Standard internazionali di sicurezza
Valutazione della sicurezza dei sistemi informatici

Nel valutare la sicurezza dei sistemi informatici, si può procedere in due diversi modi. Il primo, il **metodo sperimentale**, in genere prevede un approccio volto a dimostrare la presenza o l'assenza dei problemi sottoposti a test. Il nome del gruppo di persone che si è posto l'obiettivo di analizzare le problematiche di sicurezza della rete è *TIGER TEAMS*.

L'altro metodo, il **metodo analitico** di valutazione, prevede l'esame delle caratteristiche del sistema, dal progetto *hardware* e *software*, al fine di determinare logicamente ed analiticamente, il grado di resistenza del sistema.

Un aspetto non secondario delle valutazioni di sicurezza, è la **certificazione**, un'attestazione che la valutazione è stata condotta secondo metodologie standard. Molti sistemi di valutazione, riportano anche l'attestazione del livello di sicurezza rilevato dalla valutazione.

L'acquirente di un prodotto di sicurezza può essere certo che il prodotto che gli viene offerto fornisce la protezione richiesta attraverso la consultazione di enti certificatori.

Certificatori ufficiali 1

Coloro che definiscono i criteri e gli standard ora disponibili in tutto il mondo, sono quasi totalmente annoverabili tra le fila delle agenzie di sicurezza interna degli Stati Uniti. Così tra gli sviluppatori troviamo:

- **DoD** - ***D****epartment* ***o****f* ***D****efence*
- **NCSC** - ***N****ational* ***C****omputer* ***S****ecurity* ***C****enter*
- **NSA** - ***N****ational* ***S****ecurity* ***A****gency*
- **NIST** - ***N****ational* ***I****nstitute of* ***S****tandards and* ***T****echnology*

Nel 1977 lo *U.S. Department of Defense* (DOD) promuove la *DoD Computer Security Initiative* che coinvolge governo e privati in varie attività per fare il punto della situazione sul tema della sicurezza e per analizzare le modalità di realizzazione di meccanismi per la valutazione di sistemi sicuri.

Negli stessi anni ('73/'74) NBS (*National Bureau of Standard*) chiamato attualmente NIST (*National Institute for Standard and Technology*) propone due attività:

- definizione di standard di crittografia da adottare dalle agenzie federali che dà origine nel '77 al DES (commissionato alla IBM)
- definizione di standard per lo sviluppo e valutazione di sistemi sicuri

Nel 1979 la *Mitre Corporation* definisce un insieme di criteri per la valutazione della sicurezza di un sistema.

In questo contesto vengono presentati i seguenti set di criteri:

- **TCSEC** (***T****rusted* ***C****omputer* ***S****ecurity* ***E****valuation* ***C****riteria* - *Orange Book* del DoD)
- **CCITEC** (***C****ommon* ***C****riteria for* ***I****nformation* ***T****echnology* ***E****valuation* ***C****riteria*)

Certificatori ufficiali 2

Nel 1981 nasce all' interno di **NSA** (*National Security Agency*) il **CSC** (*Computer Security Center*)

con l' obiettivo di continuare e potenziare l'iniziativa del DoD.

Nel 1985 nasce NCSC (*National Computer Security Center*) che unisce il CSC e tutte le agenzie federali. Obiettivi:

- essere un punto di riferimento per governo e industrie per la sicurezza di sistemi operativi con informazioni classificate
- definire i criteri per la valutazione di sicurezza di sistemi di elaborazione e sistemi di sicurezza
- incoraggiare la ricerca anche per sistemi distribuiti
- sviluppare strumenti di verifica e test per la fase di certificazione di un sistema di sicurezza
- Risultato più noto è la pubblicazione di *Orange Book*

Nel 1991 NSA e NIST avviano un progetto comune che nel '92 porta alla definizione dei nuovi criteri federali basati anche su i criteri canadesi *Canadian Tusted Computer Product Evaluation Criteria* (CTCPEC) del '89, ed i criteri europeri ITSEC.

In Europa la Germania ha istituito il CCSC (*Commercial Computer Security Center*) ed ha coinvolto le organizzazioni CCTA (*Central Computer and telecommunication Agency*) per gli ambienti industriali e commerciali CESG (*Communications-Electronics Security Group*) per gli ambienti militari. Inghilterra, Francia, Olanda collaborano con la Germania per la definizione dello standard europeo di sicurezza.

Nel 1990 CCSC pubblica ITSEC (*Information Technology Security Evaluation Criteria*) detti *White Books* (ultima edizione 1.2 a giugno 1991) e nel 1993 CCSC pubblica ITSEM (*Information Technology Security Evaluation Manual*).

TCSEC 1

Il primo standard che stabilisce i diversi livelli di sicurezza utilizzati per proteggere *hardware*, *software* ed informazioni memorizzate in un sistema è rappresentato dal ***T**rusted **C**omputer **S**ystem **E**valuation **C**riteria* redatto dal Dipartimento della Difesa degli Stati Uniti:

- *Orange Book*.

Tale denominazione deriva dal fatto che appartiene a una collana di libri ognuno dei quali ha una copertina di colore diverso.

Questi livelli descrivono differenti tipi di protezione fisica, meccanismi di autenticazione degli utenti, affidabilità del *software* del sistema operativo e delle applicazioni degli utenti. Questi standard impongono anche dei limiti sui tipi di sistemi che possono collegarsi all'*host* di cui si valuta la sicurezza.

L'*Orange Book* è rimasto inalterato da quando nel 1985 è divenuto uno standard del Dipartimento della Difesa. Per molti anni questo libro ha rappresentato il punto di riferimento per la valutazione della sicurezza dei sistemi *mainframe* multi-utenti e dei sistemi operativi dei *minicomputer*. Altre realtà, quali *database* e reti, sono state valutate mediante estensioni interpretative dell'*Orange Book*, quali la *Trusted Database Interpretation* e la *Trusted Network Interpretation*.

TCSEC 2

Il TCSEC classifica i sistema in 4 gruppi di requisiti fondamentali:

Politica

- Politica di sicurezza - deve definire gli oggetti, i soggetti e le regole di accesso.
- *Marking* - gli oggetti devono aver associate etichette di controllo degli accessi.

Responsabilità

- Identificazione/autenticazione - i soggetti devono essere identificati.
- Resposabilità - devono essere mantenute e protette informazioni di *audit* per poter attribuire responsabilità in caso di azioni che inficiano la sicurezza del sistema.

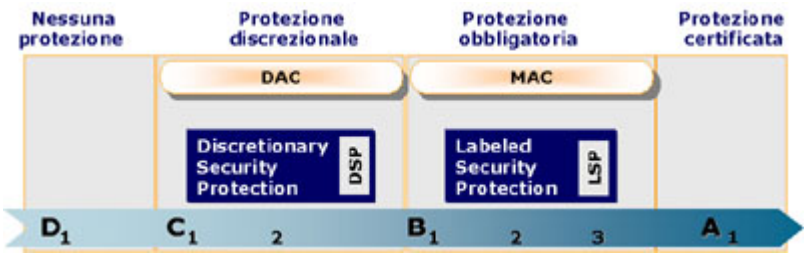
Affidabilità

- Affidabilità - i meccanismi hw e sw contenuti nel sistema devono poter essere valutati indipendentemente per verificare che i requisiti suddetti siano rispettati.
- Protezione continua - i meccanismi del sistema di sicurezza devono essere protetti da modifiche non autorizzate e manomissioni.

