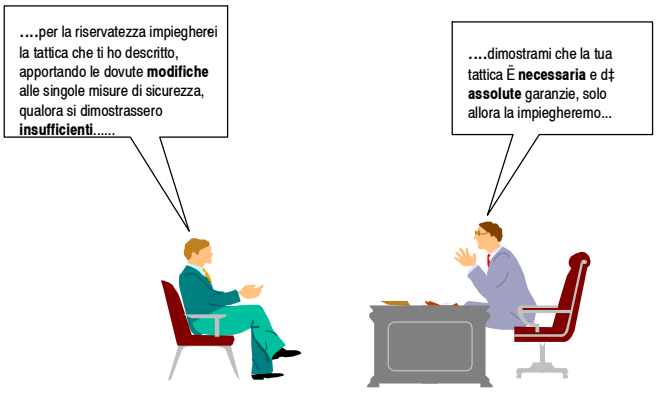
Introduzione ai criteri di valutazione della sicurezza IT

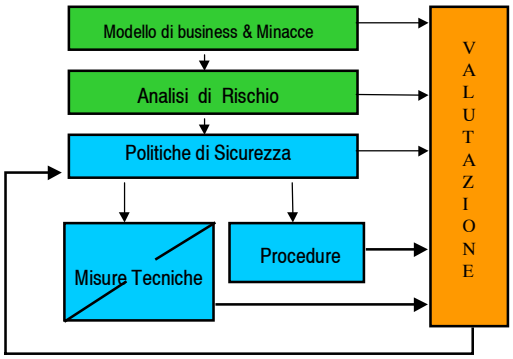
Milano 1 Dicembre 2000

Vittorio Asnaghi
IMQ - Sviluppo Servizi Informatica
vittorio.asnaghi@imq.it

Sicurezza: il problemaÖÖ...



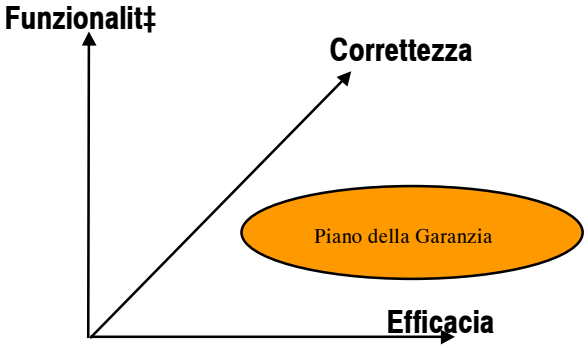
Approccio al problema



Sicurezza come...

- Riservatezza
  - ï Prevenzione dellíaccesso a informazioni da parte di non autorizzati
- Integrit‡
  - ï Prevenzione della modifica o distruzione di informazioni da parte di non autorizzati
- Disponibilit‡
  - ï Prevenzione dellíoccultamento di informazioni e dellíimpossÏbilit‡ di utilizzo delle risorse nei confronti di chi Ë autorizzato

Sicurezza comeÖ...



Funzionalit‡

- L'insieme delle caratteristiche afferenti alla sicurezza, presenti nel *servizio* svolto dal sistema o prodotto.
- In un sistema Ë la logica *applicazione* delle politiche di sicurezza tecnica.
- In diretta relazione con gli *obiettivi* di riservatezza, integrit‡, disponibilit‡.
- In pratica si realizza attraverso *misure tecniche* che contrastano le minacce.

Efficacia

- E' il grado in cui le misure tecniche contrastano le minacce da cui il sistema o prodotto si propone di difendersi.
- Quindi: non ha significato se non in relazione ad un ben determinato insieme di minacce.

Correttezza

- E' il grado di rispondenza dell'implementazione del prodotto o sistema ai requisiti espressi nelle funzionalit‡.
- Indipendente dall'efficacia e dalle minacce.
- Strettamente dipendente dalla Qualit‡ della realizzazione e quindi dalla bont‡ del processo che l'ha governata.

Criteri

- Evaluation Criteria: ITSEC (Information Technology Security Evaluation Criteria) - Europa 1991 (CEC DGXIII).
- Evaluation Criteria: ISO/IEC IS 15408 (Common Criteria) - Internazionali- 1999.
- *Evaluation Criteria: TCSEC (Trusted Computing Security Evaluation Criteria) - USA - 1985*.

