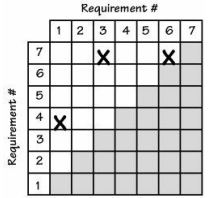
01. Introduzione alla Sicurezza (dell'informazione)

Sicurezza dell'Informazione

Domande principali

- Che cos'è un sistema sicuro?
- Che cos'è la sicurezza (dell'informazione)?
- Come si progettano sistemi sicuri?

Requisiti base di sicurezza



Il cosiddetto paradigma **CIA** (Confidentiality, Integrity, Availability) per la sicurezza dell'informazione stabilisce tre requisiti fondamentali:

- **Riservatezza (Confidentiality)**: l'informazione può essere accessibile solo a entità autorizzate.
- **Integrità (Integrity)**: l'informazione può essere modificata solo da entità autorizzate, e soltanto nei modi in cui tali entità sono autorizzate a farlo.
- **Disponibilità (Availability)**: l'informazione deve essere disponibile a tutte le parti che hanno diritto di accedervi, entro i limiti temporali specificati.

⚙️ "A" è in conflitto con "C" e "I": un problema di ingegneria.

La sicurezza come problema di ingegneria

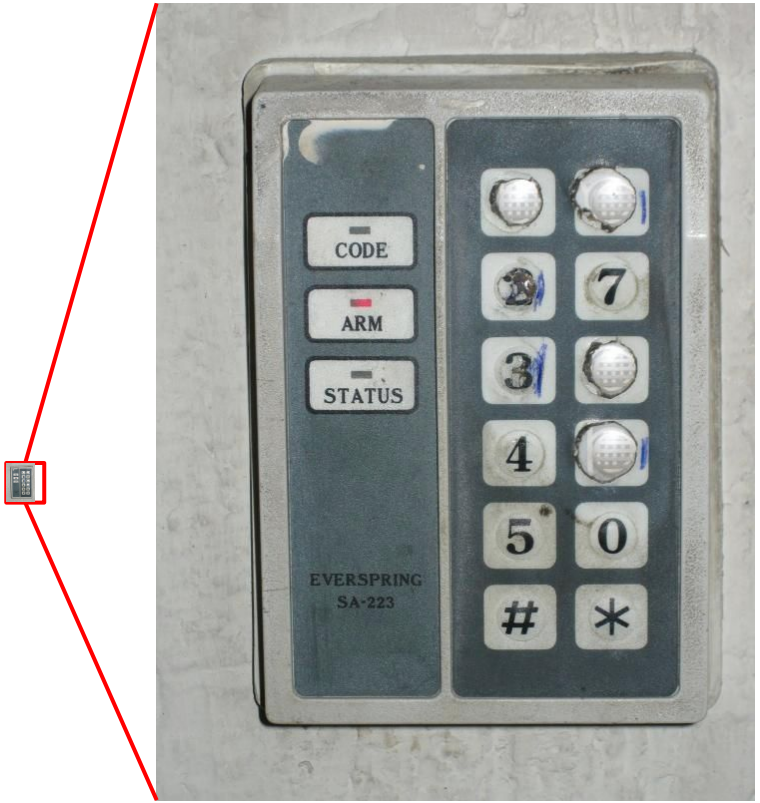
Abbiamo bisogno di alcuni concetti per inquadrarla:

- **Vulnerabilità**
- **Exploit**
  - Asset / Risorse
  - Minacce
  - Rischi

È SICURO?

PERCHÉ DA UN SENSO DI SICUREZZA?

Attenzione ai dettagli (1/2)



Attenzione ai dettagli (2/2)

