I *Common Criteria* ed il *Centro di Valutazione* della Difesa

Lo standard ISO 15408 e le attività di valutazione del Ce.Va. Difesa

C.A. Vittorio Emanuele Di Cecco
Vice Capo Reparto del RIS (settore Rappresentanze e Sicurezza)

C.F. Stefano Ramacciotti
Direttore del Ce.Va. Difesa

L'avvento di internet ha determinato un aumento esponenziale delle interconnessioni tra computer, amplificando, già da tempo, il fenomeno della pervasività[1] della rete. Infatti, qualsiasi ambito delle moderne società vede le reti di computer come i gangli del proprio sistema nervoso, in assenza dei quali si rischia la paralisi. A maggior ragione, il mondo militare, che è stato elemento trainante della evoluzione della *Information and Communication Technology* (ITC), è soggetto ai medesimi rischi che corre la moderna società civile o, addirittura, a minacce aggiuntive più subdole, paradossalmente rese più letali dalla peculiarità dell'ambito militare.

Negli ultimi due decenni l'industria del settore ha compiuto sforzi da gigante per poter fornire dei prodotti che garantissero un adeguato livello di sicurezza, pur se con alterne vicende. Talvolta venivano proposti prodotti validi, talvolta un po'meno, ma in ogni caso non si disponeva di sufficienti elementi e di idonei criteri per poterne verificare le prestazioni di targa.

E'sulla base di questi presupposti, cioè per poter valutare la "bontà" di un oggetto in termini di sicurezza e poter paragonare diversi prodotti, che nel 1983 vide la luce, ad opera del Dipartimento della Difesa americano, il *Trusted Computer System Evaluation Criteria* (TCSEC), più famoso come *Orange Book*, dal colore della copertina del suo volume.

La risposta europea venne nel 1990, quando allo standard di oltreoceano venne contrapposto l'*Information Technology Security Evaluation Criteria* (ITSEC), di impiego più generale. I tentativi di far riconoscere l'ITSEC come standard valido a livello mondiale fallirono, ma posero le basi per la nascita di un gruppo di lavoro comune, che dopo sei anni rilasciò la

1 Con "pervasività" dello strumento informatico si intende quella caratteristica dello stesso che fa sì che in quasi ogni aspetto del funzionamento di una moderna società vi sia almeno una componente che dipende dalle nuove tecnologie.

prima versione dei *Common Criteria* (CC). Nel 1999 i CC, con la versione 2.1, divengono standard ISO/IEC 15408; nel 2007 è stata rilasciata l'ultima versione, la 3.1R2.
Questa evoluzione ha determinato il vantaggio sia di adeguare lo standard di valutazione ai rapidi progressi messi a segno dalla tecnologia, che di renderlo più confacente alle reali esigenze del mercato, che non può permettersi tempi molto lunghi per una valutazione.

Lo schema nazionale

Tra i primi utenti dei citati standard di valutazione non potevano che esservi le Autorità Nazionali per la Sicurezza dei Paesi più avanzati, sempre alla ricerca delle tecnologie più idonee per la protezione delle informazioni.
In ambito italiano le prime direttive in merito alla sicurezza informatica vengono emanate nel 1985 con la PCM-A.N.S. 1/R/A, completamente revisionata nel 1993. E', però, nel 1995 che l'Autorità Nazionale per la Sicurezza (A.N.S.) emana le varie PCM-ANS serie TI (Tecnologia dell'Informazione) con le quali viene definito lo "schema nazionale[2]" per ottenere la certificazione dei prodotti; in queste direttive, per la prima volta, si fa esplicito riferimento alla necessità di utilizzare prodotti o sistemi certificati ITSEC per la trattazione delle informazioni classificate in ambito Difesa.
Successivamente, nel 2002, lo schema in parola è stato modificato (DPCM 11.04.2002) con la possibilità di valutare i prodotti, oltre che in conformità ai criteri ITSEC, anche con lo standard internazione ISO/IEC 15408 - *Common Criteria*. L'anno successivo, con il DPCM 30.11.2003, si è avuta la separazione tra il percorso classificato e quello non classificato.
Mentre con la PCM-ANS/TI-001 era stata sancita la nascita dei laboratori autorizzati all'applicazione dello schema nazionale, denominati Centri di Valutazione (Ce.Va.), con il DPCM del 2003 nascono gli analoghi laboratori che espletano l'attività in seno allo schema nazionale "non classificato", i Laboratori per la Valutazione della Sicurezza (LVS).

