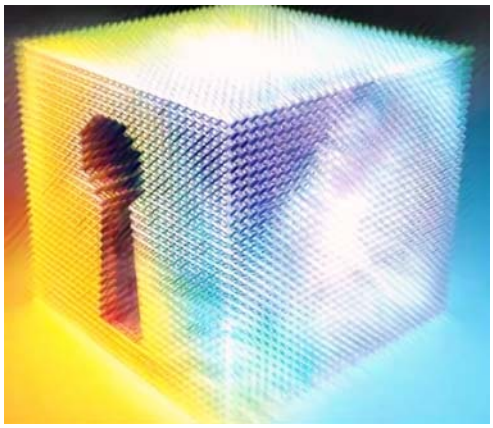
Seminario di Sicurezza Informatica

VALUTAZIONE DELLA SICUREZZA



Manuela Ottobretti

Università degli Studi di Perugia
Laurea Specialistica in Informatica

A.A. 2008/2009

1. Cosa si intende per Valutazione della sicurezza?
La valutazione è un processo nel quale la sicurezza è raccolta e analizzata tramite il confronto con criteri generali di funzionalità e di affidabilità. Il risultato misura il livello di fiducia ovvero indica il grado con cui il sistema sia conforme a particolari criteri.
I criteri utilizzati dipendono dagli obiettivi e dalla metodologia di valutazione.
La valutazione della sicurezza informatica si occupa da prima di decidere le azioni e gli investimenti economici per ridurre l'esposizione ai rischi, valutare l'opportunità di acquisire prodotti e servizi, sapere fino a che punto è possibile fidarsi di prodotti, sistemi e servizi e infine di pubblicizzare le caratteristiche di sicurezza di un determinato prodotto o servizio.

1.1 Caratteristiche generali per la valutazione sono:
Imparzialità: il Laboratorio per la Valutazione del Software (LVS) non deve avere interessi economici connessi con il risultato della valutazione;
Ripetibilità: un LVS deve ottenere lo stesso risultato ripetendo la valutazione;
Riproducibilità: un qualsiasi altro LVS deve ottenere lo stesso risultato ripetendo la valutazione;
Obiettività: il risultato della valutazione non deve essere determinato da giudizi soggettivi.

2. Quadro per il confronto dei criteri di valutazione
2.1 La valutazione è rivolta a:
- **Prodotti**: componenti SW da utilizzare in un varietà di applicazioni e in ambienti con diversi gradi di sicurezza;
- **Sistemi**: una raccolta di prodotti assemblati per soddisfare le specifiche esigenze di una determinata applicazione.
Per il primo caso la verifica riguarda il soddisfacimento o meno di determinati requisiti specificati all'interno delle Security Classes dell'Orange Book e dei *Protection Profiles* definiti dai FC e CC.
Per quanto riguarda i sistemi, invece, l'analisi deve partire dalla valutazione di ogni singolo componente del sistema come descritto all'interno dell'ITSEC.

2.2 Scopi della valutazione:
- **Valutazione**: si valuta se il prodotto ha le proprietà di sicurezza richieste per lo stesso;
L'Orange book oltre alla valutazione vera a proprio si pone altri 2 obiettivi:
- **Certificazione**: si valuta l'idoneità di un prodotto o sistema, e vista come una dichiarazione di conformità di un dato prodotto per un determinata applicazione;
- **Accreditamento**: si decide di utilizzare un determinato sistema o prodotto piuttosto che un altro.

2.3 Metodi principali di valutazione:
- Orientata al prodotto: si occupa di esaminare e testare il prodotto al meglio trovando eventuali problemi.
- Orientata al processo: verifica la documentazione relativa al processo di sviluppo del prodotto, è meno costosa della precedente ed ottiene risultati ripetibili.
Ripetibilità e riproducibilità, come precedentemente asserito, infatti, sono proprietà desiderabili di una valutazione metodologica, le diverse valutazioni dello stesso prodotto dovrebbe dare lo stesso risultato.

2.4 Quadro organizzativo:
Servizi pubblici: valutazione da parte di un agenzia del governo(es. USA). Può essere lenta, e può essere altrettanto difficile trattenere personale qualificato.
Servizi privati: riguarda la valutazione da parte di un'agenzia di certificazione accreditata (Europa). I problemi che si possono porre sono:
- Come assicurarsi che la pressione cliente non influenzi la valutazione dei risultati?
- **Interpretazione deriva** (**criteria creep**): i criteri possono variare nel tempo e si possono differenziare tra più valutatori.

2.5 Struttura dei criteri di valutazione
Sicurezza e affidabilità dovrebbero essere legati ai seguenti concetti:

1 - **Funzionalità**: l'insieme delle caratteristiche afferenti alla sicurezza, presenti nel *servizio* svolto dal sistema o prodotto. Si realizza attraverso *misure tecniche* che contrastano le minacce (DAC, MAC, autenticathion, auditing)
2 - **Garanzia**: è la fiducia nella protezione offerta dalla funzionalità, a sua volta distinta in:
- Efficacia: grado in cui le misure tecniche contrastano le minacce da cui il sistema o prodotto si propone di difendersi. Deve essere in relazione a un determinato insieme di minacce. (Es: valutare se i meccanismi utilizzati sono adeguati " è sufficiente l'autenticazione con password?").
- Correttezza: E' il grado di rispondenza dell'implementazione del prodotto o sistema ai requisiti espressi nelle funzionalità. Indipendente dall'efficacia e dalle minacce. Strettamente dipendente dalla qualità della realizzazione.

Come vedremo in seguito, l'Orange Book definisce delle classi di valutazione prendendo in considerazione tutti gli aspetti contemporaneamente.
L'ITSEC, invece, prevede un flessibile quadro di valutazione che permetta di far fronte a nuove requisiti di sicurezza nei quali gli aspetti citati sono affrontati indipendentemente.

2.6 Costi e benefici

Quando consideriamo i costi di una valutazione dobbiamo distinguere fra:
- costi diretti: costo vero e proprio della valutazione;
- costi indiretti: il tempo impiegato, la formazione dei valutatori per l'uso di specifici strumenti di analisi, l'impatto sul processo di sviluppo.

