GCS
T0 – Cybersecurity Overview

2024-2025

Marc Ruiz / Marc Catrisse

marc.ruiz-ramirez@upc.edu

marc.catrisse@upc.edu

Contents

- Overview of computer security
- Computer security requirements and objectives
- Computer security concepts
- A model for Computer Security
- Standards & Organizations
- References

Computer Security Concepts

A Definition of Computer Security

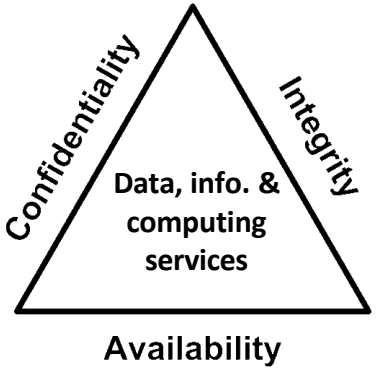
National Institute of Standards and Technology

- *The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms, May 2013)*
  - https://csrc.nist.gov/glossary
- **Cybersecurity** = **Computer security**
- *"Prevention of damage to, **protection** of, and restoration of **computers**, **electronic communications systems**, electronic communications **services**, wire communication, and electronic communication, including **information** contained therein, to **ensure** its availability, integrity, authentication, confidentiality, and nonrepudiation."*

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 communications, 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.

Security objectives (FIPS199) ➔ CIA



The **NIST FIPS 199** defines the CIA Triad, a widely recognized model, to ensure the security and integrity of information within organizations or systems

Security **objectives**:

- **Confidentiality:** Sensitive information is accessible only to authorized entities (vs. Unauthorized disclosure)
- **Integrity:** Maintain the accuracy, reliability, and consistency of data and systems (vs. Unauthorized modification or destruction)
- **Availability:** Information and resources are accessible to authorized users (vs. Disruption of access to or use)

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

CIA Triad - Related concepts

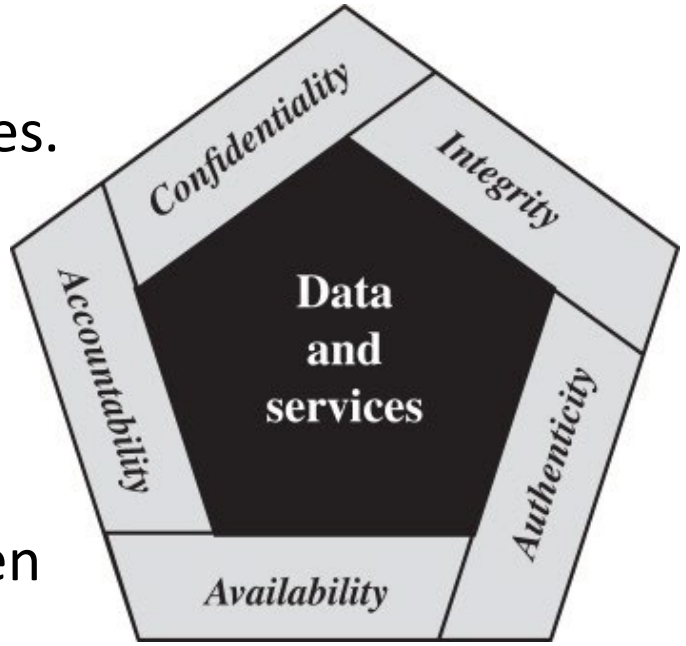
- ***Confidentiality***
  - Data confidentiality:
    - Involves data protection from unauthorized access, disclosure, or interception.
      - Measures: encryption, access control, and data masking. etc.
  - Privacy:
    - Individual's right to control their personal information (how it is collected, used, and shared)
      - Measures: anonymization, encryption, access control, etc.
- ***Integrity***
  - Data integrity: Data remains accurate, complete, and unaltered throughout its lifecycle.
    - Measures: Data validation (checksums, hash functions), encryption, access control, auditing, monitoring, etc.
  - System integrity: Computer systems and resources operate according to their intended functionality
    - Measures: Secure configuration management, access control, IDS, monitoring, etc.

CIA Triad - Related concepts

- ***Availability***
  - **Data:** Remain accessible and usable by authorized users whenever needed.
    - Measures: Redundancy, Replication, Data Backup, Recovery, etc.
  - **Systems:**
    - Measures: Redundancy and High Availability, Fault Tolerance and Resilience, Incident Response, Disaster Recovery, etc.
  - **IT Services:**
    - Measures: Redundancy and Load Balancing, Continuous Monitoring and Alerting, Backup and Recovery, etc.

