

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

SEZIONE I

PREMESSA

A chi è destinato questo documento?

L'informatica ha assunto un ruolo essenziale nella nostra società. Per questo, alcune problematiche di sicurezza informatica sono ormai di interesse generale, coinvolgendo principi fondamentali legati alla tutela dei diritti e delle attività di cittadini, aziende e Pubbliche Amministrazioni. Questo documento è stato quindi pensato per poter essere compreso, seppure forse non in tutti i dettagli, da chiunque abbia una buona cultura informatica di base. L'argomento trattato non è infatti di interesse solo per i tecnici informatici, e soprattutto le valutazioni sull'utilità e i rischi del Trusted Computing coinvolgono aspetti di rilevanza più generale.

Perché il CLUSIT si interessa al Trusted Computing?

Con Trusted Computing (TC) si intende qui¹ una piattaforma hardware/software sviluppata dal Trusted Computing Group (TCG), associazione che comprende numerose aziende del settore ICT. Il TCG ha come obiettivo sviluppare, definire e promuovere standard aperti per "hardware-enabled trusted computing"² e tecnologie di sicurezza. Secondo il TCG, 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, perché ritenuta inefficace dal punto di vista della sicurezza o focalizzata solo su alcuni interessi specifici, e 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 TCG in [1] ammette che le tecnologie sviluppate possono essere utilizzate per "forzare" gli utenti ad usare il TC per accedere a servizi (pag. 11), nonché il rischio che il TC possa essere utilizzato per minare il diritto alla privacy ed al controllo degli strumenti utilizzati (pag. 13). D'altra parte, il TCG (pag. 3) 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 responsabile del TC, ammette di non essere in grado di imporre un uso corretto della tecnologia.

Mentre il CLUSIT non intende discutere quali siano gli obiettivi del TCG, 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 piattaforme basate sul TC.

In questa analisi ci concentriamo sull'utilizzo del Trusted Computing per i Personal Computer (PC), ma esistono già specifiche per l'introduzione del TC su cellulari e PDA, e in effetti alcune aziende legate principalmente alla telefonia sono parte del TCG. Molte delle considerazioni esposte in questo documento possono essere riportate agli altri contesti in cui è

¹ Esistono in realtà altre tecnologie che possono essere classificate come "Trusted Computing". Si tratta però di soluzioni teoriche o implementate in ambiti ristretti, la cui analisi è poco interessante in questo contesto. Qui con Trusted Computing facciamo comunque riferimento alle specifiche definite dal Trusted Computing Group.

² "Uso dei computer reso fidato mediante meccanismi hardware"

previsto l'utilizzo di tecnologie TC-compliant. Trattando il caso del PC, faremo necessariamente riferimento a Microsoft Windows ed ai suoi componenti, almeno nei nostri esempi. Per quanto le tecnologie definite dal TCG non siano specifiche per questo sistema operativo, si tratta comunque del sistema operativo che, come piattaforma PC/client, copre la grande maggioranza delle installazioni, e quindi fare riferimento ad un caso più generale sarebbe semplicemente poco realistico. Allo stesso modo, faremo riferimento all'architettura PC Intel (e AMD) per quanto riguarda l'hardware, dato che, ora che anche Apple è passata a processori Intel per i propri sistemi, anche in questo caso si tratta della quasi totalità delle nuove installazioni.

SEZIONE II

EXECUTIVE SUMMARY

Il Trusted Computing è al centro di accessi dibattiti sulle funzionalità di sicurezza che fornisce, ma anche sui rischi che comporta la sua diffusione. Data la rilevanza del tema per la sicurezza dei sistemi informativi, il CLUSIT ha deciso di pubblicare questo documento come contributo tecnico ad una discussione sul tema. Nel seguito il documento affronta principalmente il caso del Trusted Computing come definito dal Trusted Computing Group e implementato nei personal computer (PC), in quanto si tratta di un caso di particolare interesse generale e di più facile comprensione dal punto di vista del rischio e del mercato.

