

Viva il Trusted Computing!

Il Trusted Computing è morto!

Alessio "isazi" Sclocco - isazi@olografix.org

Mircha Emanuel "ryuujin" D'Angelo - ryuujin@olografix.org

Sommario

- Introduzione
- Scenari
- Cos'è il Trusted Computing ?
- Ancora scenari
- Conclusione

Introduzione

In questo intervento abbiamo intenzione di introdurvi al Trusted Computing.

Non c'è bisogno che siate dei tecnici per comprenderci.

Non siamo qui a vendere niente ne' ad evangelizzarvi su qualcosa, siamo qui per spingervi a farvi delle domande.

Se di domande volete farne anche a noi siete i benvenuti :)

Scenari

I moderni utenti di computer hanno accesso ad una miriade di servizi, la maggior parte dei quali richiede una password di accesso.

Queste password se non sono scelte con cura e tenute al sicuro possono rappresentare un problema per la sicurezza dell'utente stesso.

Il proliferare delle password poi spinge molti utenti ad utilizzarne una per tutti i servizi.

Scenari (2)

I dati presenti all'interno dei nostri computer diventano sempre più importanti per le nostre vite.

Il furto di questi dati può arrecare gravi danni anche all'utente più casalingo.

Eppure la maggior parte delle informazioni presenti all'interno dei nostri computer sono leggibili da terzi in locale e persino da remoto.

Scenari (3)

Sempre più servizi basano il proprio funzionamento sulle reti e sulla computazione distribuita.

La collaborazione di norma si basa sulla fiducia.

Se non ci si può fidare dei nodi che partecipano alla computazione non ci si può fidare neanche dei risultati di questa.

La presenza di nodi malfidati può indebolire i servizi e quindi gli utenti che li utilizzano.

Scenari (4)

Sempre più spesso i contenuti passano attraverso internet per essere distribuiti.

Pensate a musica, video, film, software, e-book....

Questo nuovo modo di distribuire i contenuti stà modificando sia le abitudini dell'utente che il mercato.

Trusted Computing

Cominciamo la nostra avventura dal significato di fiducia.

fi|dù|cia

1 sentimento di sicurezza, tranquillità, speranza e sim., che deriva dal confidare in qcn. o in qcs., nelle possibilità proprie o altrui.

2 prestigio, buona reputazione.

(dizionario De Mauro)

Trusted Computing (2)

Trust

Trust is the expectation that a device will behave in a particular manner for a specific purpose.

(Trusted Computing Group)

In the US Department of Defense, a '**trusted system or component**' is defined as '**one which can break the security policy**'.

(Ross Anderson)

Trusted Computing (3)

Ora che sappiamo cosa significa “trusted”, cos'è il Trusted Computing ?

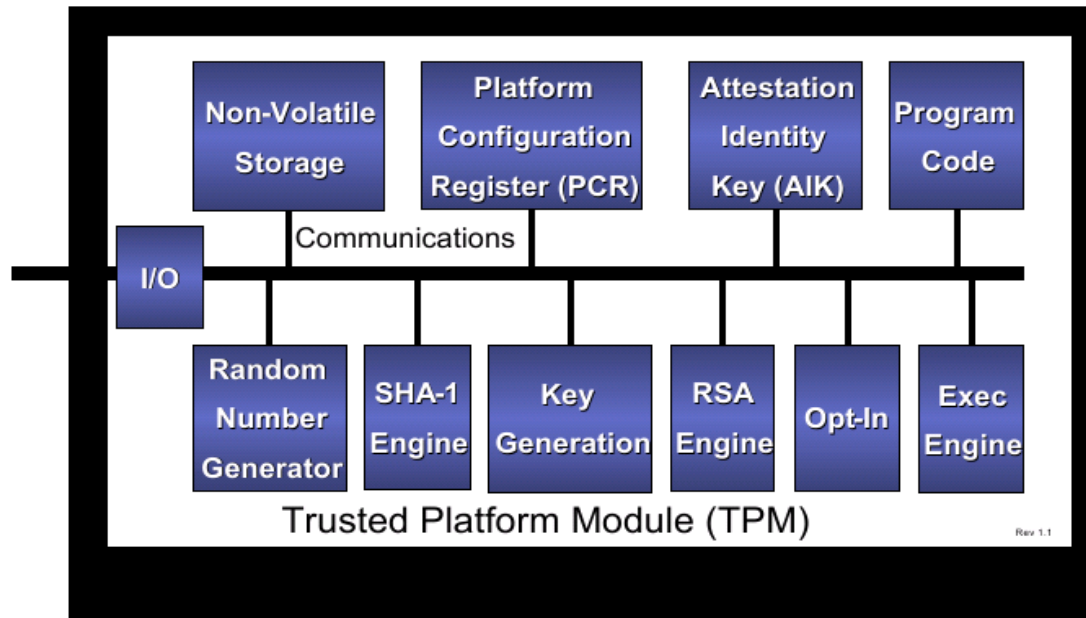
Il TC è un insieme di specifiche riguardanti hardware e software che le maggiori aziende dell'information technology mondiale, riunite in un consorzio, hanno sviluppato per produrre computer più "fidati".

