# Cybersecurity Management
# GCS-0.1.Cybersecurity Overview

2022-2023

Prof. Raül Roca

raul.roca-canovas@upc.edu

linkedin.com/in/roca-cybersecurity

# Contents

- Overview of computer security
- Computer Security Concepts
- Threat Consequences and Actions
- Standards & Organizations
- References

# Computer Security Concepts

# A Definition of Computer Security

- *The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms, May 2013*
  - **Measures and controls**
    - Objectives → Confidentiality, integrity, and availability (CIA)
    - Information system assets (HW,SW, firmware, and digital information)

- **Cybersecurity** = **Computer security**

National Institute of Standards and Technology

# Information Security vs. Cybersecurity

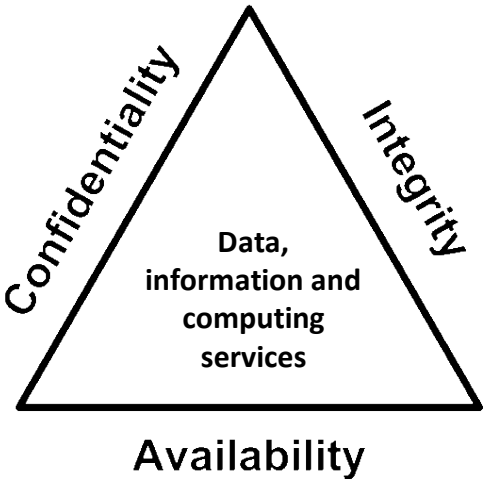
- **Information Security**
  - Protects **information**, regardless of its format
    - *Paper documents, digital and intellectual property in people's minds, and verbal or visual communications.*
  - Includes natural hazards, personal mistakes or physical security
- **Cybersecurity**
  - Protects **digital assets** in **cyberspace**
    - *Network HW, SW and information (processed, stored or transported by internetworked information environments).*
  - Is a part of information security.
  - Does not include natural hazards, personal mistakes or physical security.
  - Component: offensive and adverse human behavioral

A Definition of Computer Security

# Security objectives (FIPS199) → CIA

The **NIST FIPS 199** lists CIA as the 3 security **objectives** for I and IS:

- **Confidentiality** (vs. Unauthorized disclosure)
- **Integrity** (vs. Unauthorized modification or destruction)
- **Availability** (vs. Disruption of access to or use )




*NIST standard FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems, February 2004)*

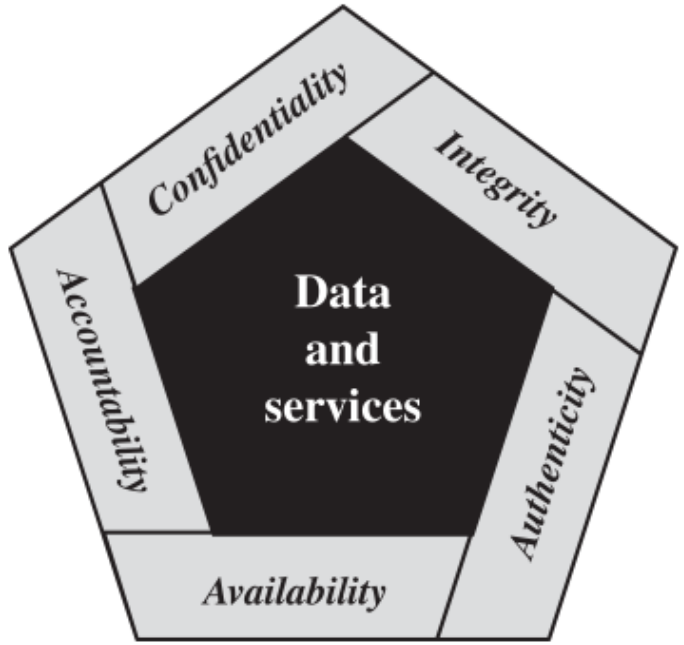
# A Definition of Computer Security
# CIA Triad → related concepts

