

Quaderni Clusit

006

I rischi del Trusted Computing

Claudio Telmon

I rischi del Trusted Computing

Claudio Telmon



Quaderni CLUSIT – Febbraio 2007

CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Copyright © 2007 Claudio Telmon.

Copyright © 2007 CLUSIT

Tutti i diritti sull'Opera sono riservati all'Autore e al Clusit.

Sono tuttavia attribuiti i seguenti diritti:

1. I Soci Clusit fruitori dell'Opera hanno il diritto di utilizzare l'Opera nell'ambito della propria attività professionale purchè: a) riconoscano la paternità dell'Opera in capo all'Autore e al Clusit; b) non la utilizzino per scopi commerciali; c) non creino opere derivate e/o alterino l'Opera e/o la trasformino e/o la sviluppino.
2. I diritti attribuiti ai Soci Clusit sopra riportati sono estesi a tutti i fruitori dell'Opera dopo che la stessa sarà rilasciata in forma elettronica sul sito www.clusit.it in area pubblica.

L'Autore e il Clusit non garantiscono che l'Opera sia esente da errori. Qualora vengano segnalati errori, nel limite del possibile si provvederà a correggerli nelle eventuali edizioni successive.

L'Autore e il Clusit non assumono alcuna responsabilità in relazione al contenuto dell'Opera e/o ai risultati attesi e/o ai risultati conseguenti all'uso della stessa e, pertanto, non risponderanno di eventuali e qualsivoglia danni diretti e/o indiretti che dovessero derivarne.

In particolare non viene garantito che il contenuto dell'Opera sia esauriente, completo, preciso o aggiornato.

Eventuali denominazioni di prodotti e/o aziende e/o i loghi e/o i marchi e/o i segni distintivi eventualmente citati nell'Opera sono di esclusiva proprietà dei rispettivi titolari.

Presentazione

La sicurezza, nel senso più generale del termine, costa e non solo in termini economici! L'introduzione di un'architettura di sicurezza in un sistema ha impatti sull'usabilità del sistema, sui tempi di uso e risposta, e sulla privacy delle persone che operano all'interno del sistema. Tutte queste ricadute si esplicano in maniera piuttosto vistosa nel caso di misure nell'ambito di quella che viene ormai definita la homeland security, non sono così immediate nel caso delle tecnologie per la Sicurezza ICT. Anche se è vero che le diverse tecnologie usate in tale ambito sfruttano pesantemente un forte monitoraggio delle attività svolte all'interno di un sistema, non è difficile usarle con cognizione di causa evitando abusi. L'avvento delle Trusted Platform (TP) basate sul paradigma del Trusted Computing sembrano però sconvolgere questo stato delle cose.

Una Trusted Platform (TP) è di fatto un PC che contiene al suo interno una componente (TPM) il cui comportamento può essere alterato solo dal costruttore della piattaforma stessa. L'inalterabilità di questa componente consente di fatto la realizzazione di un sistema che è in grado di rilevare la modifica a dati e programmi prima che il sistema li utilizzi. A titolo di esempio, questo significa che queste piattaforme sono in grado di rilevare ogni forma di trojan o rootkit, e non sono invece in grado di rilevare modifiche del codice a tempo di esecuzione, e quindi attacchi quali buffer overflow o format bug. Sono inoltre in grado di attestare inequivocabilmente la loro identità riducendo quindi notevolmente il margine ad attacchi basati su IP spoofing o altre forme di impersonificazione. In sostanza, queste componenti inalterabili sono il meccanismo attraverso cui un sistema discerne il "bene dal male", ovviamente sulla base della concezione che di questo concetto possiede il costruttore della piattaforma, con tutto ciò che ne consegue.

Siamo quindi di fronte all'ennesima tecnologia bivalente cioè il cui uso etico potrebbe contribuire a migliorare sensibilmente lo stato delle cose ma che può anche essere usata per avvantaggiare pochi a scapito di molti; e purtroppo la storia ci insegna che in questi casi prima o poi qualcuno cade in tentazione. Prendere una posizione netta in questo contesto è estremamente difficile e si va da coloro che hanno una fiducia cieca nella tecnologia e nell'uomo a chi è particolarmente scettico sulle virtù dell'uomo, posizione questa molto ben rappresentata dal seguente motto: "*Technological progress is like an axe in the hands of a pathological criminal*", pronunciato da A. Einstein in relazione alle tecnologie che dalla fine della seconda Guerra hanno portato alla costruzione di armamenti nucleari.

Nel caso del TP la situazione non è così drammatica anche se valori come la libertà di scelta e la privacy stanno assumendo nella società dell'informazione una valenza sempre maggiore. Va inoltre detto che anche le diverse parti interessate all'ambito Trusted Computing, si stanno muovendo molto cautamente sugli aspetti di deployment della tecnologia. Poco meno di dieci anni fa si parlava del TC (allora associato al progetto Palladium della Microsoft) come di un prodotto di imminente uscita, oggi, anche se diversi prodotti sono realizzati con questa tecnologia, l'uso della stessa è di fatto fermo; in parte grazie anche alle perplessità che l'intera comunità ha sollevato rispetto ai rischi legati all'introduzione massiccia di questa tecnologia.

Il CLUSIT che è impegnato in prima linea nella promozione della cultura della sicurezza in tutti i suoi aspetti, non poteva ignorare questo fenomeno e quindi doveva intervenire sul tema. Lo ha fatto con questo contributo, la cui stesura è stata affidata ad un "vecchio" della sicurezza informatica italiana: Claudio Telmon.