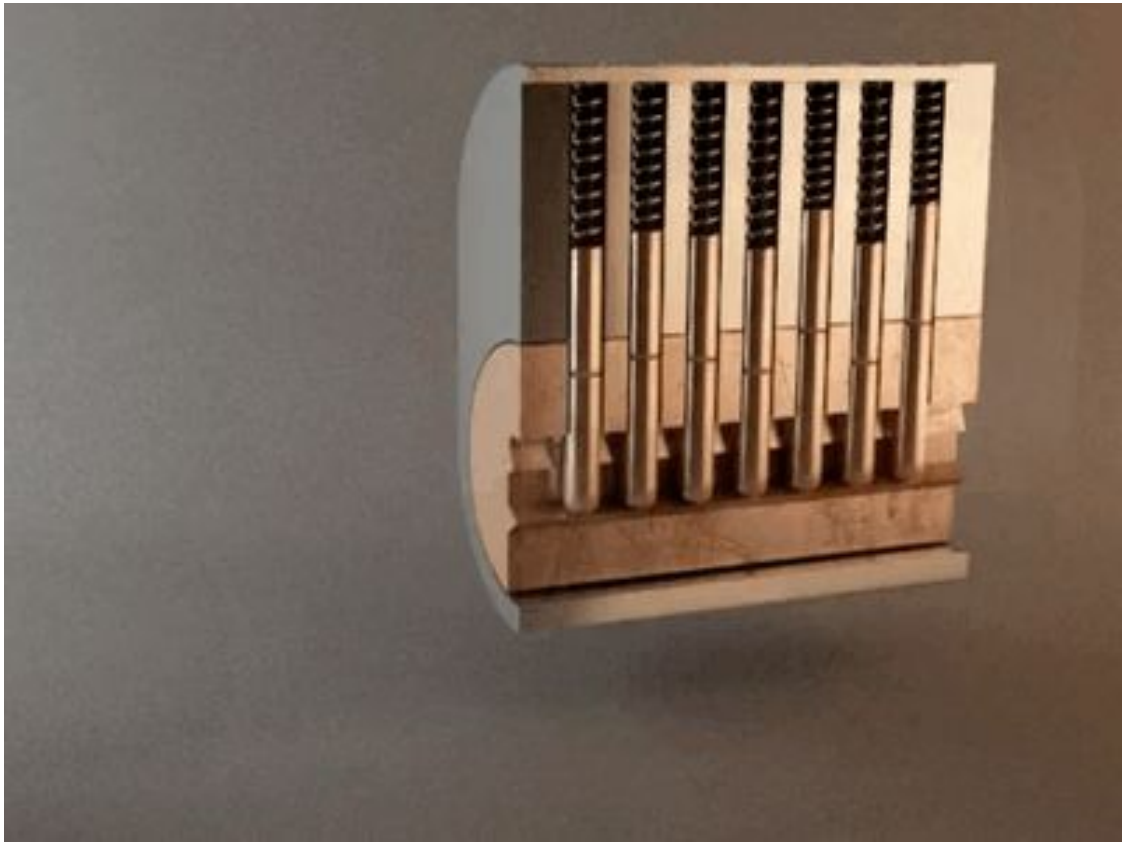
Una porta di un aeroporto

Vulnerabilità *vs.* **Exploit**

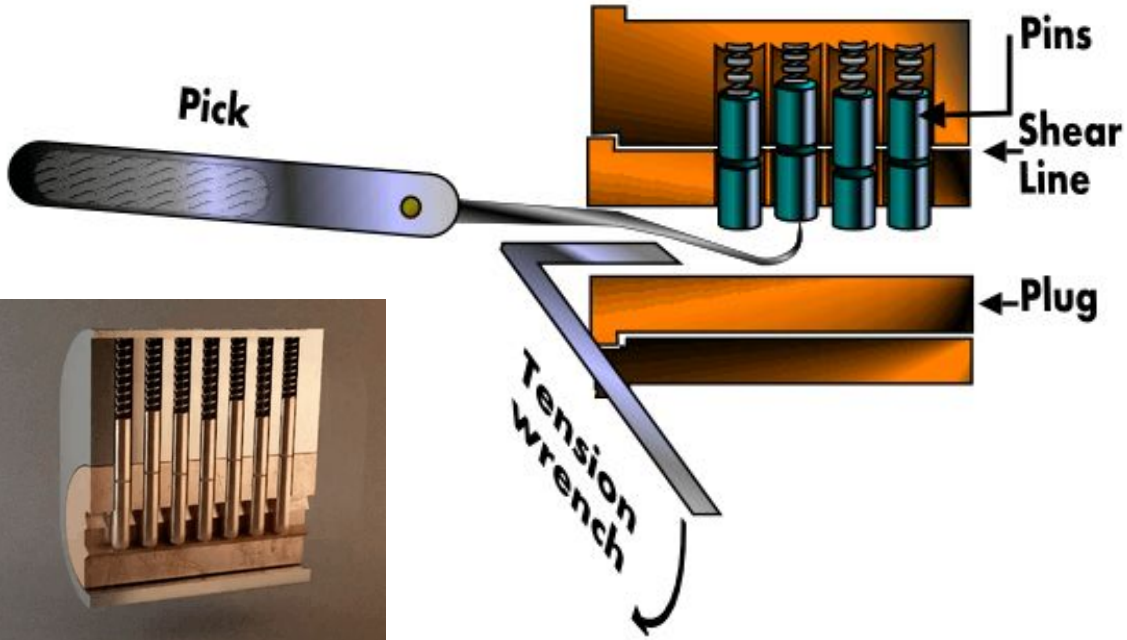
Vulnerabilità: qualcosa che consente di violare uno dei vincoli del paradigma CIA.