Con Trusted Computing, secondo quanto indicato dal TCG, si intende un insieme di componenti hardware e software che hanno lo scopo di fornire le seguenti funzionalità³:

- effettuare dei controlli sull'integrità di componenti del sistema, come ad esempio applicazioni e componenti del sistema operativo;
- permettere l'accesso ad informazioni riservate solo ai componenti che hanno superato i controlli di integrità; in pratica, il software autorizzato può accedere a dati riservati solo se non risulta manomesso;
- fornire l'*attestazione* a terzi sullo stato di integrità del sistema, realizzata in sostanza mediante meccanismi di firma digitale e generalmente anche di certificati digitali. Questa funzione ha alla propria radice una chiave detta *Endorsement Key*.

Queste funzionalità di base permettono poi di realizzarne altre, come meccanismi di autenticazione remota.

Un componente importante del Trusted Computing è il Trusted Protection Module (TPM), un modulo che sui personal computer viene realizzato principalmente mediante un processore dedicato, attualmente saldato sulla scheda madre ma in futuro probabilmente integrato nel processore (CPU) del computer. Il componente hardware è fondamentale per garantire l'inviolabilità del meccanismo anche da parte di chi abbia il pieno controllo fisico del sistema. In particolare, il TPM contiene l'endorsement key generata in fase di produzione del sistema, che identifica univocamente il sistema ed è alla base dei meccanismi di attestazione.

Il Trusted Computing distingue inoltre due diverse figure di utilizzatore:

- l'*owner (proprietario)* del sistema, che può controllare le modalità di utilizzo dei meccanismi di Trusted Computing (ma comunque non può manomettere i meccanismi);
- lo *user (utente)*, che comprende gli utilizzatori del computer, del sistema operativo e degli applicativi, ivi comprese le funzionalità privilegiate di gestione del sistema operativo; l'*utente* può utilizzare i meccanismi del TPM, ma non può controllarne la configurazione.

L'utilizzo principale del Trusted Computing, in termini di sicurezza, consiste nell'assicurare che dati "riservati", nel senso più ampio del termine, possano essere acceduti solo da determinate applicazioni, se sono integre e quando il sistema si trova in uno stato definito.

³ La definizione è necessariamente imprecisa, ma sufficientemente corretta per questo summary; maggiori dettagli si possono trovare in questo documento e sul sito <http://www.trustedcomputinggroup.org>

Questi limiti sono garantiti essenzialmente mediante cifratura dei dati e controllo da parte del TPM su chi può accedere alla chiave di decifratura. Alcuni possibili utilizzi sono:

- permettere a un'azienda di garantire che i suoi dati siano accessibili solo dai sistemi che ha autorizzato, con i programmi che ha autorizzato (e che non consentono la copia di quei dati); mediante il meccanismo dell'endorsement, è possibile garantire che anche sistemi di terzi, ad esempio quelli di consulenti, pur potendo accedere ai dati, non ne possano sottrarre o diffondere copie;
- un sistema di protezione (antivirus ecc.) che verifichi se i componenti del sistema sono stati sostituiti o modificati; i meccanismi di controllo di integrità, non manomissibili, permettono di verificare i componenti fondamentali del sistema operativo ed attraverso quelli il resto del sistema;
- un sistema di Digital Right Management che permetta di riprodurre il contenuto protetto solo mediante alcune applicazioni, autorizzate dal detentore dei diritti, che assicurano che la fruizione sia limitata secondo i termini della licenza.

Questi utilizzi si basano essenzialmente su due fattori:

- la presenza di un componente hardware non manomissibile, neppure dal *proprietario* del sistema;
- un meccanismo di attestazione che, grazie al meccanismo dei certificati, permette anche a terzi di avere informazioni affidabili sull'integrità del sistema.

Per valutare l'utilità del Trusted Computing, è necessario innanzitutto confrontarlo con le altre tecnologie di sicurezza già disponibili. I moderni processori dispongono già di meccanismi hardware a supporto di funzionalità di sicurezza, in grado di controllare i dati accessibili ai diversi processi; il principale di questi meccanismi è costituito dai cosiddetti livelli di privilegio: determinate operazioni sono eseguibili solo se si dispone di un livello di privilegio sufficientemente elevato. Con questi meccanismi sarebbe possibile implementare un sistema di attestazione analogo a quelli del Trusted Computing; tuttavia il loro reale utilizzo, al di là delle potenzialità più o meno teoriche, ha due limiti:

- chi controlla fisicamente il computer è comunque in grado di renderli inefficaci, ad esempio estraendo il disco rigido e modificandone direttamente il contenuto; non prevedono infatti controlli di integrità;
- la granularità con cui sono effettuati i controlli non è molto fine, ed è focalizzata più sui diritti degli utenti che su quelli dei singoli processi; la causa principale è la complessità che comporterebbero controlli più fini, che renderebbe il sistema assai poco flessibile.