Qualità della documentazione

TCSEC 3

Sulla base dei requisiti (politica, responsabilità, affidabilità) raggruppa i sistemi di sicurezza in 4 classi:



D Protezione minima

C Protezione discrezionale

- C1 protezione discrezionale.
- C2 protezione degli accessi controllata.

B Protezione obbligatoria

- B1 protezione basata su etichette.
- B2 protezione strutturata.
- B3 domini di sicurezza.

A Protezione certificata

- A1 progetto certificato.

Ogni classe aggiunge requisiti rispetto alla classe precedente. **TCB** (***T**rusted **C**omputing **B**ase*) è l'insieme dei meccanismi (hw, sw e fw) che realizzano le politiche di sicurezza di un sistema o prodotto sotto valutazione.

Livello D

Il **livello D** (o D1), rappresenta la forma più lasca di sicurezza. Questo standard definisce le condizioni che si hanno quando un intero sistema non è sicuro. Non esiste alcuna protezione sull'*hardware*, il sistema operativo può essere facilmente compromesso e non sono stabilite regole per l'autenticazione degli utenti né le modalità di accesso alle informazioni del sistema. Questo livello di sicurezza fa tipicamente riferimento a sistemi operativi quali MS-DOS, MS- *Windows* e *Apple Macintosh System* 7.x.

Questi sistemi operativi non sono in grado di discriminare tra utenti differenti e non prevedono un meccanismo specifico per identificare chi sta effettivamente operando sul sistema. Inoltre, questi sistemi non impongono alcun controllo sulle informazioni cui si può avere accesso sul disco rigido.

Livello C1

Il **livello C** prevede due sottolivelli di sicurezza, **C1** e **C2**.

Il **livello C1**, conosciuto anche come livello di tipo *Discretionary Security Protection*, descrive le caratteristiche di sicurezza tipicamente presenti su un sistema *Unix*.

Sono previsti alcuni **meccanismi di protezione** per l'*hardware* in modo che non possa essere facilmente compromesso, anche se questa eventualità è ancora possibile. Gli utenti devono identificarsi sempre nei confronti del sistema mediante un *login* e una *password*; questo permette di garantire a ciascun utente i diritti di accesso ai programmi e alle informazioni del sistema. Fondamentalmente questi diritti di accesso si riassumono nei permessi (*permission*) che regolano l'accesso a *file* e cartelle. Questi meccanismi (conosciuti come *Discretionary Access Controls*) permettono al proprietario di un *file* o di una *directory* (o all'amministratore del sistema) di impedire a determinati utenti o gruppi di utenti l'accesso a specifici programmi ed informazioni.

Tuttavia, l'amministratore del sistema ha la possibilità di effettuare qualunque tipo di operazione. Di conseguenza, un amministratore poco accorto può compromettere la sicurezza dell'intero sistema senza che nessun altro utente se ne renda conto. Inoltre, molti dei compiti giornalieri di un amministratore possono essere svolti soltanto attraverso un *login* di tipo *root*.

Stante la decentralizzazione dei sistemi informatici moderni, non è improbabile la situazione per cui più di due o tre persone, all'interno della stessa organizzazione, conoscono la *password* di *root*. Questo rappresenta un problema perché risulta impossibile individuare la persona che ha operato delle modifiche sulla configurazione del sistema.

Il **Tcb di un C1** (protezione discrezionale) prevede i seguenti aspetti:

- Politica: Controllo degli accessi discrezionale. Il Tcb deve poter definire e controllare gli accessi dei singoli utenti sulle singole risorse (*file* e programmi) (meccanismi ACL).
- Responsabilità: Identificazione e Autenticazione. Il Tcb deve poter identificare gli utenti che richiedono un accesso (meccanismo delle *password*).
- Affidabilità: L'esecuzione del Tcb dovrà essere protetta. Le feature periodicamente validate, i meccanismi verificati aderenti a quanto descritto nella documentazione.
- Documentazione:
    - *User Guide* delle *feature* di sicurezza (per l' utente).
    - Manuale delle *facility trusted* (per l'amministratore del sistema).
    - Documentazione della fase di test (funzionale).
    - Documentazione di progetto (moduli, interfacce tra moduli).

Livello C2

Il **livello C2** intendeva risolvere i problemi lasciati aperti dal livello C1. Insieme a quelle tipiche di quest'ultimo livello, le caratteristiche del C2 comprendono la creazione di un ambiente ad **accesso controllato**. Questo ambiente permette di restringere ulteriormente la possibilità che gli utenti eseguano determinati comandi o accedano a *file* attraverso l'uso delle *permission* ma anche di **livelli di autenticazione**. Inoltre, questo livello di sicurezza richiede che il sistema venga monitorato (***auditing***), ovvero che venga scritto un *record* informativo per ognuno degli eventi che si verificano sul sistema stesso.

Il **meccanismo di *auditing*** viene utilizzato per tenere traccia di tutti quegli eventi che riguardano la sicurezza del sistema, come ad esempio le attività svolte dall'amministratore. Un tale meccanismo richiede anche l'uso di tecniche di autenticazione dal momento che, senza di esse non si può essere sicuri dell'identità effettiva della persona che ha eseguito un determinato comando. Lo svantaggio dell'uso di meccanismi di *auditing* risiede nel fatto che essi comportano un carico aggiuntivo e richiedono risorse computazionali.

Mediante l'uso di autorizzazioni aggiuntive, gli utenti di un sistema C2 possono garantirsi i permessi per svolgere operazioni di amministrazione del sistema senza avere per questo bisogno della *password* di *root*. Ciò permette di tenere traccia di chi ha svolto specifici compiti relativi all'amministrazione del sistema dal momento che vengono svolti da un utente e non dall'amministratore stesso.

Queste autorizzazioni aggiuntive non devono essere confuse con i permessi di tipo SGID e SUID applicabili ad un programma. Esse sono piuttosto autorizzazioni specifiche per l'esecuzione di certi comandi o per l'accesso alle tabelle del *kernel*. Ad esempio, gli utenti che non hanno autorizzazioni d'accesso alla tabella dei processi potranno soltanto avere visibilità dei propri processi quando eseguono il comando ps.

Il **Tcb di un C2** (protezione degli accessi controllati):

- Politica - Riuso degli oggetti. Riassegnazione ad alcuni soggetti di un mezzo (settori di disco, nastro magnetico) che ha contenuto uno o più oggetti non deve avere traccia di dati relativi al precedente oggetto contenuto.
- Responsabilità - *Audit*. Il Tcb deve avere il controllo degli accessi con meccanismi di *account* sui singoli utenti, di *audit* delle attività di ciascun utente.
- Affidabilità - (come C1).
- Documentazione - (come C1).