Puntiamo l'attenzione su quelli indiretti, poiché mentre nel primo caso i costi di valutazione sono potenzialmente ripartiti su un gran numero di clienti, nel secondo caso i costi andranno a pesare sul singolo cliente o proprietario.
Benefici: la valutazione può essere richiesta, ad esempio, per dei contratti di governo o per la commercializzazione di prodotti. La valutazione, inoltre, può migliorare la percezione degli utenti rispetto a un prodotto o sistema.

3. Prospettiva storica dei metodi di valutazione

Le *istituzioni militari e governative* sono state le prime conducenti di ricerca in materia di sicurezza del computer. Il lavoro per creare un insieme di linee guida per la valutazione della sicurezza di prodotti e sistemi informatici ebbe inizio nel 1967 negli USA di cui il primo prodotto fu **l'Orange Book** (1983) o **TCSEC** (Trusted Computer System Evaluation Criteria), che rappresenta il punto focale della Rainbow Series, rilasciato nelle sua prima versione ufficiale nel 1983 dalla NCSC (U.S. National Computer Security Center) su commissione del DoD (Departement of Defense).
L'Orange Book fa parte di una collezione di documenti sui requisiti della sicurezza, sulla gestione della sicurezza e sua valutazione, pubblicato dal NSA (US National Security Agency) e NCSC (US National Computer Security Center). I documenti di questa serie sono conosciuti grazie al colore della loro copertina come **Raimbow Series**.
I concetti introdotti dall'Orange Book sono adattati a degli specifici aspetti ad esempio:
- *Red Book*: Computer Networks (Trusted Network Interpretation),
- *Purple Book*: DBMS (Trusted Database Management System Interpretation).

Alla fine degli anni Ottanta anche in Europa si cominciò a sentire l'esigenza di sviluppare criteri di valutazione della sicurezza dei sistemi informatici. Nel Regno Unito, ad esempio, è il caso del Memorandum Number 3: a uso del governo ed elaborato dalle proposte del Dipartimento dell'Industria e Commercio, denominato Green Book.
In Germania, l'Ente per la sicurezza dell'informazione ha pubblicato, nel 1989, una prima versione dei propri criteri; allo stesso tempo, in Francia, sono stati elaborati criteri denominati Livre bleu-blanc-rouge (Libro bianco, rosso e blu).
In seguito Francia, Germania, Paesi Bassi e Regno Unito hanno riconosciuto la necessità di accostarsi al problema in modo armonizzato e di definire criteri di sicurezza comuni poiché le industrie erano contrarie all'adozione di criteri di sicurezza diversi in ogni paese e i concetti e gli approcci di base adottati dai vari paesi coincidevano, anche per quanto riguarda le varie applicazioni in ambito commerciale, governativo e militare.

L'elaborazione di questi criteri comuni ha portato alla formazione del cosiddetto **ITSEC** (Information Technology Security Evaluation Criteria) che altro non è che il risultato dell'armonizzazione dei criteri comuni, commissionato nel 1991 dalla Comunità Europea.
ITSEC fù ampiamente utilizzato per un periodo di 10 anni fino alla nascita dei Common Criteria (CC). L'attività di ricerca su questo tema non si è però fermata e ha portato la Commissione delle Comunità Europee ad elaborare nel 1993 un nuovo documento per la definizione di metodologie di valutazione sulla base dei criteri descritti in ITSEC, intitolato *Information Technology Security Evaluation Manual* (TSEM).
Nel 1989 anche il Canada rilasciò la prima versione del Canadian *Trusted Computer Product Evaluation Criteria (**CTCPEC**)* . Il CTCPEC faceva affidamento al TCSEC, ma inserendo alcune nuove idee, sposando, ad esempio, la separazione fra i cosiddetti criteri funzionali e i criteri per la valutazione dell'affidabilità del sistema.
Nel 1991 il NIST (*National Institute for Standard and Technology*) e l'NSA (*National Security Agency*) hanno avviato un progetto congiunto, denominato *Federal Criteria Project*, che ha portato, nel dicembre del 1992, alla definizione dei **Federal Criteria** per la valutazione della sicurezza dei prodotti informatici. L'approccio scelto è quello di mantenere forme di compatibilità con i TCSEC ma basarsi su principi più simili a quelli dei criteri ITSEC e CTCPEC. Un concetto centrale nei criteri federali è quello che secondo la terminologia anglosassone viene definito il *protection profile*.
A completamento di questa presentazione sommaria dei criteri di sicurezza va citato lo sviluppo, dei CC. Varie organizzazioni in carica sulla valutazione della sicurezza si uniscono insieme nel Common Criteria Editing Board (CCEB) e producono i **Common Criteria** in modo da allineare i vari criteri di valutazione quali TCSEC, ITSEC, CTCPEC e i Federal Criteria. Nel 1999 i Common Criteria diventano uno standard internazionale: ISO 15048. Il CCEB viene succeduto dal CCIB (CC Implementation Board, 2004). Nei CC la stretta separazione fra classi funzionali e livelli di garanzia, adottata nel ITSEC, viene abbandonata, per seguire i Federal Criteria nell'uso dei Protection Profiles, in modo da predefinire delle classi di protezione.

4. Orange Book

Noto anche come TCSEC - Trusted Computer System Evaluation Criteria è stato commissionato dal DoD (1983/85). Come detto è la prima metodologia completa per la valutazione della sicurezza ed è il punto focale della Rainbow Series.
Non tratta di sicurezza ma di livelli di fiducia: un prodotto/sistema è fidato se è dotato di determinate protezioni. Principalmente orientato alla valutazione dei sistemi operativi multiutente.
Oltre a quello di protezione in ambito militare richiesto dal DoD e per cui è nato, i criteri sono stati sviluppati con gli obiettivi di:
1. Fornire agli utenti un metro con cui valutare il grado di fiducia che può essere immesso nei sistemi informatici;
2. Fornire una base per decretare i requisiti di sicurezza nelle specifiche di acquisizione;
3. Fornire una guida per sviluppatori e costruttori di sistemi per quanto riguarda la realizzazione delle caratteristiche di sicurezza ed i livelli di assicurazione che devono inglobare i loro prodotti affinché siano rispettati i requisiti di fiducia per le applicazioni sensibili.