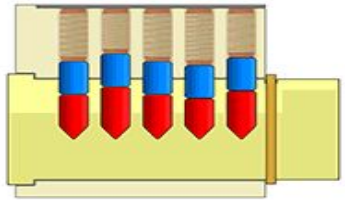
Exploit: un modo specifico di utilizzare una o più vulnerabilità per raggiungere un obiettivo specifico che viola tali vincoli.

Come funziona un lucchetto

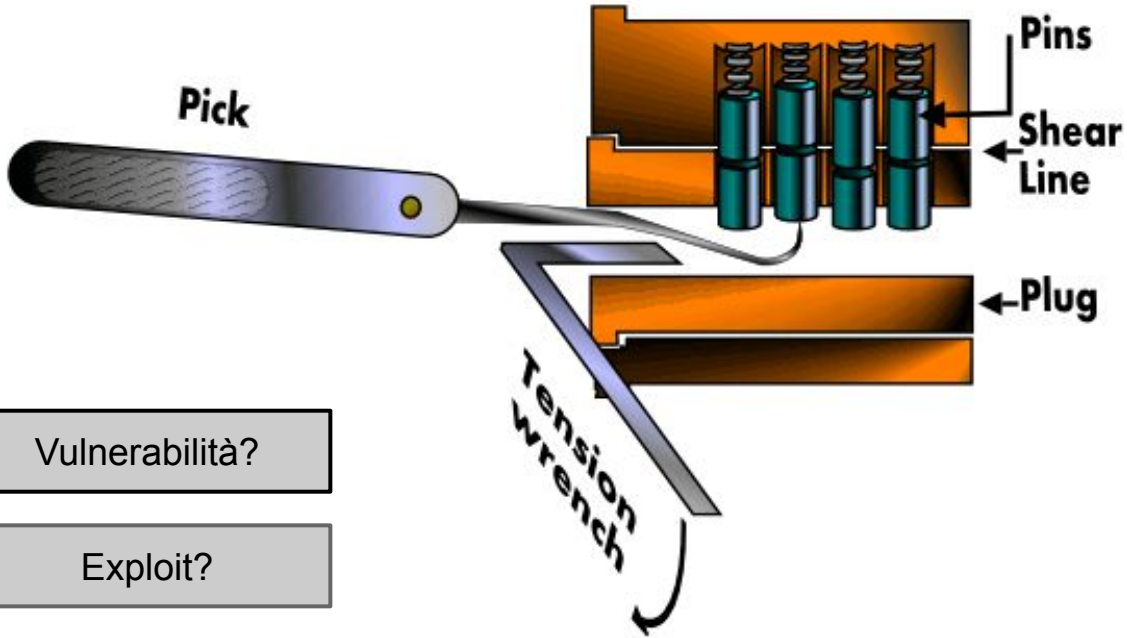


