Common Criteria 4 IT Security Evaluation - parte 1: Intro e modello generale

Sintesi di Common Criteria ... parte 1

I contenuti dei titoli tra parentesi quadre sono da scrivere. Se la parentesi quadra è solo a destra, il contenuto è incompleto.

Nel testo, i vocaboli *assicurazione* e *confidenza* sono sinonimi.

5 Simboli e termini abbreviati

Acronimo	Nota
API	Application Programming Interface
ASE	Assurance class: Security Target Evaluation
ASE_CCL	Conformance Claims
ASE_ECD	Extended Components Definition
ASE_INT	ST Introduction
ASE_OBJ	Security Objectives
ASE_REQ	Security Requirements
ASE_SPD	Security Problem Definition
ASE_TSS	TOE Summary Specification
ATM	Automated Teller Machine
CAP	Composed Assurance Package
CC	Common Citeria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
CEM	Common Methodology for Information Technology Security Evaluation

Acronimo		Nota
CM	Configuration Management	
DAC	Discretionary Assurance Level	
EAL	Evaluation Assurance Level	
GHz	Gigahertz	
GUI	Graphical User Interface	
IC	Integrated Circuit	
IOCTL	Input Output Control	
IP	Internet Protocol	
IT	Information technology	
MB	Megabyte	
NAT	Network Address Translation	
NdT	Nota del Traduttore	
OS	Operating System	
OSP	Organisational Security Policies	
PC	Personal Computer	
PCI	Peripheral Component Interconnect	
PKI	Public Key Infrastructure	
PP	Protection Profile	
RAM	Random Access Memory	
RPC	Remote Procedure Call	
SAR	Security Assurance Requirements	
SFP	Security Function Policy	
SFR	Security Functional Requirements	
SPD	Security Problem Definition	
ST	Security Target	
TCP	Transmission Control Protocol	
TOE	Target Of Evaluation	
TSF	TOE security functionality	
TSFI	TSF Interface	

6 Overview

6.1 Target Of Evaluation (TOE)

TOE è il sistema da analizzare: un insieme di hardware + software + firmware + direttive (documentazione). Può essere un prodotto IT o parte di esso, o una tecnologia non trasformata in prodotto.

Ai fini dei CC, la valutazione di un TOE contenente parte di un prodotto IT non deve essere confusa con la valutazione dell'intero prodotto IT.

Nei CC un TOE può avere diverse rappresentazioni. Ad es.:

- un elenco di file;
- un singolo file compilato;
- una confezione con CD-ROM e manuali,

- una versione installata ed operativa.

Un prodotto IT di solito può essere installato e configurato in modi diversi. Nell'ambito dei CC si deve specificare quali configurazioni sono in valutazione, per evitare che si possa considerare una configurazione che non soddisfi i requisiti valutati. Quindi vi può essere differenza tra le direttive del prodotto (più configurazioni) e quelle del TOE (una, o poche, configurazione). Se un TOE prevede più di una configurazione, l'insieme delle configurazioni previste formano comunque il TOE.

6.2 Pubblico target dei CC

I CC interessano:

- **consumatori**;
- **sviluppatori**;
- **valutatori**.

I CC sono scritti per assicurare che la valutazione soddisfi le necessità dei *consumatori*. Questi devono esprimere i loro requisiti di sicurezza in modo non ambiguo, utilizzando una struttura dati detta **Protection Profile** (PP), che non dipende dalla implementazione del TOE.

Per assistere gli *sviluppatori*, i CC prevedono la definizione dei requisiti di sicurezza secondo una struttura dati detta **Security Target** (ST), la cui struttura dipende dall'implementazione del TOE. IL ST si può basare su uno o più PP per relazonarsi con i requisiti dei consumatori.

I CC contengono dei criteri, utilizzati dai *valutatori*, per giudicare se il TOE è conforme ai requisiti di sicurezza.

Altri gruppi di utenti possono trarre benefici dai CC di un TOE. Ad es.:

- addetti alla sicurezza dei sistemi;
- revisori;
- architetti e progettisti della sicurezza; ...

6.3 Le parti dei CC

I CC sono presentati in tre parti:

- **Parte 1, introduzione e modello generale**;
- **Parte 2, componenti per la sicurezza funzionale**; definisce un insieme di componenti funzionali da utilizzare come template standard; sono organizzati in famiglie e classi;
- **Parte 3, componenti per la garanzia di sicurezza**; insieme di componenti di garanzia da usare come template standard; anche questi organizzati per famiglie e classi. Inoltre questa parte definisce i criteri di valutazione per PP e ST e presenta 7 pacchetti di assicurazione predefiniti, detti Evaluation Assurance Level (EAL).

Esiste un quarto documento: **Common Methodology for Information Technology Security Evaluation** (CEM); documenta i metodi di valutazione per la sicurezza IT utilizzando i CC come base.

La seguente tabella indica la relazione tra uso dei documenti predetti e la tipologia d'utente.

	consumatori	**sviluppatori**	**valutatori**
parte 1	info generali. guida alla struttura delle PP	info generali e di riferimento. obbligatorio per lo sviluppo delle specifiche di sicurezza di un TOE	obbligatorio come riferimento e per la guida alla struttura di PP e ST
parte 2	guida per formulare i requisiti di un TOE	obbligatorio come riferimento per interpretare i requisiti funzionali e formulare le specifiche funzionali di un TOE	obbligatorio come riferimento per interpretare i requisiti funzionali
parte 3	guida per determinare il livello di sicurezza richiesto	riferimento per interpretare i requisiti di assicurazione e determinare gli approcci per l'assicurazione del TOE	riferimento per interpretare i requisiti di assicurazione

6.4 Contesto di valutazione

La valutazione deve essere effettuata seguendo uno **schema di valutazione** che definisce gli standard, controlla la qualità della valutazione e indica i regolamenti cui si devono conformare i valutatori e i loro strumenti. I CC non indicano uno schema obbligatorio. Ma per confrontare due diverse valutazioni si deve fare attenzione che siano stati usati gli stessi schemi.

In alternativa si usi la stessa metodologia. Per i CC questa metodologia è esposta dal CEM.

Può essere necessario sottoporre il risultato della valutazione ad un **processo di certificazione**. Ovvero un processo di ispezione del risultato, indipendente dagli attori che hanno effettuato la valutazione.

Gli *schemi di valutazione* e i *processi di certificazione* sono responsabilità delle **autorità di valutazione** e sono al di fuori dello scopo dei CC.

7 Modello generale

7.1 Risorse e contromisure

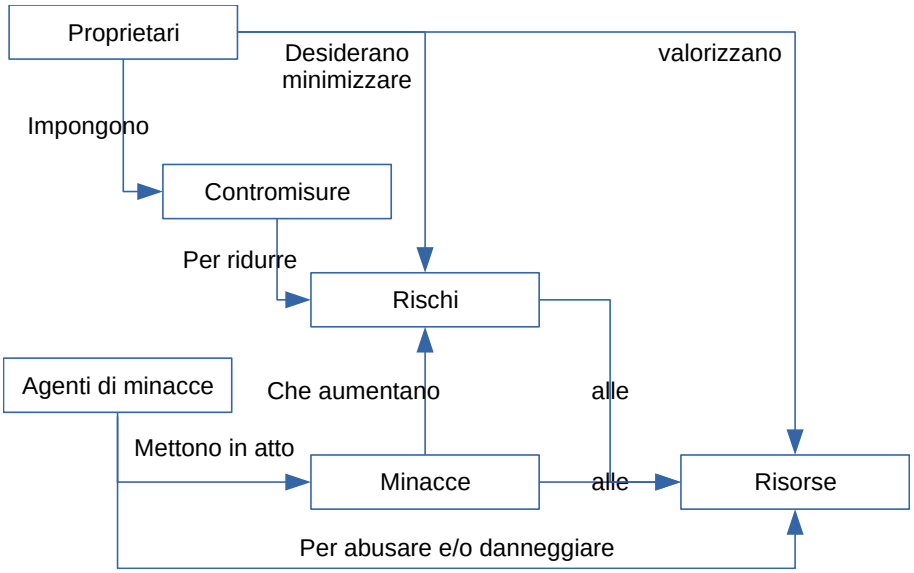
La sicurezza si occupa della protezione di **risorse**. Ovvero entità che hanno un valore (soggettivo). Ad esempio:

- contenuti di un file o server;
- autenticità dei voti espressi in una elezione
- disponibilità di un processo di commercio elettronico; ...

L'ambiente in cui è collocata la risorsa è chiamato **ambiente operativo**. Ad es.:

- la stanza elaboratori di una banca;
- una rete di computer connessa ad Internet;
- una LAN; ...

I proprietari delle risorse possono richiedere che la disponibilità, modifica, ... di queste risorse sia protetta dalle **minacce** tramite **contromisure**. Come illustrato nel seguente diagramma.



La salvaguardia delle risorse è responsabilità dei proprietari. Gli agenti delle minacce (hackers, utenti malevoli o non malevoli, processi, incidenti) possono cercare di abusare delle risorse.

