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. Definizione di Cybersecurity . . . 3
   1.1. Cosa dovrebbe essere protetto? . . . 3
   1.2. Assets . . . 3
   1.3. Security Concepts e Relazioni . . . 4
   1.4. Threats . . . 4
2. Security Goals . . . 6
   2.1. Confidentiality . . . 6
      2.1.1. Encryption . . . 6
      2.1.2. Access Control . . . 6
      2.1.3. Authentication . . . 6
      2.1.4. Authorization . . . 7
      2.1.5. Physical Security . . . 7
   2.2. Integrity . . . 7
   2.3. Availability . . . 7
   2.4. Other Security Concepts . . . 7
      2.4.1. Authenticity . . . 7
      2.4.2. Accountability . . . 7

1. Definizione di Cybersecurity

Definizione secondo il NIST (National Institute of Standards and Technology)

La prevenzione di danni, la protezione e il ripristino di computers, servizi di comunicazione, sia cablati che wireless e tutte le informazioni che trasportano al fine di garantire la loro disponibilità, integrità, autenticità e confidenzialità.

Mentre una definizione di **Computer Security** potrebbe essere: *Misure e controlli che garantiscono la confidenzialità, l'integrità e la disponibilità di **assets** che includono hardware, software, firm-ware e tutte le informazioni che vengono processate, salvate e comunicate.*

Per **asset** intendiamo quello che è importante per un sistema ovvero quello che vuole proteggere.

1.1. Cosa dovrebbe essere protetto?

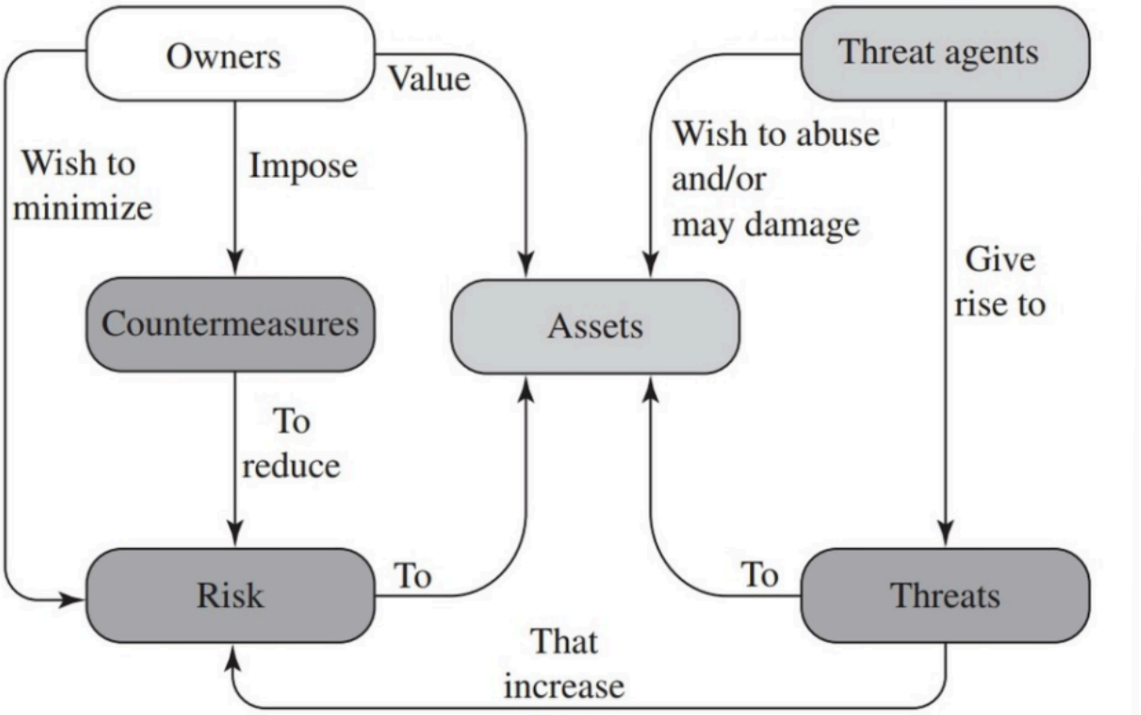
- Dati Personali
  - Nel nostro sistema cosa intendiamo per dati personali? Nome, Cognome, Email?
  - A che cosa servono questi dati nel sistema?
  - Chi può vedere questi dati?
  - Come ci assicuriamo che possano vederli soltanto le persone scelte?
- Dati dell'Azienda?
  - Dati Finanziari
  - Informazioni riservate riguardo a prodotti dell'Azienda
  - Dati personali dei dipendenti
  - Informazioni sull'infrastruttura di rete dell'Azienda

