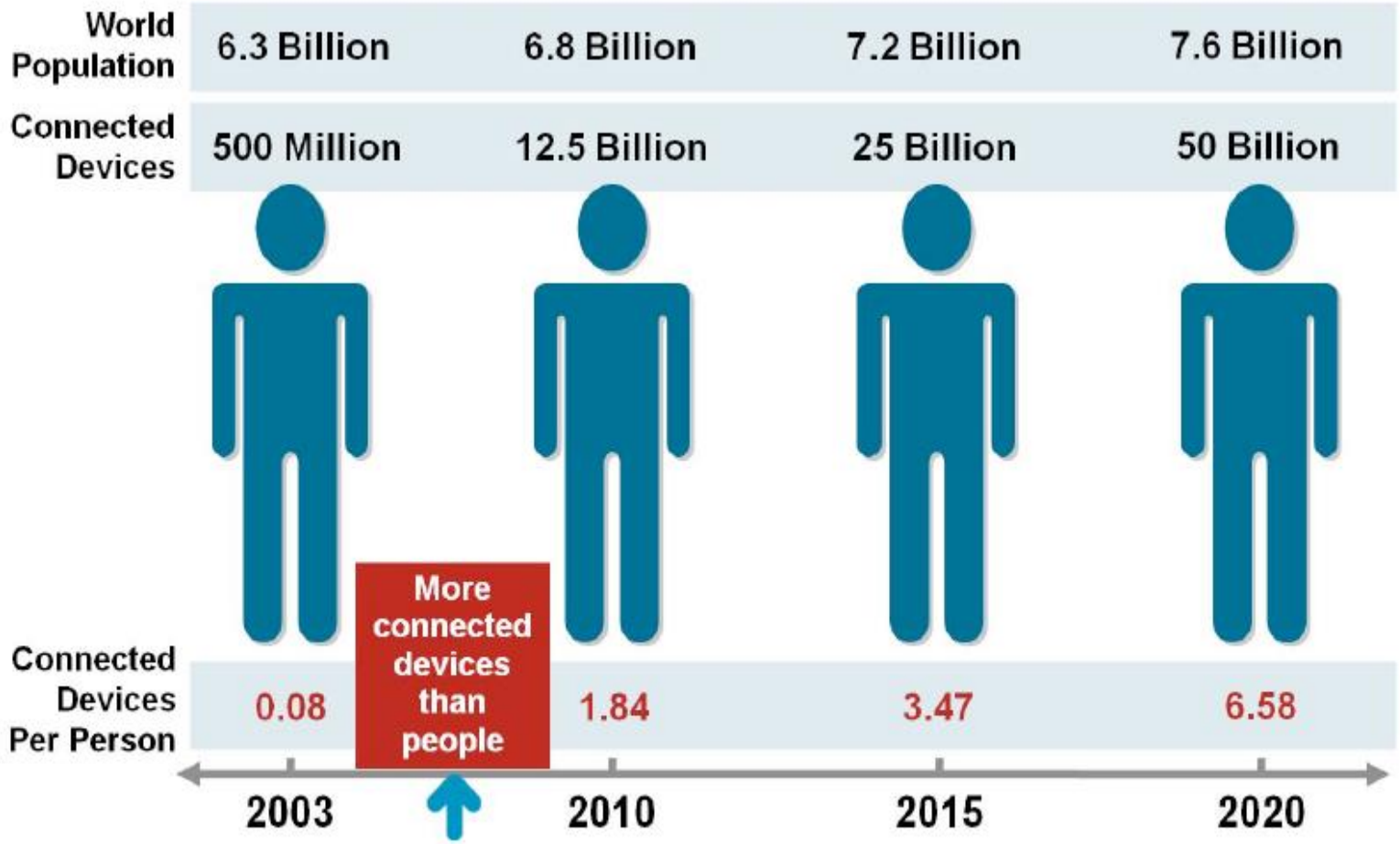
Basic concepts of security computer

Pr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Course outline

- Introduction
- Definitions
- Security properties
- Classification of attacks
- Technical aspects of security

Introduction



Source: Cisco IBSG, April 2011

Introduction

- What are we protecting?
  - Material
  - Documentation
  - Networks,
  - Web applications
  - Software
  - Data, …

Definitions

- **Information security:**

  Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. *(*(ISO/IEC 27000:2018)

- **Computer Security:**

  It is a subdiscipline of information security that focus on reducing vulnerability in computer systems.