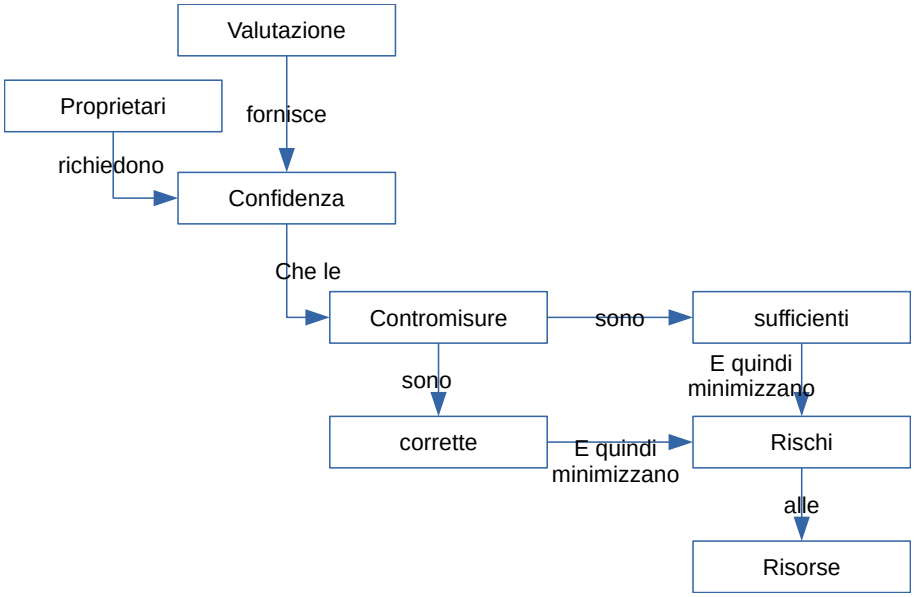
Le minacce possono consistere ad es. in perdita di riservatezza nei dati, perdita della loro integrità, o indisponibilità della risorsa, ...

Le contromisure possono essere di tipo IT (firewall, ...) o non IT (vigilanza, procedure, ...) [rif.2].

La valutazione dei rischi di attacco alle risorse ha bisogno di dimostrare due importanti aspetti:

- dimostrare che le contromisure sono sufficienti,
- e che sono corrette (fanno ciò che dichiarano).

Quindi le contromisure possono essere soggette a valutazione di sicurezza perché i consumatori (proprietari delle risorse) vogliono incrementare la loro confidenza riguardo sufficienza e correttezza delle contromisure, come indicato nel seguente diagramma.



Sufficienza delle contromisure

In una valutazione, la sufficienza delle contromisure è analizzata tramite il *Security Target* (ST).

ST comincia con una descrizione delle risorse e delle minacce. Quindi descrive le contromisure, intese come **Security Objectives**, e dimostra la loro sufficienza per contrastare le minacce.

ST divide le contromisure in due gruppi:

a) obiettivi di sicurezza per il TOE, la cui correttezza sarà determinata nella valutazione;

b) gli obiettivi di sicurezza per l'ambiente operativo; queste non sono oggetto di valutazione.

Dopo di che le contromisure in a) sono ulteriormente dettagliate sviluppando i **Security Functional Requirements** (SFR) con un linguaggio standard descritto in *CC parte 2*.

Quindi ST dimostra che:

- gli SFR soddisfano gli obiettivi di sicurezza per il TOE;
- questi + gli obiettivi di sicurezza dell'ambiente operativo contrastano le minacce;
- perciò SFR + obiettivi di sicurezza dell'ambiente operativo contrastano le minacce.

Correttezza del TOE

Un TOE progettato o implementato non correttamente può presentare vulnerabilità, sfruttabili da attaccanti che vogliono abusare le risorse. Per determinare la correttezza del TOE si può:

- testare il TOE;
- esaminare i suoi dati progettuali;
- esaminare la sicurezza fisica del suo ambiente di sviluppo.

Il ST fornisce una descrizione di queste attività in forma di **Security Assurance Requirements** (SAR), con un linguaggio standard descritto in *CC parte 3*. I SAR assicurano la correttezza del TOE, ma la loro affidabilità dipende dall'accuratezza con cui sono stati sviluppati.

Correttezza dell'ambiente operativo

Anche l'ambiente operativo può presentare errori di progettazione e/o implementazione che danno luogo a vulnerabilità utilizzabili da attaccanti per abusare le risorse. Ma nei CC l'ambiente non viene valutato.

Il consumatore di un TOE è comunque libero di utilizzare altri metodi per determinare la correttezza dell'ambiente operativo.

7.2 Valutazione]

Per i CC esistono due tipi di valutazione:

- **valutazione ST/TOE**, descritta a seguire;

- **valutazione dei PP**, definita nei *CC parte 3*.

Nei CC spesso si usa in termine *valutazione* per indicare valutazione ST/TOE.

Il processo di valutazione ST/TOE avviene in due fasi:

a) **valutazione ST**, determina la sufficienza del TOE e dell'ambiente operativo;
b) **valutazione TOE**, determina la correttezza del TOE.

La valutazione ST avviene applicando i criteri di Security Target Evaluation (definiti in CC parte 3) al Security Target. Il metodo per applicare i criteri è determinato dalla metodologia di valutazione utilizzata.

[da completare pag. 45 rif. 241]

[8 Definire i requisiti di sicurezza]

[8.1 Operazioni]

[da scrivere]

L'operazione di iterazione

[da scrivere]

L'operazione di assegnazione

[da scrivere]

L'operazione di selezione

[da scrivere]

L'operazione di perfezionamento

[da scrivere]

[8.2 Dipendenze tra componenti]

[da scrivere]

[8.3 Componenti estese]

[da scrivere]

[9 Protection Profiles e Packages]

[da scrivere]

[9.1 Introduzione]

[da scrivere]

[9.2 Packages]

[da scrivere]

[9.3 Protection Profiles]

[da scrivere]

[9.4 Usare i Protection Profiles e i Packages]

[da scrivere]

[9.5 Usare Protection Profiles multipli]

[da scrivere]

[9.6 Protection Profiles, PP-Modules e PP-configurations]

Introduzione

[da scrivere]

PP-Modules

[da scrivere]

PP-Configurations

[da scrivere]

Usare PP-Modules e PP-Configurations in security targets

[da scrivere]

10 Valutazione dei risultati

10.1 Introduzione

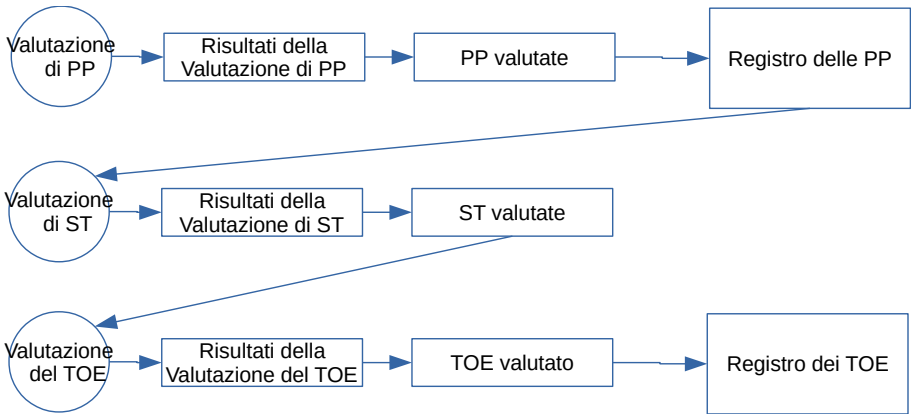
Le valutazioni di PP e ST/TOE secondo le indicazioni del CEM, danno luogo ad una serie di risultati.

Le valutazioni dei PP generano cataloghi di PP valutati.

Una valutazione ST da' risultati intermedi, che sono utilizzati nelle strutture di valutazione del TOE.

Le valutazioni ST/TOE danno cataloghi di TOE valutati. Nella maggior parte dei casi questi cataloghi si riferiranno a prodotti IT da cui derivano i TOE, e non ad un TOE specifico. Perciò l'esistenza di un prodotto IT nel catalogo non deve essere interpretato come se l'intero prodotto sia stato valutato: l'estensione della valutazione ST/TOE è definita dal ST.

Il complesso del processo di valutazione è illustrato nel seguente diagramma.



Gli ST possono essere basati su componenti quali packages, PP valutati o non valutati, o costruite a partire da zero.

I risultati della valutazione devono essere obiettivi e riproducibili. E l'esistenza di un insieme di criteri di valutazione è una precondizione essenziale per avere risultati significativi e confrontabili tra autorità di valutazione diverse.

Il risultato di una valutazione riguarda uno specifico tipo di investigazione delle proprietà di sicurezza di un TOE. E non garantisce che il suo uso sia valido in qualunque ambiente applicativo. La decisione di usare un TOE in uno specifico ambiente applicativo è basata sulla considerazione di più elementi di sicurezza, di cui la valutazione è una parte.