Essential Security Requirements

- ***Authenticity***
  - Data, communications, or transactions are genuine
    - Not altered or tampered with by unauthorized parties.
  - Origin and integrity of information can be verified and trusted.
  - Confidence in the validity of a transmission
- ***Accountability***
  - Ability to trace and assign responsibility for actions taken within an information system.
  - It involves logging and auditing user activities, enforcing accountability policies, etc.



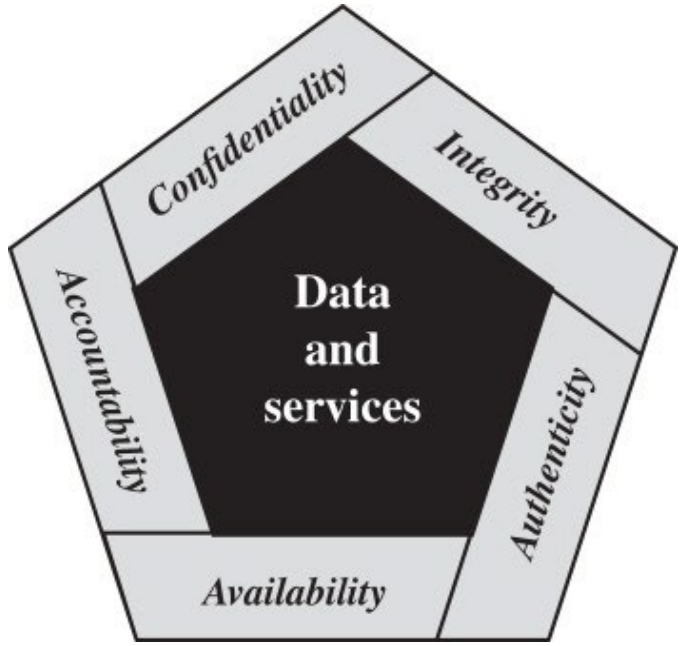
Note that FIPS 199 includes authenticity under integrity

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
- Characterization:
  - Adversary Group: Define the scope adversary group (Internal/External)
  - Techniques: Used by the threat actor (e.g Network Scanning)
  - Required Resources: Sw used to identify which service is vulnerable and can be targeted
  - Motivation
  - Intention: What wants to steal or what services can be targeted

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
- Characterization
  - Type
  - Pattern: Define behavior or pattern of the attack
  - ID ATT &CK MITRE framework

A Model for Computer Security

- ***Attacks (threats carried out)***
  - **Based on action**
    - **Active** ➔ direct interaction with the target system or network
      - The attacker actively tries to exploit vulnerabilities, gain unauthorized access, or manipulate data (malware, MitM, SQL injection, phishing, etc.)
    - **Passive** ➔ The attacker intercepts and monitors data transmissions or network traffic without directly altering or modifying the data
      - Eavesdropping, sniffing network traffic, analyzing metadata to gather information about systems, users, or sensitive data
  - **Based on origin**
    - **Insider** ➔ origin = security perimeter
      - Ex: Unauthorized access to sensitive data, privilege scalation
    - **Outsider** ➔ origin = outside the perimeter
      - Ex: DoS, phishing emails

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

- Action, device, procedure, or technique designed to detect, prevent, or mitigate security risks, threats, vulnerabilities, or attacks
  - sensitive information
  - information systems
- Can take various forms:
  - **Technical Controls**: Security mechanisms implemented through technology: firewalls, IDPS, antivirus, etc.
  - **Administrative Controls**: Policies, procedures, guidelines, and standards established by organizations to govern security practices, user behavior, and operational processes.
  - **Physical Controls**: Measures implemented to secure physical access (surveillance cameras, biometric authentication systems, etc.)

A Model for Computer Security

Computer Security Terminology (RFC 2828)

Risk

- Potential for harm or loss resulting from the exploitation of vulnerabilities in information systems or networks
- *Measure of degree*
  - *get_degree (entity_threatened, circumstance_or_event)*;
  - It reflects the severity and impact of the risks posed by threats and vulnerabilities.
  - RFC 2828 does not prescribe specific quantitative methods or metrics.
- *Risk = Function (**impacts, likelihood** of occurrence)*:
  - Likelihood of occurrence: Probability that a specific threat will exploit a vulnerability and cause harm or loss to the system or network.
  - Impact of exploitation: The magnitude or severity of the potential consequences resulting from the exploitation of vulnerabilities (operational disruptions, financial losses, reputational damage, etc.)

A Model for Computer Security

Computer Security Terminology (RFC 2828)

Security Policy

- Formal set of criteria: Rules, guidelines, and procedures

  ➔ provision of security services
- established by an organization
- to govern and manage its information technology (IT) infrastructure, systems, networks, and data assets
- *Objective: Maintain a condition of security for* ***<u>systems and data</u>***

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, unauthorized access, social engineering and/or DoS.