Definitions

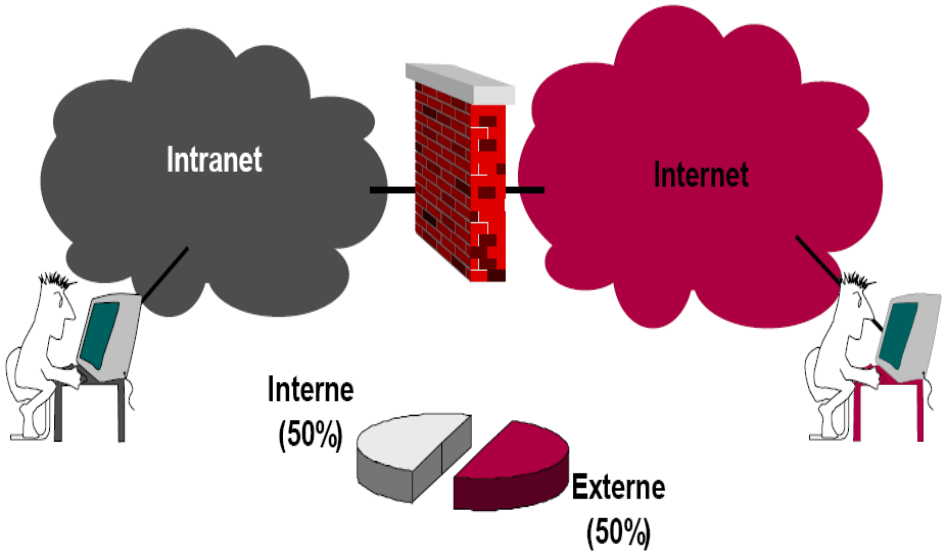
- **Vulnerability:**
  - Is a weakness or flaw in the protection of the system, in the form of a threat that can be exploited to intervene on the entire system or an intruder that attacks assets (hardware, software, processes, etc.).
- **Threat:**
  - Is a person or entity (e.g.. web application, software, etc.) that can exploit a vulnerability in a system to modify, gain or prevent access to a computer device or even compromise it.

Definitions

- **Attack :**

A action malicious that compromises the security of data or computer systems.

Where are the attacks coming from?



Definitions

- **Countermeasure**
  - It is the set of actions carried out to prevent the threat.
- **Risk :**
  - It signifies the probability that a threat will exploit a vulnerability in the system.
  - Three important factors in determining risk: the nature of the threat, the vulnerability of the system, and the importance of the impact which could be damaged or rendered unavailable. The risk can be formalized as follows:

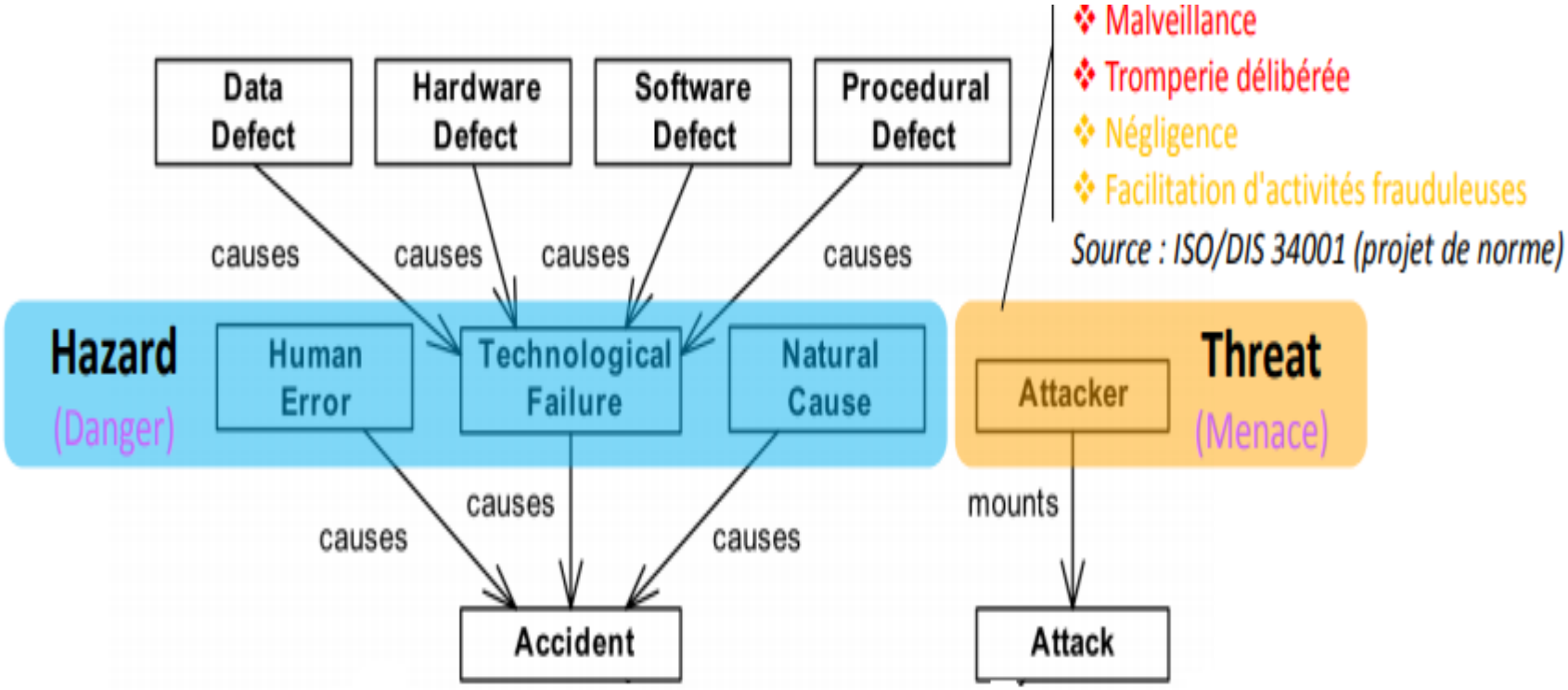
Risk=Threat*Vulnerability*Impact

Traditional system

- **Vulnerability:**
  - Windows not secure
  - No alarm system
  - Traditional keys, ….
- **Threat:**
  - Thief,
  - Assassin, …
- **Attack :**
  - Money theft
  - Document theft
  - Kill, …
- **Countermeasure:**
  - Alarm system,
  - Camera,…
- **Risk :**
  - High
  - weak,…

- **Vulnerability:**
  - Weak passwords,
  - No firewall
  - Absence of IDS,
- **Threat:**
  - Hacker,
  - Government
  - Company competitor,
  - Zombie, …
- **Attack :**
  - Information theft,
  - Denial of service,
- **Countermeasure:**
  - Anti-virus,
  - Strong password, …
- **Risk :**
  - Weak,
  - High,…

Accidents vs. Attacks



Source: Common Concepts Underlying Safety, Security, and Survivability Engineering - Donald G.Firesmith(Carnegie Mellon University)

Definitions

Access control:

Associates access rights with aperson/applicationto access a resource according to the principle of AAA.

- Authentication (Authentication):

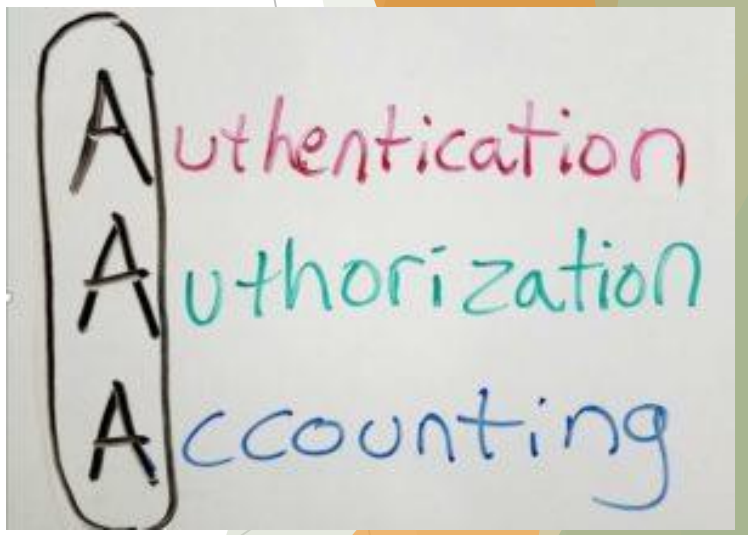
Verification of the user's identity

- Authorisation (Authorization):

Verification of the rights/privileges of the authenticated user for the proposed action.

- Traceability (Accounting):

Trace the accesses that have been controlled and carried out.



Course outline

- Definitions
- Security properties
- Classification of attacks
- Technical aspects of security

Security properties

- Security features,
- Security requirements,
- security services, …

What do users of computer systems expect?

1. Confidentiality

- Confidentiality data means that secret information can only be read by authorized entities.
- To achieve this property, there are two complementary methods:
  - control and limit access
  - Encryption algorithms
- The attacker's main objective The goal is to obtain the plaintext message. To do this, it intercepts the encrypted message and uses cryptanalysis techniques.
- **Examples of attacks:** Sniffing, intercepion message.

2. Integrity

- Integrity is a mechanism that has been put in place to ensure that the information received has not been altered during the transmission of the data.
- Methods for verifying data integrity:
  - Checksum (C*hecksum*),
  - error checking (*Cyclic Redundancy Code*),
  - Hash function.
- **Examplesof attacks:** Message modification, scrambling.