Exploitation di un lucchetto



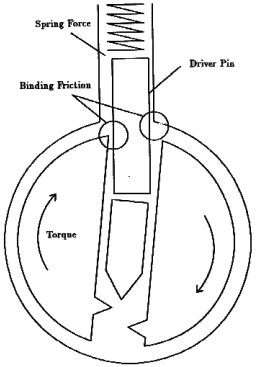


Exploitation di un lucchetto

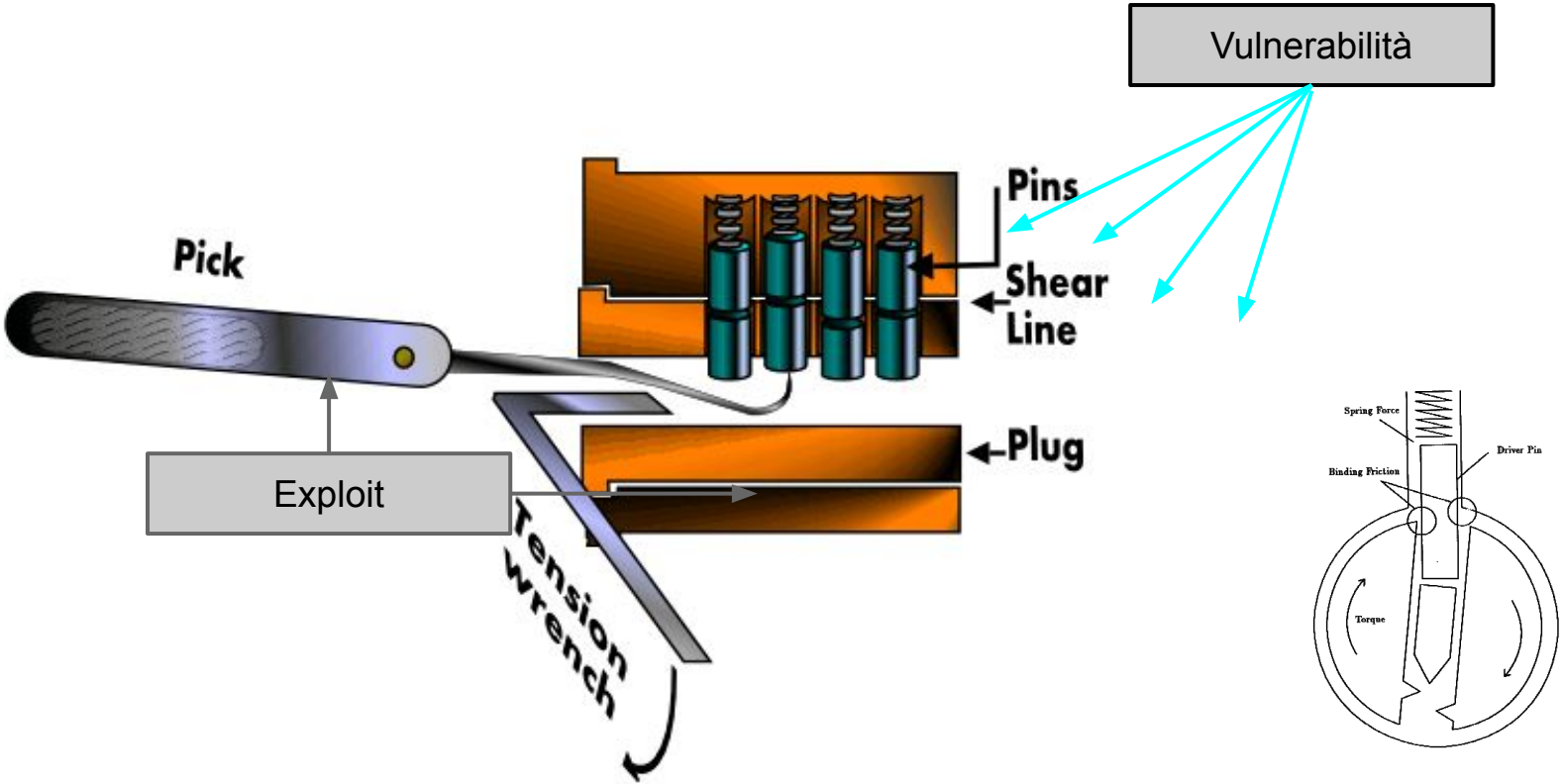


Vulnerabilità?

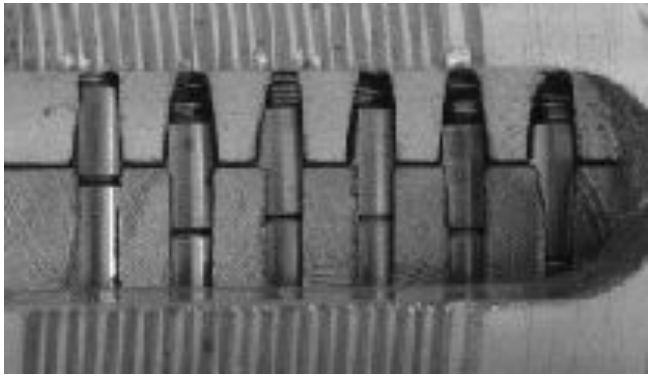
Exploit?