I compiti dei CE.VA.

I Centri di Valutazione sono chiamati a prestare la loro opera ogniqualvolta una persona fisica o giuridica, le amministrazioni pubbliche e qualsiasi altro ente, associazione od organismo richieda la fornitura o lo sviluppo di un prodotto per la trattazione di informazioni classificate. Il principale compito di un Ce.Va. è di verificare che le funzioni di sicurezza, di cui il sistema informativo è dotato, siano efficaci nel contrastare le minacce dichiarate e che siano state correttamente realizzate.
Quindi, un Ce.Va. svolge attività di valutazione in merito ad un insieme di *software* (SW), *firmware* e/o *hardware* (HW) possibilmente con le relative guide d'uso[3], al termine della quale redige il cosiddetto "Rapporto Finale di Valutazione" (RFV).
Altro compito a cui può essere chiamato un Ce.Va. è quello di assistere il committente[4] ed il fornitore[5] nella redazione/revisione della documentazione (*deliverables*) necessaria alla condotta della valutazione (va da sé che il personale valutatore che abbia prestato assistenza non potrà partecipare alla valutazione dell'Oggetto della Valutazione, O.d.V., che secondo il linguaggio proprio dei CC diviene *Target Of Evaluation*, TOE). Ultimo possibile compito è quello di fornire all'Ente Certificatore (EC)[6] gli elementi utili per l'individuazione delle metodologie più idonee da adottare, informandolo sulle attività compiute ai fini della valutazione. Questo nel rispetto degli ovvi obblighi di riservatezza, sia in termini di tutela del segreto di stato, che del segreto commerciale.

La valutazione

Il fine di una valutazione è verificare, con puntigliosità ed adeguato approfondimento, non solo che il prodotto preveda le funzioni di sicurezza (SF) descritte nelle specifiche (*Security Target*, ST), ma anche quanta fiducia (*confidence*) possa essere ad esse accordata (compresi i meccanismi che le realizzano), che siano efficaci (*effective*) nel contrastare le minacce dichiarate e che siano realizzate correttamente (*correct*).
Correttamente significa senza commettere errori, spesso presenti nel software, analizzando tutte le vulnerabilità individuate nel ST. Infatti, si può affermare che non esista SW che non abbia al suo interno errori - volontari e non - e che tutte le vulnerabilità individuate siano state correttamente contrastate, che non sia cioè "attaccabile" da avversari più o meno esperti, comunemente identificati con gli hacker.
Il risultato fornisce una misura del livello di fiducia, in pratica esso definisce di quanto il sistema è conforme ai particolari criteri scelti come riferimento.
Così come una D.O.C. o una D.O.C.G. non garantiscono che un vino sia "buono", ma solo che segue fedelmente un disciplinare tecnico e quale è stato il livello di approfondimento nei controlli, l'applicazione di un elevato livello di certificazione non significa che il prodotto è più sicuro, ma che è stato più rigorosamente e approfonditamente controllato. Pertanto si può avere nei confronti dell'oggetto una ragionevole