3. Authentication

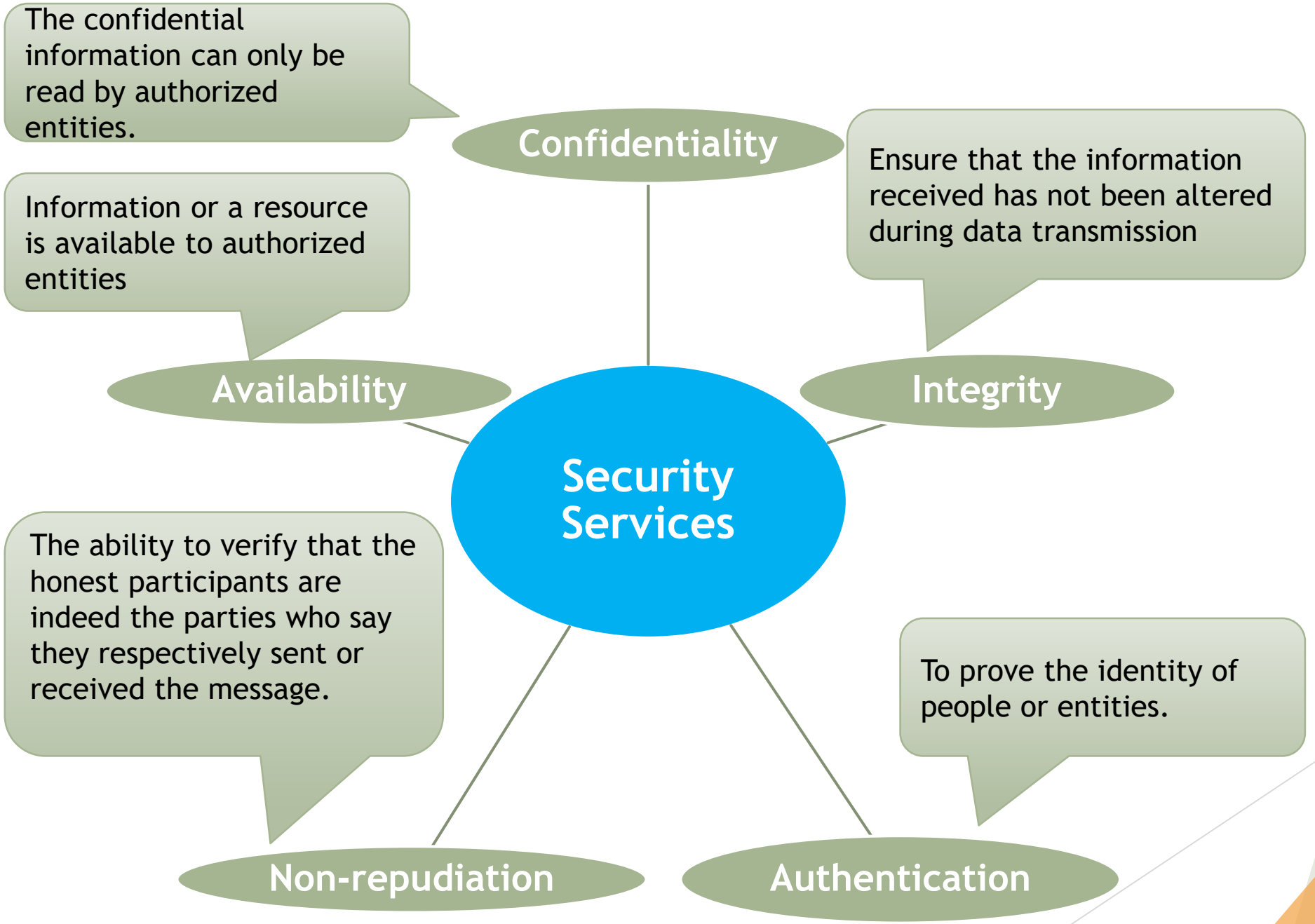
- Authentication is a mechanism for proving the existence of people or entities and proving their identity.
- The approaches used to authenticate an entity:
  - Digital signature,
  - Authentication protocol
  - Login and passwords,
  - Certificate
- **Examples of attacks:** identity theft.

4. Availability

- Information or a resource is available to authorized entities (e.g.. client, server, mobile, terminal, etc).
- The information or service is always accessible and cannot be blocked/lost.
- The service can be a web application, software, a client-server application, etc.
- **Examples of attacks:** Denial of service, bombardment and saturation of the network.