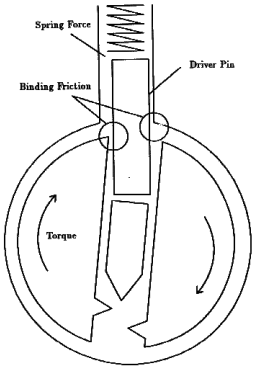


Exploitation di un lucchetto



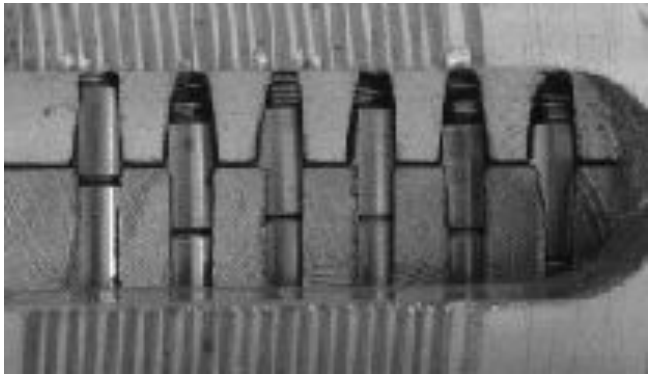
Possibili soluzioni

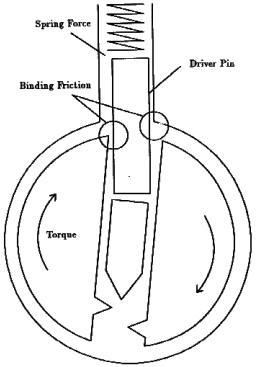




Come possiamo risolvere questa vulnerabilità?

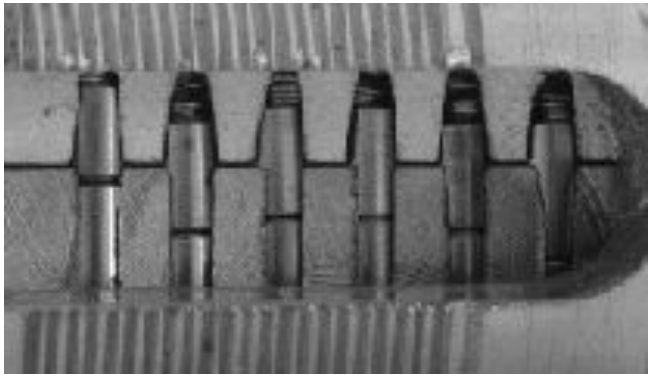
Possibili soluzioni

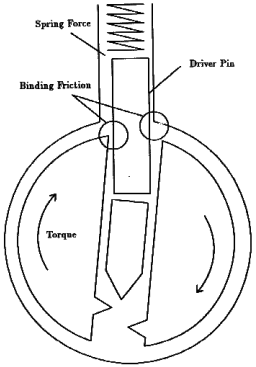


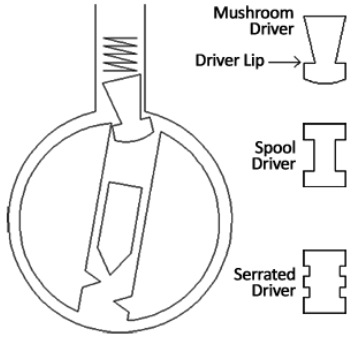


In generale non possiamo eliminare completamente la vulnerabilità… Possiamo rendere l'exploit più difficile!!!

Possibili soluzioni







In generale non possiamo eliminare completamente la vulnerabilità… Possiamo rendere l'exploit più difficile!!!

Un lucchetto migliore:

- Più pin
- Pin che complicano la rotazione del cilindro
- Nessun riscontro per l'attaccante sulla correttezza della posizione di ciascun perno.
- Meno margine per sperimentare con i movimenti.
- …

Forse è meglio cambiarlo!

Vedete dei problemi?

Vulnerabilità *vs.* **Exploit**

Vulnerabilità: qualcosa che consente di violare uno dei vincoli del paradigma CIA.

Esempi:

- Software che non controlla il codice nei PDF.
- **Disallineamenti meccanici dei pin in serrature fisiche**

Exploit: un modo specifico di utilizzare una o più vulnerabilità per raggiungere un obiettivo specifico che viola tali vincoli.