Ciò che distingue effettivamente il Trusted Computing è il primo punto: chi ha il controllo fisico del computer, sia esso l'*utente*, il *proprietario* o altro, non essendo comunque in grado di estrarre le informazioni dal TPM non è in grado di manomettere il meccanismo.

Non vi sono motivi evidenti per cui il Trusted Computing non debba invece avere anch'esso gli stessi problemi di granularità degli altri meccanismi; per questo motivo, sembra improbabile che il Trusted Computing venga utilizzato per proteggere l'insieme delle funzionalità, dati e applicazioni del computer; è più probabile che venga utilizzato per alcune specifiche tipologie di dati ed applicazioni.

Va detto però che questi meccanismi possono garantire l'integrità dei componenti, ma non l'assenza di vulnerabilità: se la chiave per decifrare un documento è accessibile solo ad un'applicazione, e questa presenta delle vulnerabilità, i meccanismi del Trusted Computing

non garantiscono in generale che quella vulnerabilità non possa essere sfruttata per eseguire copie del documento.

Per valutare i rischi del Trusted Computing, è necessario inquadrare la tecnologia del contesto sociale e di mercato italiano e mondiale. I microprocessori per personal computer sono prodotti principalmente da AMD e Intel, mentre Microsoft ha una posizione fortemente dominante nel mercato dei sistemi operativi e dei prodotti per Office Automation. Queste tre compagnie sono nel Trusted Computing Group, insieme ad altri attori importanti del mercato dei PC: quando riterranno che il Trusted Computing debba essere utilizzato nei loro prodotti, esso diventerà parte della quasi totalità dei nuovi sistemi. Molti servizi si baseranno quindi sulla possibilità di utilizzare questa tecnologia, trascurando la parte marginale di mercato che non la supporta; la prassi di supportare solo le tecnologie più diffuse è del resto molto comune, almeno nell'informatica; oltretutto, in questo caso, non supportare il Trusted Computing potrebbe essere una scelta non conveniente per il fornitore del servizio, trattandosi di un meccanismo che gli permette un maggiore controllo sul rispetto di contratti e licenze. Sarà rapidamente esclusa di conseguenza la possibilità di non utilizzare il Trusted Computing, almeno per la maggior parte degli utenti, a meno di rinunciare a molti servizi. Avranno inoltre una considerevole rilevanza, anche in termini di sicurezza, i servizi di certificazione utilizzati per i meccanismi di attestazione. Infine, è da tenere conto che i personal computer dei cittadini saranno sempre più utilizzati per attività critiche come l'utilizzo di servizi di e-government, home banking e commercio elettronico, ma anche per la fruizione di prodotti audio/video (film, musica, tv...).

Si possono individuare i seguenti rischi legati alla diffusione e all'utilizzo del Trusted Computing:

1. condizionamento del mercato del software

- non è pubblicamente noto quali brevetti siano legati al Trusted Computing, né il Trusted Computing Group è in grado di garantire sull'utilizzo che potrà esserne fatto da parte dei detentori per influenzare il mercato o limitare la concorrenza;
- l'utilizzo di applicazioni certificate secondo criteri accettabili da parte dei produttori di contenuti, potrà rendere estremamente difficile lo sviluppo di prodotti se non per le aziende che hanno accordi specifici con i produttori di contenuti stessi, fino a rendere di fatto irrilevante l'utilizzo di formati standard aperti. Questo vale particolarmente per il mercato dei contenuti multimediali; i produttori di contenuti possono trovare più semplice e conveniente richiedere l'utilizzo di una specifica applicazione per l'accesso ai loro prodotti, eliminando di fatto la concorrenza per quell'applicazione, anche in assenza di accordi di cartello. La prassi di supportare un unico prodotto, anche senza alcuna malizia e senza alcun legame con il Trusted Computing, si può già vedere quotidianamente con i siti web che sono accessibili in modo completo solo con Internet Explorer (la maggior parte degli utenti non notano questo aspetto proprio perché Internet Explorer è il prodotto ampiamente dominante).