Alla base del funzionamento del TC c'è un chip, il TPM o **T**rusted **P**latform **M**odule.

Il TPM è fidato per definizione.

Trusted Computing (4)

Architettura del TPM



Come si può notare gran parte delle funzionalità del TPM si basano sulla crittografia a chiave pubblica.

Trusted Computing (5)

Un sistema che si voglia definire fidato deve essere in grado di fornire almeno queste tre funzionalità:

- **Protected capabilities**
- **Integrity measurements**
- **Integrity reporting**

Tutte queste funzionalità vengono fornite grazie al TPM.

Trusted Computing (6)

Protected capabilities

Le "protected capabilities" sono un insieme di istruzioni aventi il permesso per accedere a delle aree di memoria dette **shielded locations**.

Queste shielded locations non sono accessibili in altro modo.

Solo all'interno di queste particolari locazioni è possibile operare su dati sensibili.

Trusted Computing (7)

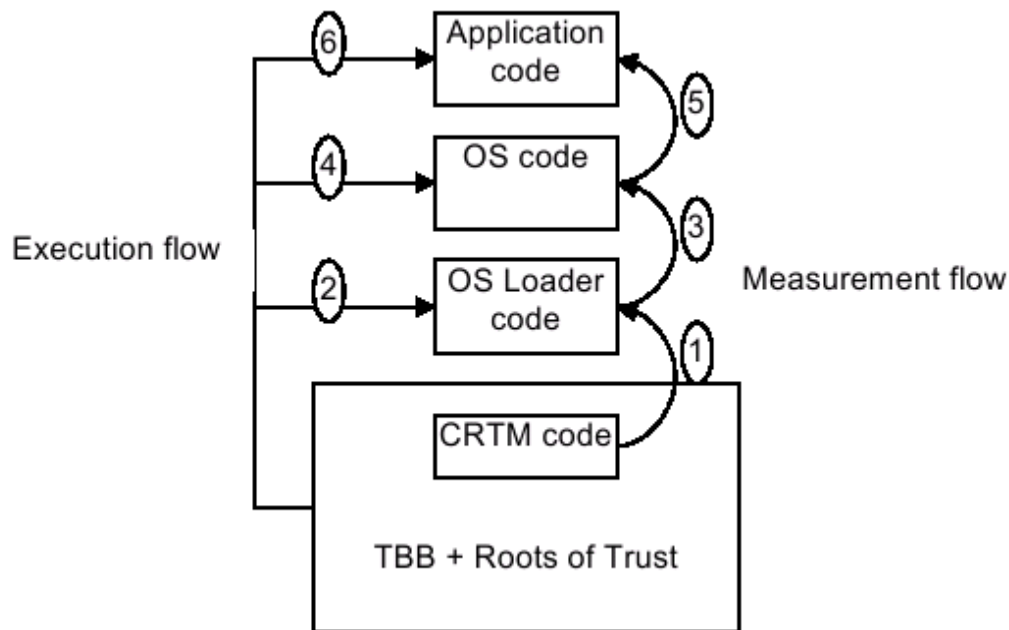
Integrity measurement

L'integrity measurement è un processo che consiste in:

- Ottenere informazioni su caratteristiche del sistema che ne possono compromettere l'integrità;
- Creare un resoconto di queste informazioni;
- Salvare questo resoconto in un PCR o Platform Configuration Register.

Trusted Computing (8)

Integrity measurement (2)



La misurazione parte da uno stato conosciuto, la **root of trust**.

Se possibile la fiducia viene estesa transitivamente.