Esempi:

- Un PDF malevolo che manda e-mail per conto di chi lo apre
- **Grimaldelli e tecniche di scasso**

La sicurezza come problema di ingegneria

Abbiamo bisogno di alcuni concetti per inquadrarla:

- Vulnerabilità
- Exploit
- **Asset / Risorse**
- **Minacce**
- Rischi

Sicurezza =! Protezione

Dà un senso di sicurezza?

Dà un senso di sicurezza?

"The Cheyenne Mountain nuclear bunker is a Cold War hardened installation with **North American Aerospace Defense Command (NORAD) centers** and associated computer systems [...]"
http://en.wikipedia.org/wiki/Cheyenne_Mountain_nuclear_bunker

Asset & Minacce

Asset (Risorse): identifica ciò che è di valore per un'organizzazione.

In questo corso, ci concentriamo sugli asset IT.

Esempi:

- Hardware (es. laptop, computer, telefoni)
- Software (es. applicazioni, sistema operativo, database)
- Dati (es. dati memorizzati in un database)
- Reputazione (pensate ai social media)

Minacce: potenziale violazione della CIA (Confidenzialità, Integrità, Disponibilità); circostanze che possono causare una violazione della CIA.

Esempi:

- Denial of service (DoS): ad esempio software o hardware non disponibili
- Furto d'identità: ad esempio accesso non autorizzato a software o dati
- Fuga di dati: ad esempio rilascio non autorizzato di informazioni

Attacchi & Attori malevoli

Attacco: uso intenzionale di uno o più exploit con l'obiettivo di compromettere la riservatezza, l'integrità o la disponibilità (CIA) di un sistema.

Esempi:

- Allegare un file PDF "malevolo" a un'e-mail
- Forzare una serratura per entrare in un edificio

Attori malevoli: chi o ciò che può causare il verificarsi di un attacco.

Esempi:

- Individuo malevolo che allega un exploit in un e-mail sotto forma di PDF
- Ladro che tenta di entrare in un edificio

Attaccanti, Hacker, Pirati informatici …

I mass media hanno creato falsi miti e controversie intorno a queste e ad altre parole.

Attaccanti, Hacker, ...

I mass media hanno creato falsi miti e controversie intorno a queste e ad altre parole.

Hacker: una persona con una conoscenza avanzata dei computer e delle reti informatiche, e con la volontà di imparare “tutto”.

Black hats: Hacker malevoli.

Attaccanti != Hacker

Professionisti della sicurezza (white hats)

- Identificare vulnerabilità.
- Sviluppare metodi per il rilevamento degli attacchi.
- Sviluppare contromisure contro gli attacchi.
- Progettare soluzioni di sicurezza.

Elementi essenziali del bagaglio di competenze di un professionista della sicurezza (detto anche “hacker etico”).

La sicurezza come problema di ingegneria

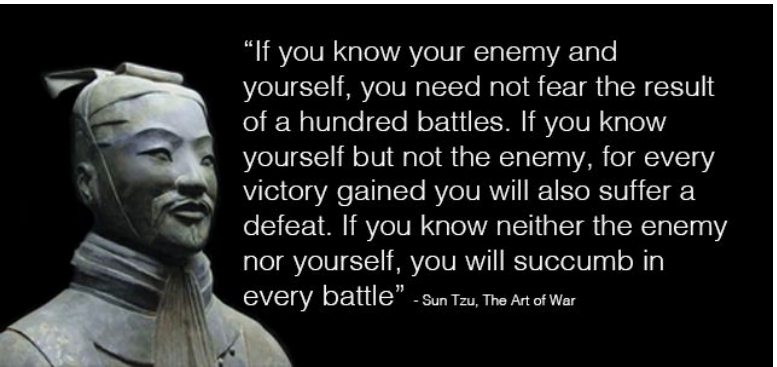
Abbiamo bisogno di alcuni concetti per inquadrarla:

- Vulnerabilità
- Exploit
- Asset / Risorse
- Minacce
- **Rischi**

La sicurezza come “gestione del rischio”

Rischio: valutazione statistica ed economica dell’esposizione a un danno dovuto alla presenza di vulnerabilità e minacce.

Rischio = Asset × Vulnerabilità × Minacce



La sicurezza come “gestione del rischio”

Rischio: valutazione statistica ed economica dell’esposizione a un danno dovuto alla presenza di vulnerabilità e minacce.

Variabili indipendenti

Rischio = Asset × Vulnerabilità × Minacce

Variabili controllabili

La sicurezza come “gestione del rischio”

Rischio: valutazione statistica ed economica dell’esposizione a un danno dovuto alla presenza di vulnerabilità e minacce.

