Cybersecurity

Alessio Marini, 2122855

Appunti presi durante il corso di **Cybersecurity** nell'anno **2025/2026** del professore Angelo Spognardi.
Gli appunti li scrivo principalmente per rendere il corso più comprensibile **a me** e anche per imparare il linguaggio Typst. Se li usate per studiare verificate sempre le informazioni 🙏🏻.

Contatti:

alem1105

marini.2122855@studenti.uniroma1.it

September 27, 2025

Indice

1. Definition of Cybersecurity

Definition by NIST (National Institute of Standards and Technology)

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.

1.1. A definition of Computer Security

Computer Security: Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system **assets** including hardware, software, firm-ware, and information being processed, stored, and communicated.

An asset is something important for the system.

1.2. Assets

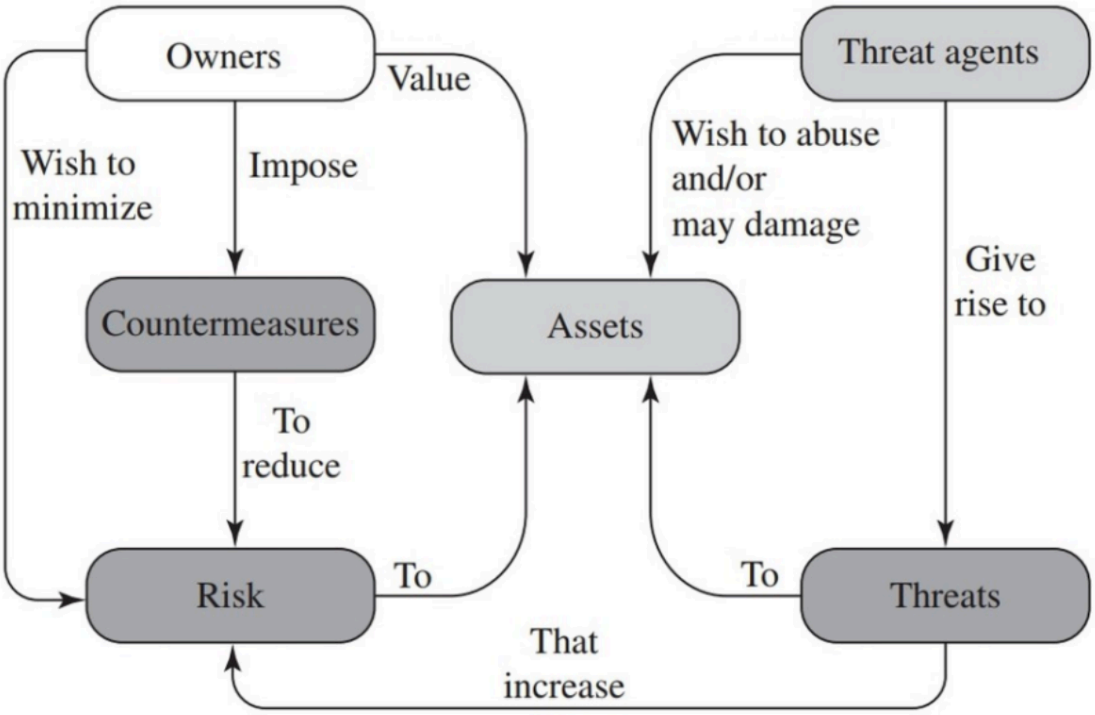
The asset is a key concept, the assets are important for a person or a company and need to be protected.

Some examples:
- Patient records
- Equipment
- Keys for net-banking

What should be protected?

- **Personal Data** of users like name, surname, email ecc...
- **Company Data** like financial data, internal information about products or personal data of the customers, partners ecc...

1.3. Security Concepts and Relationships



1.4. Threat Agent (Adversary)

Who conducts or has the intent ro conduct detrimental activities.

1.5. Countermeasure

A device or technique that ha as its objective the impairment adversarial activity.

1.6. Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event.

1.7. Threat

Any circumstance or event with the potential to adversely impact organizational operations.

1.8. Vulnerability

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

Observation about Security

The security of a system, application or protocol is relative to:

- A set of desidere properties
- An adversary with specific capabilities

For example the file access permissions in Linux or Windows are not effective against someone who can boot from a CD or USB drive.

1.9. Threats

There are different type of threats.

