→ **Principio** → Un problema di sicurezza, o vulnerabilità, può essere inteso come → **Via Alternativa**

→ Basta toglieve un tassello e un attacco non funziona, ma ci sono troppe alternative (vie). Se voglio prevenire un attacco è difficile é uaroso.

→ **Informatica = = Complessità**

- Sistema operativo che si basa su infrastrutture (HW e SW)
- Applicazioni che si basa sul Sistema Operativo
- → Software, milioni di righe di codice

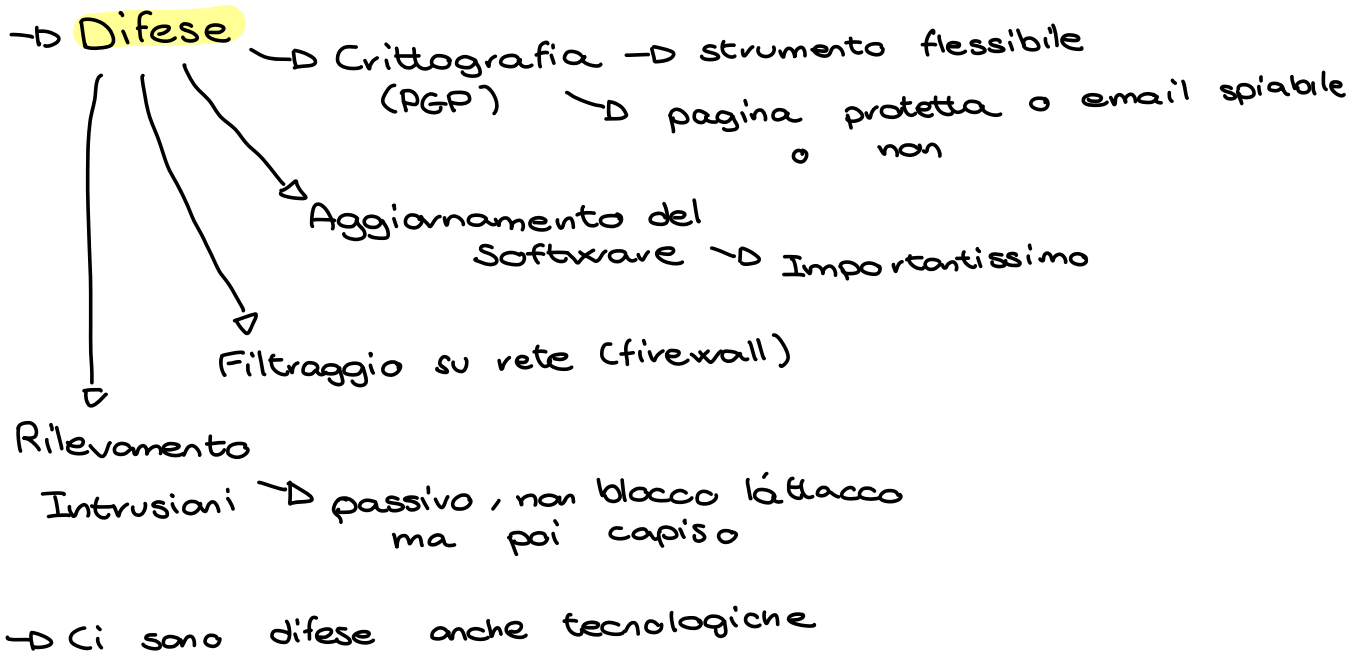
→ **Vulnerabilità** → difetto, predisposizione, non sempre è un attacco

→ **Exploit** → utilizzo del difetto, l'attaccante vuole un app. che sfrutti l'exploit

→ **Tipi di attacchi**

- → ricerca di errori nel Software
- → penetrazione tramite infrastrutture di rete (sequenza)
  - → spoofing, finge di essere una macchina
  - → intercettare i dati
- "**Social Engineering**" (attacco tramite la fiducia degli utenti)
  - → telefonate
  - → postIt
- **Preliminare**
  - → versioni
  - → Raccolta Info
- **DOS** (Denial of Service) → puramente negativo → Difficile da evitare

→ Ogni azione di sicurezza deve avere una valida motivazione → **Costo = benefici** → no paranoia!



→ Ci sono difese anche tecnologiche