4.1 Requisiti fondamentali di sicurezza

Nell'ambito dei *TCSEC* il problema della *riservatezza* dell'informazione è visto come primario rispetto a quello dell'*integrità* e della *disponibilità* secondo un approccio adottato tipicamente in campo militare, almeno all'epoca della pubblicazione di tali criteri. *L'Orange Book,* definisce sette classi di sistemi, che in seguito vedremo. L'assegnazione di un sistema ad una delle sette classi avviene sulla base dei seguenti **requisiti fondamentali**:
- Security policy: politiche di sicurezza precise e ben definite, distinzione fra DAC e MAC
- Marking of objects: si assegna a ciascun oggetto un livello di criticità attraverso un etichetta (come vedremo non richiesta fino alla classe B1).
- Identification of subject: ogni soggetto deve essere identificato e autenticato.
- Accountability: capacità del sistema di tenere traccia delle attività delle varie entità (verifica: log mantenuti e protetti, cammini fidati - Trusted Path). Se ne occupa il TCB:

- ***TCB*** - *Trusted Computing Base:* (insieme di componenti HW e SW definiti e conosciuti come fidati) deve tener traccia attraverso registri di controllo di eventi rilevanti sulla sicurezza (login, operazioni sugli oggetti, logout);

- Assurance: la fiducia che può essere riposta nel livello di sicurezza fornito dal sistema. Il sistema deve mantenere componenti HW, FW e SW affidabili, valutabili separatamente per assicurare che il sistema svolga i proprio compiti in maniera corretta (meccanismi affidabili e verifica indipendete). Si articola in tre categorie: affidabilità delle operazioni, del processo di sviluppo e documentazione;
- Documentation: gestori e utenti di un sistema sicuro necessitano di una guida per installare e utilizzare tutte le proprietà di sicurezza; cosi come i valutatori necessitano di documentazioni sulla progettazione per poterli sottoporre a test. Sono divisi in:

- una guida utente con caratteristiche di sicurezza (SFUG)
- una guida amministratore chiamata *Trusted Facility Manual (TFM*)
- documentazione di test: piani di test, procedure, prove e risultati dei test.

Tutte le classi richiedono questa documentazione, e più il livello della classe aumenta tanto più i requisiti funzionali e di garanzia aumento.
- Continuos protection: gli accessi ad oggetti con importanza rilevante per quanto concerne la sicurezza dovrebbero essere continuamente monitorati; i meccanismi di sicurezza non dovrebbero essere manomessi.

4.2 Scala TCSEC

L'Orange book stabilisce quattro categorie di sicurezza:
- **D – Minimal Protection**: è riservato a quei sistemi che sono stati valutati, ma che non riescono a soddisfare i requisiti di valutazione per essere inseriti nelle altre classi. In genere nessun sistema viene inserito in questa classe perché la valutazione è una operazione molto costosa e quindi i fabbricanti tendono a predisporre sistemi che rientrino in una delle classi superiori.
- **C – Discretionary Protection** ('need to know'): prevede una protezione discrezionale (necessità di sapere) e la responsabilità dei soggetti sulle azioni che intendono avviare attraverso l'inclusione di capacità di controllo. Forniscono politiche DAC e politiche per il riuso degli oggetti.
- **B – Mandatory Protection** (based on labels): requisito fondamentale è la politica MAC, la protezione è obbligatoria, diventano necessari i meccanismi per etichettare la criticità dei dati ed altri che assicurino che utenti non autorizzati non possano passare informazioni vitali per il sistema senza una adeguata autorizzazione.
- **A – Verified Protection**: caratterizzata dall'uso di metodi di verifica formale di sicurezza per assicurare che i controlli di sicurezza obbligatori e discrezionali impiegati nel sistema sono in grado di proteggere efficacemente le informazioni classificate o altre informazioni sensibili memorizzate o elaborate dal sistema.

Le categorie di sicurezza sono definite in modo incrementale: tutti i requisiti di una divisione sono automaticamente inclusi fra i requisiti di tutte quelle superiori. Prodotti in categorie superiori forniscono maggiori meccanismi di sicurezza e una maggiore garanzia attraverso una più rigorosa analisi. Inoltre le categorie C, B e A sono suddivise a loro volta in una serie di classi gerarchiche: C1, C2, B1, B2, B3 e A1.

4.3 Classi di valutazione TCSEC:

C1: Discretionary Security Protection

Un sistema è definito C1 se è composto da una serie di processi, utenti e dati che cooperano allo stello livello di integrità. Applica una separazione fra dati e utenti. La classe C1, ha requisiti funzionali minimi solo per l'identificazione e l'autenticazione un nome (username) che li riconosce univocamente sul sistema e una password che ne convalida l'identità. Richiede un controllo di accesso discrezionale (DAC) sulla base di singoli utenti o gruppi. Il sistema inoltre deve mantenere l'integrità dei dati utente/password impedendo gli accessi non autorizzati. Anche i requisiti di garanzia sono minimi, copre solo i test per difetti evidenti e la documentazione necessaria risulta essere la stesura di una guida utente, di un manuale per gli amministratori di sistema (TFM) e della documentazione per i test e di progetto. Questa classe è stata utilizzata solo per un breve periodo, e nessun prodotto è stato valutato in questa classe dopo il 1986 poiché un

sistema appartenente a questa classe non offre particolari strumenti di sicurezza; per questo motivo il livello C1 è adatto ad ambienti di tipo non professionale.

C2: Controlled Access Protection
La **Classe** C2, detta di protezione ad accesso controllato, è un'estensione della classe C1. A questa classe appartengono i sistemi che effettuano un controllo più rigido sugli accessi a oggetti del sistema da parte di soggetti autenticati, con la possibilità di definire gli accessi a diversi livelli di granularità: DAC a granularità dei singoli utenti. E' obbligatorio tenere traccia di tutte le operazioni di una certa rilevanza dal punto di vista della sicurezza. Si effettuano test per i soli difetti evidenti. Anche se i sistemi C2 restano collocati a un livello di sicurezza abbastanza basso molti prodotti commerciali, compresi anche i SO e DBMS appartengono a questa classe che è considerata come la "*più ragionevole classe per applicazioni commerciali*" (European Computer Manufacturers Association, 1993) nonostante i sistemi C2 risultino piuttosto deboli.
I sistemi C2 spesso prevedono degli strumenti in grado di guidare l'installazione dei prodotti secondo le specifiche C2 stesse, in modo da assicurare un implementazione conforme.