LíOrange Book (TCSEC)

- Prima edizione 1983, commissionato dal DoD.
- 7 livelli di Garanzia/Funzionalit‡: D, C1, C2, B1, B2, B3, A1, in cui D significa nessuna garanzia, A1 massima garanzia e funzionalit‡.
- A livelli crescenti corrispondono funzionalit‡ crescenti e requisiti crescenti di correttezza ed efficacia.

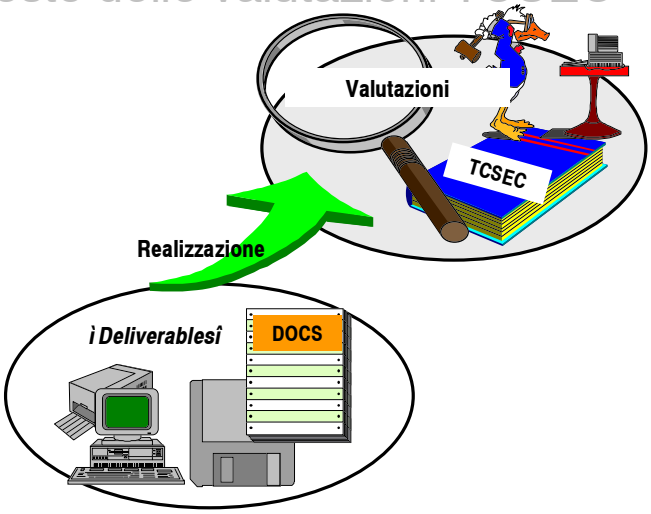
LíOrange Book (2)

- Requisiti funzionali crescenti
  - Es. C1: solo Discretionary Access Control.
  - Es. C2: aggiunta Object Reuse.
  - Es. B1: aggiunta:
    - Etichette
    - MAC - Mandatory Access Control
    - etc.
  - Es. B2: aggiunta:
    - Etichette sui device
    - Maggiori requisiti sul MAC
    - etc.

Orange Book (3)

- Rendicontazione
  - Es.: C1: solo Identificazione e Autenticazione.
  - Es. C2: aggiunta di funzionalit‡ di mnitoraggio (Audit). Funzionalit‡ di Audit via via pi˘ complesse per i livelli B1, B2, B3.
  - Es. B2: introduzione dei percorsi sicuri (Trusted Path).

Il contesto delle valutazioni TCSEC



I criteri ITSEC

- Nati da uníopera di armonizzazione dei criteri nazionali in UK, D, NL, F alla fine degli anni 80, come risposta alla difficile applicabilit‡ di TCSEC.
- Prima edizione 1990
- Ultima edizione 1991 (V 1.2).
- Manuale ITSEM 1993 (V1.0)

I criteri ITSEC (2)

- Definiscono solo modalit‡ per valutare la garanzia.
- La funzionalit‡ Ë di definizione esterna (non Ë stabilita dai criteri).
- Serve un documento esterno, diverso per ogni prodotto o sistema: il Security Target.

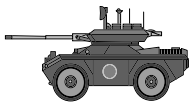
ITSEC - Il Security Target: i Livelli

- 7 Livelli di Garanzia: da E0 (nessuna Garanzia) a E6 (massima Garanzia).
  A ciascun livello compete un livello di rigore nel processo di sviluppo (deliverables) e un set di verifiche nell'operazione di valutazione.
- 3 Livelli di Robustezza dei meccanismi: basic, medium, high, determinati sulla base di:


tipologia attaccante


tempo


collusione


apparecchiature

Altri contenuti del Security Target

- líambito díuso del prodotto o del sistema
- gli obiettivi di sicurezza in relazione alle minacce
- le funzioni che li realizzano.

