Department of Information Engineering and Mathematics

a.a. 2018-2019

Cybersecurity: a guided overview

Mauro Barni
University of Siena

Cybersecurity (computer security)

- NIST Internal/Interagency Report NISTIR 7298 defines 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**."*

CIA TRIAD

Confidentiality

- **Data confidentiality**:
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy**:
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity

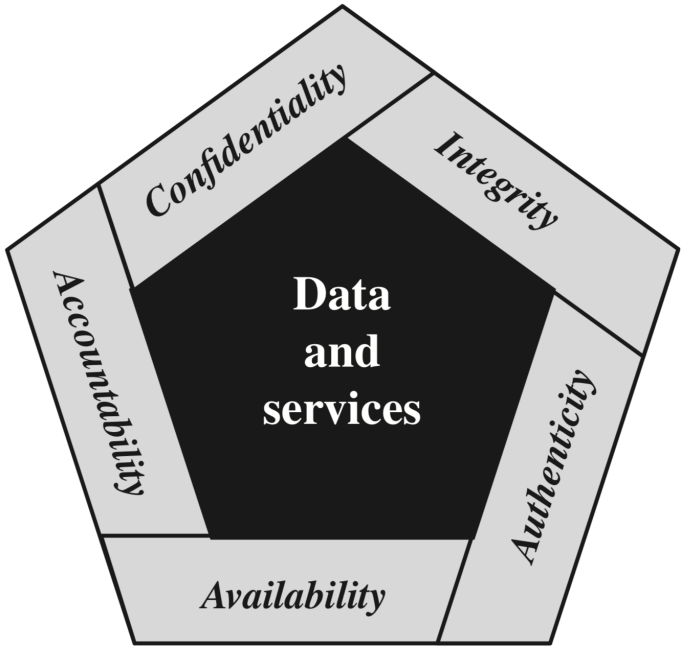
- **Data integrity:**
  - Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity**
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability

Assures that systems work promptly and service is not denied to authorized users.

Two additional concepts

- **Authenticity:** The property of being genuine and being able to be verified and trusted. It includes verifying that users are who they say they are and that each input arriving at the system came from a trusted source.



- **Accountability**: It supports traceability, nonrepudiation, deterrence, fault isolation, after-action recovery and legal actions.

To-be-protected assets

- **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

Vulnerabilities

Lack of confidentiality → **Leaky system**

For instance, non authorized users get access to private information

Lack of integrity → **Corrupted system**

For instance, stored information may differ from what it should be

Lack of availability → **Unavailable system**

Using the system or network becomes impossible or impractical

Threats and attacks

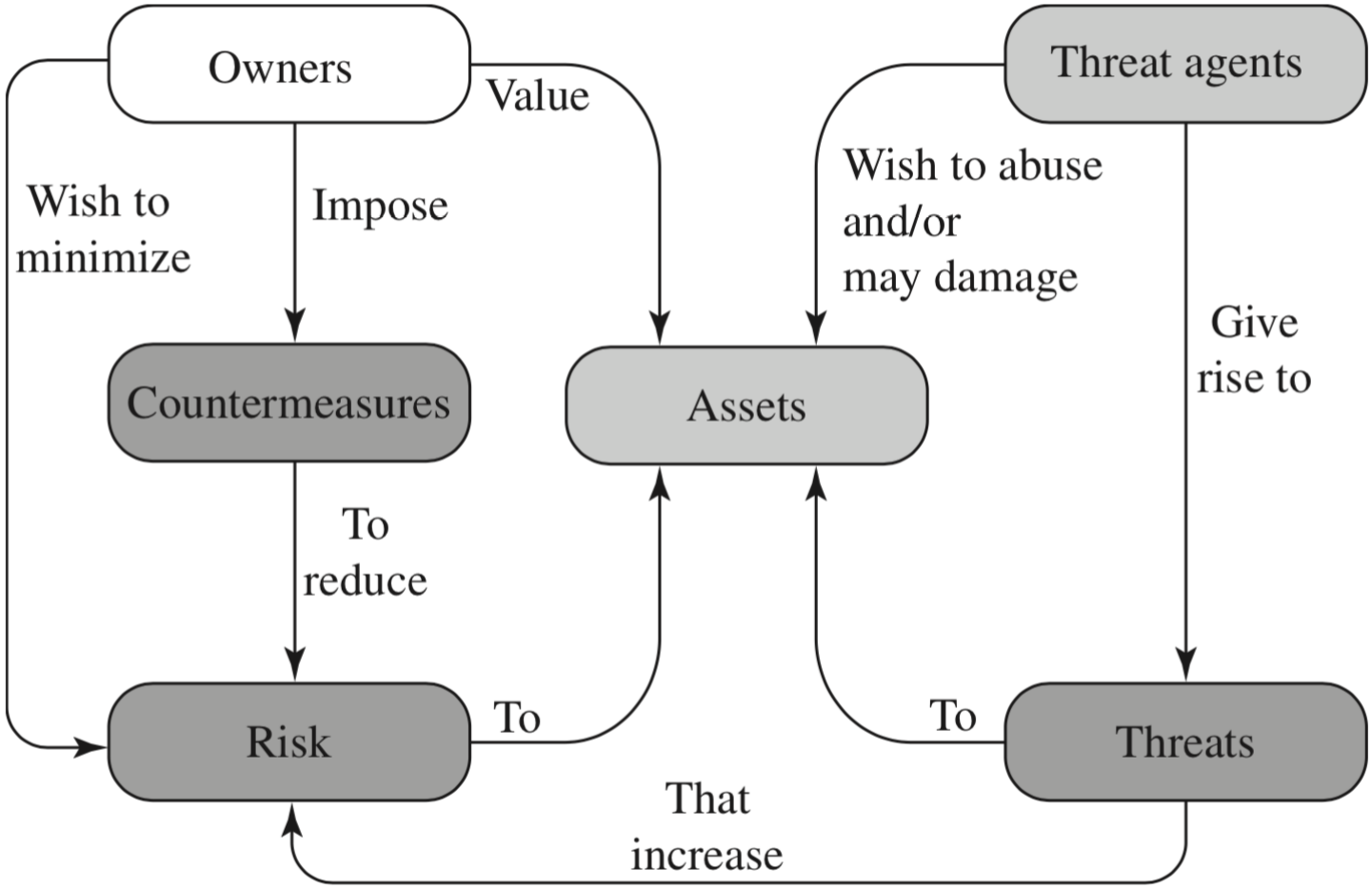
- A **threat** represents a potential security harm to an asset
- An **attack** is a threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security, or threat consequence
- The agent carrying out the attack is called **attacker** or **threat agent**