10.2 Risultati di una valutazione PP

CC parte 3 indica i criteri di valutazione che un valutatore deve seguire per definire se un PP è completo, consistente e tecnicamente ragionevole; e quindi utilizzabile per sviluppare un ST.

I risultati della valutazione devono includere una "Dichiarazione di Conformità".

10.3 Risultati di una valutazione PP-Configuration

Questi risultati provengono dalla valutazione di PP-Configuration e ST/TOE in relazione alla Classe ACE (Protection Profile Configuration Evaluation) descritta CEM.

Le PP-Configurations valutate integrano il catalogo delle PP valutate, e sono collegate alle Base-PP che sono presenti nelle PP-configurations.

CC parte 3 ACE contiene i criteri di valutazione che un valutatore deve seguire per affermare se un PP-Configuration è completo, consistente e tecnicamente ragionevole, e quindi può essere utilizzato per lo sviluppo di un ST.

I risultati della valutazione devono includere anche una "Dichiarazione di Conformità".

10.4 Risultati della valutazione di un ST/TOE

CC parte-3 contiene i criteri di valutazione che un valutatore deve consultare per determinare se vi è una sufficiente assicurazione che il TOE soddisfi i SFR nel ST. Quindi la valutazione del TOE darà luogo ad una affermazione pass/fail per il ST.Se sia il ST che il TOE hanno valore pass, il relativo prodotto può essere incluso in un registro Vi deve essere anche una "Dichiarazione di Conformità".

I risultati della valutazione successivamente possono essere soggetti ad un processo di certificazione, che al di fuori dello scopo dei CC.

10.5 Dichiarazione di Conformità

Indica la sorgente dei requisiti soddisfatti da un PP o un ST che supera la valutazione. Contiene:

a) la **versione** del CC cui è conforme il PP o il ST;

b) l'adesione a CC parte 2 (requisiti funzionali di sicurezza) come:

- **conforme a CC parte 2**, se tutti i SFR del PP o ST sono basati sui componenti funzionali di CC parte 2; oppure:
- **conforme a CC parte 2 estesa**, se almeno un SFR del PP o ST non è basato sui componenti funzionali in CC parte 2;

c) l'adesione a CC parte 3 (assicurazione dei requisiti di sicurezza) come:

- **conforme a CC parte 3**, se tutti i SAR del PP o ST sono basati sui componenti di assicurazione in CC parte 3; oppure:
- **conforme a CC parte 3 estesa**, se almeno un SFR del PP o ST non è basato sui componenti di assicurazione in CC parte 3.

Inoltre la dichiarazione di conformità può includere una affermazione in relazione ai packages organizzata in uno di questi modi:

- *package name conformant* - un PP o un ST è conforme a un package definito (ad es. EAL) se:
  - i SFR di quel PP o ST sono identici agli SFR nel package, o
  - i SAR di quel PP o ST sono identici ai SAR nel package.
- *package name augmented* - un PP o un ST è una estensione di un package definito se:
  - i SFR di quel PP o ST contengono tutti i SFR del package, e in più almeno un SFR addizionale o un SFR che sia gerarchicamente superiore a un SFR del package;o
  - i SAR di quel PP o ST contengono tutti i SAR del package, e in più almeno un SAR addizionale o un SAR che sia gerarchicamente superiore a un SAR del package;o

Quando un TOE è valutato con successo a valle di un ST, ogni dichiarazione di conformità del ST si applica anche al TOE.

Infine, la dichiarazione di conformità può includere anche due affermazioni in relazione ai PP:

a) *PP conformant* - un PP o TOE che soddisfa specifiche PP che sono elencate come parte dei risultati di conformità;

b) *conformance statement* (solo per PP) - che descrive il modo in cui PP o ST devono conformasi a questo PP; può valere **strict**, oppure **demonstrable**.

Oltre alle conformità su esposte,

- un PP-Configuration deve fornire una affermazione di conformità (*strict* o *demonstrable*) alle ST che aderiscono alle Base-PP;
- un ST può dichiarare conformità con uno o più PP-Configuration.

10.6 Uso dei risultati della valutazione ST/TOE

Una volta che un ST e un TOE sono stati valutato, i proprietari della risorsa hanno l'assicurazione (secondo quanto definito nel ST) che il TOE, con l'ambiente operativo, contrasti le minacce. Questi risultati possono essere utilizzati dai proprietari per decidere se accettare il rischio di esporre le risorse alle minacce.

Ma il proprietario della risorsa deve controllare se:

a) il Security Problem Definition nel ST coincide con il problema di sicurezza del proprietario della risorsa;

b) l'ambiente operativo del proprietario della risorsa sia conforme agli obiettivi di sicurezza per l'ambiente operativo descritto nel ST.

Se uno dei precedenti punti non è soddisfatto, il TOE non è utilizzabile per gli scopi del proprietario della risorsa.

Una volta che il TOE sia operativo, è possibile che possano evidenziarsi errori o vulnerabilità precedentemente sconosciute. In tal caso lo sviluppatore può correggere il TOE, o cambiare il ST per escludere le vulnerabilità. In entrambi i casi le precedenti valutazioni possono non essere più valide.

Se è necessario ristabilire la confidenza, di deve effettuare una nuova valutazione. A questo fine si può usare i CC ma il dettaglio di come fare non è lo scopo di questa parte di CC.

A Security Targets (informativo)

A.1 Obiettivo e struttura di questo allegato

Questo allegato spiega il concetto di Security Target. Non definisce i criteri ASE, che sono in CC parte 3.

È composto di quattro parti principali:

a) *cosa deve contenere un ST*. Incluse le relazioni tra i contenuti che lo compongono.

b) *Come deve essere usato un ST*. E alcune delle domande cui può rispondere.

c) *ST a bassa assicurazione*. Sono ST con contenuti ridotti.

d) *Dichiarazioni di conformità con gli standard*. Come dichiarare il TOE conforme a certi standard.

A.2 Contenuti obbligatori di un ST

I contenuti obbligatori di un ST sono dettagliati in CC parte 3 e rappresentati sommariamente nella seguente figura. Questa può essere considerata una struttura valida per il documento di ST anche se si possono avere strutture alternative. Ad es. se la motivazione dei requisiti di sicurezza è particolarmente corposa, può essere inclusa in una appendice invece che nella sezione dei requisiti di sicurezza.

Segue un elenco delle sezioni, che sarà ulteriormente dettagliato in seguito.

a) *Una introduzione al ST,* contiene tre descrizioni narrative del TOE a diversi livelli di astrazione;

b) *una dichiarazione di conformità*, per indicare se il ST è conforme a un PP e/o package, ed eventualmente quali;

c) *una definizione del problema della sicurezza*, con minacce, OSP e assunzioni;

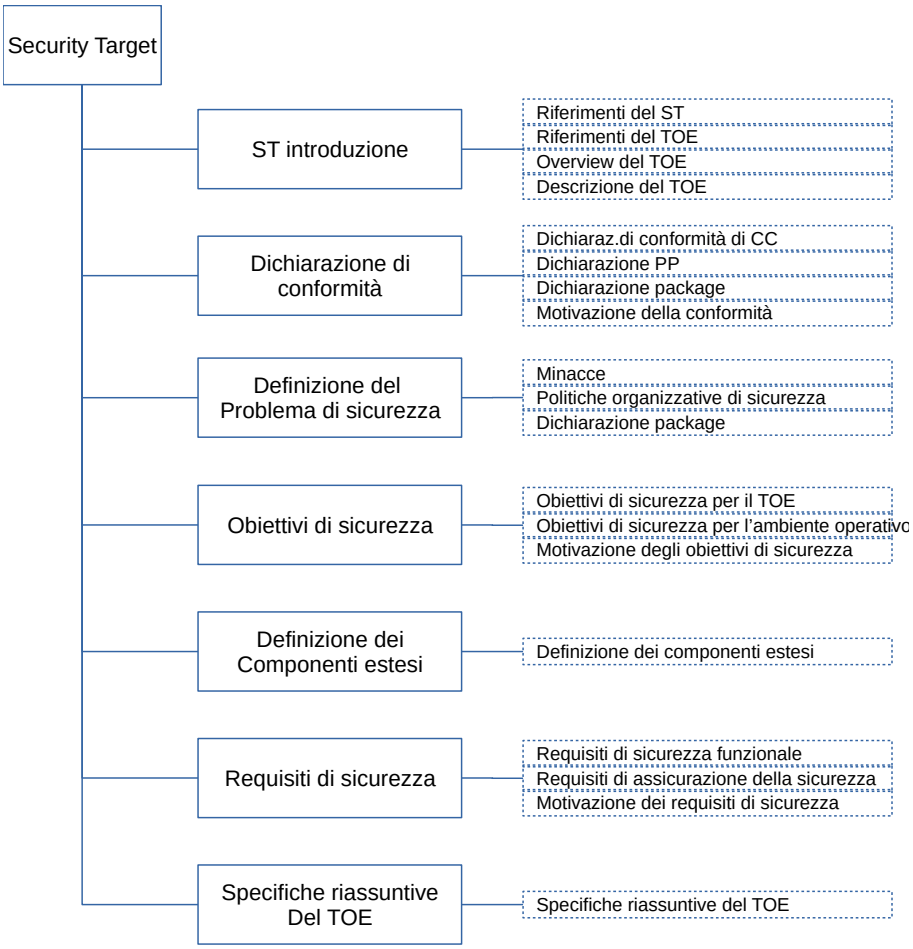
d) *gli obiettivi di sicurezza*, che mostrano come la soluzione del problema della sicurezza è diviso tra obiettivi di sicurezza per il TOE e obiettivi di sicurezza per l'ambiente operativo del TOE;

e) *la definizione dei componenti estesi*, questa parte è opzionale, e può definire nuovi componenti rispetto quanto previsto da CC parte 2 e 3. Questi componenti sono necessari per definire requisiti funzionali estesi e requisiti di assicurazione estesi;

f) *requisiti di sicurezza*, in cui si espongono gli obiettivi di sicurezza del TOE in un linguaggio standardizzato. Questo linguaggio permette la definizione dei SFR. In più questa sezione definisce i SAR;

g) *una specifica riassuntiva del TOE*, che mostra come i SFR sono implementati nel TOE.