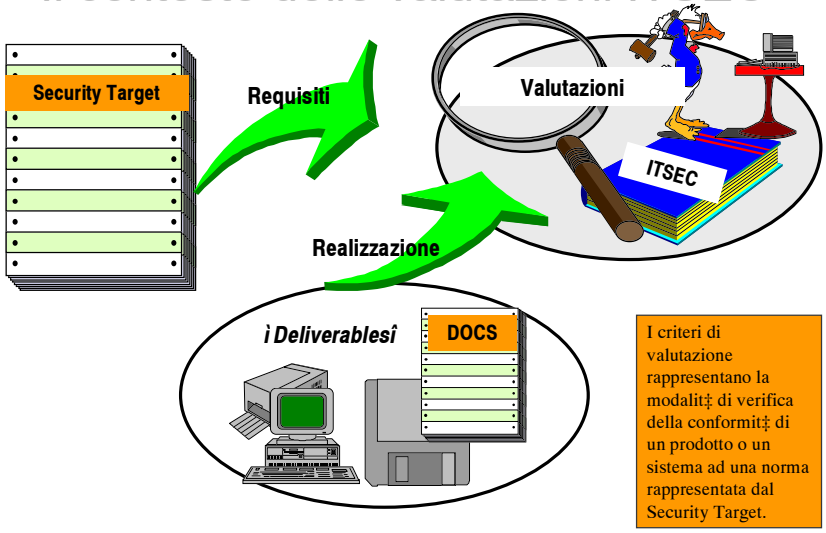
ITSEC - definizione delle funzioni: la classificazione

- Consigliato l'uso di uno schema per suddividere le funzionalit‡ (*generic headings*):
  - Identificazione e Autenticazione
  - Controllo dell'Accesso
  - Rendicontazione (Accountability)
  - Monitoraggio (Audit)
  - Riuso degli oggetti
  - Accuratezza
  - Affidabilit‡ del servizio
  - Scambio dei dati

Funzionalit‡ - classificazione (cont.)

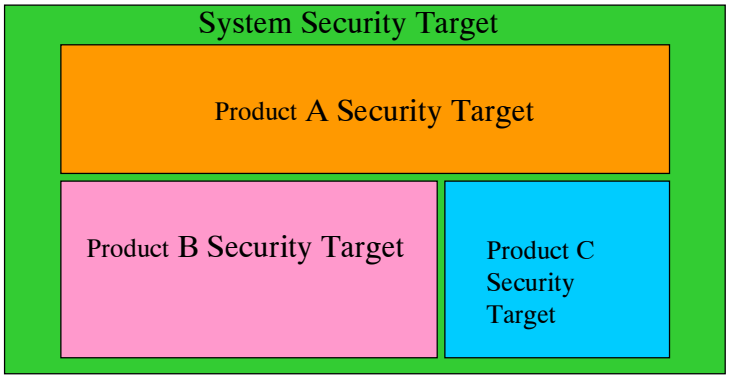
- La classe Scambio dati si suddivide inoltre in:
  - Autenticazione
  - Controllo dell'Accesso
  - Riservatezza dei dati
  - Integrit‡ dei dati
  - Non ripudio

Il contesto delle valutazioni ITSEC



I criteri di valutazione rappresentano la modalit‡ di verifica della conformit‡ di un prodotto o un sistema ad una norma rappresentata dal Security Target.

Composizione dei security target di COTS per i sistemi.



ITSEC - La Garanzia - Efficacia

- Adeguatezza delle Funzioni indicate nel Security Target a rispondere alle minacce, indicate nel Security Target.
- Integrazione delle funzioni (protezione da attacchi indiretti).
- Implicazioni delle Vulnerabilit‡ note.
- Robustezza dei meccanismi che implementano le funzioni.
- Facilit‡ d'uso sicuro.
- Analisi per gli aspetti sia di sviluppo che di esercizio.
- Test di intrusione effettuati dal valutatore.

Efficacia: alcuni concetti

- Attacco diretto: quello previsto in input dalla funzione a cui Ë diretto (es: indovinare la password)
- Attacco indiretto: quello che aggira la funzione (es: impadronirsi del file <login_nome, pwd_cifrata>)
- Vulnerabilit‡: debolezza intrinseca del prodotto/sistema che puÚ tradursi n una violazione degli obiettivi di sicurezza se esiste una minaccia che la sfrutti.

Esempio di analisi di Efficacia - Robustezza dei Meccanismi

- Robustezza dei Meccanismi: verifica della capacit‡ di un meccanismo di resistere ad attacchi diretti.