Variabili indipendenti

$$\text{Rischio} = \underline{\text{Asset} \times \text{Vulnerabilità}} \times \text{Minacce}$$

Variabili controllabili

Sicurezza: riduzione delle vulnerabilità e contenimento danni al prezzo di costi

Sicurezza *vs.* Bilancio costi

Costi diretti

- Gestione
- Operativo
- Apparati / Attrezzature

Costi indiretti (altrettanto importanti)

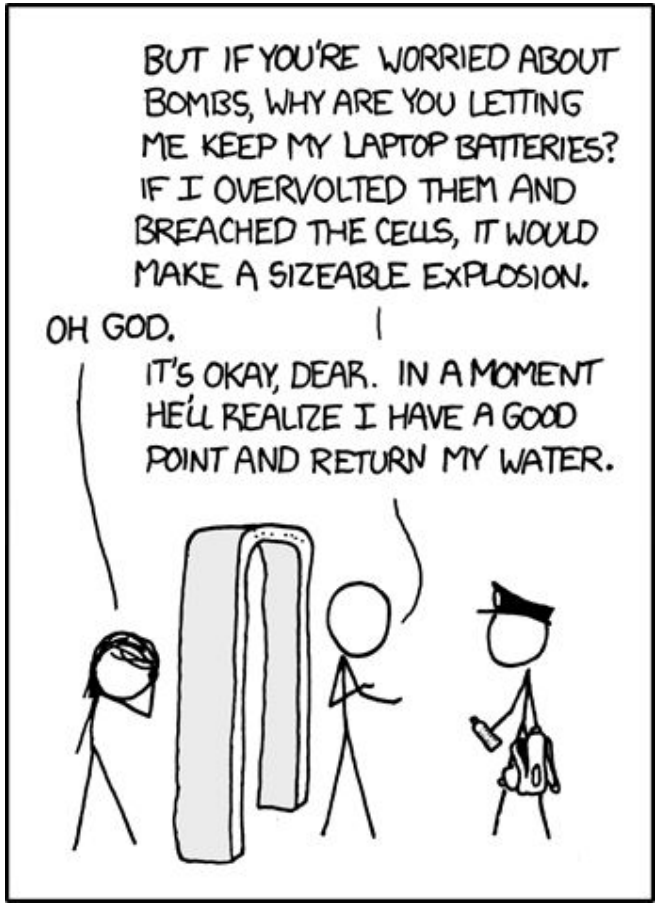
- Minore usabilità
- Basse performance
- Minore privacy (dovuta a controlli di sicurezza)
- Minore produttività (gli utenti sono più lenti)

Più soldi ⇏ Più sicurezza

Buttare più soldi sul problema non lo risolverà necessariamente

Esempi:

- Firewall molto costoso ma non configurato
  - Meglio non averlo
- Autenticazione complessa che rallenta gli utenti
  - Gli utenti scriveranno le password sui post-it
- Sicurezza aeroportuale
  - …


BUT IF YOU'RE WORRIED ABOUT BOMBS, WHY ARE YOU LETTING ME KEEP MY LAPTOP BATTERIES? IF I OVERVOLTED THEM AND BREACHED THE CELLS, IT WOULD MAKE A SIZEABLE EXPLOSION.
OH GOD.
IT'S OKAY, DEAR. IN A MOMENT HE'LL REALIZE I HAVE A GOOD POINT AND RETURN MY WATER.

Fiducia & Assunzioni

- Dobbiamo fissare dei confini.
- Parte del sistema sarà considerata sicura — elemento di fiducia.
  Esempi:
  - Possiamo fidarci dell'addetto alla sicurezza?
  - …del software che abbiamo appena installato?
  - …del nostro stesso codice?
  - …del compilatore?
  - …del BIOS?
  - …dell'hardware?
- Problema del tipo "uovo e gallina".

Conclusioni

La sicurezza è un complesso problema ingegneristico che consiste nell'equilibrare requisiti in conflitto.

Un sistema con poche vulnerabilità ma con un alto livello di minaccia può essere meno sicuro di un sistema con molte vulnerabilità ma con un basso livello di minaccia.

Attaccanti, hacker, pirati informatici, ... sono concetti molto distinti e non devono essere confusi.

La sicurezza ha un costo.