Principii di Progettazione

- Panoramica
- Principii
  - Privilegio minimo
  - Fallimento "sicuro"
  - Economia dei meccanismi
  - Mediazione completa
  - Progettazione "aperta"
  - Separazione dei privilegi
  - Minimizzare i meccanismi condivisi
  - Accettabilità psicologica
  - Kerckhoffs

Panoramica

- Semplicità
  - Riduzione della complessità
  - Minori possibilità di inconsistenza
  - Facilità di comprensione
- Restrizioni
  - Minimizzare l'accesso
  - Inibire la comunicazione

Privilegio minimo

- Un soggetto dovrebbe ricevere solo quei privilegi necessari per completare il proprio task
  - Focalizzarsi sulle funzioni, non sull'identità
  - Diritti aggiunti quando servono, revocati qppena cessa la necessità d'uso
  - Dominio di protezione minimo

Fallimento "sicuro"

- L'azione di default è la negazione dell'accesso
- Se un'azione fallisce, il sistema deve essere sicuro come al momento dell'inizio dell'azione

Economia dei meccanismi

- Mantenere il meccanismo il più semplice possibile
  - KISS
- Più è semplice, meno cose possono andare male
  - In presenza di errori, è più facile individuarli e correggerli
- Interfacce ed interazioni

Mediazione completa

- La verifica delle credenziali va fatta ad ogni accesso
- Usualmente fatto al primo accesso
  - E.g.: in UNIX i diritti d'accesso verificati all'apertura di un file, ma non susseguentemente
- Se i diritti cambiano, si ha un accesso non autorizzato

Progettazione "aperta"

- La sicurezza non dovrebbe dipendere dalla segretezza del progetto o dall'implementazione
  - Da non Confondere con "open osurce"
  - "Security through obscurity" -sicurezza via segretezza (del progetto/implementazione)- fallisce
  - Non va applicato all'informazione (e.g. password o materiale crittografico)

Separazione dei privilegi

- Richiedere molteplici condizioni per assegnare i diritti
  - Separazione dei compiti
  - Difesa in profondità (onion-ring)

Minimizzare i meccanismi condivisi

- I meccanismi non dovrebbero essere condivisi
  - L'informazione può fluire via i canali condivisi
  - Canali coperti (subliminali)
- Isolamento
  - Macchine virtuali
  - Sandboxes

Accettabilità psicologica

- I meccanismi di sicurezza non dovrebbero creare difficoltà nell'accesso autorizzato alle risorse
  - Mascherare la complessità introdotta dal meccanismo di sicurezza
  - Facilità di installazione, configurazione ed uso
  - Criticità del fattore umano

Principio di Kerchoffs (1883)

- Si assume che tutti i dettagli implementativi dell'algoritmo di cifratura siano pubblici, (*come pure i protocolli*): solo la chiave è segreta.

Sommario

- I principii della progettazione sottendono tutti i meccanismi relativi alla sicurezza
- Richiedono:
  - Buona comprensione degli obiettivi perseguiti dai meccanismi e dell'ambiente in cui verranno calati
  - Accurata analisi e progettazione
  - Accurata implementazione