- **Active** vs **passive** attacks
- **Inside** vs **outside** attacks

Countermeasures

- A **countermeasure** is any means taken to deal with a security attack
- Countermeasures may aim at
  - **preventing** attacks
  - **detecting** attacks
  - **responding** to attacks
  - **recovering** from the effects of attacks

A summarizing picture



A zoo of attacks

Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

An **unauthorized disclosure** is a threat to confidentiality

A zoo of attacks

Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.

Deception is a threat to either system or data integrity (or accountability)

A zoo of attacks

Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.

Disruption is a threat to availability or system integrity

A zoo of attacks

Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Usurpation is a threat to system integrity

Attacks vs assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted USB drive is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

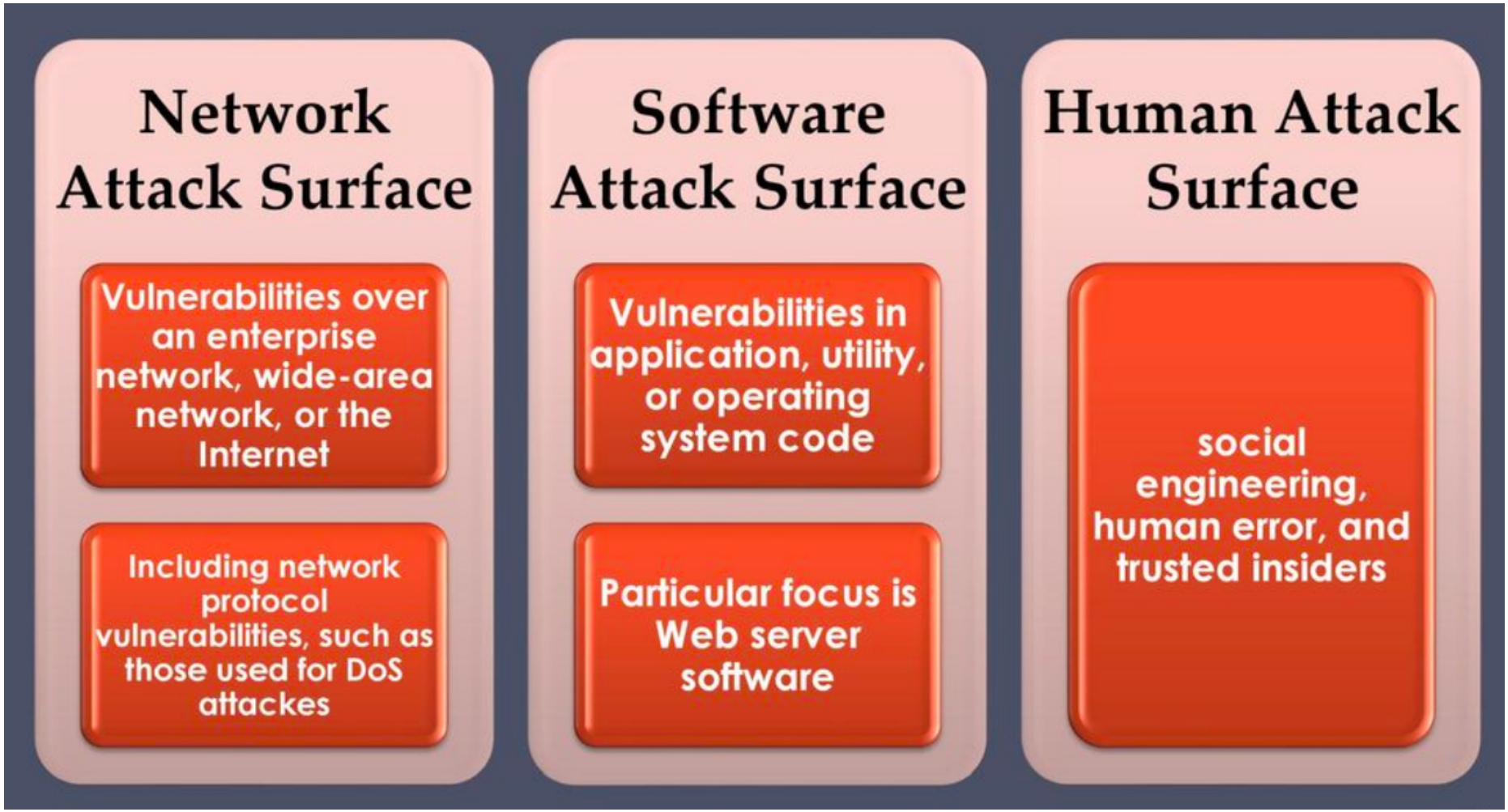
Countermeasures

- In FIPS 200 ("*Minimum Security Requirements for Federal Information and Information Systems*"), NIST identifies 17 functional requirements for securing a system
- Each requirements involves one or both
  - computer security technical measures (either hardware or software)
  - management measures

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology

Before starting: attack surface

- An **attack surface** consists of the reachable and exploitable vulnerabilities in a system.
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Code that processes incoming data, e-mail, XML, office documents, and industry-specific custom data exchange formats
  - An employee with access to sensitive information vulnerable to a social engineering attack