- **Confidentiality**
  - Data confidentiality
  - Privacy

- **Integrity**
  - Data integrity
  - System integrity

# A Definition of Computer Security
# Essential Security Requirements

- **Authenticity**
  - genuine
  - verified and trusted
  - confidence in the validity of a transmission
- **Accountability**
  - requirement for actions of an entity
  - traced uniquely to that entity

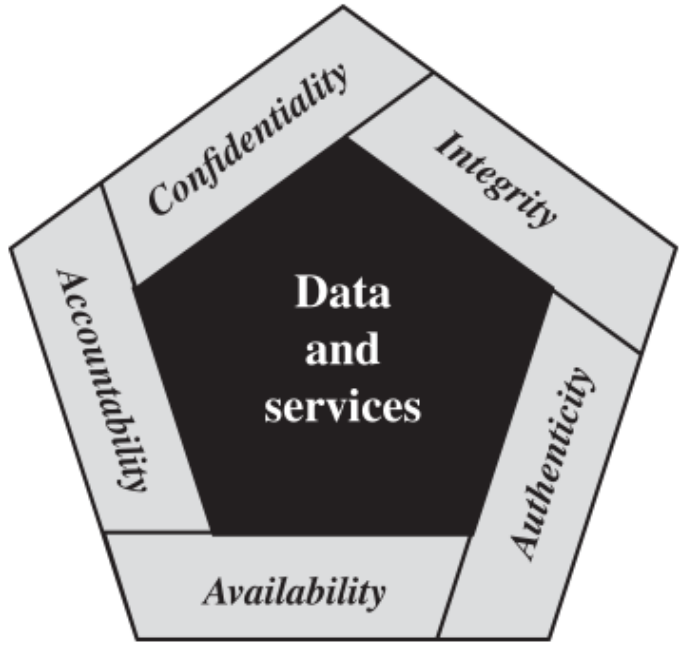



*Note that FIPS 199 includes authenticity under integrity*

# A Definition of Computer Security
# Essential Security Requirements

*In other words,…*

- **Authenticity**
  - This means verifying!
- **Accountability**
  - This means we must be able to trace!




*Note that FIPS 199 includes authenticity under integrity*

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

| | | | |
|---|---|---|---|
| Adversary (threat agent) | Attack | Countermeasure | Risk |
| Security Policy | System Resource (Asset) | Threat | Vulnerability |

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

**Adversary (threat agent)**

- Individual, group, organization, or government
- conducts or has the intent to conduct
  - detrimental or malicious activities

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

## Attack

- malicious activity
  - attempts to
    - collect, disrupt, deny, degrade, or destroy
    - information system resources or the information itself

A Model for Computer Security

# Computer Security Terminology

## Asset (system resource)

- **Hardware**
  - Including computer systems and other data processing, data storage, and data communications devices.
- **Software**
  - Including the operating system, system utilities, and applications.
- **Data**
  - Including files and databases, as well as security-related data, such as password files.
- **Communication facilities and networks**
  - Local and wide area network communication links, bridges, routers, and so on.

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

## Countermeasure

- Device or techniques with the objective
  - weakening → operational effectiveness of adversarial activity
  - prevention of
    - espionage, sabotage, theft, or unauthorized access to or use of
      - sensitive information
      - information systems

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

## Risk

- Measure of  degree
  - get_degree (entity_threatened, circumstance_or_event);
- *Risk = Function (**impacts, likelihood** of occurrence)*

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

## Security Policy

- A set of criteria → provision of security services
- defines & **constrains** → activities of a data processing facility
  - Objective: Maintain a condition of security for **systems and data**

A Model for Computer Security

# Computer Security Terminology (RFC 2828)

## Threat

- Any circumstance or event with the potential to adversely impact
  - organizational operations & assets (mission, functions, image, or reputation)
  - Individuals
  - or the Nation
- through an information system via
  - unauthorized access, destruction, disclosure, modification of information, and/or DoS.