	APPARECCHIATURE		
ESPERIENZA	Nessuna	Domestiche	Speciali
Profano	1	n/a	n/a
Competente	4	4	n/a
Esperto	6	8	12

	COLLUSIONE		
TEMPO	Solo	Con Utente	Con Amministratore
Minuti	0	12	24
Giorni	5	12	24
Mesi/Anni	16	16	24

RdM: **1<base<=12, 12<media<=24, alta>24**

ITSEC - La Garanzia - Correttezza

- Analisi per gli aspetti sia di sviluppo sia di esercizio.
- Modalit‡ di implementazione delle funzioni, con esplicito riferimento alla tracciabilit‡.
- Sistema e strumenti di sviluppo.
- Controllo della configurazione.
- Rigore del processo di generazione, delivery, configurazione e startup, e di esercizio.

Garanzia - Correttezza

- La correttezza si riversa nella *tracciabilit‡* delle informazioni che descrivono le funzionalit‡ nei vari stadi: requisiti, architettura, disegno, inplementazione, test, distribuzione, installazione, configurazione, startup, esercizio.
- Le tabelle che seguono indicano i documenti che lo sponsor deve fornire e che il valutatore deve esaminare nell'analisi di correttezza. La struttura Ë gerarchica, cioË ogni livello eredita i requisiti dei livelli che lo precedono.

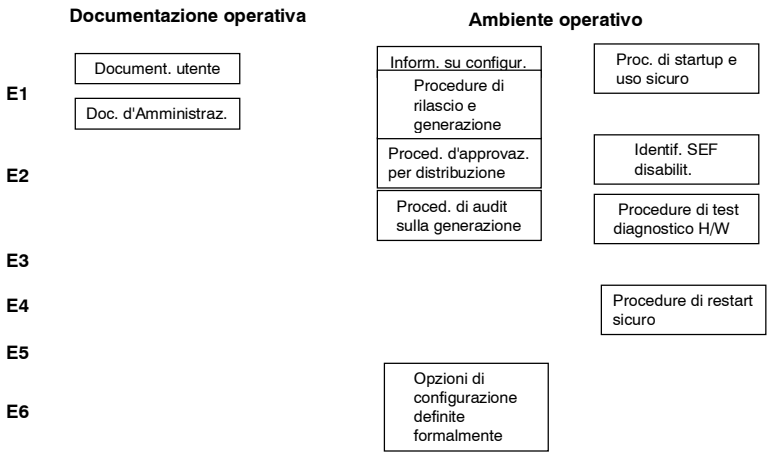
CRITERI DI CORRETTEZZA - PROCESSO DI SVILUPPO

	Requisiti	Architettura	Dettaglio	Implementazione
E1	Security Target	Informale		Evidenza di Testing
E2			Informale	Evidenza di Testing Funzionale
E3				Sorgenti - Disegni - Ev. Testing Mecc.
E4	Spec. Funzionali Semiformali Modello di politica di sicurezza	Descr. Semiform.	Descr. Semiform.	
E5				Tracciamento stretto con il disegno
E6	Specifica Formale delle funzioni	Descrizione Formale		

CRITERI DI CORRETTEZZA - AMBIENTE DI SVILUPPO

	Controllo di configurazione	Linguaggi e Compilatori	Sicurezza degli sviluppatori
E1	Identificazione univoca del TOE		
E2	Sistema di Controllo di Configurazione		Procedure di Sicurezza
E3	Procedura di Accettazione	Solo linguaggi formalmente definiti	
E4	Controllo di config. assistito da strum.	Opzioni di compilazione documentate	
E5	Controllo di config. su tutti gli oggetti Procedura di Integrazione	Librerie run time a livello sorgente	
E6	Strumenti soggetti a contr. di configuraz.		

Criteri di correttezza - Esercizio



Correttezza - Livelli di Rigore della documentazione

- Indicare: devono essere forniti i fatti rilevanti (Livelli E1, E2).
- Descrivere: devono essere forniti i fatti rilevanti e questi devono essere descritti singolarmente (Livelli E3, E4).
- Spiegare: devono essere forniti i fatti rilevanti, questi devono essere descritti singolarmente e per ciascuno deve esserne data giustificazione (Livelli E5, E6).