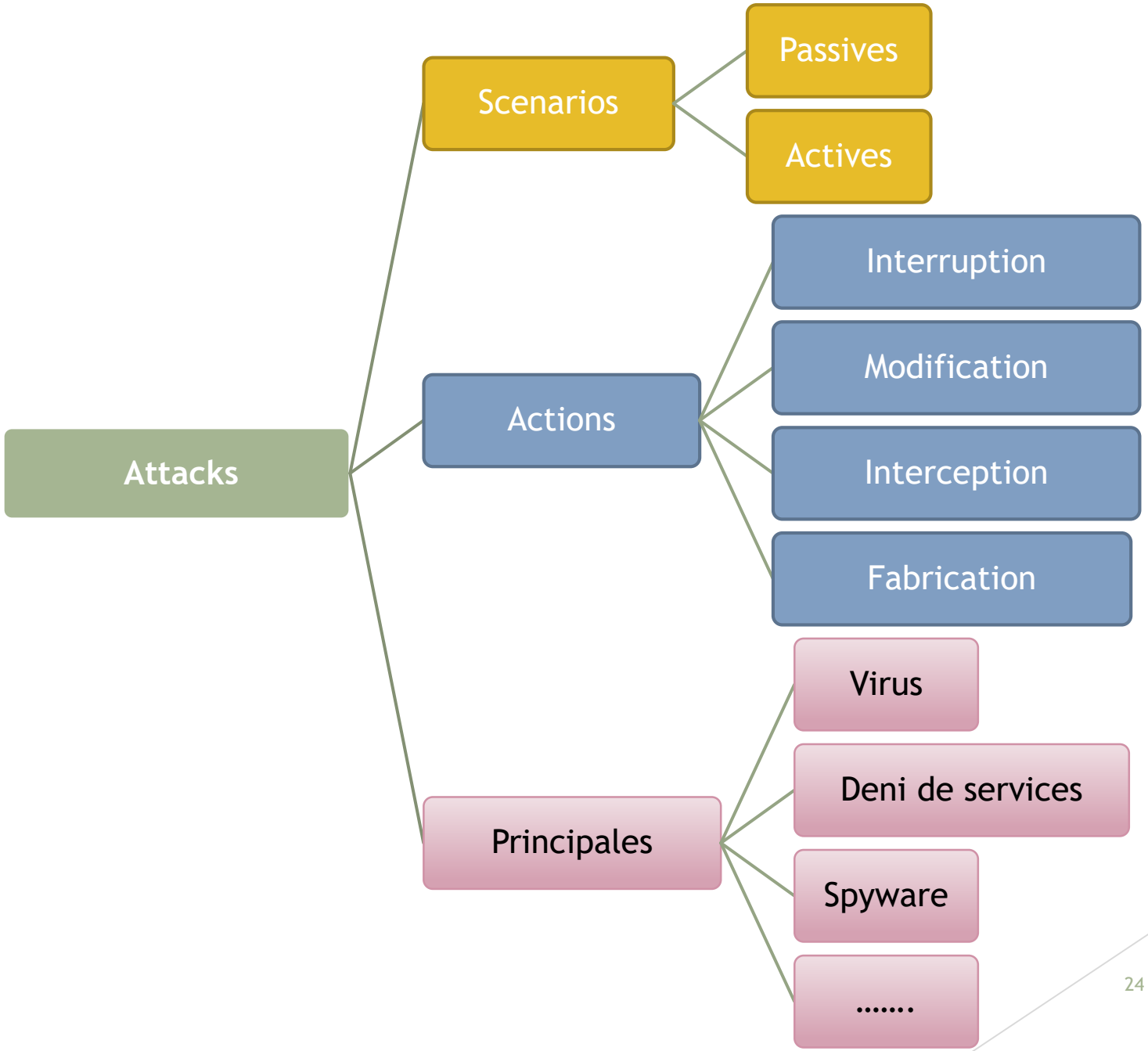
5. Non-repudiation

- There non-repudiation: ensure that a transaction cannot bedenied.
  - non-repudiation of origin proves that the data was sent.
  - non-repudiation of arrival proves that they have been received.
- A digital signature is used to achieve non-repudiation.
- **Examplesattacks:** Journal modification, repudiation.


The confidential information can only be read by authorized entities.
Confidentiality
Ensure that the information received has not been altered during data transmission
Information or a resource is available to authorized entities
Availability
Integrity
Security Services
The ability to verify that the honest participants are indeed the parties who say they respectively sent or received the message.
To prove the identity of people or entities.
Non-repudiation
Authentication

Course outline

- Definitions
- Security features
- Classification of attacks
- Technical aspects of security


Attacks
Scenarios
Passives
Actives
Actions
Interruption
Modification
Interception
Fabrication
Principales
Virus
Deni de services
Spyware
.....