Livello B

Livello B1

Il livello B di sicurezza comprende tre sotto-livelli. B1 (*Labeled Security Protection*) è il primo sotto-livello che supporta la sicurezza di differenti gradi, come ad esempio *secret* e *top secret*. Questo livello stabilisce che ad un oggetto (ad esempio un *file*) sottoposto ad una politica di controllo obbligato dell'accesso non possano essere modificate le *permission* neanche da parte del proprietario dell'oggetto stesso.

Il **Tcb di un B1** (protezione basata su etichette)

- Politica - Etichette. Etichettatura di soggetti e oggetti (processi, *file*, segmenti, *device*) - Controllo degli accessi obbligatorio. Basato sulle etichette.
- Responsabilità (come C2).
- Affidabilità. Verifica delle specifiche di disegno. Deve essere rimossa ogni imperfezione

rilevata al momento del test.
- Documentazione. Deve fornire almeno un livello informale della politica di sicurezza (specifiche di disegno).

Livello B2

Il livello B2 (*Structured Protection*) richiede che ogni oggetto del sistema venga contrassegnato con una etichetta (*label*). I dispositivi (dischi, terminali, *tape*) possono avere uno o più livelli di sicurezza associati. B2 è il primo livello che affronta il problema delle comunicazioni tra oggetti cui sono assegnati gradi di sicurezza diversi.

Il **Tcb di un B2** (protezione strutturata)

- Politica - Le politiche di controllo degli accessi (mandatoria e discrezionale) devono essere estese a tutti i soggetti e oggetti del sistema.
- Responsabilità - Il Tcb supporterà un canale protetto (*Trusted Path*) per le fasi di *login* e autenticazione.
- Affidabilità - Il Tcb deve essere strutturato in moduli critici e non ai fini della protezione. Deve avere un'interfaccia ben definita. Il progetto e la realizzazione devono essere soggetti a test sofisticati e revisioni. Richiede meccanismi di autenticazione e strumenti per la configurazione. Il sistema deve essere relativamente resistente a tentativi di penetrazione.
- Documentazione - Il Tcb deve essere basato su un modello ben definito e documentato. (specifiche di disegno).

Livello B3

Il livello B3 (*Security Domains*) rafforza il concetto di dominio mediante l'utilizzo di *hardware* specifico. Ad esempio viene utilizzato *hardware* appositamente predisposto alla gestione della memoria per proteggere un dominio sicuro da accessi non autorizzati. Questo livello richiede inoltre che i terminali degli utenti siano collegati al sistema mediante connessioni sicure.

Il **Tcb di un B3** (domini di sicurezza)

- Politica. (come B2).
- Responsabilità. (come B2).
- Affidabilità. Il Tcb non deve poter essere manomesso, deve poter essere analizzato e testato. Quindi il codice deve essere ben strutturato e deve usare tecniche di ingegnerizzazione del *software* in fase di progetto e realizzazione per avere minima complessità. Deve prevedere un amministratore del sistema. Deve avere un buon sistema di *auditing* e procedure di *recovery*. Deve essere altamente resistente ai tentativi di penetrazione.
- Documentazione. (come B2).

Livello A

Il livello A (*Verified Design*) è il più alto livello di sicurezza previsto dall'*Orange Book*. Questo livello comprende delle fasi di progettazione, controllo e verifica del sistema altamente sicure.

Per raggiungere un tale livello di sicurezza è necessario considerare tutte le componenti di un sistema a partire da quelle dei livelli più bassi; il progetto deve essere matematicamente verificato, si deve effettuare un'analisi dei canali di comunicazione e la distribuzione delle componenti stesse del sistema deve essere sicura. Questo significa che sia l'*hardware* che il *software* devono essere protetti durante la fase di consegna per prevenire intrusioni nel sistema globale di sicurezza.

Il **Tcb di un A1** (progetto certificato)

- si distingue da quello di un B3 dal fatto che la sua affidabilità deriva dall'aver utilizzato un modello formale delle politiche di sicurezza, una specifica formale di alto livello del progetto. Il modello deve essere estendibile.

ITSEC

ITSEC

Armonizza i criteri di valutazione della sicurezza definiti separatamente da vari paesi europei (Gran Bretagna, Francia, Germania, ...). Permette la selezione di funzioni di sicurezza in un sistema/prodotto e definisce 7 livelli di valutazione di affidabilità che rappresentano la capacità del sistema/prodotto di realizzare le specifiche di sicurezza attraverso le funzioni suddette.

ITSEM

Manuale per la valutazione della sicurezza di prodotti e sistemi che fornisce le basi per una unificazione dei metodi di valutazione della sicurezza definiti dai vari Enti certificatori oltre che un sussidio dei concetti espressi in ITSEC.

Utilizzatore/Fornitore

L'**utilizzatore** del Sistema è la persona o l'ente proprietario del sistema e dei dati in esso elaborati. Costui dispone di una propria politica di sicurezza e deve verificare che il sistema che gli viene offerto sia in grado di soddisfare tale politica. Deve inoltre confrontare sistemi diversi per poter decidere quale risponda meglio alle sue esigenze.

Il **fornitore** del sistema è responsabile del sistema finale consegnato all'utilizzatore e deve convincere l'utilizzatore sull'adeguatezza delle funzioni fornite dal sistema. Il fornitore deve cautelarsi qualora l'utilizzatore subisca danni imputabili ad un cattivo funzionamento del sistema dal punto di vista della sicurezza.

I requisiti funzionali sono le contromisure previste attraverso le quali si esprime la sicurezza del TOE (*Target Of Evaluation*), mentre i requisiti di tipo qualitativo esprimono le modalità e l'accuratezza con cui le contromisure di sicurezza sono realizzate.

ITSEC tratta soltanto i requisiti di tipo qualitativo, ma include 10 classi predefinite di requisiti funzionali. Se non utilizzate (non è obbligatorio) suggerisce di far riferimento a 8 gruppi generici (*generic headings*).

Requisiti funzionali suggeriti

Identification and authentication
funzioni che consentono di verificare l'identità degli utenti che chiedono l'accesso a risorse controllate dal TOE.

Access control
funzioni che controllano l'accesso alle risorse (diritti di accesso e loro verifica).

Accountability
funzioni che tracciano le attività di utenti/processi con lo scopo di attribuire tali attività a chi le ha svolte.

Audit
funzioni che registrano e analizzano gli eventi che potrebbero rappresentare una minaccia.

Object reuse
funzioni che controllano il riuso delle risorse (memoria centrale o di massa).

Accuracy
funzioni che assicurano che i dati transitino attraverso i processi o passino da un oggetto ad un altro senza subire alterazioni.

Reliability of service
funzioni che assicurano la accessibilità delle risorse a entità legittime entro tempi prefissati, individuano errori ed effettuano il *recovery*.