2. inefficacia sostanziale delle norme

Il mercato dell'informatica è particolarmente esposto a questo problema, per due motivi:

- si tratta di un mercato per sua natura globale, e quindi le norme nazionali, con l'esclusione forse di quelle degli Stati Uniti, rischiano di non essere applicabili se non escludendo il paese dal mercato;
- i lunghi tempi dei contenziosi non sono compatibili con quelli estremamente brevi del mercato: una condanna può facilmente arrivare con un ritardo tale da

non consentire di rimediare ai danni prodotti dall'illecito

Il Trusted Computing permette di imporre regole sull'utilizzo dei dati e dei sistemi garantite dalla tecnologia ed indipendenti dalle norme vigenti nei diversi paesi, che diventerebbero quindi nella pratica inefficaci. Anche in questo caso, il mercato dei contenuti multimediali è l'esempio più immediato: vincoli imposti tecnicamente dal produttore dei contenuti multimediali potrebbero essere resi efficaci dal Trusted Computing indipendentemente dalle norme in vigore nel paese di fruizione.

3. privacy

Si tratta di uno dei rischi più ampiamente discussi; i meccanismi di attestazione infatti prevedono la comunicazione di informazioni sullo stato del sistema attraverso canali sui quali l'utente ha un controllo limitato. Tuttavia per molti utenti, in particolare per l'utenza domestica, la stessa possibilità si ha già ora con un gran numero di protocolli, generalmente proprietari e cifrati, utilizzati ad esempio da sistemi operativi e applicazioni per scaricare eventuali aggiornamenti; se questa situazione può essere considerata accettabile, allora il maggior rischio introdotto dal Trusted Computing è limitato. È altresì vero che attraverso questi canali cifrati sarebbe più facile realizzare in modo diffuso meccanismi di analisi delle attività degli utenti, sia per quanto riguarda la navigazione Internet che sul proprio computer, ad esempio con la scusa di controlli di DRM sull'accesso ai contenuti dei siti.

Diversa è invece la situazione per gli utenti, le aziende e le Pubbliche Amministrazioni che per propria politica controllano questo tipo di comunicazioni. È possibile infatti che per usufruire di determinati servizi, come ad esempio l'accesso a informazioni protette da meccanismi di DRM, ma anche servizi di consulenza ed in outsourcing, siano costrette a consentire fra i propri sistemi e Internet comunicazioni cifrate e sostanzialmente incontrollate, che altrimenti sarebbero impedito.

4. censura

Il fatto di poter controllare i singoli utilizzi dei documenti fa sì che sia possibile "ritirare" completamente un documento, semplicemente non autorizzando più l'accesso. Ad esempio, un documento imbarazzante, indipendentemente dalla sua diffusione, può essere reso inaccessibile dall'autore semplicemente non autorizzando più nessun accesso. Meccanismi di questo tipo, che si appoggerebbero a strumenti di DRM basati sul Trusted Computing, potrebbero avere un impatto molto pesante sulla libertà di stampa, e forse anche sulla disponibilità di informazioni rilevanti per indagini e processi.

5. vulnerabilità dei sistemi

Come detto, una vulnerabilità di un'applicazione potrebbe consentire l'accesso a dati (ad esempio protetti da meccanismi di DRM) che altrimenti sarebbero protetti. Questo potrebbe portare utenti che desiderino accedere liberamente a quei dati a non aggiornare i propri sistemi in presenza di vulnerabilità, perché l'aggiornamento eliminerebbe la vulnerabilità stessa e ripristinerebbe quindi i controlli indesiderati. L'interesse dell'utente a vulnerabilità ed exploit per il proprio sistema potrebbe avere gli effetti più diversi, anche difficili da immaginare ma tutti inquietanti. Si noti che non necessariamente l'uso sarebbe illegittimo: dato il rischio di inefficacia sostanziale delle norme già citate, mantenere il proprio sistema vulnerabile potrebbe essere una condizione per far valere un diritto sancito da una norma.