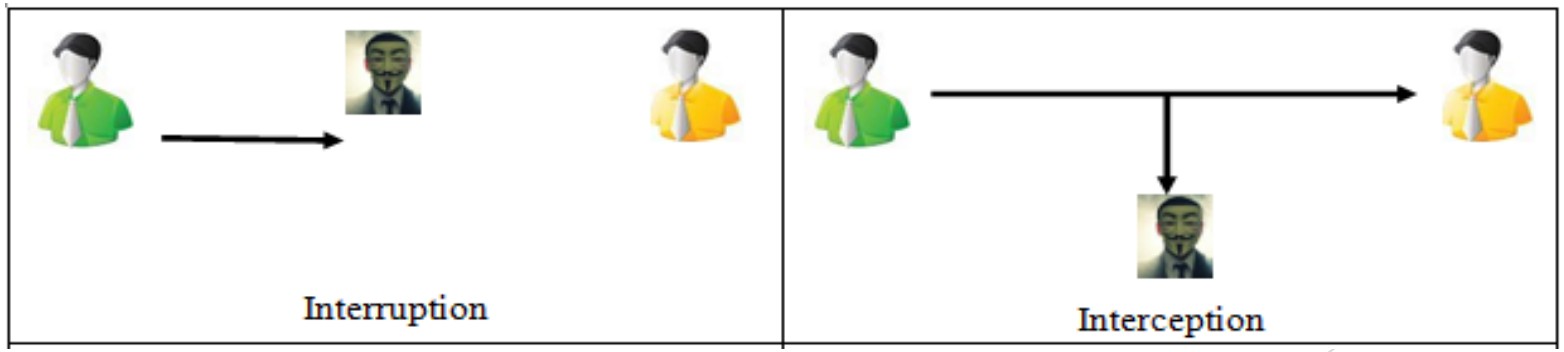
Actions of the attackers

Interruption:

- The threat blocked the messages transmitted between the entities.
- This attack targets the information availability where legitimate users cannot access the requested information.

Interception:

- The threat intercepts only the messages exchanged.
- This type of attack targets the confidentiality of information.
- The threat obtains the message and uses cryptanalysis techniques to find the plaintext.



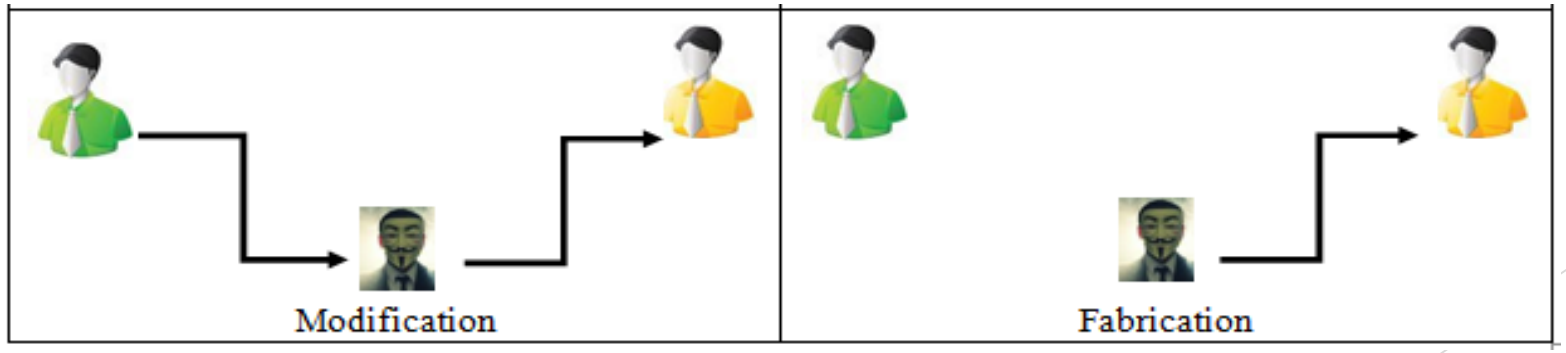
Actions of the attackers

Modification:

- The threat takes the sent message and makes modifications on this one, then sends the latter to the recipient.
- This attack targets integrity data.

Creation:

- The threat created new messages to achieve his goal.
- This attack targets authenticity entities and information.



Attack scenarios:

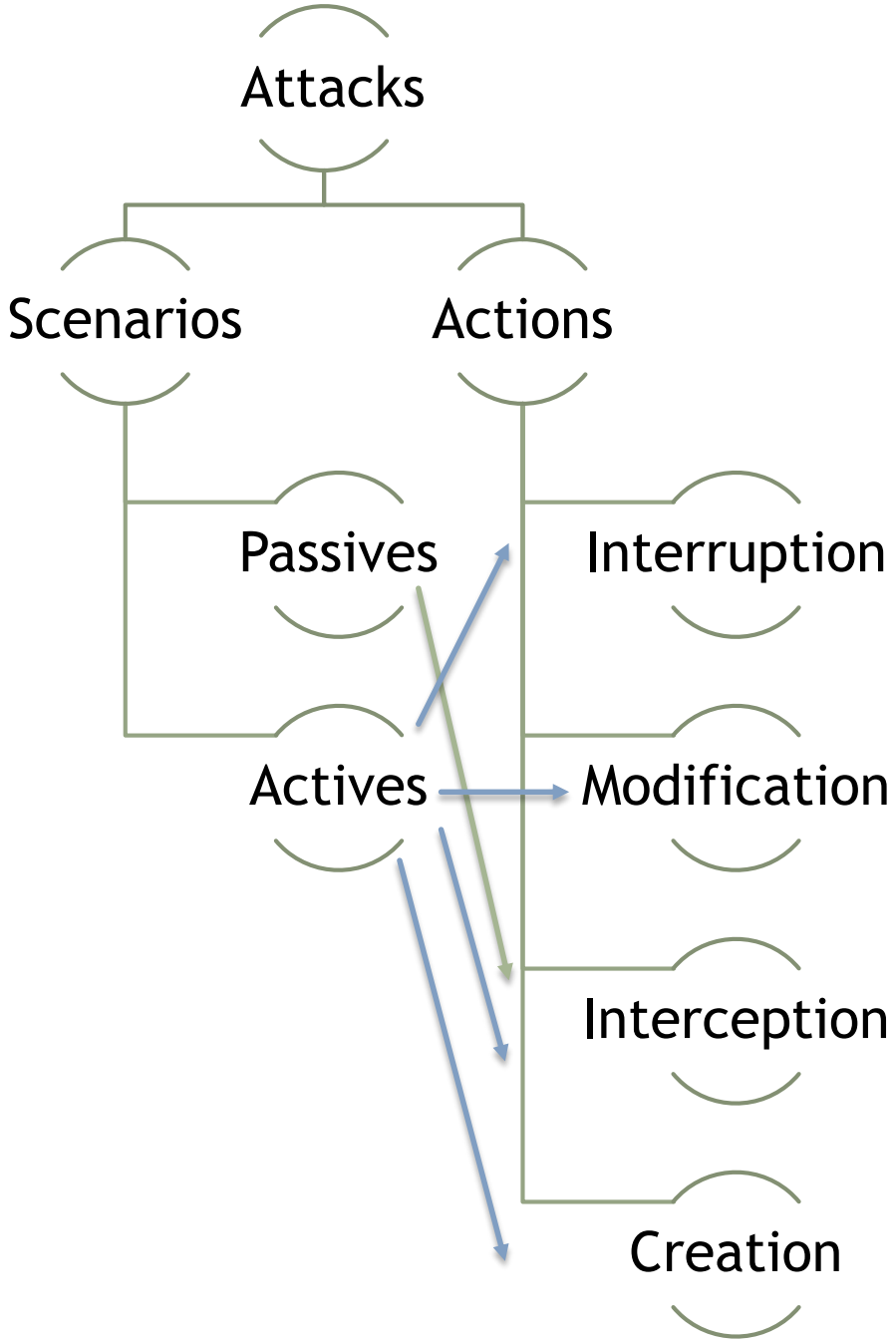
Passive attacks:

- The intruder intercepts the messages were transmitted, but without any action being taken.
- The aim of this threat is to break the *confidentiality* messages, therefore, sensitive information reaches a person other than its legitimate recipient.

Attack scenarios

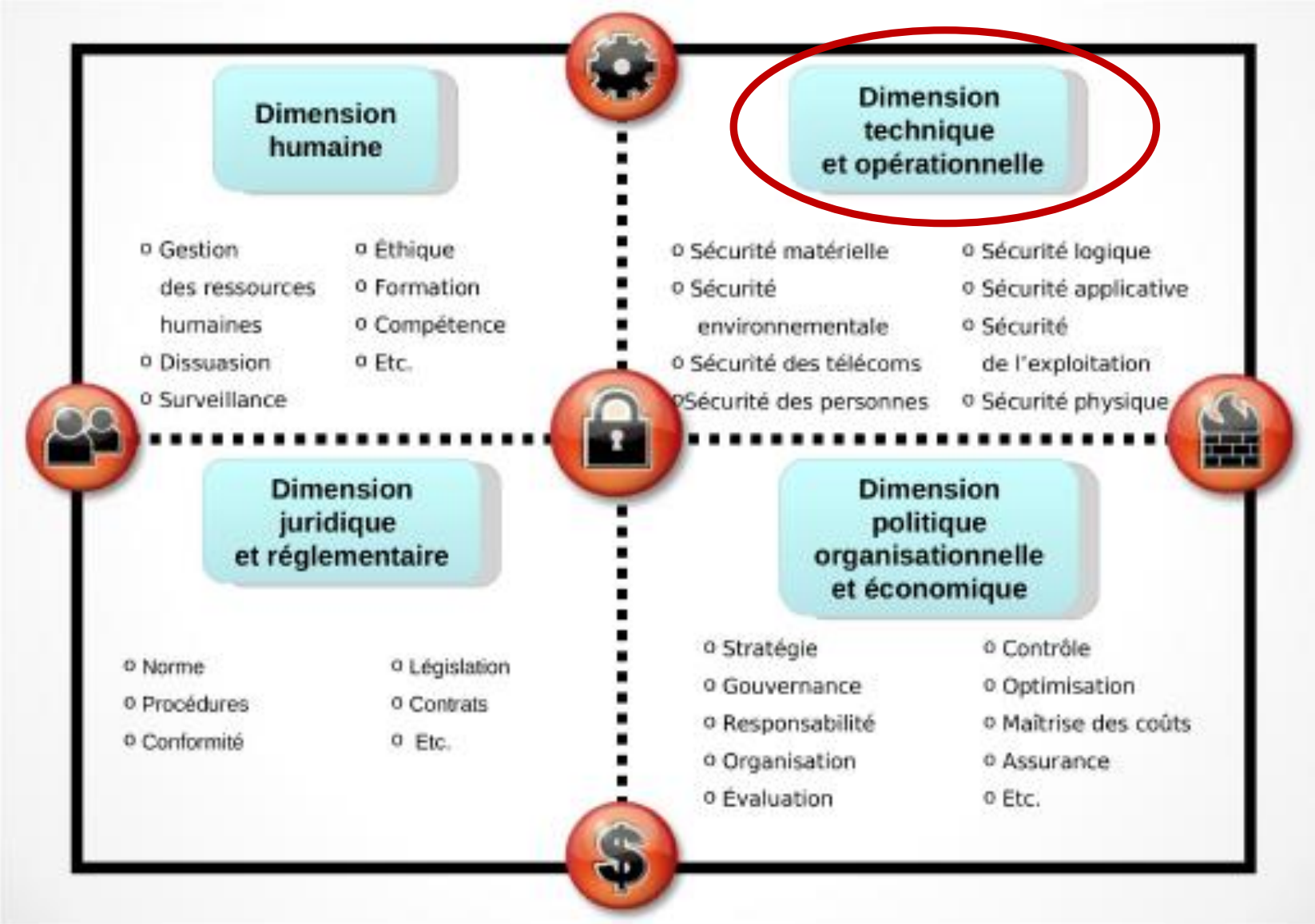
Active attacks:

- the threat is made by a intervention in a communication channel between communicating entities.
- The goal of this threat is to break *integrity*, *there availability*, *and authenticity*.


Attacks
Scenarios
Actions
Passives
Actives
Interruption
Modification
Interception
Creation

Course outline

- Senior Generals
- Security properties
- Classification of attacks
- Technical aspects of security


Dimension humaine
Gestion des ressources humaines
Dissuasion
Surveillance
Éthique
Formation
Compétence
Etc.
Dimension technique et opérationnelle
Sécurité matérielle
Sécurité environnementale
Sécurité des télécoms
Sécurité des personnes
Sécurité logique
Sécurité applicative
Sécurité de l'exploitation
Sécurité physique
Dimension juridique et réglementaire
Norme
Procédures
Conformité
Législation
Contrats
Etc.
Dimension politique organisationnelle et économique
Stratégie
Gouvernance
Responsabilité
Organisation
Evaluation
Contrôle
Optimisation
Maîtrise des coûts
Assurance
Etc.

Technical aspects of security

- Physical security
- Logical Security
- Application Security
- Operational Security
- Information security
- Network security

Technical aspects of security

- **Physical security:**
- We must give importance to securing the material computer science and the environment where he operates to avoid risks.
- The main risks are:
  - fire, dust, power surge, water, theft, local intrusion, etc.

Technical aspects of security

- **Logical security:**

Logical security is provided by core software, the operating system, and system administrators.

- Its aim is to:
  - To ensure security services and in particular, confidentiality, integrity and authentication using cryptographic mechanisms.
  - Using software engineering science to test the security and evaluate the quality of software developments,
  - Perform various procedures: intrusion and malicious application detection and logical access control.

Technical aspects of security

- **Application security:**
- There are several types of applications such as: Web application, mobile application, management software, etc.
- Using these applications in different infrastructures requires good design of the application's source code, which is application security.

Technical aspects of security

- **Application security:**

Example: The guide to securing web applications OWASP

- It offers articles, methodologies, documentations, tools, source code, and technologies in the field of web application security.
- It provides training for developers, designers, architects, and business owners on the risks associated with the most common web application security vulnerabilities.

OWASP
The Open Web Application Security Project

Technical aspects of security

- **Operational security:** It addresses the following points:
  - IT infrastructure management;
  - configuration and update procedures;
  - incident management and resolution;
  - backup plan;
  - contingency plan;
  - test plan;
  - regular and, if possible, dynamic inventories;
  - analysis of log and accounting files;
  - maintenance contract management;

Technical aspects of security

- **Information security:**
- Information security is a science that studies the mechanisms protection of information transmitted via a communication medium between the various participants in order to protect the information against risks of threats.
- This discipline provides the tools and the means necessary to achieve the information sensitivity criteria, which are security objectives.

Technical aspects of security

- **Network security:**
- Most computer devices (PC, mobile, etc.) are interconnected via one or more networks (wired local network, Internet, Wi-Fi, etc.)
- The main reason for most attacks in the digital world is the weakness network security.
- To secure the network, we need to protect different layers of the OSI architecture.

Quiz

- Which of the following are not security properties?
  - Authentication
  - Confidentiality
  - Anonymity
  - Integrity
  - Traceability
- In a passive attack, the intruder can:
  - Interruption
  - Modification
  - Interception
  - Manufacturing