Esistono anche ST a bassa assicurazione, che hanno contenuti ridotti, descritti oltre. Dove non specificato altrimenti, si intende ST a contenuto completo.



A.3 Usare un ST

Come deve essere usato un ST

Un ST tipico soddisfa due ruoli:

- prima e durante la valutazione, il ST indica "*cosa deve essere valutato*". In questa fase il ST serve da accordo tra lo sviluppatore e il valutatore per definire con precisione le proprietà di sicurezza del TOE e lo scopo della valutazione. La correttezza tecnica e la completezza sono i maggiori problemi in questo ruolo. Oltre si descriverà come usare il ST in questo ruolo.
- Dopo la valutazione, il ST specifica "*cosa è stato valutato*". In questo ruolo il ST serve come accordo tra lo sviluppatore (o il venditore) del TOE e il potenziale consumatore del TOE. Il ST descrive con precisione le proprietà di sicurezza del TOE in modo astratto, e il consumatore può fidarsi di questa descrizione perché il TOE è stato valutato secondo il ST. In questo ruolo i maggiori problemi sono la facilità d'uso e la comprensibilità. Oltre si descriverà come il ST deve essere usato in questo ruolo.

Come un ST non deve essere usato

Non si deve usare un ST come:

- *una specifica di dettaglio*, un ST è progettato per essere una specifica di sicurazza ad un livello odi astrazione relativamente elevato. In generale non deve contenere specifiche di dettaglio del protocollo, di algoritmi, di meccanismi e delle operazioni.
- *una specifica completa*, un ST non è una specifica di carattere generale. Tutte le proprietà non rilevanti per la sicurezza, quali l'interoperabilità, grandezza fisica, peso, voltaggio, etc. non devono essere parte del ST. Quindi un ST può essere una parte di una specifica completa.

A.4 Introduzione al ST (ASE_INT)

Descrive il TOE in modo narrativo su tre livelli di astrazione:

a) il riferimento ST e il riferimento TOE, identificano i materiali per il ST e il TOE cui si riferisce il ST;

b) una overview del TOE, che lo descrive brevemente;

c) la descrizione del TOE, che lo descrive in maggiore dettaglio

Riferimento ST e riferimento TOE

Un ST contiene un riferimento che lo identifica. Un riferimento tipico consiste di titolo, versione, autori e data di pubblicazione.

Inoltre in ST contiene un riferimento che identifica il TOE conforme al ST. Un tipico riferimento TOE consiste nel nome dello sviluppatore, nome del TOE e sua versione. Questo riferimento può non essere unico, in quanto un TOE può essere valutato più volte, con più ST.

Se un TOE è costituito di uno o più prodotti conosciuti, è possibile costruire di conseguenza il suo riferimento, utilizzando i nomi dei prodotti che lo compongono. Si faccia attenzione a non sviare il consumatore: non è permesso utilizzare il nome del prodotto se non vengono considerate in valutazione alcune parti principali delle funzionalità di sicurezza.

I riferimenti del ST e del TOE facilitano la loro indicizzazione e il riferimento quando si includono nelle sintesi di elenchi di TOE/Prodotti valutati.

Overview del TOE

La overview del TOE ha lo scopo di illustrarlo ad un potenziale consumatore che sta consultando un elenco di TOE/Prodotti valutati per trovare un TOE che soddisfi le sue esigenze di sicurezza, sia supportato dal suo hardware, software e firmware. La lunghezza tipica di una overview del TOE è di parecchi paragrafi.

A questo fine la overview del TOE descrive il suo utilizzo e le sue caratteristiche principali, identifica il suo tipo e i principali hardware/software/firmware non-TOE necessari.

Uso e principali caratteristiche di sicurezza di un TOE

La descrizione dell'uso e le principali caratteristiche di sicurezza del TOE ha lo scopo di dare una idea molto generale di cosa possa fare in termini di sicurezza, e a che fine possa essere utilizzato in un contesto di sicurezza. Questa sezione deve essere scritta per potenziali consumatori del TOE, descrivendo uso e caratteristiche di sicurezza principali in termini di attività operative, usando un linguaggio per loro comprensibile.

Un esempio può essere: "Il MauveCorp MauveRAM Dtabase v.2.11 è un database multiutente ideato per essere utilizzato in un ambiente di rete. Permette l'attività contemporanea di 1024 utenti. Permette autenticazione con password/token e biometrica, protegge contro la corruzione accidentale dei dati e puo effettuare il roll-back di 10000 transazioni. ..."

La overview del TOE identifica la sua tipologia: firewall, VPN-firewall, smart card, crypto-modem, web server, database, web server e database, LAN, LAN con web server e database, etc.

Nel caso la tipologia non sia classificabile, si usa il valore "*none*".

In alcuni casi un TOE può ingannare un consumatore. Ad esempio:

- a causa del suo tipo, ci si può aspettare certe funzionalità, che il TOE non ha. Ad esempio:
  - un TOE di tipo ATM-card che non supporta alcune funzionalità di identificazione/autenticazione
  - un TOE firewall che non supporta protocolli di uso comune;
  - un TOE tipo PKI che non ha la funzionalità di revoca del certificato.
- oppure, per il suo tipo, ci si può aspettare che il TOE operi in determinati ambienti operativi, quando in realtà non lo fa. Esempi:
  - un TOE di tipo sistema operativo per PC che non può funzionare in sicurezza a meno che il PC sia senza connessione di rete, floppy drive e player CD/DVD.
  - un firewall che non possa funzionare in sicurezza a meno che tutti gli utenti che si possono connettere al firewall siano benigni.

Hardware/software/firmware non-TOE necessari

Molti TOE (sopratutto il software) si basano su altri componenti non-TOE quali hardware, software e/o firmware. In questi casi la overview del TOE deve identificare tali componenti non-TOE. Non è necessaria una identificazione piena, ma deve essere abbastanza dettagliata per permettere ai potenziali consumatori di determinare i principali componenti necessari per l'uso del TOE.

Esempi di identificazioni sono:

- un PC standard con processore da almeno 1 GHz e almeno 512 MB di RAM, con la versione 3.0 Update 6b, c, o 7, o la versione 4.0 del sistema operativo Yaiza;

- un circuito integrato CleverCard SB2067;
- l'installazione del Dicembre 2002 della LAN dell'Ufficio del Direttore Generale del Dipartimento del traffico; ...

Descrizione del TOE

Questa è una descrizione narrativa del TOE, probabilmente estesa su più pagine. Deve fornire ai valutatori e potenziali consumatori la possibilità di capire in generale le capacità di sicurezza del TOE, con un dettaglio superiore a quello fornito dalla overview. La descrizione del TOE può essere anche usata per descrivere un contesto più ampio in cui si inserisce il TOE.

La descrizione del TOE discute la sua portata fisica: una lista di tutte le parti hardwae, firmware, software e guide che lo costituiscono. Questa lista deve avere un livello di dettaglio sufficiente per dare al lettore una comprensione generale delle parti.

La descrizione del TOE deve anche discutere la sua portata logica: le caratteristiche di sicurezza logiche offerte dal TOE, con un livello di dettaglio sufficiente a dare al lettore una comprensione generale di queste caratteristiche. Questa descrizione deve essere maggiormente dettagliata rispetto le principali caratteristiche di sicurezza descritte nella overview.

Una proprietà importante delle portate fisiche e logiche è che descrivono il TOE in modo tale da non lasciare dubbi se una certa parte o caratteristica sia all'interno del TOE o se sia al di fuori. Questo è importante sopratutto se il TOE è legato e non è facilmente separabile con entità non-TOE.

