6 Glossario e riferimenti bibliografici

Introduzione

6.1 Sono qui riportate le definizioni dei termini tecnici che hanno un significato specifico, nel contesto del presente documento. I termini tecnici che non compaiono nel glossario sono stati impiegati in modo conforme al significato comunemente accettato. Tra parentesi è riportato il termine originale inglese, accompagnato dal numero relativo.

Definizioni

Ambiente operativo (Operational Environment - 6.46) Insieme di misure organizzative, procedure e norme da applicare, quando si usa il TOE.

Ambiente di sviluppo (Developer Environment - 6.28) Insieme di misure organizzative, procedure e norme applicate nella produzione del TOE.

Amministratore (Administrator - 6.5) Persona di riferimento per il TOE, responsabile del mantenimento della sua capacità operativa.

Attività del responsabile della valutazione (Evaluator Actions - 6.36) Parte dei criteri di valutazione di una determinata fase, o aspetto della valutazione, che specifica ciò che il responsabile della valutazione deve fare per verificare le informazioni fornite dal committente e le attività complementari che egli deve eseguire.

Canale nascosto (Covert Channel - 6.21) Utilizzo di un meccanismo non previsto per la comunicazione, per trasferire informazioni con modalità che violano la sicurezza.

Certificazione (Certification - 6.12) Rilascio di una dichiarazione formale che conferma i risultati della valutazione e la corretta applicazione dei criteri di valutazione adottati.

Classe di funzionalità (Functionality Class - 6.39) Insieme predefinito di funzioni complementari di sicurezza che può essere implementato sul TOE.

Cliente (Customer - 6.23) Persona o organizzazione che acquista un TOE.

Coesione della funzionalità (Binding of Functionality - 6.11) Aspetto della valutazione dell'efficacia del TOE che specifica la capacità delle funzioni e dei meccanismi di sicurezza di mutuarsi per formare un insieme integrato ed efficace.

Committente (Sponsor - 6.64) Persona o organizzazione che richiede una valutazione.

Componente (Component - 6.14) Parte identificabile e autonoma del TOE.

Componente elementare (Basic Component - 6.10) Componente identificabile al più basso livello gerarchico della specifica prodotta in fase di progetto di dettaglio.

Configurazione (Configuration - 6.16) Scelta di uno degli insiemi di combinazioni possibili delle caratteristiche del TOE.

Conformità (Correctness - 6.20) Proprietà della rappresentazione del TOE, grazie alla quale esso esprime, esattamente, il target di sicurezza indicato per un determinato sistema o prodotto.

Consegna (Delivery - 6.24) Processo con cui una copia del TOE viene trasferita dal responsabile dello sviluppo al cliente.

Controllo della configurazione (Configuration Control - 6.17) Sistema di controllo imposto a oggetti sottoposti a controllo, passibili di cambiamento, prodotti nel corso del processo di sviluppo, produzione e manutenzione del TOE.

Costruzione (Construction - 6.18) Processo di creazione del TOE.

Definizione dei requisiti (Requirements - 6.53) Fase del processo di sviluppo, nel corso della quale viene prodotto il target di sicurezza del TOE.

Descrizione del prodotto (Product Rationale - 6.49) Esposizione delle capacità di un prodotto in termini di sicurezza che fornisce le informazioni necessarie al potenziale acquirente per poter decidere se il prodotto consente o meno di realizzare gli obiettivi di sicurezza del suo sistema.

Disponibilità (Availability - 6.9) Proprietà che si ottiene impedendo che l'accesso alle informazioni o alle risorse sia negato senza autorizzazione.

Documentazione (Documentation - 6.30) Informazioni scritte (o registrate in altra forma) relative al TOE, necessarie ai fini della valutazione. Possono (ma non devono, necessariamente) essere riunite in un unico documento redatto allo scopo.

Documentazione per l'amministrazione (Administration Documentation - 6.4) Informazioni sul TOE fornite dal responsabile dello sviluppo del sistema e destinate all'amministratore.

Documentazione operativa (Operational Documentation - 6.45) Informazioni fornite dal Responsabile dello sviluppo del TOE, per specificare e spiegare ai clienti le modalità d'uso.

Documentazione per l'utente (User Documentation - 6.75) Informazioni sul TOE fornite dal responsabile dello sviluppo e destinate agli utenti finali.

Efficacia (Effectiveness - 6.32) Proprietà del TOE che esprime la misura in cui esso garantisce la sicurezza, nel contesto del suo impiego operativo previsto o effettivo.