Data exchange (vedi ISO 7498-2)
funzioni che garantiscono la sicurezza delle informazioni trasmesse sui canali di comunicazione (autenticazione, controllo degli accessi, confidenzialità, integrità, non ripudio).

Security Target

È un documento che costituisce il riferimento per le attività di progettazione e valutazione di un TOE (un sistema o un prodotto) e descrive gli obiettivi di sicurezza in termini di

- Riservatezza.
- Integrità.
- Disponibilità.

La sua struttura è diversa se il TOE è un sistema o un prodotto. è redatto dallo Sponsor (chi richiede la valutazione del TOE).

Valutare la sicurezza di un TOE consiste nello stimare il grado di fiducia che è possibile riporre nelle funzioni di sicurezza adottate e specificate nel *Security Target* e verificare che il TOE rispetti gli obiettivi di sicurezza per cui viene realizzato.

Fasi del processo di valutazione 1

Le fasi del processo di valutazione consistono in:

- **Preparazione** - attivazione dei contatti, studio del *Security Target*.
- **Valutazione** - fase centrale.
- **Conclusione** - produzione dell' *Evaluation Technical Report* (ETR) che però non indica il livello di valutazione.
- **Certificazione** - emissione del certificato che riporta il livello di sicurezza (E1,...E6) emesso da un Ente Certificatore (in Italia ce ne sono 4).

Livelli di fiducia

- E0: Il TOE ha una sicurezza inadeguata.
- E1: Prevede un *Security Target* e una descrizione informale (linguaggio naturale) dell'architettura del TOE. I test devono dimostrare che il TOE soddisfa il suo *Security Target*.
- E2: Prevede una descrizione informale del progetto dettagliato del TOE. Deve essere valutata la prova dei test e ci deve essere un sistema di controllo della configurazione e una procedura approvata di distribuzione.

- E3: Oltre a quanto previsto per E2 devono essere valutati i disegni del codice sorgente e/o *hardware* corrispondenti ai meccanismi di sicurezza e deve essere valutata la prova dei test di tali meccanismi.
- E4: Prevede un modello formale (di tipo matematico) della politica di sicurezza. Le funzioni di sicurezza, il progetto architetturale e quello dettagliato devono essere specificati con un sistema semiformale (basato su strumenti specifici: ad es. il *Claims Language* dell'ITSEC che utilizza il linguaggio naturale inglese per il quale sono fissate strutture di frasi molto rigide e parole chiave).
- E5: Oltre ai requisiti di E4 deve esserci una stretta corrispondenza tra il progetto dettagliato e il codice sorgente e/o i progetti dell'*hardware*.
- E6: Oltre ai requisiti di E5 le funzioni di sicurezza e il progetto architetturale devono essere specificati in modo formale consistente con il modello formale della politica di sicurezza.

Fasi del processo di valutazione 2

Un sistema è un'aggregazione di prodotti in esecuzione in un ambiente definito
La struttura secondo ITSEC/ITSEM prevede le seguenti componenti:

- Introduzione.
- Descrizione del sistema.
- Descrizione della politica di sicurezza.
- Descrizione degli obiettivi di sicurezza.
- Descrizione delle minacce.
- Descrizione delle funzioni di sicurezza.
- Descrizione dei meccanismi di sicurezza (opzionale).
- Dichiarazione della robustezza dei meccanismi richiesta.
- Dichiarazione del livello di assicurazione.

Introduzione

- Obiettivi del documento.
- Riferimenti a normative e documenti interni ed esterni.
- Definizione ed acronimi, glossario.

Descrizione del sistema

- Obiettivo del sistema.
- Descrizione e caratteristiche delle informazioni trattate.
- Apparati necessari per l'esercizio del sistema.
- Planimetria del sistema e interconnessioni.
- Misure di sicurezza fisica utilizzate.
- Relazioni con il resto del sistema (se si tratta di un sottosistema).

Descrizione della politica di sicurezza e obiettivi

Vengono definiti gli obiettivi espressi in termini di riservatezza, confidenzialità e disponibilità che riguardano:

- beni che richiedono protezione (informazioni, processi, responsabilità e ruoli degli utenti, ...).
- Risorse fisiche (singoli apparati, PC, ...).
- Risorse astratte (configurazione del sistema, processi, algoritmi, ...).
- Vengono definite le regole da seguire affinchè gli obiettivi della sicurezza possano essere raggiunti (regole di accesso alle risorse, modalità di connessione, utilizzo di *password*, ruoli, responsabilità, profili utente).

Minacce

Individuare le azioni che possono portare alla violazione degli obiettivi di sicurezza. Le minacce possono essere:

- interne;
- esterne;
- intenzionali;
- accidentali;
- attive;
- passive;
- attività critica ==> analisi dei rischi.

Funzioni di sicurezza

- Realizzano le contromisure necessarie per soddisfare gli obiettivi di sicurezza del sistema.
- ITSEC ne suggerisce 8 gruppi (*Generic Headings*) che però non sono obbligatori.
- Per ogni funzione occorre specificare le motivazioni che hanno portato alla sua realizzazione, come è stata realizzata (caratteristiche principali) e le relazioni della funzione con l'esterno.

Meccanismi di sicurezza

Un meccanismo di sicurezza costituisce il mezzo con cui è possibile realizzare una o più funzioni di sicurezza.

- Un *Security Target* può indicare alcuni meccanismi (facoltativo).
- Occorre tener conto di quelli già presenti nei prodotti del sistema.
- è necessario analizzare le interconnessioni tra i meccanismi per garantire una migliore integrazione.
- Se non vengono specificati i meccanismi significa che si lascia completa libertà a chi realizza le funzioni.

Robustezza di un meccanismo

La robustezza di un meccanismo è definita su una scala di valori (alto medio, basso) tenendo conto delle variabili:

- tempo (minuti, giorni, mesi);
- tipo di attaccante (inesperto, competente, esperto);
- collusione (nessuna, utente autorizzato, gestore del sistema);
- apparecchiature usate (nessuna, sofisticate);
- il *Security Target* deve dichiarare la robustezza richiesta tenendo conto che quella complessiva coincide con quella del meccanismo più debole;

Livello di assicurazione

Valutare l'assicurazione di un TOE significa verificare che le misure di sicurezza realizzate:

- verifichino i requisiti definiti nel *Security Target*;
- siano in grado di contrastare efficacemente le minacce individuate e a quale livello.

L'Assicurazione si valuta in parallelo da due punti di vista: Efficacia e Correttezza. Per quanto riguarda l'efficacia questa valutazione mira a stabilire se le funzioni di sicurezza adottate sono

idonee agli scopi per cui sono state scelte, indicati nel *Security Target* e se i meccanismi che le realizzano sono in grado di contrastare i possibili attacchi. Se la verifica dell'Efficacia ha esito negativo il valutatore assegnerà un livello di valutazione E0 indipendentemente dal risultato della valutazione della Correttezza. Infatti se le funzioni non sono idonee, non ha senso valutare se i corrispondenti meccanismi sono stati realizzati correttamente.