Esempi di TOE legati con entità non-TOE:

- il TOE è un coprocessore crittografico di una piccolo IC (circuito integrato) di smart card, invece dell'intero IC;
- il TOE è un IC di smart card, eccetto il processore crittografico;
- il TOE è la parte NAT (Network Address Translation) di un Firewall MinuteGap v18.5.

A.5 Dichiarazione di conformità (ASE_CCL)

Questa sezione di un ST descrive come sia conforme con:

- la parte 2 e la parte 3 di questo Standard Internazionale;
- i Protection Profile (se del caso)
- Packages (se del caso).

Questa descrizione di conformità è composta di due voci: la versione di CC usata e se il ST contiene requisiti di sicurezza estesi.

La descrizione di conformità di un ST a Protection Profile significa che il ST elenca i package di cui dichiara la conformità (si veda 10.5 Dichiarazione di Conformità).

La descrizione di conformità del ST ai package significa che il ST elenca i package di cui dichiara la conformità (si veda 10.5 Dichiarazione di Conformità).

Un Security Target può usare PP-Configuration(s) allo stesso modo di un Protection Profile standard. Cioè, la dichiarazione di conformità di un ST può contenere una *dichiarazione PP* che identifica le PP-Configuration(s) cui il ST è conforme.

A.6 Definizione del problema di sicurezza (ASE_SPD)

Introduzione

La definizione del problema di sicurezza identifica il problema di sicurezza che deve essere indirizzato. Questa definizione è assiomatica. Cioè il processo che porta alla sua formulazione è al di fuori dello scopo del CC.

Ma si deve notare l'utilità del risultato di una valutazione dipende fortemente dal ST, e l'utilità del ST dipende fortemente dalla qualità della definizione del problema di sicurezza.Perciò spesso è utile spendere risorse significative e utilizzare processi ben definiti per ottenere una buona definizione del problema di sicurezza.

In accordo con CC parte 3, non è obbligatorio scrivere tutte le sezioni: un ST con minacce non ha necessità di avere OPS, e viceversa. Ancora: un ST può omettere le assunzioni.

Inoltre si noti che se il TOE è fisicamente distribuito, può essere meglio discutere le minacce di rilievo, OPS e assunzioni separatamente per i distinti domini dell'ambiente operativo del TOE.

Minacce

Questa sezione della definizione del problema di sicurezza illustra le minacce che devono essere contrastate dal TOE, da suo ambiente operativo, o da una combinazione di entrambi.

Una minaccia consiste in una azione avversa operata da un agente della minaccia su una risorsa.

Le azioni avverse sono azioni che influenzano una o più proprietà di una risorsa, proprietà da cui la risorsa deriva il proprio valore.

Gli agenti delle minacce possono essere descritti come entità individuali, ma in alcuni casi possono essere meglio descritti come tipi di entità o gruppi, etc.

Esempi di agenti di minacce sono hackers, utenti, processi di computer e incidenti. Gli agenti di minacce possono essere ulteriormente descritti tramite aspetti, come esperienza, risorse, opportunità e motivazione.

Esempi di minacce:

- un hacker (con una consistente esperienza, equipaggiamento standard, e pagato per farlo) da remoto copia file confidenziali dalla rete di una società;
- un worm degrada seriamente le prestazioni di una rete geografica;
- un amministratore di sistema viola la privacy di un utente;
- qualcuno su Internet in ascolto di comunicazioni elettroniche confidenziali.

Politiche di sicurezza organizzative (OSP)

Questa sezione della definizione del problema di sicurezza illustra le OPS che devono essere imposte tramite il TOE, il suo ambiente operativo e da una combinazione di entrambi.

Le *Organisational Security Policies* (OSP) sono regole di sicurezza, procedure, o linne guida imposte (o che si presume siano imposte) ora e/o in futuro da una reale o ipotetica organizzazione nell'ambiente operativo. OSP possono essere stabilite da una organizzazione che controlla l'ambiente operativo del TOE, oppure da organi legislativi o normativi. Le OSP si possono applicare al TOE e/o all'ambiente operativo del TOE.

Esempi di OSP sono:

- tutti i prodotti usati da Governo devono essere conformi iagli Standard Nazionali per la generazione e criptografia di password;
- solo gli utenti con privilegio di System Administrator e autorizzazione del Dipartimento per la Riservatezza possono gestire il Fileserver del Dipartimento.

Assunzioni

Questa sezione della definizione del problema di sicurezza illustra le assunzioni riguardo l'mbiente operaivo affinché possa fornire le funzionalità di sicurezza. Se il TOE è posto in un ambiente operativo che non soddisfa queste assunzioni, il TOE può essere essere incapace di fornire le sue funzionalità di sicurezza. Le assunzioni possono essere fisiche, sul personale e la connettività dell'ambiente operativo.

Esempi di assunzioni sono:

- assunzioni su aspetti fisici dell'ambiente operativo:
  - si assume che il TOE sia posto inuna stanza progettata per minimizzare le emissioni elettromagnetiche;
  - si assume che la console di amministrazione del TOE sia posta in un'area ad accesso limitato.
- Assunzioni riguardo aspetti del personale dell'ambiente operativo:
  - si assume che gli utenti del TOE siano addestrati abbastanza per potervi operare;
  - si assume che gli utenti del TOE siano autorizzati per la gestione di informazioni classificate come Segreto Nazionale;
  - si assume che gli utenti del TOE non scrivano le loro password.
- Assunzioni riguardo la connettività dell'ambiente operativo:
  - si assume che sia disponibile una stazione di lavoro PC con almeno 10GB di spazio su disco per far girare il TOE;
  - si assume che il TOE sia l'unica applicazione non-OS che giri su questa stazione di lavoro;
  - si assume che il TOE non sia connesso ad una rete non attendibile.

Si noti che durante la valutazione queste assunzioni sono considerate vere e non vengono provate in alcun modo. Per questo motivo le assunzioni posono riguardare solo l'ambiente operativo. Non si possono fare

assunzioni riguardo il comportamento del TOE perché una valutazione consiste nel valutare asserzioni riguardo il TOE e non nell'assumere che le asserzioni siano vere.

A.7 Obiettivi di sicurezza (ASE_OBJ)

Gli obiettivi di sicurezza sono dichiarazioni sintetiche e astratte della soluzione prevista al problema definito dalla definizione del problema di sicurezza. Il ruolo degli obiettivi di sicurezza è triplice:

- fornisce al problema una soluzione di alto livello, in linguaggio naturale;
- dividere questa soluzione in due soluzioni parziali, per mettere in rilievo che entità diverse devono ciascuna indirizzare una parte del problema;
- dimostrare che queste soluzioni parziali formano una soluzione completa al problema.

Soluzione di alto livello

Gli obiettivi di sicurezza consistono in un insieme di dichiarazioni brevi e chiare, senza eccessivo dettaglio, che insieme formano una soluzione di alto livello al problema di sicurezza. Il livello di astrazione degli obiettivi di sicurezza mira ad essere chiaro e comprensibile a qualificati consumatori potenziali del TOE. Gli obiettivi della sicurezza sono espressi in linguaggio naturale.

Soluzioni parziali

In un ST la slouzione di sicurezza di alto livello, come descritta dagli obiettivi di sicurezza, è divisa in due soluzioni parziali. Queste soluzioni parziali sono dette obiettivi di sicurezza per il TOE e obiettivi di sicurezza per l'ambiente operativo. Ciò riflette il fatto che queste soluzioni parziali sono fornite da due diverse entità: il TOE e l'ambiente operativo.

Obiettivi di sicurezza per il TOE

Il TOE fornisce funzionalità di sicurezza per risolvere una certa parte definita dalla definizione del problema di sicurezza. Questa parte della soluzione è detta obiettivi di sicurezza per il TOE e consiste in un insieme di obiettivi che il TOE deve raggiungere al fine di risolvere la sua parte del problema.

Esempi di obiettivi di sicurezza per il TOE sono:

- il TOE deve mantenere confidenziali i contenuti di tutti i file trasmessi tra lui e il Server;
- il TOE deve identificare e autenticare tutti gli utenti prima di permettere l'accesso ai Servizi di tramissione forniti dal TOE;
- il TOE deve limitare l'accesso degli utenti ai dati in accordo alla politica dell'Accesso ai Dati descritta nell'allegato 3 del ST.

Se il TOE è fisicamente distribuito, può essere meglio suddividere la sezione di ST contenente gli obiettivi di sicurezza in più sottosezioni che riflettono tale suddivisione.

Obiettivi di sicurezza per l'ambiente operativo

L'ambiente operativo del TOE implementa misure tecniche e procedurali per assistere il TOE nel fornire correttamente le sue funzionalità di sicurezza (che sono definite dagli obiettivi di sicurezza per il TOE). Questa soluzione parziale è chiamata obiettivi di sicurezza per lìambiente operativo e consiste in un insieme di dichiarazioni che descrivono le mete che l'ambiente operativo deve raggiungere.