A Model for Computer Security

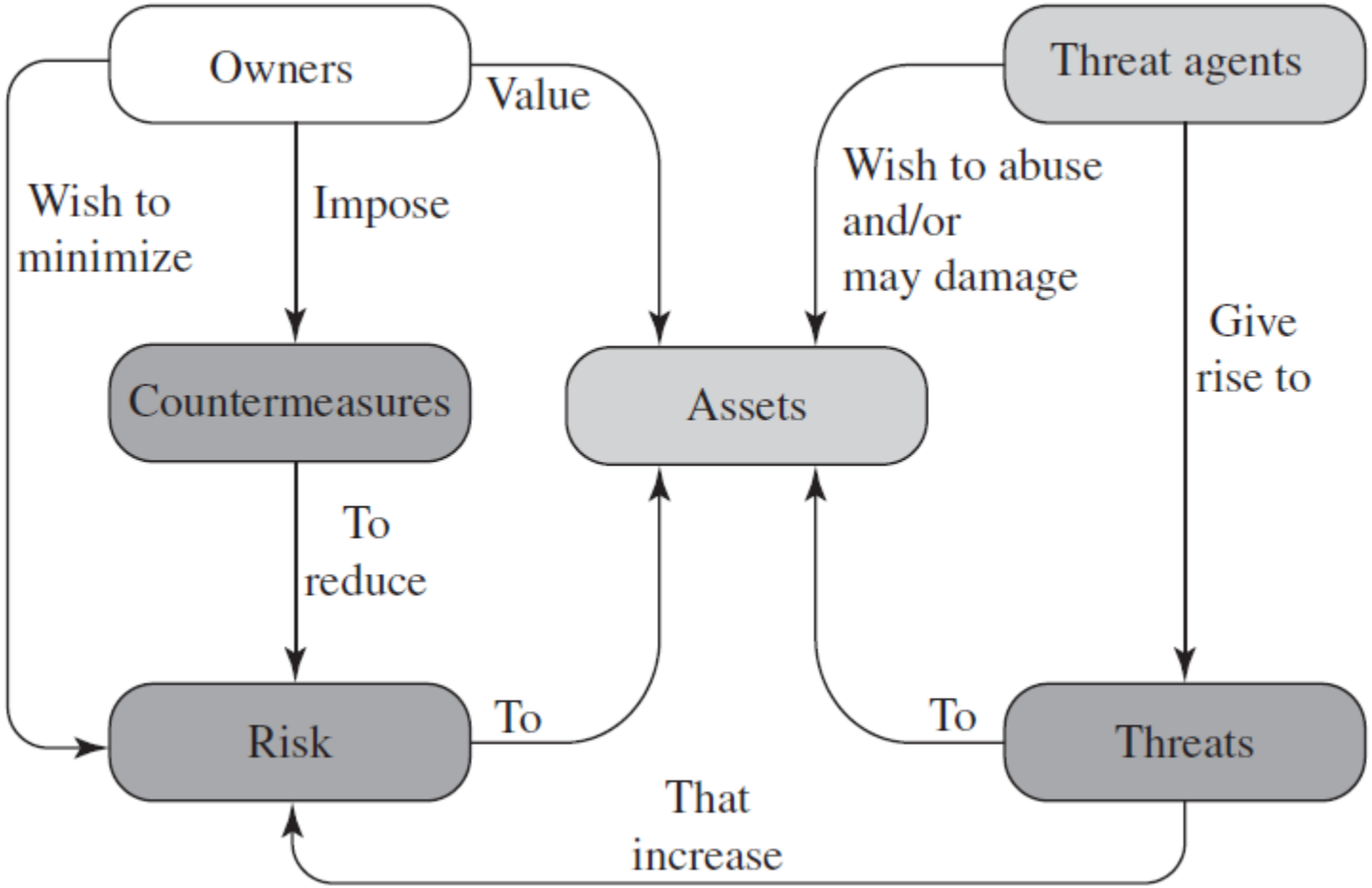
# Computer Security Terminology (RFC 2828)

## Vulnerability

- Weakness
  - in an
    - information system
    - system security procedures
    - internal controls, or implementation
  - that could be exploited or triggered by a threat source.

