A can be either in the browser or on the network (Man-in-the-middle)



# Example 3: Falsification

- Attacker forges new information
- Breaks **authenticity**, **accountability** and **integrity**
- **Active attack**
- **Example:**
  - Forging a signature through a crypto vulnerability (e.g. MD5 collisions)
  - Credential theft



# Example 4: Interruption

- Attacker interrupts a service
- Breaks **availability**
- **Active attack**
- **Examples:**
  - DoS on E-Voting
  - DoS on power grid