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

A Model for Computer Security

Computer Security Terminology (RFC 2828)

Vulnerability

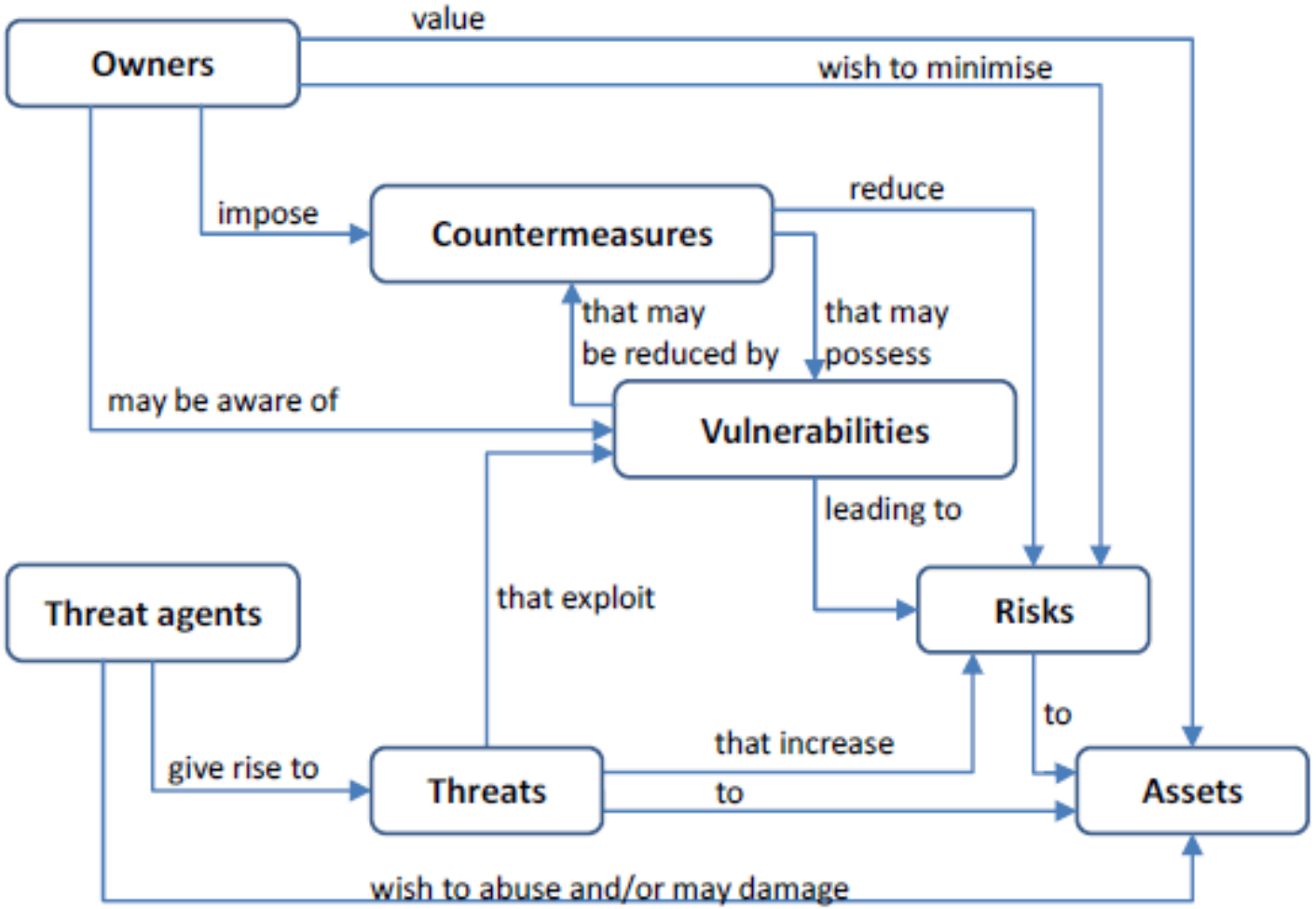
- *Weakness in an*
  - information system, system security procedures, internal controls, or implementation
- *that could be exploited or triggered by a threat source.*
- *Characteristics:*
  - Nature: Can manifest in various forms
    - Software bugs, programming errors, misconfigurations, design flaws, etc.
  - Scope: Can affect different components of an organization's infrastructure
    - OS, applications, databases, web servers, network devices, cloud services, etc.
  - Severity: Potential impact it could have on the security, operations, and reputation of an organization if exploited.
  - Exploitation: Can be exploited by threat actors through various attack vectors:
    - Remote attacks, local attacks, social engineering techniques, phishing emails, malicious software, etc.

A Model for Computer Security

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

A Model for Computer Security

Security Concepts and Relationships



Source: ISO/IEC 15408-1:2005 - Information technology

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*