1.2. Assets

Per assets intediamo cosa è importante per una persona o azienda o in generale il sistema che dobbiamo rendere sicuro.

Ad esempio per un computer gli assets principali sono:
- Hardware
- Software
- Dati
- Comunicazioni e Reti

1.3. Security Concepts e Relazioni



- Per il proprietario sono importanti gli **assets**, vuole minimizzare i rischi su quest'ultimi e quindi impone delle **contromisure** per ridurli.
- Gli attacanti vogliono danneggiare o rubare gli assets.

Vediamo i principali termini:

- **Threat Agent (Attacante)**: Chi fa o ha intenzione di svolgere attacchi
- **Countermeasure**: Un dispositivo o una tecnica di difesa
- **Risk**: Una situazione che mette a rischio un elemento del sistema
- **Threat**: Qualsiasi situazione o evento che potrebbe influenzare il sistema
- **Vulnerability**: Una debolezza nel sistema, può apparire in molte forme, ad esempio nel codice, nel personale, in qualche procedura ecc...

Osservazione sulla Sicurezza

La sicurezza di un sistema, applicazione o altro è sempre relativa a:

- Un insieme di proprietà
- Un avversario con delle abilità specifiche

Ad esempio, i permessi di accesso ai file su Linux o Windows non avranno effetto su un attaccante che accede al sistema tramite un CD.

1.4. Threats

Per quanto riguarda le minacce, ci sono diversi tipi di attacchi:

- **Active Attack**: Un attacco che vuole alterare le risorse del sistema o influire sulle sue operazioni. Ne esistono di diversi tipi:

    - Replay
    - Masquerade
    - Modification on Messages
    - Denial of Service
- **Passive Attack**: Un attacco che mira a sfruttare le informazioni contenute in un sistema senza danneggiarlo. L'obiettivo è quindi quello di rubare informazioni per renderle pubbliche o ricattare oppure anche analizzare il sistema per un attacco futuro.
- **Inside Attack**: Un attacco iniziato da qualcuno all'interno del sistema, di solito quest'ultimo ha dei permessi nel sistema ma non completi.
- **Outside Attack**: Un attacco che inizia dall'esterno del sistema da una persona non autorizzata.

2. Security Goals

Esistono 3 concetti fondamentali da considerare che possiamo indicare con l'acronimo **C.I.A.**:

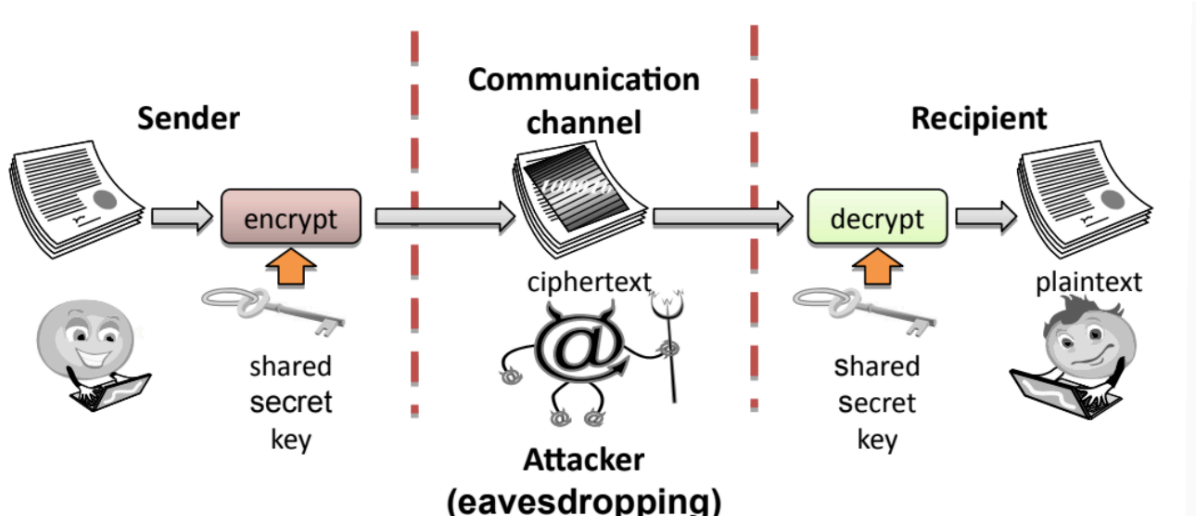
- **Confidentiality**
- **Integrity**
- **Availability**

2.1. Confidentiality

Evitare che dei non autorizzati accedano a delle informazioni riservate, per garantirla eistono diversi strumenti.

2.1.1. Encryption

Modificare le informazioni con dei **secret**, chiamati **encryption key**, in modo che diventino leggibili soltanto per chi ha un altro **secret** ovvero la **decryption key**. In alcuni casi le key combaciano mentre in altri no.



2.1.2. Access Control

Sono delle regole che servono a determinare quali persone possono accedere a determinate informazioni o servizi.

Ad esempio possiamo garantire l'accesso ad una stanza soltanto ad un determinato gruppo di dipendenti.

2.1.3. Authentication

Identificare qualcuno e quali permessi ha, l'identificazione può avvenire in diversi modi, ad esempio:

- Un oggetto (tessere elettroniche, chiavi, ecc...)
- Password
- Impronta digitale, retina ecc...

2.1.4. Authorization

Determina se una persona autenticata può accedere a delle risorse, basandosi sulle regole dell'**accesso control**. Questa dovrebbe servire a prevenire il tentativo di «imbrogliare» il sistema da parte di attaccanti.

2.1.5. Physical Security

Delle barriere fisiche per non permettere l'accesso a delle zone protette, ad esempio le stanze dove ci sono i server con informazioni importanti.

2.2. Integrity

Le informazioni non devono essere alterate senza permesso. Possiamo provare a garantirla con diversi strumenti:

- **Backups**: Degli «snapshot» di tutti i dati archiviati
- **Checksums**: Il risultato di un'operazione che mappa il contenuto di un file in un valore numerico. Queste sono fatte in modo che anche un piccolo cambiamento nel file cambi il risultato finale, in questo modo è molto rato che due file diversi abbiano lo stesso risultato.
- **Data correcting codes**: Sono dei metodi di mantenimento dei dati che rilevano anche dei piccoli cambiamenti e li correggono in automatico.

2.3. Availability

I servizi offerti e le informazioni accessibili da chi ha il permesso di farlo devono essere sempre disponibili. Proviamo a garantirla con:

- **Physical Protections**:
- **Computational redundancies**: Computer o dischi che servono come «fallback» nel caso di errori nei dispositivi principali.

2.4. Other Security Concepts

Altri concetti importanti nella sicurezza informatica sono: **Authenticity, Accountability e Anonymity**.

2.4.1. Authenticity

Dobbiamo essere in grado di capire che un sistema, una persona o in generale qualcosa o qualcuno sia affidabile.

Uno strumento semplice come esempio è la firma o **digital signature**

2.4.2. Accountability