La valutazione della correttezza mira a stabilire se le funzioni di sicurezza ed i corrispondenti meccanismi sono stati realizzati correttamente (con la dovuta accuratezza e coerentemente con quanto specificato nel *Security Target*) e prende in esame separatamente il Processo costruttivo e gli Aspetti operativi del TOE.

Confronto

Sia ITSEC che TCSEC forniscono i criteri base per la valutazione della sicurezza da effettuare a carico di organizzazioni di certificazione e costituiscono per gli utenti una guida per la comprensione delle caratteristiche di sicurezza dei sistemi da acquisire.

Orange Book

- Le classi di sicurezza inglobano sia requisiti funzionali che di affidabilità.
- È orientato alla valutazione di prodotti.
- Non specifica, se non marginalmente le azioni che il valutatore deve eseguire.
- Non richiede documentazione specifica a chi pretende la valutazione.

ITSEC

- Separa i requisiti funzionali da quelli di affidabilità.
- È più flessibile poiché si adatta sia alla valutazione di sistemi che di prodotti.
- Specifica le azioni che il valutatore deve eseguire.
- Per ogni fase del processo di valutazione specifica la documentazione che lo Sponsor (chi richiede la valutazione) deve fornire, il suo contenuto e le prove che devono essere fornite per dimostrare che il TOE soddisfa i requisiti richiesti.

Common Criteria

I ***C****ommon* ***C****riteria* (CC - secondo la terminologia ISO IS 15408 - *Information technology - Security techniques - Evaluation criteria for IT security*) rappresentano il risultato di uno sforzo, iniziato nel 1993 e destinato a superare i limiti dei precedenti standard e a sviluppare una comune metodologia per la valutazione della sicurezza nel mondo dell'Informatica applicabile in campo internazionale.

I rappresentanti degli Stati Uniti, Canada, Francia, Germania, Olanda e Regno Unito, in collaborazione con l'ISO (*International Standard Organization*), si sono accordati per lo sviluppo di uno standard internazionale di valutazione della sicurezza in ambito informatico con l'obiettivo di rilasciare dei nuovi criteri che fornissero utili risposte all'esigenza di standardizzazione di un mercato informatico sempre più globale. Tali nuovi criteri dovevano inoltre permettere il reciproco riconoscimento della valutazione dei prodotti di sicurezza.

- Nel 1996 è stata rilasciata la versione 1.0 dei *Common Criteria*.
- Nel 1998 si è avuto il rilascio della versione 2.0 , (DIS 15408) divenuto standard con l'approvazione dell'ISO, mentre si è in attesa della prossima versione 2.1.

- Nel gennaio 1999 è stata rilasciata una versione *draft* (v 0.6) della *Common Evaluation Methodology* avente lo scopo di armonizzare le modalità di valutazione da parte degli enti valutatori. Tale metodologia è alla base per il reciproco riconoscimento.

Documentazione

Il documento relativo alla seconda versione finale, si compone di tre parti per un totale di più di 600 pagine. L'elenco che segue, riepiloga le tre parti:

- Parte 1: Introduzione e descrizione del modello generale.
- Parte 2: Requisiti delle funzioni di sicurezza.
- Parte 3: Requisiti e livelli dell'affidabilità della sicurezza.

Il documento, nonostante il linguaggio comprensibile a chi è prossimo all'informatica ed in genere alla sicurezza, diventa complesso a causa del diffuso utilizzo di sigle ed abbreviazioni. Sarà opportuno munirsi di un glossario, di una buona dose di pazienza e di tanto tempo a disposizione per studiarlo.

La prima parte [Introduzione e descrizione del modello generale] fornisce:

- all'utente una conoscenza generale;
- allo sviluppatore una conoscenza generale per la formulazione di requisiti e specifiche di un TOE;
- al certificatore una conoscenza generale e guida per la struttura dei PP e ST.

La seconda parte [Requisiti delle funzioni di sicurezza] fornisce:

- all'utente una guida per la formulazione dei requisiti per funzioni di sicurezza;
- allo sviluppatore dei riferimenti per interpretare i requisiti di sicurezza e definire le specifiche funzionali di un TOE;
- al certificatore una formulazione delle dichiarazioni obbligatorie dei criteri di valutazione per valutare se il TOE rispetta le funzioni di sicurezza dichiarate.

La terza parte [Requisiti e livelli dell'affidabilità della sicurezza]:

- all'utente una guida per determinare o richiedere il livello di affidabilità di sicurezza;
- allo sviluppatore dei riferimenti per interpretare i requisiti di affidabilità e definire l'approccio di affidabilità di un TOE;
- al certificatore una formulazione delle dichiarazioni obbligatorie dei criteri di valutazione per valutare l'affidabilità del TOE, dei PP o ST.

Altra documentazione

I protection profile

Alcuni documenti integrano la documentazione dei CC; si tratta dei ***P**rotection **P**rofile* o **PP** che traducono i principi e le guide contenute nei *Common Criteria* in riferimenti a prodotti o sistemi. Tra i PP si ricordano alcuni tra i più interessanti:

- *Application-Level Firewall for Low-Risk environment* (v. 2.0).
- *Traffic-Filter Firewall for Low-Risk environment* (v. 2.0).
- *Commercial Security* 1 (v. 1.0) - Ambiente semplice con sicurezza a livello base.
- *Commercial Security* 3 (v. 1.0) - Ambiente multi-*user* con *database* e necessità di un livello

di sicurezza selettivo.

Metodologia di valutazione

La documentazione disponibile si compone altresì della *draft* rilasciata della ***C**ommon **E**valuation **M**ethodology* (v. 0.6) (**CEM**), articolata in 3 parti:

- Parte 1: Introduzione e modello generale, terminologia e principi di valutazione.
- Parte 2: Metodologia di valutazione, *Protection Profile* & *Security Target*, Livelli e componenti di affidabilità.
- Parte 3: Ampliamento della metodologia.

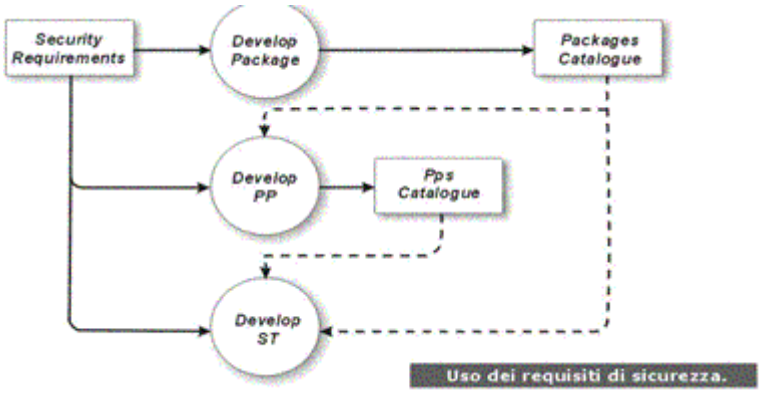
Tale documento pone l'attenzione sull'attività degli enti che sono preposti alla valutazione della sicurezza dei prodotti/sistemi informatici garantendo che il loro operato sia congruente con i requisiti dei CC stessi. Si presenta come uno strumento che dovrebbe garantire la consistenza dell'applicazione dei principi contenuti nei CC in caso di valutazioni ripetute nel tempo e secondo schemi diversi.

