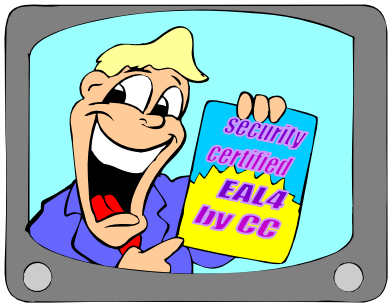
SecLab
laboratorio di idee sulla sicurezza ICT
Newsletter di Secure Edge - your safety .net

Anno I - numero 5 - 17 maggio 2003

Security Certification vs. Marketing Hype

di Sandro Fontana - sfontana@secure-edge.com

Il 29 ottobre 2002 sarà ricordato sicuramente come il giorno in cui tutto il mondo dell'ICT emise un borbottio di malcelato stupore: dopo poco più di nove mesi dalla e-mail di Bill Gates[BG01] a tutti i dipendenti Microsoft nella quale egli annunciava che da quel momento, la priorità più alta della Microsoft sarebbe stata il Trustworthy Computing, il sistema Windows 2000[1] aveva ricevuto la certificazione



Evaluation Assurance Level 4 [2]
secondo il processo di valutazione dei Common Criteria v. 2.1[MS02]

Secondo le parole di Mike Nash General Manager e Vice President della Security Business Unit (SBU) di Microsoft:

"[…] per gli attuali e potenziali futuri utenti di Windows 2000, questa certificazione secondo i Common Criteria fornisce un alto livello di assicurazione della sicurezza."

Finalmente avevamo un sistema operativo Microsoft, con *la sicurezza certificata*:
il mondo non sarebbe stato certamente più quello di prima …
… o invece si?

Prima di stappare bottiglie di champagne (o Coca Cola, se siete quel tipo di persone), vale la pena cercare di capire quale è il significato di questa certificazione, partendo in ogni modo dall'inizio della storia.

Obiettivamente parlando, in questi ultimi due anni, la Microsoft ha effettuato una serie di iniziative totalmente dedicate alla sicurezza, in totale allineamento a quanto indicato da Gates:

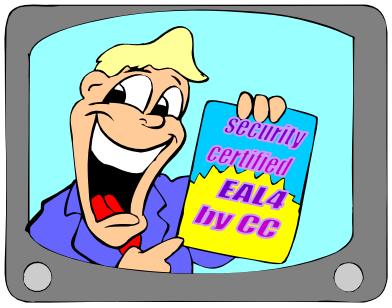
"[…] l'Azienda deve focalizzare tutte le sue energie sulla sicurezza, anche se questo significa fermare temporaneamente lo sviluppo di nuove funzionalità."

"[…] quando ci troviamo a dover scegliere tra aggiungere features o risolvere un problema di sicurezza, noi siamo obbligati a scegliere la sicurezza."

[1] Windows 2000 Server/Advanced Server/Professional con Service Pack 3 e la patch Hotfix Q326886
[2] Valutazione effettuata dai *Common Criteria Testing Lab* della Science Applications International Corporations

Come esempio di queste iniziative, ricordiamo che in questi ultimi mesi parecchie migliaia di software engineers in tutto il mondo sono stati sottoposti ad uno speciale addestramento su come scrivere codice sicuro[3]; successivamente circa 8.500 software engineers sono stati coinvolti in un processo di revisione di milioni di righe di codice, allo scopo di effettuare su questo un'intensa analisi di sicurezza:

solo questo processo di revisione ha significato due mesi di blocco dello sviluppo di nuovo software.
Tutto ciò, nel 2002, è costato alla Microsoft più di 100M$[IN02].



Ora, è indubbio che Microsoft debba investire nella security.

Dall'apparizione di Nimda nel 2001, anche gli analisti del mercato come Gartner Group hanno iniziato a sostenere le caratteristiche di sicurezza di altri sistemi operativi (fondamentalmente Linux), e molti responsabili ICT delle Aziende di Fortune 500 hanno pubblicamente iniziato a parlare di diversificazione negli investimenti IT a scapito dei sistemi e del software Microsoft.

Un'intervista[IS03] fatta ai responsabili di sistemi ICT ed ai Security Officer delle grandi aziende americane, rivela da un lato una scarsa fiducia (57%) nella capacità di Microsoft di aumentare il livello di sicurezza del software Windows, dall'altro la presenza di un'enorme maggioranza (80%) orientata a prendere in considerazione sistemi operativi ed applicazioni non-Microsoft (Linux, Apache, LotusNotes, Netscape, Opera), scelta dovuta proprio alle problematiche legate alla mancanza di sicurezza della piattaforma Microsoft.