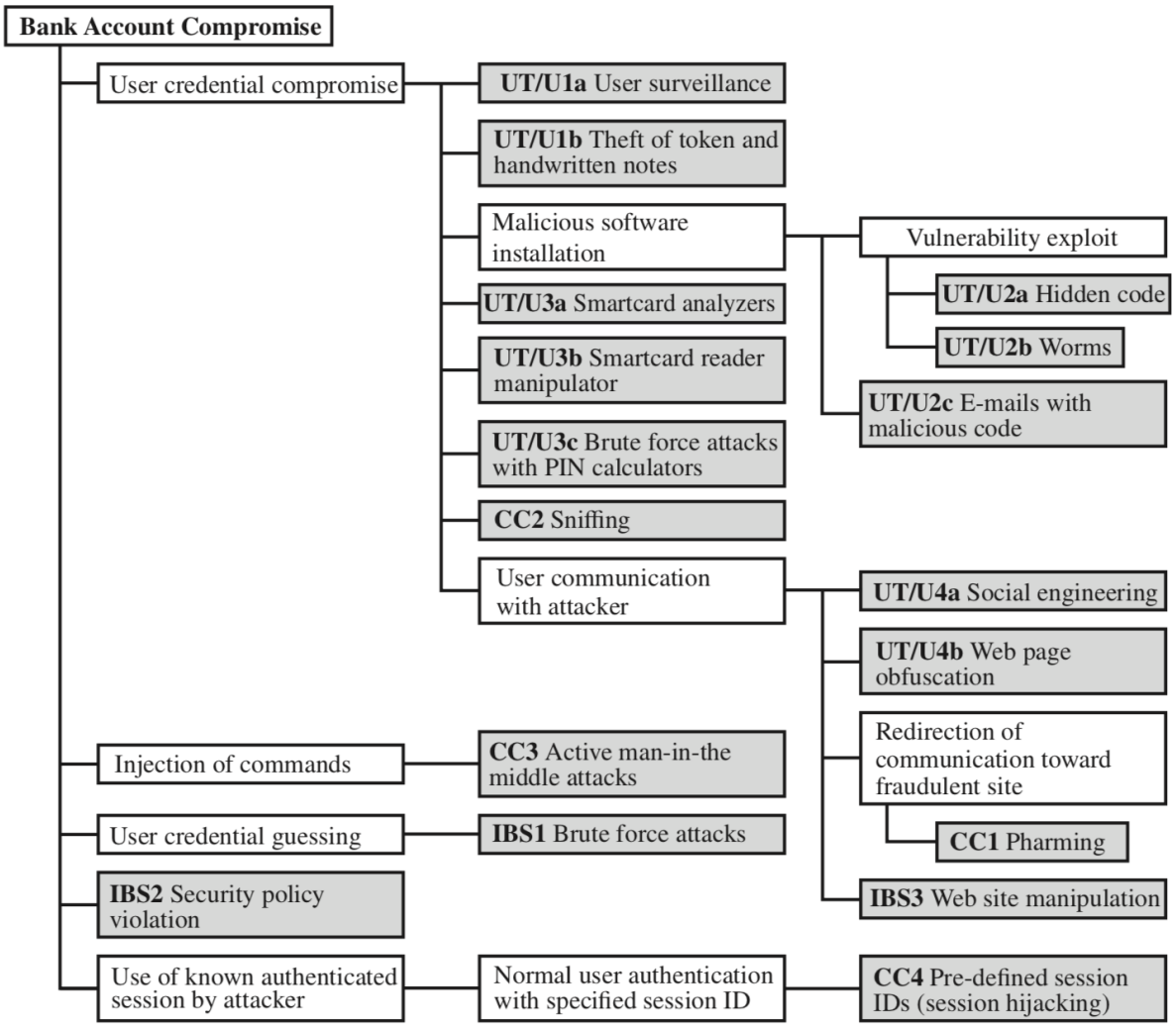

Network Attack Surface
Vulnerabilities over an enterprise network, wide-area network, or the Internet
Including network protocol vulnerabilities, such as those used for DoS attackes
Software Attack Surface
Vulnerabilities in application, utility, or operating system code
Particular focus is Web server software
Human Attack Surface
social engineering, human error, and trusted insiders

Before starting: attack trees

- **Attack trees** can be used to identify vulnerabilities in a hierarchical way to ease the deploy of countermeasures
- **Root** = security incident, goal of the attack
- **Nodes** = the ways by which an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes
- **Leaves** = initial point of the attack

- Intermediate nodes may be either **AND** or **OR** nodes

Attack tree: an example



Countermeasures

Access Control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulations, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Countermeasures

Configuration Management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication: Identify information system users, processes acting on behalf of users, or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response: (i) Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Countermeasures

Physical and Environmental Protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and Services Acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

Countermeasures

System and Communications Protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Secure design principles

- **Simplicity.** The design of security measures in both hardware and software should be as simple and small as possible.
- **Fail-safe default.** Access decisions should be based on permission rather than exclusion, i.e. the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.
- **Complete mediation.** Every access must be checked against the access control mechanism.
- **Open design.** The design of a security mechanism should be open rather than secret.

Secure design principles

- **Least privilege.** Every process and every user of the system should operate using the least set of privileges necessary to perform the task