Trusted Computing (9)

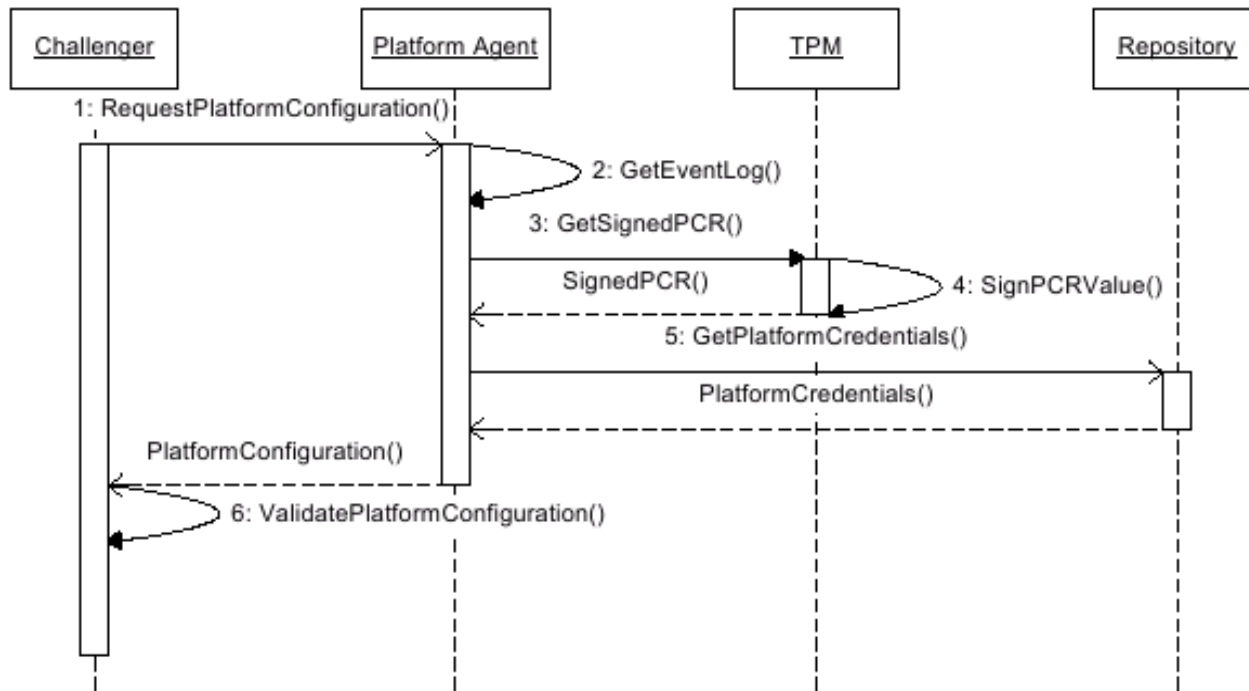
Integrity reporting

La procedura di integrity reporting permette due operazioni:

- Accedere al contenuto di una shielded location per salvarne il contenuto;
- Verificare l'autenticità delle informazioni salvate.

Trusted Computing (10)

Integrity reporting (2)



Challenger

An entity that requests and has the ability to interpret integrity metrics.

Ancora scenari: password

E' sicuramente possibile sfruttare le funzionalità di base del TC per fornire un elegante e sicuro sostituto dell'autenticazione mediante password.

"A user can generate an RSA public/private key pair on the TCPA chip. The private key can be configured never to leave the chip. This private key can be used with protocols like SSL to provide strong user authentication over the internet."

(David Safford)