E' chiaro che Microsoft ha dei seri problemi di immagine quando si affrontano temi come l'affidabilità, la sicurezza e la stabilità dei servizi e dei prodotti di rete; ma è in questi frangenti, come sempre è successo nei momenti critici della storia della Microsoft, che la guida di Bill Gates diventa ancora di più determinata.

Dalla sua e-mail iniziale sono nati gli interventi, le dichiarazioni pubbliche, i cospicui investimenti diretti ed indiretti ed in ultimo una prima certificazione sulla sicurezza di Windows 2000, alla quale, dichiara la Microsoft[FAQ02], seguiranno le certificazioni per Windows XP e Windows Server 2003, flagship della Microsoft.

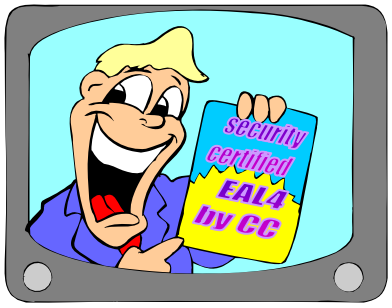
Tutto questo è molto bello e sarà sicuramente una cosa buona per gli utenti; contemporaneamente però la Microsoft continua a sostenere la *nondisclosure of vulnerability* ed il fatto che il *close-source software* è più sicuro dell'open-source, continuando a commissionare studi sia per dimostrare le migliori performance dei sistemi Windows sia per dimostrate un più basso TCO (total cost of ownership) dei suoi sistemi a lungo termine.

[3] Microsoft ha pubblicato anche un libro sull'argomento: Writing Secure Code di Michael Howard e David LeBlanc

Vista in questa ottica, ci si inizia a chiedere se la filosofia del Trustworthy Computing non sia altro che una parte di una campagna di PR.

Se poi a questo punto prendiamo in esame il significato della certificazione ricevuta da Windows 2000 e di come la Microsoft l'ha comunicata, il dubbio diventa certezza:

siamo di fronte ad un'enorme campagna di PR.



Cercherò di spiegare perché.

Fermo restando che gli sforzi di Microsoft sono reali e che l'aumento del livello di sicurezza nel software prodotto è un obiettivo realmente necessario alla Microsoft per riconquistare la fiducia del mercato e continuare la scalata anche del settore di mercato dei server *mission critical*, resta il fatto che la certificazione ricevuta non significa veramente molto in termini di sicurezza:

ne consegue che tutta la comunicazione fatta, riguardo questo evento,
si configura come un puro *marketing hype*.

Per sostenere questa affermazione, dobbiamo analizzare un poco la struttura e la logica dei Common Criteria, con il supporto di alcuni documenti[JSS03].

I Common Criteria[CC--] definiscono processi indipendenti per la valutazione dei sistemi e dei prodotti dell'ICT nell'ottica della sicurezza.

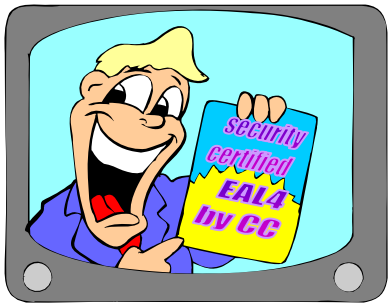
Una certificazione secondo i CC è un procedimento piuttosto costoso da mettere in esercizio, ma sicuramente riconosciuto in tutto il mondo[4], essendo di fatto un'evoluzione ed integrazione dei precedenti TCSEC (USA 1985 - DoD 5200.28-STD [Orange Book]), ITSEC (Europa 1990), CTCPEC (Canada 1992) ed in ultimo essendo stato accettato e fatto proprio dall'ISO (ISO/IEC 15408 - 1999).

La necessità di queste metodologie è di dare all'utente finale (Azienda o Governo) un modo indipendente di valutazione e confronto tra sistemi (prodotti), nell'ottica della sicurezza: come si dice, dare la possibilità di confrontare le mele con le mele.