2 Insieme di procedure e di regole nazionali necessarie per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione in accordo a un sistema di criteri di riferimento.
3 Fino allo scorso anno si parlava di prodotti IT (SW/HW, idoneo a fornire una determinata funzionalità, progettato per essere utilizzato o incorporato in uno o più sistemi), o di sistemi (insieme di prodotti, funzionalmente o fisicamente interconnessi, destinati al trattamento automatico delle informazioni per un utilizzo specifico in un ambiente definito), con le relative guide utente e di amministratore. Con la ver. 3.1 dei CC si sono registrati importanti cambiamenti a cominciare dalle definizioni di base stesse.
4 Il soggetto pubblico o privato che richiede al fornitore lo sviluppo o la fornitura di un prodotto o di un sistema.
5 Il soggetto pubblico o privato fornitore del prodotto o del sistema.
6 L'organismo pubblico responsabile della certificazione dei prodotti e dei sistemi informatici, dell'accreditamento dei centri di valutazione nonché della definizione, dell'applicazione e dell'aggiornamento dello schema nazionale. L'ANS è l'"Autorità di certificazione" (DPCM 3.02.2006) che emette il Certificato di Valutazione sulla base della documentazione presentata dall'Ufficio Centrale per la Sicurezza - UCSi (Ente di Certificazione). Il RUD Infosec è invece l'articolazione di cui si avvale l'UCSi per la certificazione dei prodotti e sistemi destinati a trattare informazioni classificate in ambito Difesa.

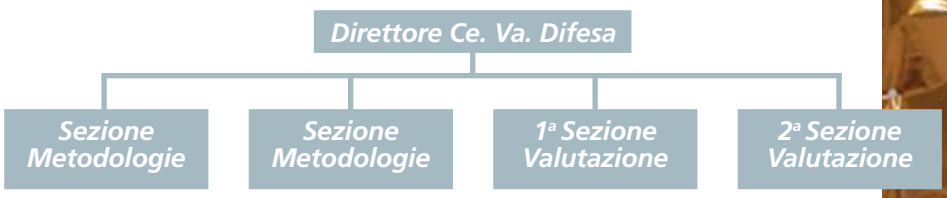
maggiore fiducia all'aumentare del livello di garanzia, perché la probabilità che un'eventuale vulnerabilità venga scoperta cresce al crescere del livello di garanzia stesso.
La valutazione si conclude con il citato RFV sottoposto all'approvazione dell'EC, il quale è responsabile del controllo del rapporto stesso e, qualora non ravvisi problematiche particolari, del rilascio del Rapporto di Certificazione unitamente al Certificato vero e proprio.
Per portare a valutazione un prodotto il fornitore, su richiesta del committente, deve redigere il citato ST. La funzione di questo documento è quella di definire la sicurezza di un prodotto IT in base a: gli obiettivi di sicurezza[7] (che rispondono alla domanda sicuro per fare cosa), l'ambiente di sicurezza[8] (sicuro in quale contesto) e, passando dai requisiti funzionali, i requisiti di *assurance*. Nello specifico il compito del Ce.Va. sarà quello di valutare le funzioni di sicurezza del TOE, le TOE *Security Functions* (TSF). Queste costituiscono l'insieme delle contromisure di tipo tecnico (HW, SW e *firmware*) del TOE, per definire il sottoinsieme di regole contenute nella politica di sicurezza TOE stesso, la TOE *Security Policy* (TSP). La TSP è fondamentale e stabilisce come i beni debbano essere gestiti, protetti e distribuiti all'interno del TOE stesso.
Il ST, che non deve essere confuso con i noti Requisiti di Sicurezza (RSI, RSS e RSC), rappresenta il primo di una serie di documenti e materiali che il fornitore deve consegnare. Oltre questo, infatti, deve essere inviata al Ce.Va. tutta la documentazione che descrive in modo sempre più minuzioso l'architettura del sistema all'aumentare del livello di garanzia richiesto, l'*high level* ed il l*ow level design*, e tutto quanto serva a giustificare le scelte progettuali fatte.
In base a quanto presentato, ed ai test di penetrazione condotti, sarà possibile esprimere una valutazione in merito alla correttezza di implementazione delle SF e alla loro efficacia.

