Criteri di valutazione di SW sicuro

Si tratta di criteri standardizzati che aiutano a valutare se un determinato SW sia sicuro o meno. I principali standard attualmente sono:

H1

- L'**orange book** (1985)
- Information Technology Security Evaluation Criteria (**ITSEC**)
- **Federal criteria**
- **Common Criteria**

Obiettivi e finalità

H3

Obiettivi

- Definire criteri e scale di valutazione per *misurare* prodotti e sistemi
- Definire *l'insieme di documenti e artefatti* in base ai quali fare la valutazione
- Definire una *metodologia* di valutazione

H4

Finalità

- Sensibilizzare sull'aspetto di **security** e **safety**
- Poter confrontare prodotti diversi
- Stabilire regole di valore internazionale

H4

Valutazione di prodotti e sistemi

Gli standard differenziano tra **prodotto** e **sistema**, stabilendo che un sistema è un insieme di prodotti.

H2

I prodotti vengono valutati secondo l'**orange book** e i **common criteria**, mentre i sistemi secondo l'**ITSEC**.

Parametri di valutazione

I parametri con cui gli standard valutano i SW sono i seguenti:

- **Politiche di sicurezza**
- **Etichettatura degli oggetti** (in base al livello di criticità)
- **Identificazione dei soggetti** (garantita mediante autenticazione)
- **Auditing**
- **Documentazione**
- **Affidabilità** (meccanismi che evitano il blocco dei sistemi)

Classi di valutazione

- **D** (***minimal protection***):
  no classi, no meccanismi di protezione
- **C** (***discretionary protection***):
  controllo di sicurezza *discrezionale*, eventualmente *autenticazione e auditing*
- **B** (***mandatory protection***):
  controllo obbligatorio
  - **B1**: politiche multilivello (Bell-Lapadula)
  - **B2**: vincoli per la protezione della memoria
  - **B3**: sistemi di prevenzione attacchi esterni e ripristino dopo anomalie
- **A** (***verified protection***):
  uso di *metodi formali* per la verifica di sicurezza

Limiti degli standard

Spesso gli standard sono limitati nella valutazione reale in quanto la sicurezza abbiamo visto essere una proprietà relativa al contesto, e non assoluta da poter attribuire a componenti o prodotti.