Modello generale

I *Common Criteria* contengono essenzialmente i principi tecnici fondamentali - di validità generale, chiari e flessibili - per descrivere i requisiti di sicurezza per i prodotti o sistemi informatici.

Tali requisiti sono descritti in modo organico e strutturato per due tipologie di situazioni:

- ***P**rotection **P**rofile* (**PP**) - Si riferiscono a famiglie o categorie di prodotti e ambienti generici senza riferimenti a specifici prodotti o sistemi e sono un insieme organico di obiettivi e requisiti di sicurezza associabili a categorie di prodotti o sistemi informatici che soddisfano le necessità di sicurezza degli utenti.
  I PP non devono fare riferimento a specifici prodotti realmente realizzati.
  Alcuni esempi per chiarire meglio:
  - *Protection Profile* per i *firewall*, per un sistema tipo utilizzato in ambiente commerciale, per sistemi multi-*user* basati su sistemi operativi di normale commercio o per un sistema di controllo accessi basato su regole predefinite.
- ***S**ecurity **T**arget* (**ST**) - Si riferisce ad uno specifico prodotto o sistema di cui si conoscono le specifiche di sicurezza, ed è un insieme organico di requisiti e specifiche di sicurezza associate ad uno specifico prodotto o sistema informatico a sua volta chiamato ***T**arget **O**f **E**valuation* (**TOE**) e che è oggetto di valutazione. Ad esempio:
  - *Security Target* per Oracle v7,
  - *Security Target* per il *firewall* XYZ, ecc.



Uso dei requisiti di sicurezza.

Tutti i requisiti di sicurezza (specifiche, descrizione, collegamenti, interdipendenze, ecc.) che si possono comporre nei PP e ST sono contenuti in un **Catalogo dei requisiti funzionali della sicurezza** [*Security Requirements*].

Allo stesso tempo i *Common Criteria* contengono i principi fondamentali per valutare i dispositivi di sicurezza dei prodotti o sistemi informatici Per ottenere ciò ci si avvale di un **Catalogo dei requisiti di affidabilità** [*Assurance Requirements*] strutturato in sette livelli di valutazione della affidabilità (EAL).

Tra i concetti chiave dei *Common Criteria*, vi sono quindi le tipologie dei requisiti:

- **Requisiti funzionali** - fondamentali per definire i comportamenti in materia di sicurezza dei prodotti e sistemi informatici. I requisiti effettivamente implementati diventano così funzioni di sicurezza.
- **Requisiti di affidabilità** - fondamentali per stabilire la fiducia che si può riporre nelle funzioni di sicurezza sia in termini di correttezza di implementazione sia in termini di efficacia di soddisfare gli obiettivi propri delle stesse funzioni di sicurezza.

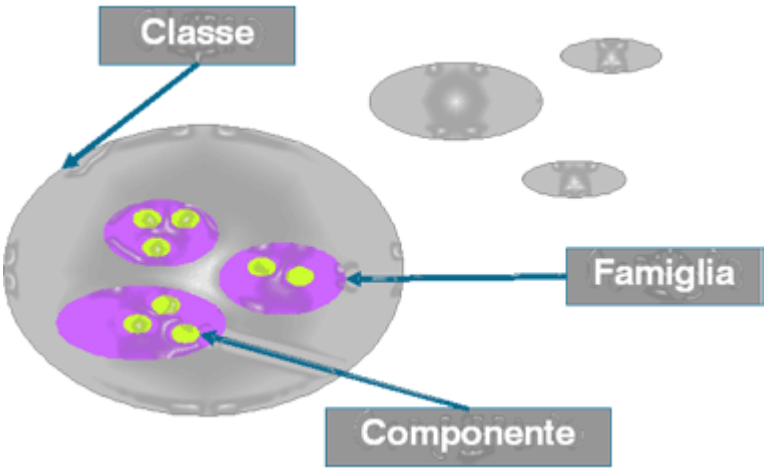
Un ST può includere uno o più *Protection Profile*.

Target Of Evaluation (TOE)

Il TOE è il prodotto o il sistema informatico oggetto della valutazione. Al TOE sono anche associati altri due elementi:

- La TOE *Security Policy* (TSP) - cioè l'insieme di regole che governano le modalità con cui i beni (*assets*) informatici sono gestiti, protetti e distribuiti all'interno del prodotto o sistema che è oggetto di valutazione.
- Le TOE *Security Functions* (TSF) - Sono considerate funzioni di sicurezza (TSF) tutte quelle parti del prodotto o sistema informatico oggetto di valutazione dalle quali dipende la garanzia della corretta esecuzione delle Politiche di Sicurezza (TSP).

Gerarchia



I componenti dei requisiti e delle funzioni di sicurezza e di affidabilità sono definiti e classificati secondo una gerarchia che prevede Classi, Famiglie e Componenti.

Le **Classi** sono un insieme organico di Famiglie che perseguono uno scopo comune. (per esempio: La classe *User Data Protection* o la Classe *Audit*).

Le **Famiglie** sono un insieme organico di Componenti che perseguono un obiettivo di sicurezza comune, ma che possono differire nel rigore o nell'intensità. (Per esempio: la famiglia *Access Contro Policy* raggruppa tutte le componenti che svolgono questa funzione).

Le **Componenti** sono l'insieme minimo e non divisibile che può essere utilizzato ed inserito nei PP o ST. (Per esempio: *Access Control*.1 raggruppa le funzioni di controllo accessi di livello 1).

Questa impostazione dovrebbe garantire flessibilità pur suggerendo di muoversi all'interno di requisiti predefiniti.

Classi funzionali dei requisiti di sicurezza

Ogni classe è individuata da una sigla di tre lettere che è ripetuta su tutte le famiglie e componenti che appartengono alla stessa classe.

FAU - La classe *Security Auditing* comprende il riconoscimento, la registrazione, la conservazione e l'analisi delle informazioni connesse con le più significative attività che coinvolgono la sicurezza. Le registrazioni così ottenute possono essere esaminate per determinare quali attività di sicurezza sono avvenute e chi le ha attivate.

FCO - *Communications* - Questa classe è formata da due famiglie col compito di assicurare l'identità delle parti che sono coinvolte nello scambio di dati. Queste famiglie hanno il compito di garantire l'identità di chi origina le informazioni trasmesse (*proof of origin*) e di garantire la identità di chi riceve le informazioni trasmesse (*proof of receipt*), assicurano inoltre che chi origina il messaggio non possa negare di averlo spedito ed il ricevente non possa negare di averlo ricevuto.

FCS - Questa classe fornisce le funzionalità crittografiche nel caso ciò sia richiesto, per soddisfare più severi obiettivi di sicurezza. Fanno parte di questa classe molte funzioni tra cui. Identificazione ed autenticazione, non-rigetto, percorsi e canali fidati, separazione dei dati, ecc.