B1: Labelled Security Protection (etichettati)
La **Classe** B1, richiede l'implementazione delle etichette dei dati per importanza in modo da escludere o includere gli utenti individualmente. Il sistema deve garantire omogeneità nelle etichette mentre i dati vengono trasferiti. All'interno della classe B1 sono presenti tutti quei prodotti che si occupano di dati classificati e applicano politiche MAC conformi al modello Bell-LaPadula (uso di un modello formale). Ogni soggetto ed ogni oggetto è etichettato e l'integrità delle etichette deve essere protetta. Identificazione e autenticazione contribuiscono a determinare l'etichetta di sicurezza del soggetto. Seguendo questo tipo di approccio sorge il problema di come considerare un'etichetta quando l'oggetto viene esportato in un sistema esterno a quello in cui tale etichetta è stata definita. Solitamente questa situazione viene gestita in modo differente a seconda di come il dato è esportato: se la comunicazione avviene secondo uno schema multilivello, tutti gli oggetti possono essere esportati mantenendo la propria etichetta, mentre se la comunicazione avviene a un singolo livello il dato viene valutato dalla TCB e da utenti autorizzati in base alla sua criticità e quindi ri-etichettato secondo una nuova definizione compatibile con il nuovo sistema.
Per ottenere un elevato grado di sicurezza, questa classe richiede inoltre un contenuto più approfondito dei documenti di supporto e una fase di test sia a livello di prodotto sia a livello di codice sorgente, tali da rimuovere il maggior numero possibile di errori. Alla classe B1 appartengono sistemi complessi che comprendono la gestione della sicurezza a più livelli, spesso in ambiente Unix: sono classificati a questo livello il sistema V/MLS (da AT&T), e SO di venditori come Hewlett Packard, DEC e Unisys e DBMS come Trusted Oracle 7, INFORMIX-Online/Secure, Secure SQL Server.

B2: Structured Protection
La **Classe** B2 richiede un criterio di sicurezza formale strutturato. I sistemi di autenticazione degli utenti risultano essere più severi per garantire la validità e la sicurezza delle informazioni necessarie per autenticare. L'obbligo di controllo di accesso è richiesto per tutti gli oggetti. Etichettatura è estesa, ed è introdotto un *Trusted Path* per login e autenticazione iniziali.
La classe B2 aumenta la sicurezza dei sistemi multilivello principalmente aggiungendo nuovi vincoli alla fase di progettazione del sistema; occorre infatti progettare meccanismi di protezione della memoria per rendere possibile l'esecuzione di processi in uno spazio di indirizzamento riservato. Eventuali procedure di comunicazione tra entità differenti devono essere protette e monitorate. Il controllo di tipo MAC prevede anche la supervisione di dispositivi fisici. Inoltre, all'interno di questa classe, la descrizione delle politiche di sicurezza deve passare obbligatoriamente attraverso un modello formale, ad es. deve essere specificata mediante il modello Bell-LaPadula; è anche richiesto un Descriptive Top Level Specification (DTLS). La fase di test per i prodotti appartenenti a questa classe punta soprattutto alla difesa da attacchi esterni.
B2 è il livello valutato per il sistema operativo Trusted Xenix.

B3: Security Domain

La **Classe** B3, richiede al sistema di sicurezza di essere essenziale eliminando qualsiasi parte di codice non inerente la sicurezza. Sono inoltre richieste funzioni aggiuntive per segnalare all'amministratore le necessarie misure di sicurezza. Particolarità della classe B3 è l'elevata resistenza ad attacchi provenienti dall'esterno. Inoltre deve essere presente un amministratore delle politiche di sicurezza, un meccanismo di auditing in grado non solo di registrare tutte le azioni, ma anche di rilevare possibili intrusioni in atto, e infine deve essere possibile ripristinare il sistema in modo sicuro *Trusted Recovery* (recupero della fiducia dopo un guasto del sistema). Meccanismi di controllo monitorano le occorrenze o le accumulazioni di eventi rilevanti per la sicurezza e rilasciano automaticamente degli avvertimenti (warnings) in situazioni sospette. Necessaria la coerenza tra il modello formale della politica di sicurezza e quello informale (DTLS). Soddisfa i requisiti dei reference monitor. Valutazione B3 per le versioni di sistema operativo Wang's XTS-300 (e XTS-200), che gira in macchine Wang con HW di base x86.

A1: Verified Design
I prodotti appartenenti alla classe A1 sono funzionalmente equivalente a quelli della classe B3 ma raggiungono un più alto livello di garanzia attraverso l'uso di metodi formali.
La valutazione per la classe A1 richiede pertanto: un modello formale della politica di sicurezza, un Formal Top Level Specification (FTLS), prove di coerenza tra il modello e FTLS (formale, dove possibile), analisi formale dei canali nascosti, l'eventuale esistenza di canali nascosti deve essere giustificata, la larghezza di banda può essere limitata.
In aggiunta più rigorose configurazioni di gestione e distribuzione di controllo dovrebbero assicurare che la versione installata al sito del cliente sia la stessa della Master Copy valutata.
Valutazione A1 per le componenti di rete: LAN MLS (da Boeing) e Gemini Trusted Network Processor sistema operativo SCOMP.

Quanto l'Orange Book è stato scritto c'era la considerazione di definire più alte classi di affidabilità oltre A1 con maggiori requisiti sull'architettura del sistema, sui test, sulle specifiche e sulle verifiche formali e progettazione di ambienti affidabili.

4.4 Limiti e contributi del TCSEC
Il TCSEC era lontano dall'essere perfetto. Il suo campo di applicazione era limitato. Il processo di valutazione era difficile e spesso privo di risorse necessarie. Infine, le valutazioni del TCSEC erano riconosciuti solo negli USA, e le valutazioni di altri paesi non erano validi negli Stati Uniti.
La sua esistenza ha accresciuto la consapevolezza del settore commerciale di esigenze di sicurezza per computer. Le carenze del TCSEC hanno stimolato un'ondata di nuovi approcci in materia di valutazione che ha influenzato significativamente la tecnologia della valutazione.

