Cybersecurity

Salim Benayoune

Cyber Security Intelligence

- Intitulé de la matière : Cyber Security Intelligence
- Code : CSI
- Unité d'Enseignement : UEM2
- Crédit : 3
- Coefficient de la Matière : 2
- Cours : 1H30/ semaine
- TP : 1H30 /semaine

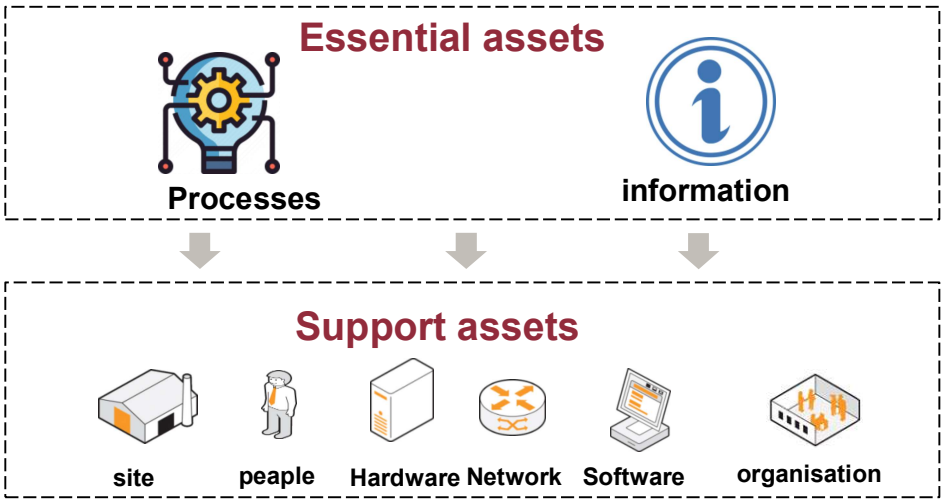
- Mode d'évaluation : Examen (60%), contrôle continu (40%)

What is an Information System ?

- An information system (IS) is a structured framework comprising people, processes, data, and technology, all working together to collect, process, store, and disseminates information for the purpose of supporting decision-making, coordination, control, analysis, and visualization within an organization

ISO/IEC 27005:2008

ISO Organisation internationale de normalisation



Definition of Cybersecurity

Cybersecurity is a range of **technical**, **organizational**, and **procedural** measures aimed at protecting information **assets** and ensuring the **confidentiality**, **integrity**, and **availability** of digital resources end assets.

This includes the development and implementation of **security protocols**, **encryption techniques**, **access controls**, **intrusion detection systems**, and **incident response plans** to mitigate risks posed by cyber threats such as malware, phishing, ransomware, and insider attacks.

The objective of cybersecurity is to **mitigate vulnerabilities** and defend against potential cyberattacks, thereby preserving the integrity and functionality of critical infrastructure, businesses, governments, and individuals in the **cyberspace**.

The challenges of I.S. security

The objective of security is to reduce the risks on the information system, to limit their impact on the operation and business activities of organizations

The purpose of managing security within an information system is **not to obstruct**:

- It contributes to the quality of service that users have a right to expect
- It guarantees staff the level of protection they need

CIA Triad

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

Terminology (RFC 4949)

Adversary (threat agent) : Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack :Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure : A device or techniques that has as its objective the impairment of the operational effectiveness of adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk : A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

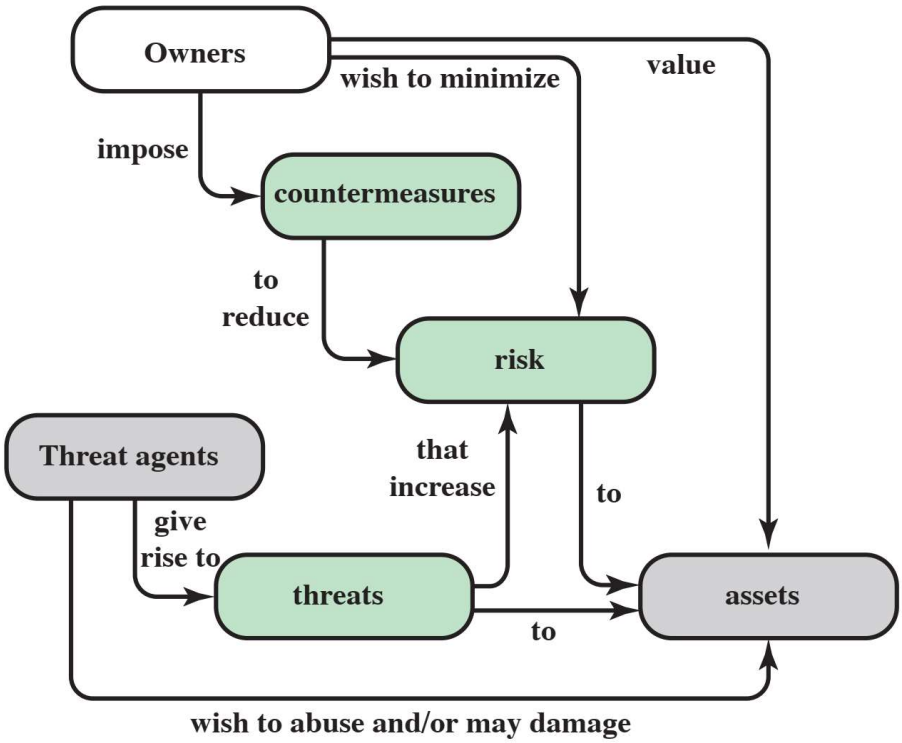
Terminology (RFC 4949)