Si tratta di un lavoro il cui scopo principale è fornire al lettore gli elementi per cogliere il dibattito in corso evitando però, per i motivi sopra menzionati di prendere posizioni troppo

nette. Si tratta quindi di un lavoro particolarmente difficile, che l'autore ha però svolto egregiamente cercando di descrivere con la massima oggettività possibile le diverse implicazioni (sia positive che negative) derivanti dall'adozione su scala mondiale di queste tecnologie. Il contributo, dopo una prima parte introduttiva dedicata ai concetti di base usati nel testo, si dedica ad una descrizione esauriente di quelli che la comunità internazionale individua come alcuni tra i principali rischi legati all'introduzione sul mercato di tale tecnologia, quali: condizionamenti del mercato, violazione della privacy e abusi di posizione. Particolare enfasi è stata posta a quello che probabilmente è oggi il tema più caldo e a cui l'intera comunità della sicurezza ICT è chiamata a rispondere:

“valutati i rischi sull'uso di una TP, siamo proprio certi che con il bagaglio di conoscenze oggi in nostro possesso non si riesca a concepire una tecnologia che fornisce prestazioni equivalenti al TP in termini di sicurezza, ma che comporti meno rischi? Siamo certi che non ci sia altra strada per migliorare le sicurezza dei prodotti ICT?” Ancora una volta, la risposta a questi quesiti non è unica e dipende dalle convinzioni che sono radicate in ciascuno di noi, è però importante porsi queste domande e disporre di tutti gli elementi per formulare una risposta quantomeno coerente, e proprio questo è l'obiettivo che questo contributo si prefigge.

In conclusione, tutti coloro che in questi anni non hanno avuto, per i motivi più diversi, l'opportunità di interessarsi al dibattito in corso sul tema del trusted computing possono, grazie a questo sforzo di Claudio Telmon, recuperare il tempo perso, e non solo riallinearsi allo stato dell'arte sul tema, ma essere in grado di cogliere le diverse sfumature tra le posizioni presenti sulla rete. Se poi troveranno l'argomento particolarmente interessante, attraverso la bibliografia predisposta dall'autore potranno raggiungere il livello di approfondimento voluto.

Prof. Danilo Bruschi
Presidente del
Comitato Tecnico-Scientifico Clusit

Abstract

Il Trusted Computing è una tecnologia sviluppata dal Trusted Computing Group, associazione che comprende numerose aziende del settore ICT. Il Trusted Computing Group ha come obiettivo sviluppare, definire e promuovere standard aperti per “hardware-enabled trusted computing” e tecnologie di sicurezza. Secondo il Trusted Computing Group, l’obiettivo principale della tecnologia proposta è aiutare gli utenti a proteggere le loro risorse informatiche.

Tuttavia, l’iniziativa è stata da più parti criticata, sia giudicandola inefficace dal punto di vista della sicurezza o focalizzata solo su alcuni interessi specifici, sia ritenendo che essa esponga l’attività dei sistemi abilitati ad un forte controllo da parte di alcune organizzazioni, con pesanti conseguenze sulla privacy e sugli equilibri del mercato del software e delle informazioni.

Lo stesso Trusted Computing Group ammette che è possibile forzare gli utenti ad usare il Trusted Computing per accedere a servizi, nonché il rischio che il Trusted Computing possa essere utilizzato per minare il diritto alla privacy ed al controllo degli strumenti utilizzati. D’altra parte, il Trusted Computing Group non possiede licenze o brevetti per l’implementazione delle specifiche, non si ritiene responsabile per come le singole aziende implementeranno le specifiche o altri servizi e, pur auspicando un uso corretto del Trusted Computing, ammette di non essere in grado di imporre un uso corretto della tecnologia.

Mentre il CLUSIT non intende discutere quali siano gli obiettivi del Trusted Computing Group, in conformità con il proprio statuto vuole analizzare sia le potenzialità di questa tecnologia dal punto di vista della sicurezza, sia gli eventuali rischi associati, allo scopo di permettere al cittadino, alle aziende ed alle Pubbliche Amministrazioni di valutare consapevolmente l’opportunità di utilizzare il Trusted Computing.

L’autore

Claudio Telmon

Membro del Comitato Direttivo del CLUSIT, si occupa da più di dieci anni di sicurezza ICT come consulente freelance, con particolare attenzione alla sicurezza dei sistemi distribuiti e all’analisi del rischio.

Ringraziamenti

Si ringraziano i membri del Comitato Tecnico Scientifico del CLUSIT per i consigli ed i suggerimenti dati nel corso della revisione del documento.

INDICE

SEZIONE I Premessa	9
A chi è destinato questo documento?	9
Perché il CLUSIT si interessa al Trusted Computing?	9
SEZIONE II Executive summary	11
SEZIONE III Alcuni concetti fondamentali	17
Il rischio e le contromisure	17
Il concetto di “Trust”	19
Il Digital Rights Management	24
SEZIONE IV il trusted computing	27
Cos’è il Trusted Computing	27
Quali sono gli obiettivi del Trusted Computing?	31
Quale sicurezza fornisce?	31
SEZIONE V I rischi del trusted computing.....	37
Lo scenario	37
Gli effetti certi	38
I rischi.....	39
Il mercato del software	39
Il rischio di inefficacia sostanziale delle norme	41
La privacy.....	45
La censura	47
La vulnerabilità dei sistemi	48
L’abuso da parte di terzi.....	49
Altri rischi	50
SEZIONE VI Ma allora, il Trusted Computing è un problema?	51
Il rischio è reale?	51
Cosa si può fare per gestirlo?	51
Soluzioni tecniche	51
SEZIONE VII glossario	57
SEZIONE VIII Riferimenti.....	61

CLUSIT

Associazione Italiana per la Sicurezza Informatica

Sede legale presso:

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO

www.clusit.it – info@clusit.it

tel. 347 23 19 285