UNIVERSITÀ DEGLI STUDI
DI GENOVA

Università degli Studi di Genova

Computer Security

Lorenzo Vaccarecci

2024-2025

Indice

Capitolo 1

Introduzione

1.1 Information Security

- La sicurezza concerne la protezione degli **asset** dalle **minacce (threats)**
- I proprietari (**owners**) valorizzano i loro asset e vogliono proteggerli
- I proprietari analizzano le minacce e valutano i rischi. Questo aiuta la selezione di **contromisure** che riducono le **vulnerabilità**

$$Risk_E = P(E) \cdot I_E$$

Dove E è l'evento che rappresenta la minaccia, $P(E)$ è la probabilità che l'evento si verifichi e I_E è l'impatto che l'evento ha.

$$Risk_{Tot} = \sum_{e \in E} (P(e) \cdot I_e)$$

$P(\cdot)$ può essere:

- 0.7 - 1 : Alta
- 0.4 - 0.7 : Media
- ≤ 0.3 : Bassa

1.2 Security Properties

- Confidentiality: l'informazione non è conosciuta da non autorizzati, bisogna permettere solo a chi ne ha diritto attraverso **security policies**. Qualche volta si dice **privacy** per gli individui, **secrecy** per le organizzazioni, **anonymity** invece per nascondere l'identità.
- Integrity: l'informazione non deve essere modificata in modo malizioso.
- Authentication: i dati o i servizi devono essere accessibili solo da chi autorizzato. Solitamente il metodo di autenticazione è qualcosa che si ha, qualcosa che si conosce o qualcosa che sei (impronta digitale, firma, biometrica).
- Availability: i dati o i servizi devono esere accessibili e utilizzabili in qualsiasi momento. Questo significa che bisogna prevenire da attacchi DoS (**Denial of Service**)
- Accountability: le azioni sono registrare e rintracciabili dalle parti responsabili.

1.3 Protection Countermeasures

- Prevention: prevenire gli attacchi attraverso la progettazione di sistemi e impiegando tecnologie di sicurezza.
- Detection: i metodi principali sono il **logging** e il **MACs** (file hash per rilevare alterazioni).
- Response: varia dal ripristinare backup all'informare le autorità competenti o le parti coinvolte.
- Remediation

1.4 Managing security: implementing a solution

- Security Analysis: analizza le minacce che potrebbero compromettere l'asset e propone delle politiche e soluzioni a costi appropriati.
- Threat Model: documenta le possibile minacce al sistema, immaginando tutte le possibili vulnerabilità che possono essere sfruttate.
- Risk Assessment: valutazione quantitativa dei rischi.
- Security Policy: per ogni rischio si descrivono le contromisure da adottare.
- Security Solution: progettazione e implementazione delle tecnologie appropriate a costi appropriati.