4.4 Esempio: Sicurezza specificazioni NCSC per Unix
Sulla sicurezza di Unix Dennis Ritchie scrisse: << Unix non è stato progettato per essere sicuro ma è stato concepito con le necessarie caratteristiche per rendere la sicurezza funzionale>>.
Dal punto di vista dello NCSC tutte le versioni tradizionali di UNIX appartengono alla classe C1. Il Governo USA ha richiesto che entro il 1992 tutti i sistemi UNIX da esso impiegati raggiungessero almeno il livello C2. Inoltre, dal 1992, il Pentagono acquista solamente sistemi di classe B2, cioè sistemi molto affidabili.
Per quanto riguarda le singole versioni di UNIX possiamo fornire alcuni esempi:
- UNIX SCO versione 3.2 è certificato in classe C2;
- UNIX System V 4.1 versione ES (Enhanced Security, SVR4.1 ES), è il primo dei grandi sistemi UNIX che ha ottenuto la classificazione B2 dal Ministero della difesa USA supportando inoltre alcune caratteristiche della più rigorosa classe B3;
- La classe di sicurezza raggiunta da ULTRIX versione 4.0 è la C2;
- UNICOS può essere installato nella versione chiamata "UNICOS secure" che spinge molto a fondo i criteri di sicurezza.
È il caso di osservare che la notevole espansione del sistema UNIX in tutti gli ambienti (compresi quelli militare, giudiziario, bancario, ecc.) ha portato al proliferare di diversi UNIX "secure" per cui non è più fondata la cattiva fama di UNIX come sistema insicuro.

5. ITSEC - Information Technology Security Evaluation Criteria

ITSEC è il risultato dell'armonizzazione dei criteri di valutazione nei paesi Europei.
L'approccio evidenziato dai criteri ITSEC al problema della valutazione della sicurezza dei sistemi informatici si discosta da quello dell'*Orange Book*. Il metodo europeo per molti aspetti è più flessibile ed adattabile alla valutazione di sistemi con funzionalità non previste al momento della creazione dei criteri stessi. Il soggetto che richiede la valutazione viene denominato *sponsor* e può essere diverso da chi ha realizzato il sistema o il prodotto in questione.
Come già accennato, i TCSEC classificano i sistemi secondo una gerarchia nella quale per ciascuna classe sono specificati sia requisiti di funzionalità che di garanzia; i criteri ITSEC permettono, invece, la scelta di arbitrarie funzioni di sicurezza e definiscono sette livelli di valutazione dell'affidabilità e che rappresentano una crescente fiducia nella capacità del sistema di soddisfare le sue specifiche di sicurezza per mezzo delle funzioni suddette. La principale innovazione di questo approccio è costituita dalla netta separazione tra i requisiti di funzionalità e quelli di affidabilità. Inoltre a differenza del TCSEC è prevista la possibilità di *upgrade* delle classi funzionali.
Con il termine Assurance si intende sia la fiducia (confidence) nell'efficacia (effectiveness) delle funzioni di sicurezza, sia la fiducia nella loro correttezza (correctness).
La valutazione dell'efficacia mira a stabilire se le funzioni di sicurezza adottate sono idonee agli scopi specificati nel Security Target (ST), per cui sono state scelte e se i meccanismi che realizzano tali funzioni sono in grado di contrastare attacchi diretti.
Quest'ultimo aspetto viene misurato sulla base della cosiddetta "robustezza dei meccanismi" (strenght of mechanisms) per la quale sono stati definiti tre livelli: Base, Medio e Alto.
La fiducia nella correttezza viene espressa utilizzando una scala a sette livelli (da E0 ad E6) nella quale il livello più basso indica totale mancanza di fiducia.
Il processo di valutazione ai fini di una certificazione del sistema stesso consisterà nello stabilire se esso soddisfa o meno il suo Security Target con il livello di valutazione dichiarato del committente (Sponsor) e indicato nel Security Target stesso.
Per l'ITSEC, l'oggetto della valutazione è il TOE (Target of Evaluation) e lo sponsor è chi richiede la valutazione. La valutazione viene fatta prendendo a riferimento il security target (TS) che descrive le funzionalità offerte dal TOE, ed è un documento che deve contenere:

- una **System Security Policy** (nel caso dei sistemi) o un **Product Rationale** (nel caso dei prodotti). Insieme di leggi e regole e pratiche che stabiliscono come le informazioni critiche e le risorse devono essere gestite, protette e distribuite all'interno di uno specifico sistema (obiettivi di sicurezza, minacce, sicurezza fisica, organizzazione e procedure, misure sul personale)
- una specifica delle funzioni di sicurezza (**Security Enforcing Functions** o SEF) che permettono il conseguimento degli obiettivi individuati;
- la definizione dei meccanismi di sicurezza richiesti (opzionale);
- il livello minimo dichiarato di robustezza dei meccanismi (**strength of mechanisms**);
- il livello di valutazione desiderato (**Evaluation level**)

Col termine **SEF** (Security Enforcing Function), si intendono le contromisure raggruppate secondo un certo numero di categorie, le Generic Headings.

5.1 Tipologie funzionali ITSEC

Le singole funzioni di sicurezza vengono raggruppate, in **Generic Headings**, otto tipologie di funzioni di sicurezza che comunque possono essere integrate da nuove tipologie, con l'evoluzione delle tecnologie e delle tipologie d'attacco:
1- **Identification and Authentication**: Stabiliscono e verificano l'identità degli utenti che intendono accedere al sistema. L'identificazione avviene usualmente controllando la corrispondenza tra le informazioni fornite dall'utente e le informazioni associate all'utente e note al sistema di protezione.
2- **Access Control**: Garantiscono che un utente possa espletare le sole operazioni di propria competenza, inoltre l'accesso alle risorse autorizzato per utenti e processi, gestione e verifica dei diritti di accesso, eventuali limitazione dei diritti di accesso e della loro propagazione.
3- **Accountability**: Registrano gli accessi alle varie risorse del sistema: traccia delle azioni svolte da utenti e processi e delle azioni rilevanti per la sicurezza.