Facilità d'uso (Ease of use - 6.31) Aspetto della stima dell'efficacia del TOE che consiste nel garantire che esso non possa essere configurato o usato in un modo che non è sicuro, ma che potrebbe essere, ragionevolmente, ritenuto sicuro da un amministratore o utente finale.

Funzioni di sicurezza (Security enforcing - 6.58) Ciò che contribuisce, direttamente, a realizzare gli obiettivi di sicurezza del TOE.

Garanzia (Assurance - 6.7) Grado di fiducia che si può avere nella sicurezza fornita dal TOE.

Idoneità della funzionalità (Suitability of Functionality - 6.68) Aspetto della stima dell'efficacia del TOE che esprime l'idoneità delle sue funzioni e dei suoi meccanismi di sicurezza a sventare, nella pratica, le minacce alla sicurezza definite nel target di sicurezza del TOE.

Impiego operativo (Operation - 6.44) Processo di utilizzazione del TOE.

Implementazione (Implementation - 6.40) Fase del processo di sviluppo, in cui la specifica dettagliata del TOE viene tradotta in hardware e software.

Integrità (Integrity - 6.41) Proprietà che si ottiene impedendo che le informazioni siano modificate senza autorizzazione.

Linguaggi di programmazione e compilatori (Programming Languages and Compilers - 6.51) Strumenti impiegati nell'ambiente di sviluppo per costruire il software e/o il firmware del TOE.

Meccanismi di sicurezza (Security Mechanism - 6.59) Logica o algoritmo che implementa, sull'hardware o sul software, una determinata funzione di sicurezza o una determinata funzione rilevante ai fini della sicurezza.

Meccanismo critico (Critical Mechanism - 6.22) Meccanismo interno del TOE, il cui mancato funzionamento creerebbe una vulnerabilità nella sicurezza.

Minaccia (Threat - 6.73) Azione o evento che potrebbe pregiudicare la sicurezza.

Modello formale della politica di sicurezza (Formal Model of Security Policy - 6.37) Modello di riferimento della politica di sicurezza espresso in stile formale, vale a dire l'enunciazione astratta dei principi fondamentali di sicurezza che dovranno essere realizzati dal TOE.

Obiettivi di sicurezza (Security Objectives - 6.60) Contributo alla sicurezza che il TOE è destinato a fornire.

Oggetto (Object - 6.42) Entità passiva che contiene o riceve informazioni.

Oggetto di memorizzazione (Storage Object - 6.65) Oggetto che consente sia l'accesso di lettura, sia l'accesso di scrittura [TCSEC].

Omologazione (Accreditation - 6.3) A seconda del contesto, può avere due definizioni:

a) procedura di approvazione formale di un sistema IT per l'uso in un determinato ambiente;

b) procedura con cui vengono riconosciute la competenza tecnica e l'imparzialità di un laboratorio di prova, nello svolgimento dei compiti che gli sono propri.

Organismo di certificazione (Certification Body - 6.13) Organismo nazionale indipendente e imparziale che esegue le certificazioni.

Politica di sicurezza (Security Policy - 6.61) Cfr. politica di sicurezza interna, politica di sicurezza del sistema, politica di sicurezza tecnica.

Politica di sicurezza interna (Corporate Security Policy - 6.19) Insieme di leggi, regole e procedure che disciplinano le modalità di gestione, protezione e distribuzione delle risorse (comprese le informazioni sensibili), all'interno di un'organizzazione utente.

Politica di sicurezza del sistema (System Security Policy - 6.70) Insieme di leggi, regole e procedure che disciplinano la gestione, la protezione e la distribuzione delle informazioni sensibili e delle altre risorse dell'ambiente di un sistema specifico.

Politica di sicurezza tecnica (Technical Security Policy - 6.72) Insieme di leggi, regole e procedure che disciplinano la gestione delle informazioni sensibili e l'utilizzo delle risorse da parte dell'hardware e del software di un sistema o prodotto IT.

Procedura di accettazione (Acceptance Procedure - 6.2) Procedura con cui gli oggetti prodotti nel corso dei processi di sviluppo, produzione e manutenzione del TOE vengono, deliberatamente, posti sotto il controllo di un sistema di controllo della configurazione.

Procedura operativa (Operating Procedure - 6.43) Insieme di regole che definiscono il corretto impiego del TOE.

Processo di sviluppo (Development Process - 6.29) Insieme di fasi e di attività con cui, traducendo le specifiche in hardware e software, viene prodotto il TOE.

Prodotto (Product - 6.48) Pacchetto software e/o hardware che fornisce una determinata funzionalità progettata per essere utilizzata o incorporata in più sistemi.

Produzione (Production - 6.50) Processo con cui vengono create copie del TOE destinate a essere distribuite alla clientela.