Qui e nella pagina accanto, le foto del satellite Cosmo-Skymed (© Alenia Spazio)

I livelli di "assurance"

I livelli *assurance* sono sette e vengono descritti nel seguito.
EAL1 (TOE testato funzionalmente): rappresenta il livello di garanzia di base che risulta decisamente superiore rispetto al livello di garanzia di un TOE non valutato. Il livello EAL1 è applicabile quando è richiesta una fiducia minima nella correttezza delle operazioni, ma le minacce alla sicurezza sono poco rilevanti. Una valutazione a questo livello è tesa a garantire che il TOE sia in grado di funzionare così come indicato nella documentazione e le soluzioni individuate offrano un'adeguata protezione contro le minacce identificate.
EAL2 (TOE testato strutturalmente): è prevista una descrizione informale del progetto architetturale del TOE. Il livello EAL2 richiede la cooperazione degli sviluppatori del TOE in termini di informazioni sui processi di spedizione e di design, ed i risultati dei test funzionali, che devono indicare che il TOE soddisfa il *Security Target*. In pratica, richiede agli sviluppatori l'impegno normalmente occorrente per realizzare un buon prodotto senza significativi aumenti di tempo e di costi. Si richiede una valutazione a livello EAL2 quando è sufficiente un medio-basso livello di garanzia e/o quando in presenza di una documentazione di sviluppo non completa. E'indicato per minacce medio-basse.
EAL3 (TOE metodicamente testato e controllato): descrizione informale del progetto di dettaglio. L'esito dei test funzionali deve essere oggetto di valutazione. Inoltre deve esserci un sistema di controllo della configurazione ed una procedura di distribuzione approvata. Il livello EAL3 è, probabilmente, il massimo livello raggiungibile, senza modificare, se non in modo alquanto limitato, il processo di sviluppo adottato da uno sviluppatore che tiene conto delle *best practice* per la implementazione di codice sicuro. EAL3 è applicabile in quelle situazioni in cui è richiesto un medio livello di garanzia senza dover, per condurre la valutazione, effettuare una consistente riprogettazione del TOE stesso.
EAL4 (TOE metodicamente progettato, testato e controllato): il *source code* e gli schemi dell'*hardware* dei meccanismi di sicurezza devono essere valutati. L'esito dei test relativi ai meccanismi deve essere oggetto di valutazione. Il livello EAL4 permette ad uno sviluppatore di raggiungere il massimo livello di affidabilità raggiungibile modificando, in modo limitato e ancora con relativi bassi costi, il processo di sviluppo adottato da uno sviluppatore che tiene conto delle *best pratice* per lo sviluppo di codice sicuro. EAL4 è il livello più alto di affidabilità che probabilmente si potrà

7 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 (SF) e non tecniche (fisiche, procedurali e relative al personale).
8 Uso ipotizzato del 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, tra l'altro, lo sfruttamento di eventuali vulnerabilità note del prodotto ICT), beni colpiti, politiche di sicurezza dell'Organizzazione (modello organizzativo, definizione requisiti per le contromisure tecniche e non tecniche, ecc.).



raggiungere con prodotti/sistemi non progettati per rispondere ai CC o adattando prodotti gia esistenti. Si esplica attraverso la ricerca delle vulnerabilità più evidenti. E'indicato nei casi di una minaccia medio-alta, ed è livello più richiesto dai Committenti.
I successivi livelli (EAL 5, 6 e 7) sono molto difficili da raggiungere se il sistema non è stato concepito e sviluppato con l'intenzione di certificarlo CC. Per questi livelli non è attualmente prevista una metodologia comune di valutazione valida internazionalmente.