FDP - Quattro sono le famiglie di questa classe che definisce i requisiti di protezione dei dati utente. Tali famiglie indirizzano la protezione dei dati utente all'interno del TOE, durante l'importazione e l'esportazione, nella fase di memorizzazione e ne gestiscono gli attributi di sicurezza.

FIA - Identificazione ed Autenticazione - Le famiglie appartenenti a questa classe indirizzano i requisiti connessi con le funzioni che stabiliscono e verificano l'identità degli utenti. Tale funzione è richiesta per garantire che ogni utente sia associato con un appropriato profilo di sicurezza (attributi di sicurezza - es. identità, gruppo di appartenenza, regole di riferimento, livello di riservatezza, ecc.). Una identificazione non ambigua degli utenti autorizzati ed una corretta associazione dei relativi attributi di sicurezza con quelli dei dati e oggetti informatici è un elemento critico per garantire che le politiche di sicurezza volute siano rispettate.

Le famiglie appartenenti a questa classe permettono di determinare e verificare l'identità degli utenti, determinarne la specifica autorità per interagire con il TOE secondo specifici profili di sicurezza.

FMT - *Security Management* - Questa classe è preposta a specificare le regole di gestione delle molteplici funzioni di sicurezza presenti nel TOE, inclusi gli attributi di sicurezza ed i dati essenziali al funzionamento delle stesse funzioni. Sono specificate differenti regole di gestione, di interrelazioni tra le funzioni e le aree di competenza. Questa classe si ripropone molteplici obiettivi:

- Gestione dei dati relativi al funzionamento delle stesse funzioni di sicurezza.

- Gestione degli attributi di sicurezza. Esempio: liste di accesso, liste delle potenzialità.
- Gestione delle funzioni di sicurezza. Esempio: selezione delle funzioni attivabili, regole o condizioni di funzionamento.
- Definizione delle regole di sicurezza.

FPR - Questa classe contiene i requisiti per la *Privacy*, intesa come protezione per ogni utente contro la possibilità che un altro utente possa individuarne l'identità e farne un uso improprio. Le famiglie a disposizione sono:

- *Anonimity*: garantisce che un utente possa utilizzare una risorsa od un servizio certo che la propria identità non venga rivelata ad altri utenti.
- *Pseudonymity*: come nel caso precedente con in più la possibilità però di rendere conto (*accountable*) delle attività eseguite.
- *Unlinkability*: garantisce che un utente possa accedere più volte alle risorse ed ai servizi senza che altri utenti possano ricostruire questi passaggi.
- *Unobservability*: garantisce che un utente possa utilizzare una risorsa od un servizio senza che altri utenti possano osservare quale servizio o risorsa egli stia utilizzando.

FPT - Questa classe comprende famiglie di requisiti funzionali che fanno riferimento all'integrità e alla gestione dei meccanismi che compongono le funzioni di sicurezza del TOE e all'integrità dei dati delle stesse funzioni di sicurezza. Le famiglie di questa classe potrebbero apparire come una duplicazione della classe FDP (protezione dei dati utente) ed utilizzare anche gli stessi meccanismi.

Mentre le funzioni incluse nella classe FDP si occupano della sicurezza dei dati utente, le famiglie incluse nella classe FTP si occupano della protezione dei dati che sono essenziali al funzionamento delle stesse funzioni di sicurezza del sistema o prodotto oggetto di valutazione (TSF).

FRU - Questa classe fornisce tre famiglie che supportano la disponibilità delle risorse necessarie per il funzionamento del TOE, quali per esempio le capacità elaborative e/o di memorizzazione.
La famiglia *Fault Tolerance* fornisce la protezione contro la indisponibilità delle risorse elaborative per effetto di inconvenienti o guasti al TOE stesso.

La famiglia chiamata *Priority of Service* assicura che le risorse siano allocate alle attività più critiche o importanti e non vengano monopolizzate da attività a bassa priorità.
La famiglia *Resource Allocation* permette di porre dei limiti all'utilizzo delle risorse per evitare che un utente le monopolizzi.

FTA - Questa classe contiene le famiglie che disciplinano l'accesso allo stesso TOE definendo i requisiti per controllare l'esecuzione delle sessioni utente.

Le famiglie a disposizione sono:

- Inizio delle sessioni.
- Limitazioni nelle sessioni multiple concomitanti.
- Limitazioni negli scopi degli attributi di sicurezza utilizzabili.
- Blocco delle sessioni.
- Storia degli accessi.
- Simboli (*banners*) degli accessi.

FTP - Le famiglie comprese in questa classe forniscono i requisiti di sicurezza per un percorso fidato (*trusted*) di comunicazione tra gli utenti e le stesse funzioni di sicurezza (TSF) e per un canale fidato di comunicazione tra le TSF e gli altri prodotti informatici. Il percorso di comunicazione deve garantire che l'utente sia in comunicazione con le corrette TSF e che le TSF siano in comunicazione col corretto utente.

Classi dei requisiti di affidabilità

Le classi di affidabilità sono anch'esse codificate con una sigla di tre lettere che si ripete sulle famiglie che compongono la classe.

Di seguito una breve descrizione delle classi:

ACM - La gestione della configurazione aiuta a garantire che sia preservata la integrità del TOE richiedendo che esista adeguata disciplina e controllo dei processi di messa a punto e modifica del TOE e dei dati ad esso correlati. Tale disciplina deve prevenire che il TOE venga modificato, che ci siano aggiunte o cancellazioni di sue parti senza la dovuta autorizzazione. Inoltre il TOE deve essere fornito di appropriata documentazione sia per la sua distribuzione sia per la valutazione.

ADO - Questa classe definisce i requisiti per le misure, le procedure e gli standard che si riferiscono alla fasi di spedizione, installazione e di utilizzo sicuro del TOE garantendo che le protezioni di sicurezza offerte non siano compromesse durante le fasi di trasferimento, installazione, start-up e funzionamento.

ADV - Definisce i requisiti per la graduale messa a punto, nella fase di sviluppo, delle funzioni di sicurezza del TOE partendo dalle specifiche generali sino alla effettiva implementazione.

ADG - definisce i requisiti finalizzati alla comprensibilità, copertura e completezza della documentazione operativa fornita dallo sviluppatore. Questa documentazione, che è divisa in due categorie - una per gli utenti ed una per l'amministratore - è uno dei fattori chiave per la sicurezza dell'operatività del TOE.

ALC - definisce i requisiti per l'affidabilità attraverso l'adozione di un ben definito modello di ciclo di vita per tutti i passi dello sviluppo del TOE, inclusa la politica e le procedure per rimediare ai difetti, il corretto uso dei *tool*, le tecniche e le misure di sicurezza utilizzate per proteggere l'ambiente di sicurezza.

ATE - stabilisce i requisiti per i test che dimostrano come le funzioni di sicurezza soddisfino i requisiti funzionali del TOE. Vi fanno parte test di copertura, di profondità e funzionali, così come modalità di test indipendenti.