Security Policy : A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility to maintain a condition of security for systems and data.

Threat :Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

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

Security concepts and relationships



Fundamental Security Design Principles

Economy of mechanism	Fail-safe defaults	Complete mediation	Open design
Separation of privilege	Least privilege	Least common mechanism	Psychological acceptability
Isolation	Modularity	Layering	

Fundamental Security Design Principles

- **Economy of mechanism :**
  - The design of security measures embodied in both hardware and software should be as simple and small as possible.
  - Small design is easier to test and verify
  - With a complex design, there are many more opportunities for an adversary to discover subtle weaknesses to exploit that may be difficult to spot ahead of time.
  - Simple mechanisms tend to have fewer exploitable flaws and require less maintenance.
  - Configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process
  - The most difficult principle to honor because of a constant demand for new features in both hardware and software

Fundamental Security Design Principles

- **Fail-safe default :**
  - Access decisions should be based on permission rather than exclusion.
  - The default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.
  - A design or implementation mistake in a mechanism that gives explicit permission tends to fail by refusing permission, a safe situation that can be quickly detected.

Fundamental Security Design Principles

- **Complete mediation** means every access must be checked against the access control mechanism.
    - Systems should not rely on access decisions retrieved from a cache.
    - It is a resource-intensive approach and rarely used in file systems for example.
    - Used in firewalls
    - Zero trust networking ?

Fundamental Security Design Principles

- **Open design** means the design of a security mechanism should be open rather than secret.
    - Cryptography : encryption keys must be secret; encryption algorithms should be open to public scrutiny.
- **Separation of privilege :** a program is divided into parts that are limited to the specific privileges they require to perform a specific task.
- **Least privilege :** means every process and every user of the system should operate using the least set of privileges necessary to perform the task.
    - Example : role-based access control

Fundamental Security Design Principles

- **Least common mechanism** means the design should minimize the functions shared by different users, providing mutual security.
  - It helps reduce the number of unintended communication paths
  - It reduces the amount of hardware and software on which all users depend,
  - It is easier to verify if there are any undesirable security implications.

- **Psychological acceptability** implies the security mechanisms should not interfere unduly with the work of users.
  - Security mechanisms should be transparent to the users of the system or at most introduce minimal obstruction.

Fundamental Security Design Principles

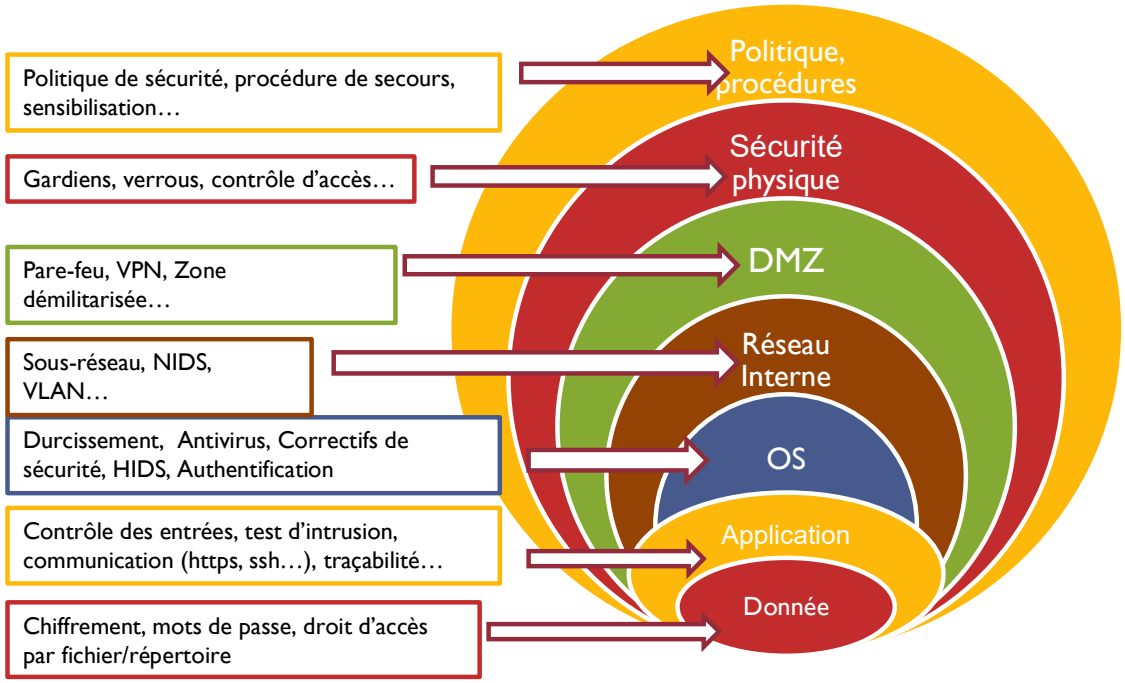
- **Isolation**
  - Public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering.
  - The processes and files of individual users should be isolated from one another except where it is explicitly desired
  - Security mechanisms should be isolated in the sense of preventing access to those mechanisms.