Il Ce.Va. Difesa

Il Ce.Va. Difesa è uno dei cinque laboratori accreditati dall'A.N.S.. La procedura di accreditamento serve a garantire la competenza tecnica del laboratorio e ad assicurare che l'intero processo di certificazione avvenga nel rispetto dei principi fondanti di: imparzialità, oggettività, ripetibilità e riproducibilità.
Il Ce.Va. Difesa è alle dipendenze del Capo del II Reparto - Informazioni e Sicurezza dello SMD, che ne è il rappresentante legale, e che esercita le sue funzioni tramite il Vice Capo Reparto per le Rappresentanze Militari e la Sicurezza. E' dal Capo Reparto del RIS che discendono le direttive per quanto concerne l'accettazione tecnico-amministrativa dei contratti di valutazione e la definizione della priorità tra le valutazioni richieste al Laboratorio. Mentre la sede legale è ubicata presso lo SMD - RIS, la sede operativa è a San Piero a Grado(Pisa), ed è ubicata nel comprensorio del Centro Interforze Studi e Applicazioni Militari (C.I.S.A.M.).
Il Ce.Va. Difesa dispone di 5 valutatori che hanno effettuato un *on-the-job-training* di 6 mesi presso il laboratorio DOMUS (ex-IBM) in Canada e che sono stati abilitati come «Valutatori della sicurezza di sistemi/prodotti informatici fino a livello EAL4[9] *Common Criteria* ISO/IEC 15408» a cura del *Communications Security Establishment* (CSE) canadese e riconosciuti valutatori dall'A.N.S..
Due sezioni, ciascuna costituita da due valutatori rappresentano l'elemento portante del laboratorio, anche se non meno significative sono le rimanenti sezioni relative alla metodologia delle valutazioni ed alla qualità.
A questo punto è doveroso condividere con i lettori la seguente osservazione. Il costo dei corsi per essere abilitati valutatori (CAN $ 250.000) e la loro durata (sei mesi), suggerisce un loro impiego di almeno cinque anni presso il Ce.Va. Difesa; questo a volte si scontra con le altre esigenze di impiego, in particolare gli eventuali obblighi legati agli avanzamenti.

Valutazioni a cura del Ce.Va. Difesa

Il Ce.Va. Difesa ha condotto fino ad oggi tre valutazioni, tutte relative al programma italo-francese Cosmo-Skymed, che in configurazione finale sarà composto da una costellazione di quattro satelliti in orbita polare per il rilevamento di dati attraverso il *Synthetic Aperture Radar* (SAR). Nell'ambito del suddetto programma nella notte tra il 7 e l'8 dicembre scorsi è stato lanciato il secondo dei quattro satelliti.
Trattando dati anche di natura militare l'Alenia Spazio ha dovuto sottoporre a certificazione tutto il sistema che, a causa della sua complessità e dell'elevato livello di *assurance* richiesto, ha visti impegnati contemporaneamente più Ce.Va. accreditati dall'A.N.S..
La prima delle tre valutazioni del Ce.Va. Difesa è stata relativa alle "Cifranti di Bordo", mentre le altre due hanno riguardato rispettivamente il SAR *Dual Centre Ciphering System* (per la parte trasmissiva della stazione del Fucino) ed il *Decipheering System* (parte ricezione di Pratica di Mare). Tutte le valutazioni richieste sono state effettuate a livello EAL4. Una valutazione a tale livello comporta numerose attività come quella di valutazione del ST, della gestione della configurazione, della consegna e della messa in opera del TOE, del processo di sviluppo del TOE, della documentazione destinata agli utenti e agli amministratori del TOE, delle misure di sicurezza connesse al ciclo di vita del TOE, di test e di stima di vulnerabilità. Una serie di attività che ha messo a dura prova tutti, sia il sistema stesso che i valutatori, dato che si è trattato delle prime attività condotte a termine dal Ce.Va. Difesa.
Attività decisamente complesse che hanno consentito di valutare positivamente un sistema di grande importanza e dalle implicazioni strategiche molto importanti. Ora sono già all'orizzonte altre importanti e simolanti attività di valutazione, a conferma che il Ce.Va. Difesa è una solida e matura realtà nel mondo della certificazione. ■

9 Il massimo livello soggetto a mutuo riconoscimento in ambito internazionale.