Per contro, le aziende produttrici di contenuti potrebbero avere più interesse a forzare l'utente a mantenere aggiornato il proprio sistema, e l'effetto potrebbe quindi essere invece opposto.

6. abuso da parte di terzi

I rischi finora esaminati riguardano abusi da parte di chi legittimamente ha accesso ai meccanismi offerti dal Trusted Computing. Tuttavia, gli stessi meccanismi potrebbero essere

accessibili a terzi, ad esempio a causa di vulnerabilità delle infrastrutture di supporto al loro utilizzo, come i sistemi di certificazione, o dell'implementazione dei meccanismi stessi. I danni che potrebbero essere causati da questi abusi sono potenzialmente molto elevati, specialmente in considerazione del fatto che la vulnerabilità coinvolgere un componente fisico (il TPM) di difficile sostituzione.

Quelli finora descritti sono rischi associati al Trusted Computing: non sono assolutamente effetti certi. La probabilità che questi rischi si concretizzino realmente dipende da molti fattori, la cui analisi è al di fuori degli obiettivi di questo documento. Certamente, molto dipenderà da come i principali attori coinvolti (primi fra tutti le aziende membre del Trusted Computing Group) implementeranno e utilizzeranno i meccanismi offerti dal Trusted Computing. Qualora si ritenga di non avere una completa fiducia nel comportamento di queste aziende, è tuttavia necessario intervenire prima che la tecnologia si diffonda, per limitarne l'efficacia almeno per gli aspetti che comportano i rischi maggiori.

La possibilità di limitare l'utilizzo del Trusted Computing mediante normative nazionali o comunitarie si scontra sia con il rischio di inefficacia sostanziale, particolarmente elevato per questa tecnologia, sia con la difficoltà nel riconoscere un qualche tipo di irregolarità nei meccanismi che si potrebbero creare a discapito della pluralità nel mercato del software e dei prodotti multimediali. Per contro, soluzioni tecniche che limitino le funzionalità offerte dal Trusted Computing ne limiterebbero in parte anche gli utilizzi. Fra le soluzioni tecniche vale la pena di citare l'owner override, in cui il proprietario può attestare uno stato del sistema diverso da quello reale, riappropriandosi del controllo sulle informazioni che entità remote possono avere sul sistema, e sulla loro affidabilità. Un'altra possibilità è che le chiavi ed i dati riservati siano conservati su una smart card direttamente accessibile al TPM; questa soluzione permetterebbe di mantenere molte delle caratteristiche di protezione del sistema, con una maggiore elasticità in termini di utenti, chiavi e sistemi.

SEZIONE III

ALCUNI CONCETTI FONDAMENTALI

Per comprendere l'analisi contenuta in questo documento sono essenziali alcune nozioni di base sul concetto di rischio, sul Digital Right Management e sul concetto di "trust" (*fiducia*) che, nell'attuale contesto informatico, ha assunto un suo specifico significato da cui il termine "Trusted Computing" deriva. Se il lettore ha già chiari questi concetti può passare direttamente al capitolo successivo, anche se una rapida lettura di questo capitolo può comunque aiutare ad inquadrare correttamente alcune considerazioni esposte nel seguito.

Il rischio e le contromisure

Il concetto di **rischio** è centrale nell'attuale impostazione della gestione della sicurezza informatica.

La scelta di quali misure di sicurezza implementare è infatti legata, fra gli altri fattori, alla tipologia ed all'entità del rischio che si deve affrontare. I principi ed i concetti che seguono non sono specifici della sicurezza informatica, ma riguardano la sicurezza e il rischio in generale; applicarli a contesti con i quali si è più familiari (la sicurezza delle automobili, degli edifici, le assicurazioni) può aiutare a facilitarne la comprensione.

