Parte II

Libertà digitali: trusted computing e censura online

Sistemi di tutela

La protezione dei contenuti digitali, allo stato attuale, viene implementata attraverso l'uso di tre strumenti:

- Il contratto
- Le leggi sul diritto d'autore
- La tecnologia

Il Trusted Computing rientra nella terza categoria, ed è lo strumento in fase di avanzato sviluppo che, attraverso lo strumento della crittografia, porta al controllo totale dei contenuti digitali.

TCG

Il TCG (Trusted Computing Group) è un'alleanza tra Microsoft, IBM, Intel, HP, AMD e tanti altri, che si propone di creare una piattaforma che sia più sicura per l'utente finale.

- Ogni singola applicazione di un sistema TC dovrebbe essere in grado di comunicare in tempo reale, in rete, lo stato del sistema, dei software in esso contenuti ed i documenti custoditi.
- Elemento centrale in un sistema NGSBC di TC è il Chip Fritz. Questo, applicato alla MB, conserva le Endorsement Keys, ossia, una serie di chiavi private per la cifratura asimmetrica dei dati.

L'ambiguità di un termine: trusted

Per il TCG “trusted” significa fidato... ma non fidato per l'utente.
Tale termine, sarebbe da intendersi come fiducia tecnica: uno strumento è dato solo se si ha la certezza che si comporterà sempre nelle modalità richieste dagli scopi per il quale è stato ideato.
Gli oppositori al TC invitano a diffidare da un sistema di cui sia oscuro ed indecifrabile il funzionamento: in questo caso non si dovrebbe concedere alcuna fiducia.

Endorsement Key

L'Endorsement Key è una combinazione di chiavi RSA a 2048 bit che viene impiantata in modo indelebile al momento della produzione del chip Fritz (o TPM).

Questa coppia di chiavi identifica in modo univoco il sistema sul quale il chip è installato e, di conseguenza, anche il software che gira in quel sistema. La sua funzione è quella di identificare il sistema come trusted, in quanto non manipolato rispetto alla situazione nota al soggetto certificatore (c.d. Certification Autority)

Altre funzioni in un sistema TC

- Una memoria a camere stagne (Curtained Memory)
- Input/Output blindato
- Sealed Storage – (L'unità di memorizzazione potrà essere letta solo dalla combinazione hw/sw data)
- Attestazione remota - Un certificato digitale creato dall'hw comunica la fotografia del sistema (hw+sw) a chi ne faccia richiesta.

Avrete il non plus ultra...

Con il TC si potrà fare in modo che solo la combinazione hw-sw certificata possa girare su una determinata macchina.

Ma certificata da chi?

Chi può fare cosa?

• Chi produce il sistema operativo, si trova in una posizione superiore a chi crea il software applicativo;

•Chi produce il BIOS, si trova in una posizione ancora più alta e può decidere quale sistema operativo può essere caricato;

•Chi produce l'hardware si trova in una posizione ancora più alta e può decidere che BIOS può essere caricato;

• Chi fa le leggi che vigono nel Paese in cui viene prodotto l'hardware può controllare tutta questa catena di poteri.

Alessandro Bottoni

Quali rischi?

I sistemi di TC, apparentemente perfetti sotto il profilo della sicurezza, suscitano dei dubbi quantomeno sul rispetto delle norme sulla privacy, soprattutto se considerati in accoppiata con altri sistemi DRM (come l'ERM).

Ross Anderson evidenzia la possibilità che i sistemi di tipo TC possano essere utilizzati per operazioni di censura da remoto.

Tutela della privacy

L'Unione Europea ha ben pensato di vagliare la compatibilità con una struttura di tipo Trusted Computing con la normativa europea in tema di privacy (2002/58/CE)

Il “Gruppo di Lavoro per la Tutela dei Dati Personali” (art. 29 95/46/CE) ha proposto delle osservazioni sull'impatto del sistema TC sulla protezione dei dati personali.
europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp86_en.pdf

“Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group”

I dubbi del Gruppo di Lavoro

- Quale sarebbe l'impatto del sistema TC in un ambiente lavorativo? Anche se l'utente finale potesse scegliere di “spegnere” il TPM... il lavoratore addetto ai terminali potrà farlo?

- L'utente sarà davvero in grado di scegliere il “terzo fidato”? Sarà lui a decidere chi “autenticherà” la sua macchina? (la buona strada del Direct Anonymous Attestation)

Tutela della privacy

La risposta del TCG agli interrogativi ed alle perplessità suscitate dal gruppo di lavoro con le “linee guida” del 2005
https://www.trustedcomputinggroup.org/specs/bestpractices/Best_Practices_Principles_Document_V2_0.pdf

Tuttavia queste linee guida “contengono principi generici che riecheggiano (piuttosto confusamente) alcuni cardini della normativa comunitaria sulla protezione dei dati personali [...] e poi rappresentano una lampante dichiarazione di ammissione del fatto che l'architettura TC costituisce intrinsecamente una minaccia alla privacy” (Roberto Caso).

L'utonto...

La funzione di remote attestation, come tutte le altre è già implementabile via sw, ma con il TC diventa (o sembra diventare) pressoché inespugnabile

The trusted computing architecture will not only protect data against intruders and viruses, but also against you. In effect, you, the computer owner, are treated as an adversary
(Set Shoen)

Double Edged Sword Systems

Tali sistemi, inoltre, sono stati qualificati come double edged sword poichè si prestano ad espletare in tutta tranquillità e sicurezza anche attività antisociali ed illegali in genere.

Dalla parte del manico...

Gli stessi strumenti posti a tutela del sistema contro il malware possono essere utilizzati anche per impedire che un determinato software (solo perché, ad esempio, non è di gradimento della casa produttrice del chip) possa essere utilizzato su quello stesso sistema.

Allo stesso modo si potrebbe impedire all'utente di fruire di le multimediali non originali.

Ci serve davvero il TC?

In un articolo sul suo sito(http://laspinanelfianco.wordpress.com/2006/08/22/creare-una-quasi-trusted-platform-con-un-livecd-ed-una-smart-card/) Alessandro Bottoni spiega come ottenere con strumenti alternativi tutte le funzioni “interessanti” del Trusted Computing...

...il tutto usando un LiveCD di Linux, una chiave di memoria USB ed una Smart Card!

Linkografia minima

http://www.no1984.org/

http://laspinanelfianco.wordpress.com/

http://www.jus.unitn.it/users/caso/DRM/Libro/sign_anelli/home.asp

http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

Grazie per l'attenzione

Avv. Giovanni Battista Gallus
Studio Legale Gallus Cardia
Cagliari
g.gallus@studiogallus.it

Francesco Paolo Micozzi
Studio Legale Nati
Cagliari
f.micozzi@studionati.it
www.studionati.it