Profilo di garanzia (Assurance Profile - 6.8) Requisito del TOE che definisce il grado di fiducia richiesto per le varie funzioni di sicurezza.

Progetto architetturale (Architectural Design - 6.6) Fase del processo di sviluppo, in cui si specificano la definizione ad alto livello e il progetto del TOE.

Progetto di dettaglio (Detailed Design - 6.25) Fase del processo di sviluppo in cui la definizione ad alto livello e il progetto generale del TOE vengono perfezionati ed espansi a un livello di dettaglio che può fungere da base per l'implementazione.

Quotazione (Rating - 6.52) Misura della garanzia che può dare il TOE, composta da un riferimento al suo target di sicurezza, da un livello di valutazione stabilito in base a una stima della conformità della sua implementazione e da un apprezzamento della sua efficacia nell'ambito dell'impiego operativo, previsto o effettivo, nonchè da una quotazione convalidata della robustezza minima dei suoi meccanismi di sicurezza.

Requisiti, definizione dei, vedi Definizione dei requisiti.

Requisiti relativi al contenuto e alla presentazione (Requirements for content and presentation - 6.54) Componente dei criteri di valutazione di una determinata fase o di un determinato aspetto della valutazione che specifica cosa deve contenere ciascun elemento di documentazione relativo a quella determinata fase o a quel determinato aspetto della valutazione e come devono essere presentate tali informazioni.

Requisiti relativi agli elementi di prova (Requirements for evidence - 6.55) Componente dei criteri di valutazione di una determinata fase o di un determinato aspetto della valutazione che specifica il tipo di prova che bisogna eseguire per dimostrare che sono stati soddisfatti i criteri relativi a quella determinata fase o a quel determinato aspetto.

Requisiti relativi alle procedure e alle norme (Requirements for Procedures and Standards - 6.56) Componente dei criteri di valutazione di una determinata fase o di un determinato aspetto della valutazione che specifica il carattere e/o il contenuto delle procedure o degli approcci normalizzati che si devono adottare o mettere in atto, quando il TOE viene impiegato in fase operativa.

Responsabile dello sviluppo (Developer - 6.26) Persona o organizzazione che produce un TOE.

Responsabile della valutazione (Evaluator - 6.35) Persona o organizzazione indipendente incaricata della valutazione.

Riservatezza (Confidentiality - 6.15) Proprietà che si ottiene impedendo che le informazioni siano rivelate senza autorizzazione.

Robustezza dei meccanismi (Strength of Mechanisms - 6.66) Aspetto della stima dell'efficacia del TOE che esprime la capacità delle sue funzioni e dei suoi meccanismi di sicurezza di resistere a un attacco diretto contro i punti deboli degli algoritmi, dei principi e delle proprietà che ne sono alla base.

Sicurezza (Security - 6.57) Combinazione di riservatezza, integrità e disponibilità.

Sicurezza, funzioni di, vedi funzioni di sicurezza

Sicurezza, meccanismi di, vedi meccanismi di sicurezza

Sicurezza, obiettivi di, vedi obiettivi di sicurezza

Sicurezza, politica di, vedi politica di sicurezza

Sicurezza del responsabile dello sviluppo (Developer Security - 6.27) Insieme di controlli di sicurezza fisica, organizzativa o relativa al personale, imposti dal responsabile dello sviluppo al proprio ambiente di sviluppo.

Sicurezza, rilevante ai fini della (Security Relevant - 6.62) Ciò che non realizza, direttamente, la sicurezza, ma che deve funzionare correttamente perchè il TOE possa realizzarla.

Sicurezza, target di, vedi target di sicurezza

Sistema (System - 6.69) Una specifica installazione IT, con un determinato scopo e un determinato ambiente operativo.

Soggetto (Subject - 6.67) Entità attiva, generalmente una persona, un processo o un'apparecchiatura [TCSEC].

Stima della vulnerabilità (Vulnerability Assessment - 6.77) Aspetto della stima dell'efficacia del TOE che consiste nell'accertare se le vulnerabilità note del TOE possano, effettivamente, compromettere la sua sicurezza, quale specificata nel relativo target di sicurezza.

Strumento (Tool - 6.74) Prodotto utilizzato nella costruzione e/o documentazione del TOE.

Target di sicurezza (Security Target - 6.63) Specifica della sicurezza necessaria per il TOE, utilizzata come base per la valutazione. Il target di sicurezza specifica le funzioni e gli obiettivi di sicurezza del TOE, le minacce che incombono su tali obiettivi e qualsiasi meccanismo specifico di sicurezza utilizzato.