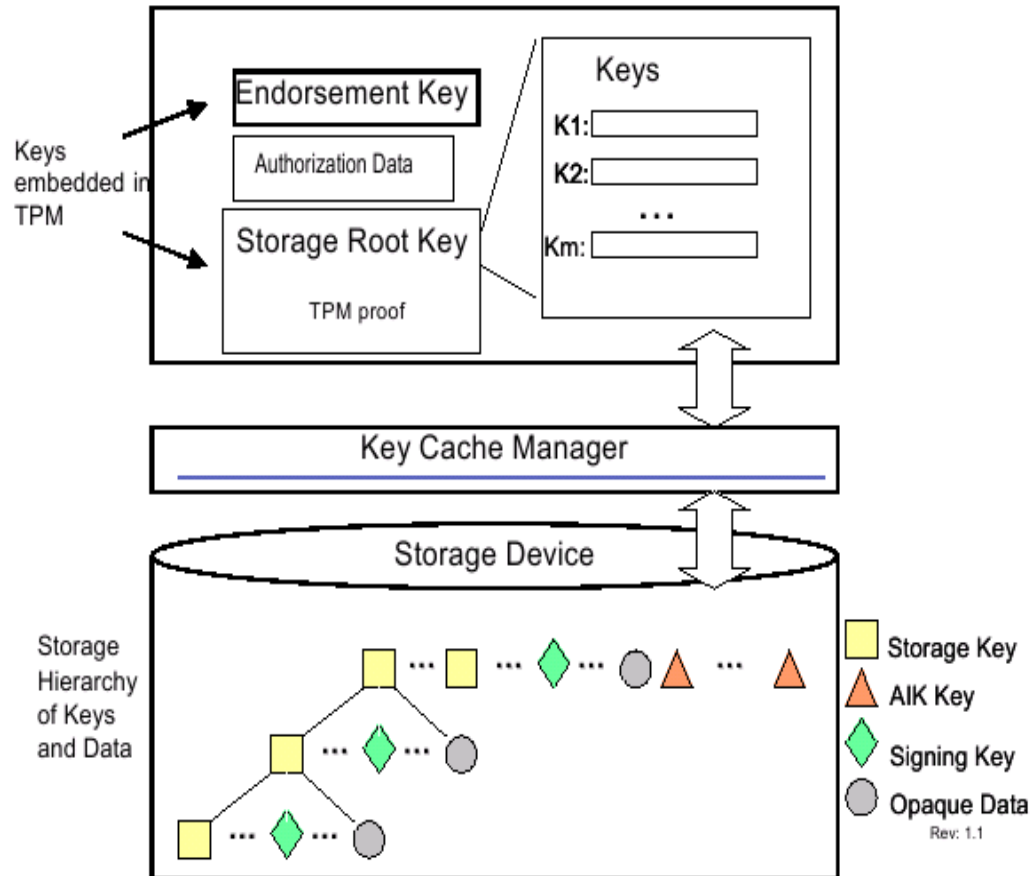
Ancora scenari: dati

Facendo affidamento sulle capacità crittografiche del TPM possiamo pensare di proteggere file, dischi o partizioni.

Tutto questo proteggendo e rendendo quindi inaccessibili anche le chiavi di cifratura.

Ancora scenari: dati (2)

TPM / RTS



Ancora scenari: computazione distribuita

Siamo già oggi in grado di rendere sicura una certa comunicazione che avviene attraverso una rete pubblica.

Quello che non siamo in grado di determinare a priori invece è lo stato dei nodi che partecipano alla comunicazione.

Il TC risponde a questa esigenza mediante la **remote attestation**.

Trusted Computing (11)

Attestation

The process of vouching for the accuracy of information.

- **Attestation by the TPM**

An operation that provides proof of data known to the TPM. This is done by digitally signing specific internal TPM data using an AIK.

- **Attestation of the Platform**

An operation that provides proof of a set of the platform's integrity measurements.

Trusted Computing (12)

- **Attestation to the Platform**

An operation that provides proof that a platform can be trusted to report integrity measurements.

- **Authentication of the platform**

Provides proof of a claimed platform identity.

Queste informazioni possono essere richieste da un challenger, anche remoto, mediante le procedure di integrity reporting.

Ancora scenari: Digital Rights Management

Cos'è il DRM ?

Il DRM è un tentativo di controllare l'utilizzo dei contenuti digitali con sistemi tecnologici e non con sistemi legislativi.

Was TCG formed to specify Digital Rights Management (DRM) technologies ?

TCG specifications do not provide all the necessary technical elements required for DRM. It is conceivable that developers could build their own DRM solutions that would operate on systems with Trusted Platform Modules, but TCG specifications alone are not DRM solutions.
(Trusted Computing Group)

Ancora scenari: censura

Ma chi è veramente in grado di controllare il TC ?

In rete si parla di **HCL**, Hardware Certified List, **SRL**, Serial Revocation List o **DRL**, Document Revocation List.

Implementare tecnologie del genere grazie al TC significherebbe impedire di mantenere il proprio sistema in uno stato fidato utilizzando determinato hardware, software o accedendo ad un determinato contenuto.

E' facile capire come questo possa essere un problema.

Ancora scenari: censura (2)

Il problema di chi controlla la tecnologia è indubbiamente attuale ed importante.

Il TPM ad esempio è alla base del TC e riceve fiducia per definizione.

L'unico problema è che non siamo noi a conferirgli questa fiducia, ma chi lo ha realizzato.

Come possiamo noi conoscere realmente qual'è il suo comportamento ?

Ancora scenari: compravendita

Immaginiamo di voler vendere un computer di seconda mano che adotti tecnologie TC.

Come possiamo recuperare le nostre chiavi dal TPM per poter continuare ad utilizzarle ?

Esistono procedure di recovery e backup ?

Ma se queste procedure esistessero non violerebbero le politiche del TC ?

Ancora scenari: guasti

Immaginiamo di utilizzare il sealed storage per la memorizzazione di tutti i dati in nostro possesso.

Immaginiamo di avere un guasto sul TPM, come possiamo recuperare le chiavi per accedere ai nostri dati ?

Se non possiamo più accedervi anche se i dati sono ancora presenti in memoria, di chi sono realmente quei dati ?

Conclusione

In Metro Olografix stiamo riflettendo sul TC e sul modo di fare informazioni su questo tema.

Abbiamo raccolto parecchio materiale su:

<http://www.olografix.org/tc>

Confidiamo nel vostro aiuto per continuare questo lavoro.