- **Least common mechanism**. System design should minimize the functions shared by different users, providing mutual security.
- **Acceptability.** Security mechanisms should not interfere unduly with the work of users, and at the same time meet the needs of those who authorize access.

Secure design principles

- **Isolation:** i) public access systems should be isolated from critical resources; ii) processes and files of individual users should be isolated from one another; iii) security mechanisms should be isolated. In object oriented systems isolation is achieved by means of **encapsulation**
- **Modularity**: i) develop security functions as separate, protected modules; ii) individual parts of the security design can be upgraded without the requirement to modify the entire system

Secure design principles

- **Layering.** Use multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This technique is often implemented according to the *defense in depth* paradigm
- **Least astonishment.** Any security mechanism (program or user interface) should always respond in the way that is least likely to astonish the user.

A (very) difficult job

Challenges making (even imperfect) security hard to reach include:

- Requirements are straightforward but the methods to reach them are not
- Attacks are often designed by looking at the problem in a completely different way, exploiting unexpected weaknesses.
- The procedures used to provide particular services are often counterintuitive and the reasons why certain steps are made unclear.

A (very) difficult job

- Key release, maintenance and distribution
- Battle of wits, but one single failure can be fatal
- Security requires regular, even constant monitoring, which is difficult in today's short-term, overloaded environment.

A (very) difficult job

- 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.
- Security is still often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process.
- Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation.

References

- W. Stallings, L. Brown, "*Computer security: principles and practices",* Pearson, 4-th edition
- Lectures notes (these slides)