A Model for Computer Security

# Security Concepts and Relationships



# A Model for Computer Security
# Vulnerabilities, Threats and Attacks

- **Categories of vulnerabilities**
  - **Corrupted** (loss of integrity)
  - **Leaky** (loss of confidentiality)
  - **Unavailable** or very slow (loss of availability)

# A Model for Computer Security
# Vulnerabilities, Threats and Attacks

- **Threats**
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset

# A Model for Computer Security
# Vulnerabilities, Threats and Attacks

- **Attacks (threats carried out)**
  - **Based on action**
    - **Active** → attempt to alter system resources or affect their operation
    - **Passive** – attempt to learn or make use of information from the system that does not affect system resources
  - **Based on origin**
    - **Insider** → origin = security perimeter
    - **Outsider** → origin = outside the perimeter

# Threat Consequences and Actions

Threats, Attacks, and Assets

# Threat Consequences and Actions. RFC 4949

| Threat Action (Attack) | Threat Consequence | *A circumstance or event …* |
|---|---|---|
| Exposure<br>Interception<br>Inference<br>Intrusion | **Unauthorized Disclosure** | *… whereby an entity **gains access** to data for which the entity is **not authorized**.* |
| Masquerade<br>Falsification<br>Repudiation | **Deception** | *… that may result in an authorized entity **receiving false data** and believing it to be true.* |
| Incapacitation<br>Corruption<br>Obstruction | **Disruption** | *… that **interrupts or prevents** the correct operation of system services and functions.* |
| Misappropriation<br>Misuse | **Usurpation** | *… that results in **control** of system services or functions by an **unauthorized entity**.* |

# Standards & Organizations

Standards

# The most important organizations

- **National Institute of Standards and Technology (NIST)**
- **Internet Society (ISOC)**
- **International Telecommunication Union (ITU-T)**
- **International Organization for Standardization (ISO)**

Standards

# Significant Security Standards and Documents

**International Organization for Standardization (ISO)**

- ISO 27000 family of related standards.
- ISO 27002
- ISO 27032

Standards

# Significant Security Standards and Documents

**National Institute of Standards and Technology (NIST)**

- **FIPS PUB 200**
  - Minimum Security Requirements for Federal Information and Information Systems
- **NIST SP 800-100**
  - Information Security Handbook: A Guide for Managers
- **SP 800-55**
  - Security Metrics Guide for Information Technology Systems
- **SP 800-27**
  - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- **SP 800-53**
  - Recommended Security Controls for Federal Information Systems

***Federal Information Processing Standards Publications** (**FIPS PUBs**) and **special publications (SPs)***

Standards

# Significant Security Standards and Documents

**International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)**

- **Recommendation X.800 Recommendation**
  - Security Architecture for Open Systems Interconnection
  - Provides a detailed overview of security threats, services, and mechanisms.

Standards

# Significant Security Standards and Documents

**Common Criteria for Information Technology Security Evaluation**

- **Common Criteria for Information Technology Security Evaluation**
  - Part 1: Introduction and General Model.
    - CCIMB-2012-09-001, September 2012.
  - Part 2: Security Functional Components.
    - CCIMB-2012-09-002, September 2012.