4- **Audit**: Permettono di indagare sugli eventi anomali o sopra determinati livelli che possono rappresentare una minaccia alla sicurezza. A questo gruppo appartengono le funzioni che hanno lo scopo di registrare ed analizzare gli eventi, oppure le funzioni che effettuano analisi statistiche al fine di individuare eventuali attacchi alla sicurezza.
5- **Object Reuse**: Garantiscono il riutilizzo di spazi di memoria, impedendo che ciò costituisca minaccia alla sicurezza. A questo gruppo appartengono le funzioni il cui scopo è quello di cancellare o inizializzare i supporti in modo che possano essere riutilizzabili
6 - **Accuracy**: Garantiscono l'integrità del SW e dei dati. A questo gruppo appartengono le funzioni il cui scopo è quello di effettuare analisi del SW e dei dati per segnalare, identificare e correggere eventuali violazioni: ad es. modifica non autorizzata dei dati, aggiunta, alterazione, cancellazione o trasferimento di dati tra processi.
7- **Reliability of Service**: A questo gruppo appartengono le funzioni il cui scopo è quello di assicurare che le risorse siano accessibili ed utilizzabili su richiesta di qualunque utente abilitato, entro i tempi prefissati
8- **Data Exchange**: A questo gruppo appartengono le funzioni il cui scopo è quello di assicurare disponibilità, riservatezza ed integrità ai canali trasmissivi ovvero la sicurezza delle trasmissioni.

5.2 Gradi di robustezza

Vengono definiti tre possibili gradi di robustezza (Base, Medio e Alto) che rappresentano crescenti livelli di capacità del meccanismo di sicurezza di resistere ad un attacco diretto:
- **BASE** se al minimo fornisce protezione contro eventi sovversivi casuali, benché possa essere violata da alcuni aggressori;
- **MEDIA** se al minimo fornisce protezione contro aggressioni caratterizzate da limitate opportunità o risorse;
- **ALTA** se può essere superata solo da aggressioni caratterizzate da un alto livello di esperienza, opportunità e risorse, con attacchi portati con successo al di sopra della normale praticabilità.

Nel documento ITSEM (Annex 6.C) vengono definite le modalità di determinazione del grado di robustezza del meccanismo basate su:
- tempo necessario per violare il meccanismo (minuti, giorni, mesi);
- complicità necessaria (senza complici, con un utente, con un responsabile);
- esperienza tecnica necessaria (diffusa, professionale, esperto);
- tipo di attrezzatura da utilizzare (nessuna, apparecchiatura normale oppure speciale).
I livelli previsti variano da E0 ad E6, secondo crescenti livelli di fiducia.
La normativa ITSEC prevede la valutazione dell'efficacia e della correttezza del sistema di protezione. Al crescere del livello di valutazione desiderato, lo sponsor deve fornire al valutatore documentazione che attesti un crescente rigore e l'introduzione di strumenti formali nelle varie fasi costruttive.

5.3 Livelli ITSEC

Il ITSEC prevede sei livelli di fiducia, chiamati livelli di valutazione, E1, E2, E3, E4, E5 e E6.
Un settimo livello, **E0**, è stato utilizzato per prodotti che non soddisfano altri livelli.
I livelli dell'ITSEC sono elencati dal più basso al più alto. Ogni livello include i requisiti del precedente livello.

1. Il Livello **E1** richiede un obiettivo di sicurezza (ST) per valutare il prodotto o il sistema; una descrizione informale dell'architettura del prodotto/sistema. Il prodotto/sistema deve essere in grado di dimostrare che il suo ST è soddisfatto.
2. Livello **E2** richiede una descrizione informale di progettazione dettagliata del prodotto/sistema del TOE, come pure il controllo di configurazione e di un processo di controllo della distribuzione. Prove di collaudo deve essere fatta.
3. Livello **E3** ha requisiti più severi sui dettagli di progettazione ed è anche necessaria una corrispondenza tra il codice sorgente e i requisiti di sicurezza.
4. Livello **E4** richiede anche di un modello formale della politica di sicurezza, un più rigoroso approccio strutturato all'architettura e di progettazione dettagliata, e di un'analisi di vulnerabilità a livello di progettazione.

5. Livello **E5** richiede una corrispondenza tra il progetto dettagliato e il codice sorgente, e un'analisi di vulnerabilità a livello di codice sorgente.
6. Livello **E6** richiede anche un ampio uso di metodi formali. Un'altro requisito è la mappatura parziale del codice eseguibile per il codice sorgente.

6. Federal Criteria

In estrema sintesi esso è una descrizione astratta di requisiti di sicurezza per la programmazione, la realizzazione e l'uso di un prodotto. È indipendente dallo specifico prodotto ed è costruito combinando requisiti per le funzioni di sicurezza e requisiti di affidabilità con una descrizione delle minacce previste e delle modalità d'uso del prodotto. I requisiti per le funzioni di sicurezza e i requisiti di affidabilità del sistema sono descritti in termini di una serie di componenti funzionali e di componenti di assurance per ognuna delle quali è previsto un ordinamento gerarchico secondo un approccio che per quanto riguarda gli aspetti funzionali è analogo a quello adottato nei CTCPEC e che qui, però, viene esteso anche agli aspetti di affidabilità. Le componenti funzionali e quelle di affidabilità proposte nei criteri consentono la costruzione di *protection profile* corrispondenti a classi TCSEC o ad altre forme di descrizione delle specifiche di sicurezza di prodotti valutati secondo altri criteri esistenti. Il contenuto di un *protection profile* è in realtà simile a quello di un *security target* come definito in ITSEC esso deve però risultare, come già accennato, indipendente dal prodotto e quindi costituisce una descrizione di requisiti di sicurezza condotta ad un livello teorico che non tiene conto del concreto sistema informatico. I FC prevedono requisiti funzionali e qualitativi separati e possibilità di *upgrade* sia dei requisiti funzionali sia di quelli qualitativi**.**

6.1 Un **Protection Profile** ha cinque sezioni:

- Descriptive Elements: 'nome' del profilo di protezione, inclusa la descrizione del problema da risolvere.
- Rationale: la motivazione del profilo di protezione, compresa la minaccia, l'ambiente, e le ipotesi di utilizzo, una serie di orientamenti sulle politiche di sicurezza che può essere supportato.
- Functional Requirements: stabilisce il limite di protezione che deve essere fornita dal prodotto.
- Development Assurance Requirements: per tutte le fasi di sviluppo.
- Evaluation Assurance Requirements: specifica il tipo e l'intensità della valutazione.