AVA - definisce i requisiti diretti alla identificazione dei punti deboli sfruttabili. In particolare quei punti deboli generati nel TOE nelle fasi di costruzione, di utilizzo, di uso improprio o configurazione non corretta.

APE - L'obiettivo della valutazione di un *Protection Profile* (PP) è di dimostrare che il PP è completo, consistente e tecnicamente corretto. Un PP già valutato può essere utilizzato come base per lo sviluppo di *Security Target* (ST). I PP già valutati possono essere inclusi in appositi registri a disposizione degli utenti.

ASE - L'obiettivo della valutazione di un *Security Target* (ST) è di dimostrare che il ST è completo, consistente, tecnicamente corretto e pertanto utilizzabile per essere utilizzato come base per la valutazione di un corrispondente TOE.

AMA - fornisce i requisiti che devono essere applicati dopo che un TOE sia stato certificato secondo i *Common Criteria*. Questi requisiti si ripropongono di garantire che il TOE, dopo la valutazione, continui a soddisfare i propri *Security Target* malgrado possibili variazioni allo stesso TOE ed all'ambiente in cui è posto. Come cambiamenti vengono considerati la scoperta di nuove minacce o punti deboli e la correzione di errori di codifica.

Evaluation Assurance Levels

I livelli di valutazione dei CC sono 7 e vengono definiti con la sigla **EAL** (***E**valuation **A**ssurance **L**evels*). I livelli sono stati definiti in modo da essere (grossolanamente) confrontabili con gli equivalenti livelli dei TCSEC e ITSEC. La tabella riporta questa corrispondenza.

Livello	**Nome**	**TCSEC**	**ITSEC**
EAL1	*Functionally Tested*		
EAL2	*Structurally Tested*	C1 - *Discretionary security protection*	E1: *Informal architectural design*
EAL3	*Methodically Tested & Checked*	C2 - *Controlled access protection*	E2: E1 + *informal detailed design & test documentation*
EAL4	*Methodically Designed, Tested & Reviewed*	B1 - *Labeled security protection*	E3: E2 + *Source code or hardware drawing & evidence of testing*
EAL5	*Semiformally Designed & Tested*	B2 - *Structured protection*	E4: E3 + *Semiformal architectural design & formal model of security policy*
EAL6	*Semiformally Verified Designed & Tested*	B3 - *Security domains*	E5: E4 + *Correspondence between detailed design & source code*
EAL7	*Formally Verified Designed & Tested*	A1- *Verified design*	E6: E5 + *Formal description & detailed architectural design*

Di seguito una breve descrizione dei livelli di affidabilità:

Il livello **EAL1** è applicabile quando è richiesta una certa fiducia nella correttezza delle operazioni, ma le minacce alla sicurezza non appaiono serie. Ciò potrebbe avere senso dove viene richiesta una generica affidabilità della sicurezza per dimostrare che un minimo di attenzione sia stata posta nella protezione dei dati. EAL1 fornisce una valutazione del TOE così come viene reso disponibile ai clienti, inclusi i risultati di test indipendenti e un esame della documentazione di guida normalmente fornita. Si presuppone che la valutazione EAL1 si possa condurre con successo anche senza il coinvolgimento degli sviluppatori del TOE e con non troppa spesa. Una valutazione a questo livello dovrebbe fornire la prova che TOE funzioni così come descritto nella documentazione e che fornisce sufficiente protezione contro le minacce identificate.

Il livello **EAL2** richiede la cooperazione degli sviluppatori del TOE in termini di informazioni sui processi di spedizione e di *design* e risultati dei test, ma non dovrebbe richiedere agli sviluppatori uno sforzo più ampio di quello richiesto nella normale messa a punto di un buon prodotto. In altri termini non ci dovrebbero essere sensibili aggravi di costo e di tempi. EAL2 è applicabile in quelle situazioni dove gli sviluppatori o gli utenti richiedono un basso o moderato livello di affidabilità della sicurezza pur in mancanza di una completa documentazione di sviluppo. Tale circostanza si potrebbe avere nel caso di sistemi proprietari o nel caso non sia facile disporre della necessaria documentazione di sviluppo.

Il livello **EAL3** permette ad uno sviluppatore coscienzioso di raggiungere il massimo di affidabilità da una appropriata progettazione della sicurezza in fase di *design* senza comunque alterare in modo sostanziale le esistenti corrette procedure di sviluppo.
EAL3 è applicabile in quelle situazioni dove gli sviluppatori o gli utenti richiedono un moderato livello di affidabilità della di sicurezza senza, per condurre la valutazione, dover effettuare un sostanziale re-*engineering* del TOE stesso.

Il livello **EAL4** permette ad uno sviluppatore di raggiungere il massimo di affidabilità da una

appropriata progettazione della sicurezza basata su un buon processo di sviluppo tra quelli disponibili in commercio che, basato sul rigore, non richieda specialisti con elevati *skill* o particolari conoscenze in materia di tecnologie di sicurezza. EAL4 è il livello più alto di affidabilità che probabilmente si potrà economicamente ottenere aggiustando prodotti già esistenti.

Il livello **EAL5** permette ad uno sviluppatore di raggiungere il massimo di affidabilità da una appropriata progettazione della sicurezza basata su un rigoroso processo di sviluppo tra quelli disponibili in commercio che preveda un utilizzo moderato di specialisti in tecniche di architettura di sicurezza. Tali TOE saranno probabilmente progettati e sviluppati col preciso intento di raggiungere il livello EAL5. è altamente probabile che per il fatto di dover soddisfare i requisiti di questo livello ci siano dei costi aggiuntivi che non dovrebbero comunque essere consistenti nel caso si utilizzino processi rigorosi di sviluppo senza ricorrere a specializzate tecnologie.
EAL5 è pertanto applicabile in quelle situazioni dove gli sviluppatori o gli utenti richiedano un elevato livello di affidabilità della sicurezza in uno sviluppo pianificato e condotto in modo rigoroso evitando di subire elevati e non ragionevoli costi a seguito dell'utilizzo di tecniche specialistiche di *engineering* di sicurezza.

Il livello **EAL6** permette agli sviluppatori di raggiungere un alto livello di affidabilità con l'utilizzo di specifiche tecnologie di sicurezza in rigorosi ambienti di sviluppo per produrre TOE di prima qualità nel caso si debbano proteggere beni informatici di alto valore contro rischi notevoli.
EAL6 è pertanto applicabile nei casi in cui si debbano sviluppare dei TOE per utilizzi in situazioni ad alto rischio dove il valore dei beni protetti giustifichi notevoli costi addizionali.

Il livello **EAL7** è applicabile allo sviluppo della sicurezza dei TOE per applicazioni in situazioni di estremo rischio e dove l'alto valore delle risorse da proteggere giustificherebbe gli elevati costi.
L'applicazione pratica dell'EAL7 è attualmente limitata a quei TOE con funzionalità di sicurezza fortemente focalizzate che siano riconducibili ad un'analisi formale estesa.