Target di valutazione, vedi TOE

Test di penetrazione (Penetration Test - 6.47) Test effettuati dal responsabile della valutazione per accertare se le vulnerabilità note possano essere sfruttate nella pratica.

TOE o target di valutazione (Target of Evaluation - 6.71) Un sistema o prodotto IT sottoposto a valutazione della sicurezza.

Unità funzionale (Functional Unit - 6.38) Parte di una componente elementare avente una funzionalità distinta.

Utente finale (End-user - 6.33) Persona che utilizza, solo, la capacità operativa del TOE.

Valutazione (Evaluation - 6.34) Stima di un sistema o prodotto software e/o hardware in rapporto a criteri di valutazione predefiniti.

Vulnerabilità (Vulnerability - 6.76) Punti deboli del TOE sul piano della sicurezza (dovuti, a esempio, a errori di analisi, progetto, implementazione o impiego operativo).

Riferimenti bibliografici

6.78 Nel testo si fa riferimento ai seguenti volumi e articoli:

AND Computer Security Technology Planning Study
J.P. Anderson
ESD-TR-73-51, ESD/AFSC,US Air Force, Bedford, Massachussetts, ottobre 1972.

BLP Secure Computer Systems: Unified Exposition and Multics Interpretation
D.E. Bell e L.J. LaPadula
Report MTR-2997 Rev. 1, MITRE Corporation, Bedford, Massachussetts, 1976.

BNM The Chinese Wall Security Policy
D.F.C. Brewer e M.J. Nash
Proceedings of the IEEE Symposium on Security and Privacy, Oakland, maggio 1989, pp. 206-214.

CESG3 UK Systems Security Confidence Levels, CESG Memorandum No. 3,
Communications-Electronics Security Group, Regno Unito, gennaio 1989.

CWM A Comparison of Commercial and Military Computer Security Policies
D.D. Clark e D.R. Wilson
Proceedings of the IEEE Symposium on Security and Privacy, Oakland, aprile 1987, pp. 184-194.

DTIEC DTI Commercial Computer Security Centre Evaluation Levels Manual, V22
Department of Trade and Industry, Regno Unito, febbraio 1989.

DTIFN DTI Commercial Computer Security Centre Security Functionality Manual, V21
Department of Trade and Industry, Regno Unito, febbraio 1989.

EXBM Mandatory Policy: Secure Systems Model
G. Eizenberg
ONERA/CERT/DERI, Toulouse, Francia, senza data.

GYPSY Report on Gypsy 2.05
D.I. Good, R.L. Akers e L.M. Smith
Report ICSCA-CMP.48, University of Texas at Austin, febbraio 1986.

IJRM The Ina Jo Specification Language Reference Manual
Unisys Corporation
Culver City, California, USA, 1989.

JSD System Development
M.A. Jackson
Prentice-Hall International, 1983.

JSP Principles of Program Design
M.A. Jackson
Academic Press, New York, 1975

LOTOS Information Processing Systems - Open Systems Interconnection - LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour
International Standard ISO 8807
International Organization for Standardization, 1989.

LWM A Security Model for Military Message Systems
C.E. Landwehr, C.I. Heitmeyer e J. McLean
ACM Transactions on Computer Systems, Vol. 2, No. 3, agosto 1984, pp. 198-222.

OSI Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture
International Standard ISO 7498-2
International Organization for Standardization, 1988.

RSL RAISE Specification Language Reference Manual,
RAISE/CRI/DOC/2/V1
Computer Resources International A/S
Birker(d, Danimarca, 1990.

SADT An Introduction to SADT

Structured Analysis and Design Technique
Report 9022-78R
SofTech Inc, 460 Totten Pond Road
Waltham, MA 02154, USA, novembre 1976.

SCSSI Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, 692/SGDN/DISSI/SCSSI
Service Central de la Sécurité des Systèmes d'Information, luglio 1989.

SSADM The SSADM Manual, ISBN 085-012-527-X
National Computing Centre Limited
Manchester, Regno Unito, 1989.

SSVDM Systematic Software Development Using VDM
C.B. Jones
Prentice Hall International, 1990.

TCSEC Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD,
Department of Defense, USA, dicembre 1985.

YSM A Note on the Yourdon Structured Method
A.J. Bowles
Yourdon Inc
ACM SIGSOFT Software Engineering Notes
Vol. 15, No. 2, aprile 1990, p. 27.

ZRM The Z Notation: A Reference Manual, ISBN-0-13-983768-X
J.M. Spivey
Prentice Hall International, 1988.

ZSIEC Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3-88784-200-6
Bundesamt fur Sicherheit in der Informationstechnik, Repubblica Federale di Germania, gennaio 1989.