7. Common Criteria

Sono uno standard che riunisce i criteri in uso presso USA, Canada, Europa dal Dicembre 1999 i CC sono divenuti uno standard internazionale **ISO 15408.** Questo standard non fornisce una lista di requisiti di sicurezza o funzionalità che il sistema deve possedere, ma descrive solo un quadro concettuale al cui interno gli utilizzatori di un sistema informatico possono specificare i loro requisiti di sicurezza, i produttori possono implementare e pubblicizzare le caratteristiche dei loro sistemi e i laboratori di test possono valutare i sistemi per determinare se effettivamente soddisfano i requisiti dichiarati.

In altri termini i *Common Criteria* assicurano che il processo di specificazione, implementazione e valutazione di un sistema rispetto alla sicurezza informatica venga condotto in una maniera rigorosa e standardizzata.

La flessibilità dell'approccio dei CC sta nel fatto che un prodotto è valutato a fronte di un certo *profilo di protezione(PP)*, strutturato in modo da soddisfare specifici requisiti di protezione. Rispetto all'ITSEC, di cui conserva molti aspetti, come la separazione tra funzionalità a garanzia, i CC forniscono cataloghi di funzionalità e requisiti di garanzia che rendono più formale e ripetibile la compilazione del Security Target.

Un sistema/prodotto è sicuro se si specifica:

- "sicuro" per fare cosa (obiettivi di sicurezza)
- "sicuro" in quale contesto (ambiente di sicurezza)
- "sicuro" a fronte di quali verifiche (requisiti di assurance).

Un *obiettivo di sicurezza* viene definito, secondo i CC, come l'intenzione di contrastare una minaccia o quella di rispettare leggi, regolamenti o politiche di sicurezza preesistenti. Il conseguimento degli obiettivi avviene attraverso l'adozione di misure di sicurezza tecniche (funzioni di sicurezza) e non tecniche (fisiche, procedurali e relative al personale). Tale obiettivo è riportato in un documento chiamato (*Security Target* - ST) che deve essere obbligatoriamente

fornito e rappresenta il documento principale della valutazione. Nel *Securuty Target* devono essere descritti l'ambiente di sicurezza, gli obiettivi di sicurezza, i requisiti funzionali e di *assurance*, la robustezza minima delle funzioni di sicurezza ed una prima descrizione ad alto livello delle funzioni di sicurezza.
L'*ambiente di sicurezza* viene descritto in termini di:
- uso ipotizzato del sistema/prodotto (applicazioni, utenti, informazioni trattate ed altri beni con specifica del relativo valore)
- ambiente di utilizzo (misure di sicurezza non tecniche, collegamento con altri apparati ICT)
- minacce da contrastare, specificando caratteristiche dell'attaccante (conoscenze, risorse disponibili e motivazione), metodi di attacco (citando lo sfruttamento di eventuali vulnerabilità note del sistema/prodotto ICT), beni colpiti
- politiche di sicurezza dell'Organizzazione.

Le verifiche previste durante il processo di valutazione mirano ad accertare che siano stati soddisfatti, da parte del sistema/prodotto, del suo sviluppatore e del valutatore, i *requisiti di assurance* che diventano sempre più severi al crescere del livello di valutazione.
I *CC* definiscono una scala di 7 livelli di valutazione (EAL1, EAL2, ... EAL7) o livelli di *assurance*, precisando, per ogni livello di tale scala uno specifico insieme di *requisiti di assurance*. Il livello EAL1, cui corrisponde il livello di sicurezza più basso, non ha corrispondenti nei precedenti criteri di valutazione.
Concetti dei CC:
- TOE - Target of Evaluation: criteri per la valutazione della sicurezza di prodotti/sistemi. Costituisce l'oggetto della valutazione.
PP - Protection Profile: serie (riutilizzabile) di requisiti di sicurezza, compresa una EAL; deve essere sviluppato da un gruppo di utenti per catturare tipiche esigenze di protezione
ST - Security Target: esprime i requisiti di sicurezza per uno specifico TOE (beni, minacce, ipotesi, ambiente operativo). E' suddiviso generalmente in:
    - Obiettivi di sicurezza
    - Requisiti funzionali relativi alla sicurezza
    - Requisiti di sicurezza informatica
    - Assunzioni
    - Rationale
EAL - Evalutation Assurance Level: definisce cosa deve essere fatto in una valutazione, ci sono sette ordini gerarchici gli EALs.

7.1 Livelli di sicurezza dei CC
EAL1 - functionally tested: il tester riceve l'obiettivo di valutazione, esamina la documentazione ed esegue alcuni test per confermare la funzionalità documentate; la valutazione non richiede alcuna assistenza da parte degli sviluppatori, l'esborso per la valutazione dovrebbe essere minimo.
EAL2 - structurally tested: lo sviluppatore fornisce la documentazione e i risultati dei test ottenuti dall'analisi delle vulnerabilità; il valutatore controlla le documentazioni di recensione e ripete alcuni di questi test; lo sforzo richiesto allo sviluppatore è piccolo.
EAL3 - methodically tested and checked: lo sviluppatore utilizza la gestione della configurazione, i documenti in materia di sicurezza per lo sviluppo e prevede la progettazione di documentazione ad alto livello e di documentazione sui test di copertura per il riesame. EAL3 è destinato agli sviluppatori che hanno già seguito una buona prassi di sviluppo, ma che non vogliono attuare ulteriori modifiche alle loro pratiche.
EAL4 - methodically designed, tested, and reviewed: lo sviluppatore fornisce un basso livello di progettazione e il codice sorgente per la valutazione di un sottoinsieme di funzioni di sicurezza (TCB); garantisce la consegna delle procedure; il valutatore svolge indipendente un analisi della vulnerabilità. EAL4 è il più alto livello che è economicamente fattibile per una linea di prodotti esistenti.
EAL5 - semiformally designed and tested: lo sviluppatore fornisce il modello formale delle politiche di sicurezza, un semi-formale alto livello di progettazione, specifiche funzionali, e l'intero codice sorgente delle funzioni di sicurezza; un canale nascosto di analisi; il valutatore esegue, indipendentemente, test di penetrazione.