[4] Attualmente 16 paesi partecipano al Common Criteria Recognition Agreement, inoltre i CC sono uno standard *de facto* nella gran parte del mondo

Ragionando per grandi linee, possiamo affermare che i CC sono composti di due parti:

- ***Protection Profile***: una serie di specifiche di requisiti standardizzati, che in pratica definiscono quello che il sistema si suppone che faccia;
- ***Evaluation rating***: un valore tra 1 e 7 che definisce il grado di certezza (Evaluation Assurance Level) sul quale possiamo contare relativamente al fatto che il sistema in esame sia conforme ad uno o più dei Protection Profile sui quali è valutato;



Quando si vuole certificare un sistema secondo i CC, bisogna quindi scegliere uno o più Protection Profile dalla lista di quelli disponibili[5], eventualmente aggiungendo alcuni altri requirements specifici.
Una volta così definito su cosa si vuole valutare il prodotto, un gruppo di esperti, tipicamente provenienti da un ente specializzato ed indipendente, determinano se il sistema in esame incontra le specifiche definite, ed a quale livello di confidenza lo fa, assegnando quindi un punteggio EAL.

Questo significa che, per interpretare il risultato di una valutazione e quindi di una certificazione secondo i Common Criteria, bisogna conoscere sicuramente *la votazione assegnata*, cioè l'EAL ma altrettanto sicuramente bisogna sapere secondo quali specifiche di requisiti è stata affrontata la valutazione.

Sapere semplicemente che un prodotto ha avuto una valutazione EAL2, o anche EAL7 (il massimo possibile) di per se **non significa nulla**.

Ritornando all'inizio di questa storia, la Microsoft avrebbe dovuto effettuare una dichiarazione non fuorviante e completa, semplicemente annunciando che:

Il sistema Windows2000 è stato certificato secondo **CAPP/EAL4**

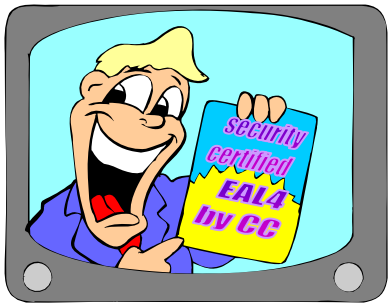
Sembrerebbe poca cosa, ma a questo punto, tutti si sarebbero chiesti cosa stava a significare quel CAPP:

… e qui sta la sorpresa!

[5] Ovvero creane uno nuovo, se ne esiste la vera necessità e naturalmente si possiede un grande conto in banca;

CCAP: Controlled Access Protection Profile PP-012

Dallo standard Common Criteria:



"CAPP stabilisce un livello di protezione appropriato ad una comunità di utenza ben gestita e non ostile, richiedendo protezione contro minacce relative a tentativi casuali o involontari di violare la sicurezza del sistema (cui si applica).

Il profilo non ha come scopo quello di essere applicabile in circostanze in cui è richiesta una protezione contro decisi tentativi di violare la sicurezza del sistema da parte di aggressori ostili e ben finanziati.

CAPP non è realmente mirato alle minacce messe in opera in modo doloso da personale addetto allo sviluppo o ad attività sistemistica

In pratica un sistema valutato secondo questo PP può essere utilizzato nello stesso modo con il quale si usa un qualsiasi altro sistema:
a] Non connesso direttamente ad Internet;
b] Non utilizzato direttamente per la gestione della posta e degli attach;
c] Con la consapevolezza che non esiste nessuna protezione contro software ostile[6], quindi ci si deve installare solo il software del quale si abbia il 100% di fiducia negli sviluppatori;
d] Qualunque attacco dall'interno[7], troverà questo sistema senza particolari difese;

❖

EAL: Evaluation Assurance Level

Come abbiamo detto, il rating di valutazione va da un minimo di EAL1 ad un massimo di EAL7.

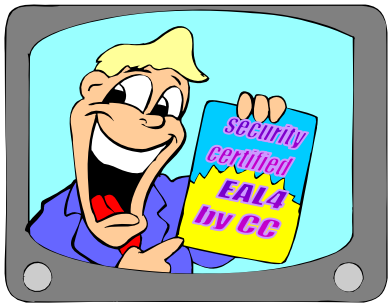
EAL1 significa che il fornitore si è presentato alla prima riunione del processo di valutazione ed è poi scomparso.

[6] Più di una volta software su CD off-the-shelf involontariamente trasportava virus
[7] Ancora oggi circa l'85% dei *security exploits* vengono effettuati dall'interno

EAL7 significa che tutte le parti del sistema sono state analizzate a livello di source code, esistono dimostrazioni matematiche per la verifica del software ed esistono dimostrazioni formali relative all'inesistenza od in alternativa alla completa identificazione di eventuali possibili *covert channel*.

E un EAL4, cosa significa ?