- **Active Attack**: An attempt to alter system resources or affect their operation. Some example:
  - Replay
  - Masquerade
  - Modification on Messages
  - Denial of Service
- **Passive Attack**: An attempt to learn or make use of information from the system that does not affect

system resources. For example an adversary could steal some information for use them in the future in a new attack.

- **Inside Attack**: Initiated by an entity inside the security perimeter (an "insider"). The insider is

authorized to access system resources but uses them in a way not approved by those who granted the authorization.

- **Outside Attack**: Initiated from outside the perimeter, by an unauthorized or ille-gitimate user of the

system (an "outsider"). On the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

2. Security Goals

There are 3 foundamental concepts in security, **C.I.A.**:

- **Confidentiality**
- **Integrity**
- **Availability**

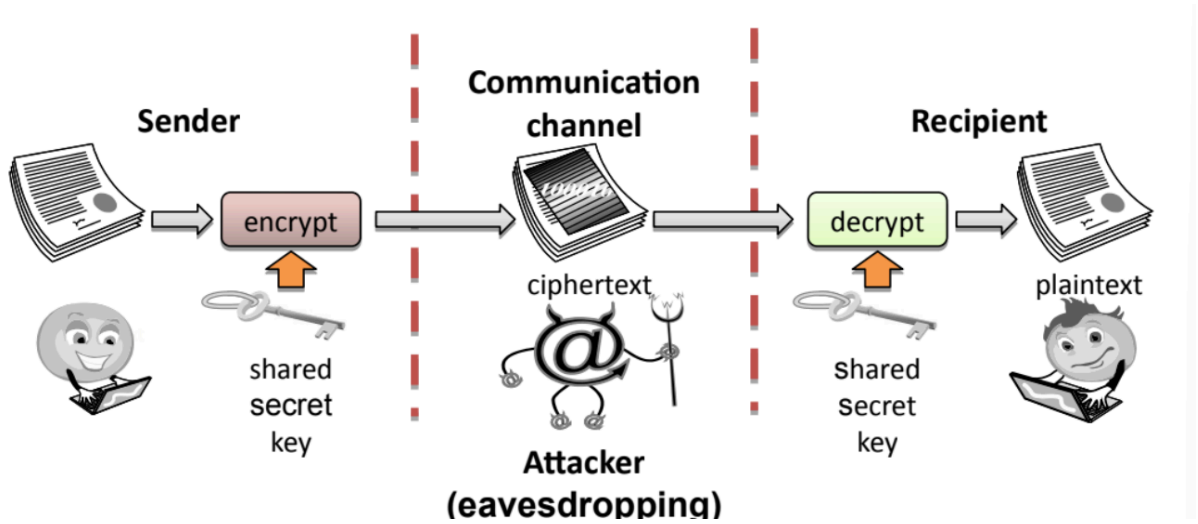
2.1. Confidentiality

The avoidance of the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others.

Let's look some **tools for confidentiality**

2.1.1. Encryption

The transformation of information using a secret, called an **encryption key**, so that the transformed information can only be read using another secret, called the **decryption key** (which may, in some cases, be the same as the encryption key).



2.1.2. Access Control

Rules and policies that limit access to confidential information to those people and/or systems with a "need to know."

For example we can grant this «need to know» with a device, a password, a role ecc...

2.1.3. Authentication

The determination of the identity or role that someone has. This determination can be done in a number of different ways:

- An object
- A password
- Fingerprint

2.1.4. Authorization

The determination if a person or system is allowed access to resources, based on an **access control policy**.

2.1.5. Physical Security

The establishment of physical barriers to limit access to protected computational resources.

2.2. Integrity

The property that something has not be altered in an unauthorized way. Some tools for integrity:

- **Backups**: Periodic archiving of data.
- **Checksums**: The computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
- **Data correcting codes**: Methods for storing data in such a way that small changes can be easily detected and automatically corrected.

2.3. Availability

The property that something is accessible and modifiable in a timely fashion by those authorized to do so.

Some tools for the availability:

- **Physical Protections**: Infrastructure meant to keep information available

even in the event of physical challenges.

- **Computational redundancies**: Computers and storage devices that serve as

fallbacks in the case of failures.

2.4. Other Security Concepts

Some other important concepts are **Authenticity, Accountability e Anonymity**.

2.4.1. Authenticity

Is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine.

An example of tool for authenticity could be **digital signature**

2.4.2. Accountability