Il TOE deve essere stato progettato e sviluppato con l'intento di raggiungere il livello EAL5 di garanzia; ulteriori costi di valutazione non devono essere esosi.
EAL6 - semiformally verified design and tested: il codice sorgente ben strutturato, Reference monitor con una bassa complessità; il valutatore effettua intensivi test di penetrazione; il costo della valutazione aumenta.
EAL7 - formally verified design and tested: lo sviluppatore fornisce una formazione funzionale specifica e di un elevato livello di progettazione, dimostra la corrispondenza tra tutte le rappresentazioni di funzioni di sicurezza. EAL7 tipicamente realizzato solo con un TOE, che ha una ben precisa funzionalità di sicurezza e si prestano ad ampie analisi formali.

7.2 Corrispondenza dei livelli di fiducia
La tabella seguente dà una vaga corrispondenza dei livelli di fiducia delle diverse metodologie. La tabella indica che il CC offre un livello che è inferiore a qualsiasi livello precedentemente offerto.

TCSEC	**ITSEC**	**CC**
D	E0	No equivalent
No equivalent	No equivalent	EAL1
C1	E1	EAL2
C2	E2	EAL3
B1	E3	EAL4
B2	E4	EAL5
B3	E5	EAL6
A1	E6	EAL7

7.3 Esempi di valutazione di SO con i CC
EAL4:
- Sun Solaris (TM) 8 Operating Environment
- HP-UX (11i) Version 11.11
- EAL4: B1/EST-X Version 2.0.1 with AIX, Version 4.3.1

EAL4+:
- AIX 5L for POWER V5.2 Programm Number 5765-E62
- Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886 Hotfix

EAL3:
- SGI Trusted IRIX/CMW Version 6.5..

7.4 Un prodotto certificato CC è sicuro?
Ogni vulnerabilità che possa compromettere il prodotto nella configurazione di valutazione, dovrebbe comportare:
- Cancellazione volontaria da parte del produttore della propria certificazione
- Il produttore dovrebbe rivalutare il prodotto per includere l'applicazione delle patch per fissare le vulnerabilità nella configurazione di valutazione
- Teoricamente la certificazione dovrebbe essere sospesa o cancellata dall'ente che l'ha emessa

ESEMPIO:
Microsoft Windows 2000 `e un prodotto certificato EAL4+, ma sono ancora pubblicate regolarmente da Microsoft patch di sicurezza per vulnerabilità. La certificazione EAL4+ di Microsoft Windows 2000, deve essere considerata sicura solo nella configurazione di valutazione specificata da Microsoft stesso.
La valutazione di Microsoft Windows 2000 resta EAL4+ solo se non si applica di nessuna patch.

8. Conclusioni
8.1 Evaluation Methodology
La Common Evaluation Methodology (CEM) specifica tutte le misure che devono essere seguite per convalidare i requisiti di garanzia di sicurezza in un ST.
Il Common Criteria Recognition Agreement (CCRA), prevede il riconoscimento delle valutazioni effettuate in altri paesi. I livelli di garanzia indirizzabili vanno da EAL1 a EAL4. Più elevati livelli di garanzia sono ammessi solo all'interno di un unico paese.

Il Common Criteria Evaluation and Validation Scheme (CCEVS) è un programma nazionale statunitense per l'esecuzione di valutazioni di sicurezza secondo i Common Criteria.

8.2 Standard di qualità

Come valutare il modo in cui un prodotto è sviluppato, con nessun riferimento al prodotto stesso? Standard come **l'ISO 9000** raccomandano alle organizzazioni come mettere in atto la gestione della qualità interna e l'affidabilità della qualità esterna per attestare la qualità dei loro prodotti. Alcuni fornitori registrati sotto il marchio di qualità ISO 9000 sostengono che è un miglior argomento di vendita rispetto a un certificato di sicurezza per un determinato prodotto e che la valutazione della sicurezza dovrebbe muoversi in questa direzione.
La proposta è interessante per le imprese che sviluppano sistemi di sicurezza: in tal modo i costi della valutazione sono molto ridotti.

8.3 Conclusioni: Uno sforzo ben speso?

L'interesse verso i criteri e le metodologie di valutazione della sicurezza, nato inizialmente in ambito militare e governativo, si è diffuso anche al di fuori degli ambienti in cui aveva avuto origine. La decisione da parte di un'azienda di sottoporre un proprio prodotto a valutazione di sicurezza può derivare o da specifici requisiti di un particolare progetto o dall'esigenza di creare un'immagine prestigiosa dell'azienda stessa inserendosi nel mercato della sicurezza attraverso prodotti affidabili e sicuri. L'azienda che offre prodotti valutati si presenta ai clienti con maggiore credibilità e può quindi aspettarsi un incremento delle vendite. L'utente di sistemi o prodotti informatici, d'altra parte, vede nella certificazione della sicurezza una prova originata da una terza parte indipendente che conferma le caratteristiche di sicurezza dichiarate dal fornitore. Inoltre, il certificato costituisce un utile strumento per il confronto tra i diversi prodotti presenti sul mercato.
La valutazione della sicurezza in accordo con i CC è stata richiesta in alcuni paesi dai clienti del settore pubblico. I maggiori venditori di Sistemi Operativi e DBMS offrono prodotti valutati. In verità, al di fuori del settore pubblico vi è stato poco entusiasmo per la valutazione dei prodotti. Una eccezione corrente sono i SW per le smart card.

La valutazione della sicurezza è, comunque, criticata per i suoi costi eccessivi. Un report presentato dall'ECMA (European Computer Manufacturers Association, 1993) apprezza il ruolo della classe C2 dell'Orange Book, nello stabilire una base per la sicurezza di tutti i SO, ma insiste sul bilanciare costi, produttività e sicurezza. Il report raccomanda di basarsi sullo standard di qualità come **ISO 9000** come alternativa alla valutazione della sicurezza.

Il costo della valutazione, infatti, varia dal 10% al 40% dei costi di sviluppo. I Problemi persistenti riguardano:
- la segretezza dei processi di valutazione;
- l'ambiguità di interpretazione dei criteri;
- i costi della rivalutazione di nuove versioni di prodotti valutati

Gli ultimi due dovuti al fatto che i certificati si riferisco a una specifica versione o una particolare configurazione del prodotto, spesso ciò porta ad avere sistemi o prodotti che si evolvono, e una rispettiva valutazione che si riferisce a una versione non più in uso di tali sistemi e che pertanto non offre garanzie di sicurezza.