Potremmo affermare che:



"il gruppo di lavoro di valutazione ha verificato la documentazione dell'architettura del sistema tramite metodi non formali"

In pratica significa che il gruppo di lavoro i documenti li ha letti, ma non li ha veramente valutati.
E' un po' come se la Finanza arrivasse per una visita ispettiva nell'ufficio Amministrativo di un'Azienda, volesse vedere tutti i libri contabili, li leggesse riga per riga, ma non facesse nessun controllo di congruenza o di riscontro con altra documentazione.

Non pensate che la cosa sia comunque a buon mercato: CAPP è un documento *UNCLASSIFIED* di cinquantuno pagine, prodotto dalla NSA ed è bene leggerlo con attenzione.
Dovete comunque produrre un mucchio di documentazione di progetto, disegni di architettura, schemi e chart di tutti i tipi, documentazione del software ed un mucchio di altra carta …
… ma senza comunque preoccuparvi di dimostrare che quanto prodotto è di qualità.

A questo punto, una definizione per CAPP/EAL4 potrebbe essere:

"I miei requirements sono inadeguati,
ma ho fatto un gran lavoro per essere seriamente sicuro di averli rispettati"

❖

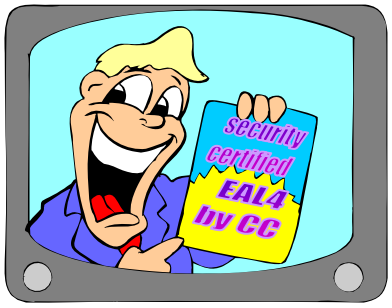
Perché mai Microsoft ha investito tutte queste risorse per avere un risultato che appare, o meglio che è, così mediocre ? Non avrebbe potuto fare di più ?

A parziale discolpa di Microsoft, si può affermare che CAPP è il più completo PP esistente relativo ai sistemi operativi, quindi il massimo che Microsoft poteva trovare.

Inoltre, a completamento della verità, Microsoft ha *rafforzato* CAPP tramite l'ALC_FLR, cioè un metodo formale comprensivo di procedure definite per il tracciamento dei difetti o imperfezioni sulle misure di sicurezza, l'identificazione

delle azioni correttive e la distribuzione delle informazioni, relativamente alle azioni correttive da intraprendere, agli utenti del TOE (target of evaluation).

L'ALC_FLR è previsto e governato nelle guidelines di applicazione dei CC ed è inteso alla gestione delle informazioni relative ai difetti nella sicurezza riscontrati dopo che è stata completata la valutazione del TOE.
E' assimilabile ad una pratica metodologica di gestione della qualità, ma non aggiunge nulla al valore della sicurezza del sistema valutato.



Insomma, con tutte queste chiacchiere a che conclusione arrivare ?

Da un lato bisogna ammettere che Microsoft non ha detto il falso, solo non ha detto tutto ed ha confezionato le sue dichiarazioni in modo che il pubblico capisse qualche cosa che in realtà non era detto.

Dall'altro lato mi viene in mente che … questo è un film già visto!

1995: Windows NT3.51 riceve la certificazione C2 secondo TCSEC (Orange Book)

Fantastico!
… se non che, dopo qualche giorno di stupore ci si rese conto di un dettaglio:
il sistema era stato certificato con alcune *piccole* parti disabilitate.

Mi sembra di ricordare: niente floppy disk né scheda di rete !

❖

References

[BG01] Trustworthy Computing
Bill Gates – Microsoft's Chairman and Chief Software Architect
http://www.itmweb.com/f020102.htm
Craig Mundie – Microsoft's Senior Vice President and CTO
http://www.microsoft.com/presspass/exec/craig/10-02trustworthywp.asp

[CC--] http://www.commomncriteria.org/

[FAQ02] Windows 2000 CC Certification - Frequently Asked Questions
http://www.microsoft.com/presspass/

[IN02] Microsoft Spent $100M on Trustworthy Computing [July 19, 2002]
Thor Olavsrud - http://www.internetnews.com/xSP/print.php/1429681

[IS03] Trustworthy yet? - Information Security February 2003
http://www.infosecuritymag.com

[JSS03] Understanding the Windows EAL4 Evaluation
Jonathan S. Shapiro – Johns Hopkins University
http://eros.cs.jhu.edu/~shap/NT-EAL4.html

[MS02] Microsoft Windows 2000 Awarded Common Criteria Certification
http://www.microsoft.com/presspass/press/2002/oct02/10-29commoncriteriapr.asp

❖