Esempio di obiettivi di sicurezza per l'ambiente operativo sono:

- l'ambiente operativo deve fornire una workstation con il OS Inux versione 3.01b per eseguire il TOE;
- l'ambiente operativo deve assicurare che tutti gli utenti umani del TOE ricevano addestramento appropriato prima che gli vvenga permesso di lavorare con il TOE;
- l'ambiente operativo del TOE deve limitare l'accesso fisico al TOE al personale amministratore e al personale di manutenzione accompagnato dal personale amministratore;
- l'ambiente operativo deve assicurare la confidenzialità dei log di audit generati dal TOE prima di inviarli al Server di Audit centrale.

Se l'ambiente operativo del TOE è formato da più siti, ognuno con differenti proprietà, può essere meglio suddividere le sezioni del ST contenenti gli obiettivi di sicurezza per l'ambiente operativo in più sottosezioni che riflettano tale composizione.

Relazione tra obiettivi di sicurezza e definizione del problema di sicurezza

Il ST contiene anche un giustificazione degli obiettivi di sicurezza, contenente due sezioni:

- un tracciamento che mostra quali obiettivi di sicurezza indirizzano quali minacce, OSP e assunzioni;
- un insieme di giustificazioni che mostrano come tutte le minacce, OSP, e assunzioni sono effettivamente indirizzate dagli obiettivi di sicurezza.

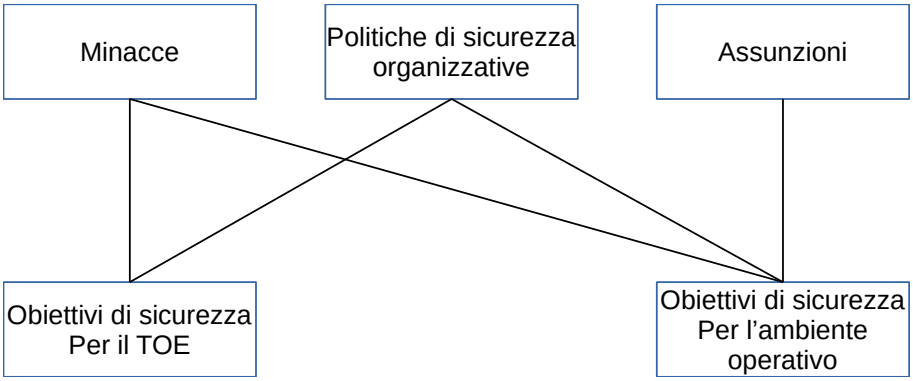
Tracciamento tra obiettivi di sicurezza e definizione del problema di sicurezza

Il tracciamento mostra come gli obiettivi di sicurezza si riferiscano alle minacce, OSP e assunzioni, come descritte nella definizione del problema di sicurezza.

a) *mancanza di obiettivi spuri*: ogni obiettivo di sicurezza si riferisce ad almeno una minaccia, OSP, o assunzione.

b) *completezza rispetto la definizione del problema della sicurezza*: ogni minaccia OSP e assunzione ha almeno un obiettivo di sicurezza che lo indirizza.

c) *correttezza del tracciamento*: poiché le assunzioni sono sempre fatte dal TOE in relazione all'ambiente operativo, gli obiettivi di sicurezza per il TOE non si riferiscono alle assunzioni. I riferimenti permessi da CC parte 3 sono indicati nella seguente figura.



Più obiettivi di sicurezza possono riferirsi alla stessa minaccia, indicando che la loro combinazione la contrasta. Similmente si può argomentare in relazione a OSP e assunzioni.

Fornire una giustificazione per il tracciamento

La giustificazione degli obiettivi di sicurezza inoltre dimostrano che il tracciamento è efficace. Tutte le minacce date, gli OSP e assunzioni sono indirizzate (ovvero, rispettivamente, contrastate, imposte e confermate) se sono raggiunti tutti gli obiettivi di sicurezza referenti una particolare minaccia, OSP o assunzione.

Questa dimostrazione analizza gli effetti della realizzazione degli obiettivi di sicurezza rilevanti nel contrastare la minaccia, imporre la OSP e confermare l'assunzione e conduce alla conclusione che raggiungono lo scopo.

In alcuni casi, dove parti di una definizione di un problema di sicurezza somiglia strettamente a qualche obiettivo di sicurezza, la dimostrazione può essere molto semplice. Un esempio è: una minaccia "T17: l'agente della minaccia X legge le Informazioni Confidenziali in transito tra A e B", un obiettivo di sicurezza per il TOE: "OT12: Il TOE deve assicurare che tutte le informazioni trasmesse tra A e B sono mantenute confidenziali", e la dimostrazione "T17 è direttamente contrastata da OT12".

Riguardo il contrasto delle minacce

Contrastare una minaccia non significa necessariamente rimuoverla, può significare diminuirla sufficientemente o mitigare sufficientemente la minaccia.

Esempi di rimozione di una minaccia sono:

- rimuovere la possibilità di eseguire l'azione ostile da parte dell'agente della minaccia;
- muovere, cambiare o proteggere la risorsa in modo tale che l'azione ostile non le sia più applicabile;
- rimuovere l'agente della minaccia (ad es. rimuovendo le macchine da una rete che frequentemente si blocca.

Esempi di diminuzione della minaccia sono:

- limitare la capacità di un agente della minaccia di eseguire azioni ostili;
- limitare l'opportunità di eseguire una azione ostile da parte dell'agente della minaccia;

- limitare la probabilità che l'esecuzione di una azione ostile abbia successo;
- ridurre tramite deterrente la motivazione per l'agente della minaccia di eseguire una azione ostile;
- richiedere all'agente della minaccia maggiore competenza o maggiori risorse.

Esempi di mitigazione degli effetti di una minaccia sono:

- eseguire backup frequenti della risorsa;
- ottenere copie di riserva della risorsa;
- assicurare una risorsa;
- assicurarsi che le azioni ostili riuscite vengano rilevate tempestivamente per effettuare le opportune azioni di contrasto.

Obiettivi di sicurezza: conclusioni

Basandosi sugli obiettivi di sicurezza e sulle loro giustificazioni, si possono tracciare le seguenti conclusioni: se vengono raggiunti tutti gli obiettivi di sicurezza allora il problema di sicurezza definito secondo la definizione del Problema di sicurezza (ASE_SPD) è risolto: tutte le minacce sono contrastate, tutte le OSP sono imposte e tutte le assunzioni sono confermate.

A.8 Definizione delle componenti estese (ASE_ECD)

In molti casi i requisiti di sicurezza (si veda la prossima sezione) in un ST sono basati su componenti elencati in CC parte 2 o CC parte 3. Comunque in alcuni casi vi possono essere requisiti nel ST che non sono basati sui componenti presenti in CC parte 2 o 3. In questi casi bisogna definire nuove componenti (componenti estese), e questa definizione deve essere riportata nella Definizione delle Componenti Estese. Maggiori informazioni sono nell'allegato C.4.

Si noti che questa sezione deve contenere solo le componenti estese, e non i requisiti estesi (requisiti basati sulle componenti estese). I requisiti estesi devono essere riportati nei requisiti di sicurezza (si veda la prossima sezione) e sono a tutti gli effetti come i requisiti basati sui componenti di CC parte 2 o 3.

A.9 Requisiti di sicurezza (ASE_REQ)

I requisiti di sicurezza consistono in due gruppi di requisiti:

a) *i requisiti funzionali di sicurezza* (SFR): una traduzione degli obiettivi di sicurezza per il TOE in un linguaggio standardizzato;

b) *i requisiti di assicurazione di sicurezza* (SAR): una descrizione di come assicurare che il TOE soddisfi i SFR.

Requisiti di sicurezza funzionali (SFR)

I Requisiti di sicurezza funzionale sono una traduzione degli obiettivi di sicurezza per il TOE. Usualmente sono ad un livello di astrazione più dettagliato, ma devono essere una traduzione completa (ovvero: tutti gli obiettivi di sicurezza devono essere completamente indirizzati) e devono essere indipendenti da ogni soluzione tecnica specifica (implementazione). I CC richiedono questa traduzione in linguaggio standardizzato per più motivi:

- per fornire una descrizione esatta di cosa viene valutato. Mentre gli obiettivi di sicurezza sono in linguaggio naturale, la traduzione in un linguaggio standard impone una descrizione più esatta delle funzionalità del TOE.
- per permettere la comparazione tra due ST. Autori diversi di ST possono usare terminologie differenti per descrivere i loro obiettivi di sicurezza, il linguaggio standardizzato impone l'uso della stessa terminologia e degli stessi concetti. Ciò permette una comparazione semplificata.

Nei CC non si richiede la traduzione degli obiettivi di sicurezza dell'ambiente operativo, perché non è valutato e quindi non richiede una descrizione volta alla sua valutazione. Si veda la biografia per aspetti di rilievo per l'accertamento della sicurezza di isistemi operazionali.

Può avvenire che parte dell'ambiente operativo siano valutate in altre valutazioni, ma non è l'obiettivo della valutazione corrente. Per esempio: un OS TOE può richiedere la presenza di un firewall nel suo ambiente operativo. Un'altra valutazione può di conseguenza valutare il firewall, ma questa valutazione non ha nulla a che fare con quella del OS TOE.