Livelli di Rigore - Esempio

- Indicare: Il TOE deve identificare e autenticare gli utenti autorizzati verificando la validit‡ della user-ID e password. Sono ammessi tre tentativi, oltre l'utente non Ë pi˘ accettato
- Descrivere: Il TOE deve identificare e autenticare gli utenti autorizzati verificando la validit‡ della user-ID e password. Il TOE verifica che:
  - la user ID immessa Ë uguale a quella in formato macchina contenuta nel TOE
  - la user ID Ë registrata nel file delle autorizzazioni degli utenti
  - la password Ë valida per quella user-ID
- Per tentativi superiori alle tre volte:
  - scrive il tipo di incidente nel file di audit, con data, ora, terminale e nome utente
  - inibisce l'accesso all'utente

Livelli di Rigore - Esempio

- Spiegare: **si forniscono in pi˘ delle affermazioni quali:**
  - la registrazione nel file di audit di tentativi di login informa l'addetto alla sicurezza che un determinato terminale o il sistema stesso Ë oggetto di un attacco
  - il nominativo dell'utente dovr‡ essere disabilitato nell'apposito file contenente le autorizzazioni degli utenti in modo da prevenire l'accesso al sistema fino a che non verr‡ autorizzato dall'addetto alla sicurezza

I Common Criteria o ISO/IEC 15408

- Uno standard internazionale che riunisca i criteri in uso presso USA, Canada, Europa.
- CC nasce come progetto sponsorizzato dai tre proponenti (CC EB). I risultati sono stati dati all'organismo di normazione (ISO/IEC JTC1 SC27 WG3), come base per lo standard ISO/IEC .
- CC Ver. 1.0 - Gennaio '96.
- CC Ver. 2.0 - Dicembre '97.
- ISO/IEC 15408 Dicembre 1999

- La compatibilit‡ verso i criteri "padri" (TCSEC, ITSEC, CTCPEC) È un requisito.

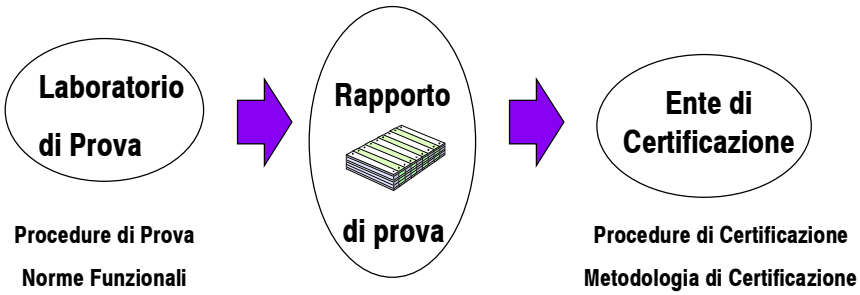
Common Criteria - ISO/IEC 15408

- Separazione tra Funzionalit‡ e Garanzia.
  - Recepimento del maggior contributo innovativo di ITSEC rispetto a TCSEC.
- Protection Profiles simile a Classi di Funzionalit‡ ITSEC.
- I Protection Profiles vanno *registrati* prima di essere utilizzati e riferiti. Vedi *classi di funzioinalit‡ ITSEC.*

Che cosa si intende per Schema di Valutazione e Certificazione

- Per Schema di Prova (o Valutazione) e Certificazione si intende
  - l'insieme delle organizzazioni coinvolte.
  - la definizione dei limiti entro cui ciascuno puÚ operare.
  - la definizione dei flussi informativi tra essi.
  - la definizione dei processi connessi con le attivit‡.
  - la definizione della modalit‡ con cui le attivit‡ verranno svolte
  - le condizioni per il mutuo riconoscimento di rapporti e certficati

Prove (o valutazioni) e Certificazione



Procedure di Prova
Norme Funzionali
Metodologia di Prova
Accreditamento
EN45001

Procedure di Certificazione
Metodologia di Certificazione
Procedure di Sorveglianza
Organismi di Controllo
Accreditamento
EN45011