- **Modularity** in the context of security refers both to the development of security functions as separate, protected modules, and to the use of a modular architecture for mechanism design and implementation.
  - Individual parts of the security design can be upgraded without the requirement to modify the entire system.

Fundamental Security Design Principles

- **Layering** refers to the use of multiple, overlapping protection approaches addressing the people
  - The failure of any individual protection approach will not leave the system unprotected.
  - Also known as defense in depth
  -

Fundamental Security Design Principles



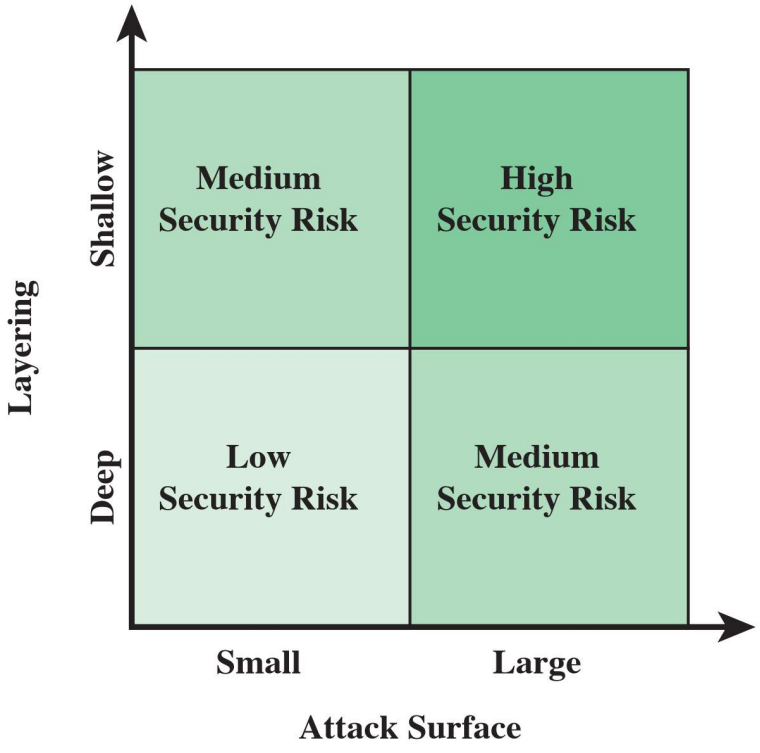
Attack Surfaces

- An attack surface consists of the reachable and exploitable vulnerabilities in a system

- **Examples :**
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available on the inside of a firewall
  - Code that processes incoming data, e-mail, XML, office documents, and industry-specific custom data exchange formats
  - Interfaces, SQL, and web forms
  - An employee with access to sensitive information vulnerable to a social engineering attack

Attack surfaces

- Network attack surface
- Software attack surface
- Human attack surface



Sources of information

- ENISA; ANSSI, CERT, NSA, NIST, CISA, CNIL...
- Press :
  - FR : 01Net, LMI, JDN, Zataz, Rue89, Réseaux-Telecoms…
  - EN : ZDNet, Slashdot, TheRegister, Dark Reading…
- Editors:
  - Sophos, Symantec, Cisco, K-labs, CERT XMCO, CERT Lexsi, Security-DB, FireEye, SANS,
- Blogs :
  - OBS, Microsoft (MSRC/MMPC), spécialistes (schneier.com/, digitalguardian.com/blog/top-50-infosec-blogs-you-should-be-reading …)
- Conferences : BlackHat, DefCon, BlueHat, SSTIC…