Certificazione di sistemi operativi sicuri

Lezione 22 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2007-8

Indice

certificazione e standard di valutazione

l'evoluzione storica degli standard di valutazione della sicurezza di sistemi informatici, dall'Orange Book agli attuali Common Criteria, può essere meglio compresa se, nel confronto dei diversi approcci, si tengono in conto i seguenti aspetti:

- **oggetto** della valutazione:
  - un **prodotto**, caratterizzato da requisiti di sicurezza **generici** (ad es. un sistema operativo)
  - un **sistema**, o collezione di prodotti assemblata per soddisfare **specifici** requisiti di sicurezza di un'applicazione
- **scopo** della valutazione
- **metodi** di valutazione, con particolare riguardo a
  - ripetibilità e riproducibilità dei risultati
  - valutazione di processo o di prodotto
- **ambito organizzativo** della certificazione
  - ad es., da agenzia pubblica o da organismi privati accreditati
- **struttura** dei criteri di valutazione

standard USA: TCSEC (Orange Book)

i **Trusted Computer System Evaluation Criteria** (US DoD, 1985):

- impiegano il modello di sicurezza Bell-LaPadula
- hanno per oggetto la TCB
- definiscono 7 classi di valutazione in 4 divisioni di livelli di fiducia, in ordine crescente di garanzia:
  - D < C1 < C2 < B1 < B2 < B3 < A1
- protezione di livello **D:** minima , **C:** DAC , **B:** MAC , **A:** verificata

i requisiti di ciascuna classe includono quelli della precedente, e riguardano:

- politica di sicurezza
- classificazione di sensibilità degli oggetti
- identificazione e autenticazione dei soggetti
- tracciabilità di eventi rilevanti alla sicurezza
- attendibilità operativa e di ciclo di vita delle garanzie di sicurezza
- documentazione delle funzionalità di protezione, di progetto e di collaudo
- protezione dei meccanismi di protezione

standard tedesco (Green Book)

gli **IT Security Criteria** (GISA, 1988):

- estendono l'ambito della protezione TCSEC a **integrità** e **disponibilità**
- a tal fine introducono nuove funzionalità di protezione, che assieme alle altre formano 10 classi di funzionalità
- separano ortogonalmente la valutazione delle **funzionalità** di protezione dal **livello di qualità** della garanzia offerta
  - sono definiti 8 livelli di qualità, che con le classi di funzionalità
  - generano 80 combinazioni possibili (non tutte significative)

fra le nuove funzionalità di protezione sono di particolare rilievo:

- ripristino dagli errori
- continuità del servizio
- sicurezza nella comunicazione dei dati

un merito specifico del metodo tedesco è il supporto alla certificazione da parte di agenzie commerciali e indipendenti

l'approccio inglese

una bozza pubblicata dal Department of Trade and Industry inglese nel 1989 propone un'innovazione radicale nella struttura degli standard di valutazione della sicurezza:

- si abbandona l'idea di predefinire le (classi di) funzionalità di protezione, per offrire invece un **linguaggio di dichiarazioni** atto a specificare tali funzionalità

permane la classificazione in livelli di valutazione della garanzia, analoga a quella degli standard predecessori e ortogonale alle dichiarazioni di funzionalità di protezione

struttura del linguaggio: modelli componibili di

- frasi per **azioni** e
- frasi per **obiettivi**
- dotate di **parametri**

l'approccio è motivato dalla rigidità delle classi di funzionalità predefinite, ma il vantaggio in generalità si paga con un maggior onere relativo alla definizione dei requisiti di sicurezza

- inoltre, la certificazione secondo questo approccio non può essere facilmente tradotta in analoga certificazione secondo gli altri standard di valutazione

standard europeo: ITSEC

l'emergere di altre iniziative di produzione di norme nazionali per la valutazione della sicurezza di sistemi informatici, verso la fine degli anni '80, poneva vari problemi di efficacia delle norme:

- confrontabilità dei criteri di valutazione
- trasferibilità della certificazione
- commerciabilità ed economicità della certificazione

queste ragioni spinsero la Commissione dell'UE a promuovere l'armonizzazione delle norme nazionali in un unico standard europeo: gli **IT Security Evaluation Criteria** (1991)

- conservano la classificazione ortogonale in classi di funzionalità e livelli di valutazione del Green Book
- tuttavia affidano allo **"sponsor della valutazione"** la specifica dell'obiettivo della valutazione (**Target of Evaluation, TOE**), assieme ad altre dichiarazioni di politica di sicurezza, funzionalità di protezione, etc., nell'idea dell'approccio inglese
- si applicano sia alla valutazione di **prodotti** che di **sistemi**, nel senso indicato sopra

successori di TCSEC e ITSEC: CFC, CC

in risposta all'evoluzione internazionale delle norme di valutazione, gli USA pubblicano nel 1992 i **Combined Federal Criteria**, meno rigidi dei TCSEC

i CFC accolgono idee da una bozza dello standard canadese, in particolare i concetti di

- **profilo di protezione**
- **obiettivo della protezione** (da non confondere con il TOE dell'ITSEC)

con i quali si demandano a utenti e produttori, rispettivamente:

- la specifica di requisiti di sicurezza
- la descrizione di come essi sono soddisfatti in un prodotto o sistema specifico

lo standard successivo, prodotto congiuntamente da USA, Canada ed Europa, mira all'unificazione mondiale dei criteri di valutazione; nei **Common Criteria** (1994):

- si rimpiazzano le classi di funzionalità ITSEC con i profili di protezione
- un **Security Target** definisce i requisiti di sicurezza per un TOE specifico, ad es. per riferimento a un dato profilo
- 7 livelli di garanzia della valutazione specificano compiti sia del produttore che del valutatore: per 4 di essi è riconosciuta la valutazione effettuata in altri paesi