Come i CC supportano questa traduzione

I CC supportano questa traduzione in tre modi:

a) fornendo un "linguaggio" predefinito e preciso, progettato per descrivere esattamente cosa viene valutato. Questo linguaggio è definito come un insieme di componenti definiti in CC parte 2. L'uso di questo linguaggio come traduzione ben definita degli obiettivi di sicurezza per il TOE verso i SFR è obbligatoria, ,anche se esistono alcune eccezioni (si veda la sezione [8.3 Componenti estese]).

b) fornendo operazioni: meccanismi che permettono all'autore del ST di modificare i SFR per fornire una trasuzione più accurata degli obiettivi di sicurezza per il TOE. Questa parte dei CC definisce le quattro operazioni permesse: assegnazione, selezione, iterazione, e l'affinamento. Sono descritti nella sezione [8.1 Operazioni].

c) fornendo dipendenze: un meccanismo che supporta una più completa traduzione verso i SFR. Nel linguaggio CC parte 2 un SFR può avere una dipendenza da un altri SFR. Questo significa che se un ST usa quel SFR, avrà bisogno anche degli altri SFR. Ciò rende più difficile per l'autore del ST di trascurare gli SFR necessari e quindi aumenta la completezza del ST. Le dipendenze sono descritte nella sezione [8.2 Dipendenze tra componenti].

Relazione tra SFR e obiettivi di sicurezza

Il ST contiene anche la giustificazione dei requisiti di sicurezza, composta da due sezioni riguardo i SFR:

- un tracciamento che mostri quali SFR indirizza no quali obiettivi di sicurezza per il TOE;
- un insieme di giustificazioni che mostrano che tutti gli obietivi di sicurezza per il TOE sono effettivamente indirizzati dai SFR.

Tracciamento tra SFR e obiettivi di sicurezza per il TOE

Questo tracciamento mostra come i SFR facciano riferimento agli obiettivi di sicurezza per il TOE in questi termini:

a) *non vi sono SFR spuri*: ogni SFR si riferisce almeno ad un obiettivo di sicurezza.

b) *completezza rispetto gli obiettivi di sicurezza del TOE*: ogni obiettivo di sicurezza per il TOE ha almeno un SFR che lo riferisce.

Più SFR si possono riferire alltesso obiettivo di sicurezza del TOE, indicando che la combinazione di questi requisiti di sicurezza soddisfano quell'obiettivo di sicurezza per il TOE.

Fornire una giustificazione per il tracciamento

La giustificazione dei requisiti di sicurezza dimostra che il tracciamento è efficace: se sono soddisfatti tutti i SFR referenti un particolare obiettivo di sicurezza per il TOE, allora è raggiunto l'obiettivo di sicurezza per il TOE.

Questa dimostrazione deve analizzare gli effetti di soddisfare i SFR pertinenti per raggiungere l'obiettivo di sicurezza del TOE e portare alla conclusione che è questo il caso[1].

Nei casi incui i SFR somigliano oagli obiettivi di sicurezza del TOE, la dimostrazione può essere molto semplice.

Requisiti di assicurazione della sicurezza (SAR)

I SAR sono una descrizione di come si deve valutare il TOE. Questa descrizione usa un linguaggio standard perché:

- deve fornire una descrizione esatta di come il TOE deve essere valutato. L'uso di un linguaggio standardizzato aiuta a creare una descrizione esatta e non ambigua.
- per permettere la comparazione tra due ST. Ustori diversi di ST possono usare una terminologia diversa nel descrivere la valutazione. Il linguaggio standard impone all'utente l'uso della stessa terminologia e concetti. Ciò permette una comparazione semplificata.

Questo linguaggio standard è definito come un insieme di componenti definiti nei CC parte 3. L'uso di questo linguaggio è obbligatorio, anche se esistono delle eccezioni. I CC migliorano questo linguaggio:

a) fornendo operazioni: meccanismi che permettono all'autore di ST di modificare i SAR. I ICC hanno quattro operazioni: assegnazione, selezione, iterazione e raffinamento. Queste sono descritte nella sezione [8.1 Operazioni].

b) fornendo dipendenze: un meccanismo che supporta una traduzione più completa dei SAR. Nel linguaggio di CC parte 3 un SAR può avere dipendenza da altri SAR. Questo significa che se un ST usa quel SAR, in generale avrà necessità anche degli altri SAR. Ciò rende pù difficile per l'autore di ST di trascurare i SAR che devono essere inclusi e quindi potenzia la completezza del ST. Le dipendenze sono descritte nella sezione [8.2 Dipendenze tra componenti].

1 NdT. Ovvero condurre alla conclusione che l'obiettivo di sicurezza del TOE è soddisfatto.

Giustificazione dei SAR e dei requisiti di sicurezza

Il ST contiene anche una giustificazione dei requisiti di sicurezza che spiega perché questo particolare insieme di SAR è ritenuto appropriato. Non ci sono requisiti specifici per questa spigazione. Il suo scopo è permettere ai lettori del ST di capire le ragioni che hanno portato alla scelta di questo particolare insieme.

Un esempio di inconsistenza è il seguente: la descrizione del problema della sicurezza menziona minacce dove l'agente della minaccia è molto capace, e nei SAR vi è una analisi di Vulnerabilità (AVA_VAN) superficiale o mancante.

Requisiti di sicurezza: conclusioni

Nella definizione del problema della sicurezza del ST il problema della sicurezza viene definito come formato da minacce, OSP e assunzioni. Nella sezione del ST degli obiettivi di sicurezza, la soluzione viene fornita in forma di due sotto soluzioni:

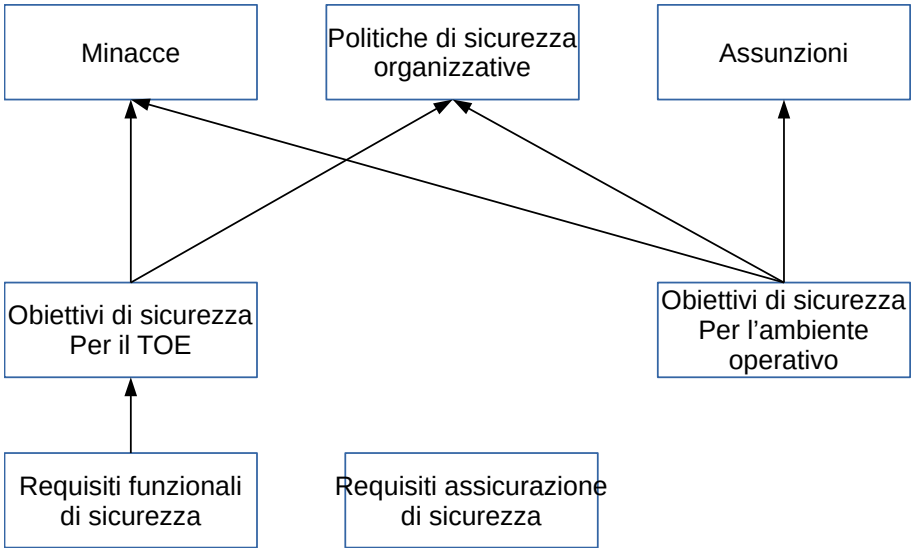
- obiettivi di sicurezza del TOE;
- obiettivi di sicurezza dell'ambiente operativo.

Inoltre si fornisce una giustificazione deli obiettivi di sicurezza che mostra che se vengono raggiunti tutti gli obiettivi si sicurezza, si risolve il problema della sicurezza: tutte le minacce sono contrastate, tutti gli OSP sono imposti e tutte le assunzioni sono confermate.

Nella sezione dei requisiti di sicurezza del ST, si traducono gli obiettivi di sicurezza del TOE in SFR, e si fornisce una giustificazione razionale dei requisiti di sicurezza, mostrando che se tutti gli SFR sono soddisfatti, vengono raggiunti tutti gli obiettivi di sicurezza del TOE.

Inoltre si fornisce un insieme di SAR per illustrare come valutare il TOE, insieme a una spiegazione per selezionare questi SAR.

Tutte le precedenti precedenti possono essere combinate in dichiarazioni: se tutti i SFR e SAR sono soddisfatti e sno raggiunti tutti gli obiettivi di sicurezza per l'ambiente operativo, allora è sicuro che sia risolto il problema della sicurezza come definito in ASE_SPD: tulle le minacce sono contrastate, tutte le OSP sono imposte, tutte le assunzioni sono confermate. Il seguente diagramma illustra queste relazioni.



La quantità di assicurazione ottenuta è definito dai SRA, e se questa quantità è sufficiente è definito dalle spiegazioni per la scelta di questi SAR.