Standards

# Significant Security Standards and Documents

**Internet Standards and the Internet Society**

- **RFC 2196**
  - Site Security Handbook: It is similar to ISO 27002 and SP 800-100.
- **RFC 3552**
  - Guidelines for Writing RFC Text on Security Considerations

# References

# List of NIST and ISO Documents. ABBREVIATIONS

- **FIPS** Federal Information Processing Standard
- **NIST** National Institute of Standards and Technology
- **NISTIR** NIST Internal/Interagency Report
- **SP** Special Publication FIPS Federal Information Processing Standard

# List of NIST Documents

- *FIPS 46 Data Encryption Standard, January 1977.*
- *FIPS 113 Computer Data Authentication, May 1985.*
- *FIPS 140-3 Security Requirements for Cryptographic Modules, September 2009.*
- *FIPS 180-4 Secure Hash Standard (SHS), August 2015.*
- *FIPS 181 Automated Password Generator (APG), October 1993 (withdrawn October 2015)*
- *FIPS 186-4 Digital Signature Standard (DSS), July 2013*
- *FIPS 197 Advanced Encryption Standard, November 2001.*
- *FIPS 199 Standards for Security Categorization of Federal Information and Inf. Systems, February 2004.*
- *FIPS 200 Minimum Security Requirements for Federal Information and Inf. Systems, March 2006*
- *FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013*
- *FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015*
- *NISTIR 7298 Glossary of Key Information Security Terms, May 2013.*

# List of NIST Documents

- *SP 800-94 Guide to Intrusion Detection and Prevention Systems, July 2012.*
- *SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007*
- *SP 800-100 Information Security Handbook: A Guide for Managers, October 2006*
- *SP 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control*
- *Systems (PACS), December 2015*
- *SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013*
- *SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Inf. Systems and Organizations, September 2011*
- *SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing, December 2011.*
- *SP 800-145 The NIST Definition of Cloud Computing, September 2011.*
- *SP 800-146 Cloud Computing Synopsis and Recommendations, May 2012.*
- *SP 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014.*
- *SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, December 2016.*
- *SP 800-92 Guide to Computer Security Log Management, September 2006*

# List of NIST Documents

- *SP 500-292 NIST Cloud Computing Reference Architecture, September 2011.*
- *SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995*
- *SP 800-16 A Role-Based Model for Federal Information Technology/ Cybersecurity Training, March 2014*
- *SP 800-18 Guide for Developing Security Plans for Federal Information Systems, February 2006.*
- *SP 800-28 Guidelines on Active Content and Mobile Code, March 2008.*
- *SP 800-30 Guide for Conducting Risk Assessments, September 2012.*
- *SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001*
- *SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View, March 2011*
- *SP 800-41 Guidelines on Firewalls and Firewall Policy, September 2009.*
- *SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, January 2015.*
- *SP 800-61 Computer Security Incident Handling Guide, August 2012.*
- *SP 800-63-3 Digital Authentication Guideline, August 2016.*
- *SP 800-82 Guide to Industrial Control Systems (ICS) Security, May 2015.*
- *SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013.*

# List of ISO Documents

- *12207 Information technology - Software lifecycle processes, 1997*
- *13335 Management of information and communications technology security, 2004*
- *27000 ISMS—Overview and Vocabulary, February 2016*
- *27001 ISMS—Requirements, October 2013*
- *27002 Code of Practice for Information Security Controls, October 2013*
- *27003 Information security management system implementation guidance, 2010*
- *27004 Information security management - Measurement, 2009*
- *27005 Information Security Risk Management, June 2011*
- *27006 Requirements for bodies providing audit and certification of information*
- *security management systems, 2015*
- *31000 Risk management - Principles and guidelines, 2009*

# Bibliography


- *Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model. CCIMB-2012-09-001, September 2012.*
- *National Research Council. Cybersecurity: Today and Tomorrow. Washington, DC: National Academy Press, 2002*
- *Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model. CCIMB-2012-09-001, September 2012.*
- *Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components. CCIMB-2012-09-002, September 2012.*
- *Lampson, B. "Computer Security in the Real World." Computer, June 2004.*
- *National Research Council. Computers at Risk: Safe Computing in the Information Age. Washington, DC: National Academy Press, 1991.*
- *Cybersecurity Fundamentals Study Guide, 2nd Edition. ISBN 978-1-60420-700-2*
- *https://www.itu.int/rec/T-REC-X/en*