A.10 Specifiche riassuntive del TOE (ASE_TSS)

Lo scopo di queste specifiche riassuntive consiste nel dare al consumatore del TOE una descrizione di come il TOE soddisfi tutti i SFR. Deve indicare in generale i meccanismi tecnici che il TOE utilizza per raggiungere questo scopo. Il livello di dettaglio deve essere tale da permettere ad un potenziale consumatore di capire la forma generale e l'implementazione del TOE.

Ad esempio, se il TOE è un PC Internet e i SFR contengono il requisito FIA_UAU.1 per l'autenticazione, la specifica riassuntiva deve indicare come avviene l'autenticazione: con password, token, scansione dell'iride, etc. È possibile indicare altre informazioni, come ad esempio gli standard utilizzati, o una descrizione di maggiore dettaglio.

A.11 Domande cui si può rispondere con un ST

Dopo la valutazione, il ST specifica "cosa è stato valutato". In questo ruolo il ST serve come accordo tra il potenziale consumer del TOE e il suo sviluppatore, o rivenditore. Quindi in questo ambito il ST può rispondere a domande di questo tipo:

a) *Come posso trovare il ST/TOE che mi serve?* leggendo la overview del TOE, che ne da' una breve descrizione.

b) *Questo TOE può essere inserito nella mia infrastruttura IT?* la overview del TOE risponde anche a questa domanda perché elenca i principali elementi necessari per far girare il TOE.

c) *Questo TOE si cala nel mio ambiente operativo?* i vincoli del TOE riguardo l'ambiente operativo sono negli obiettivi di sicurezza dell'ambiente operativo.

d) *Cosa fa il TOE (lettore interessato)?* La risposta si ottiene leggendo la overview del TOE, sintetica.

e) *Cosa fa il TOE (potenziale consumatore)?* In questo caso leggere la descrizione del TOE, che è meno sintetica.

f) *Cosa fa il TOE (tecnico)?* La descrizione di alto livello dei meccanismi usati dal TOE è nelle specifiche riassuntive.

g) *Cosa fa il TOE (esperto)?* i SFR danno una descrizione astratta molto tecnica e le specifiche riassuntive forniscono dettagli aggiuntivi.

h) *Il TOE indirizza il problema definito dal mio governo/organizzazione?* Se il governo/organizzazione ha definito la soluzione utilizzando packages e/o PP, allora la risposta è nella sezione della Dichiarazione di Conformità del ST, che elenca i package e i PP cui è conforme.

i) *Il TOE indirizza il mio problema di sicurezza (esperto)?* la definizione del problema della sicurezza risponde indicando: le minacce contrastate, le OSP imposte, le assunzioni relative all'ambiente operativo.

j) *Quanta fiducia posso avere nel TOE?* questo si può capire con i SAR nella sezione dei requisiti di sicurezza, che fornisce il livello di confidenza usato per valutare il TOE, e quindi la fiducia che la valutazione fornisce riguardo la correttezza del TOE.

A.12 Security targets a bassa confidenza

Scrivere un ST è un task impegnativo e può essere eccessivo per valutazioni a bassa confidenza. Perciò è possibile scrivere ST a bassa confidenza.

I CC permettono di usare ST a bassa confidenza solo per valutazioni EAL 1, non per valutazioni con EAL superiore. Un ST a bassa confidenza può essere conforme solo a PP a bassa confidenza. Si veda [B Specifiche dei Protection Profile (informativo)]. Un ST regolare (ovvero, non a bassa confidenza) può dichiarare conformità con PP a bassa confidenza.

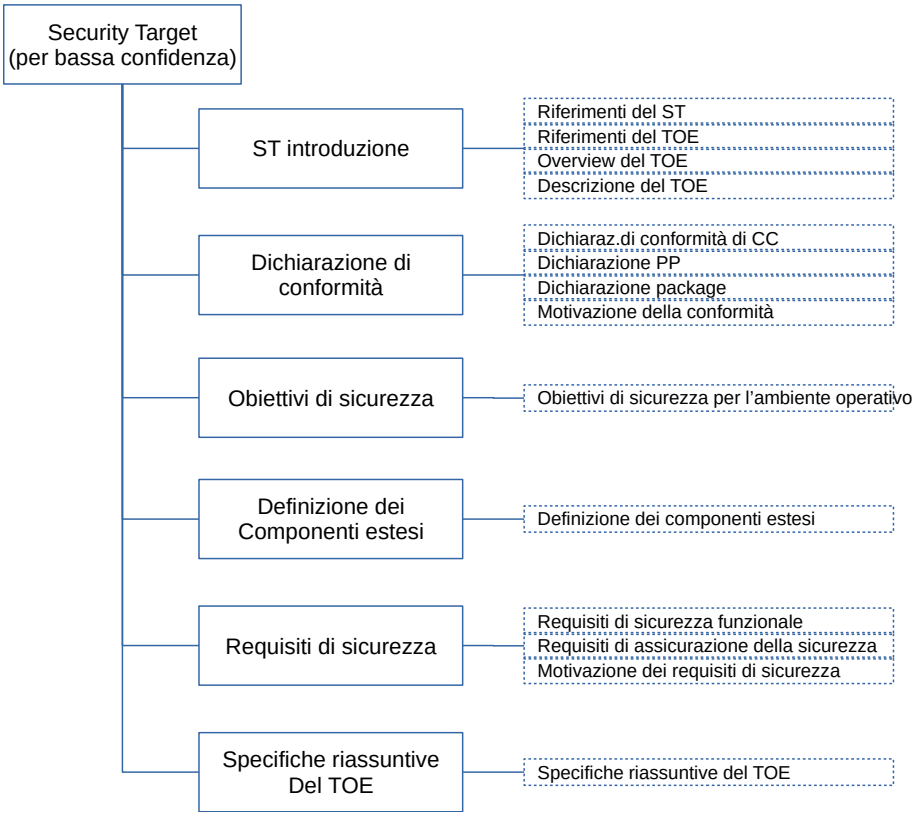
Un ST a bassa confidenza ha un contenuto ridotto rispetto un ST regolare:

- non è necessario descrivere la definizione del problema di sicurezza;
- non è necessario descrivere gli obiettivi di sicurezza del TOE. Ma è necessario descrivere gli obiettivi di sicurezza dell'ambiente operativo.
- non è necessario descrivere la giustificazione degli obiettivi di sicurezza perché nel ST non vi è definizione del problema di sicurezza,
- la giustificazione dei requisiti di sicurezza deve riguardare solo (se vi sono) le dipendenze non soddisfatte perché nel ST non vi sono gli obiettivi di sicurezza per il TOE.

Rimangono:

a) i riferimenti tra TOE e ST;
b) la dichiarazione di conformità;
c) le varie descrizioni narrative:
    1. la overview del TOE;
    2. la descrizione del TOE;
    3. le specifiche riassuntive del TOE;
d) gli obiettivi di sicurezza per l'ambiente operativo;
e) i SFR e i SAR (inclusa la definizione dei componenti estesi) e la giustificazione dei requisiti di sicurezza (solo se vi sono dipendenze non soddisfatte).

La seguente figura illustra i contenuti ridotti di un ST a bassa confidenza.



A.13 In un ST fare riferimento ad altri standard

In un ST può essere desiderabile fare riferimento ad altri standard o protocolli, come d es. un particolare standard crittografico. Vi sono tre possibili modi:

a) come OSP, o parte di essa.

   Ad es. se esiste uno standard governativo che indica come scegliere le password, può essere imposto come OSP nel ST. Divenendo poi un obiettivo per l'ambiente (come gli utenti devono scegliere la password) o, se il TOE genera password, per il TOE stesso, e quindi il relativo SFR (probabilmente della classe FIA). In entrambi i casi la giustificazione dello sviluppatore rende plausibile che gli obiettivi del TOE e i SFR sono idonei per soddisfare la OSP. Se la OSP è implementata da un SFR, il valutatore dovrà esaminare se questa affermazione è plausibile, e per farlo potrà avere necessità di analizzare lo standard.

b) come standard tecnico usaro nel raffinamento di un SFR (ad es. uno standard crittografico).

   La specifica riassuntiva del TOE è una spiegazione di come sono realizzati i SFR e non è un requisito implementativo, al contrario dei SFR e dei documenti ADV: Development. Perciò il valutatore può percepire una inconsistenza se il TSS fa riferimento ad uno standard tecnico che poi non viene citato nella documentazione ADV: development. Ma non esiste attività di routine per la verifica del soddisfacimento degli standard.

[B Specifiche dei Protection Profile (informativo)]

C Regole per le operazioni (informativo)]

C.1 Introduzione

Come detto, *Protection Profile* e *Security Target* contengono requisiti di sicurezza predefiniti. E gli autori li possono espandere tramite operazioni predefinite.

C.2 Esempi di operazioni

I quattro tipi di operazioni sono descritte nella sezione [8.1 Operazioni]. Di seguito si descrivono vari esempi di queste operazioni.

pag.100

Riferimenti

Rif.	Risorsa	Nota
1	https://www.commoncriteriaportal.org/index.cfm	portale WEB dei common criteria
2	ISO/IEC 27001, ISO/IEC 27002	contromisure di sicurezza