Esistono diverse definizioni di rischio, che derivano dal fatto che il termine è utilizzato in molti contesti. Ci atteniamo alla seguente: il **rischio** è dato dalla **probabilità** che un certo evento negativo si realizzi, moltiplicata per l'entità del danno (**impatto**) che questo evento può causare. Si noti che questa definizione differisce da un uso abbastanza comune del termine, che tiene conto solo della probabilità dell'evento (senza considerarne l'impatto). Secondo la definizione data invece, il rischio può essere alto anche se la probabilità dell'evento è bassa, purché l'impatto sia elevato. Viceversa, se un evento molto probabile ha un impatto limitato, porta comunque ad un rischio basso. Comunque sia, raramente si parla di eventi che certamente si verificheranno, mentre ci si pone il problema di eventi che magari non si verificheranno mai, come un terremoto in una certa area, un incendio, una rapina, ma per i quali l'eventualità che accadano non può essere esclusa a priori, e per i quali può essere quindi necessario predisporre delle **contromisure**.

Per capire i rischi ai quali è esposto un sistema informatico, bisogna quindi individuare questi eventi negativi, detti **minacce**, e capire quale impatto possono avere sul sistema. Le minacce sono legate a loro volta a due fattori: il primo sono le **vulnerabilità** del sistema, ovvero delle debolezze attraverso le quali il sistema può essere danneggiato. Il secondo sono i fattori che possono danneggiare il sistema attraverso le vulnerabilità; questi fattori possono essere degli attaccanti, ma anche dei fenomeni naturali (come un terremoto) o di altro tipo, come un incendio.

Per quanto riguarda gli impatti, possono essere di diversi tipi. Molti possono essere valutati economicamente, anche se non sempre questa valutazione è facile (ad esempio, il danno di immagine per una banca il cui sito web venga compromesso). Mentre alcune scuole tendono a valutare economicamente qualsiasi impatto, spesso in Italia si tendono a considerare non economicamente valutabili alcuni impatti, come la perdita di vite umane e alcuni rischi legali. Questa impostazione rende più complessa la gestione dei rischi, e di fatto vedremo che una valutazione economica nella pratica c'è sempre.

Dalla valutazione economica dell'impatto, tenendo conto della probabilità dell'evento, deriva poi una valutazione economica del rischio. Una volta stabiliti rischi e impatti, entrano in gioco le contromisure, ad esempio i **meccanismi di sicurezza**. Scopo delle contromisure è ridurre i rischi, o quando possibile eliminarli. Per ridurre i rischi si può operare in vari modi, sui diversi fattori. Nel caso della sicurezza informatica, ad esempio, gli aggiornamenti di sicurezza che vengono distribuiti per correggere problemi di sicurezza nei sistemi, servono ad eliminare delle vulnerabilità. Tuttavia, è possibile anche ridurre gli impatti, ad esempio facendo in modo che dallo sfruttamento di una vulnerabilità si arrivi a compromettere una parte limitata del sistema, possibilmente non molto critica. Infine, si possono ridurre le minacce, che è ad esempio uno degli effetti dell'attività preventiva e repressiva delle Forze dell'Ordine.

Tuttavia, i meccanismi di sicurezza hanno un **costo** e un'**efficacia**, ovvero una capacità, comunque limitata, di ridurre il rischio. Ci si può chiedere quindi, riguardo ad una contromisura, di quanto il rischio viene ridotto, ed a quale costo: è chiaro che se il costo supera la quantificazione economica del rischio, la contromisura non è conveniente. Anche quando lo è tuttavia, raramente elimina completamente il rischio. Cosa fare quindi del **rischio residuo**? Una possibilità è trovare un'altra contromisura che lo riduca ulteriormente, probabilmente senza eliminarlo del tutto. Si può allora intervenire con una terza contromisura, e così via. Quando ci si ferma? Ogni contromisura ha un costo; man mano che si aggiungono contromisure il costo complessivo aumenta (spesso anche quello della singola contromisura), e l'efficacia di ogni nuova contromisura è sempre più bassa. Alla fine, si arriva generalmente ad un punto in cui aggiungere una nuova contromisura ha un costo, non sempre quantificabile economicamente, troppo alto rispetto alla riduzione del rischio.

Un'ulteriore possibilità, almeno per alcuni tipi di rischio, consiste nel **trasferirlo** su qualcuno che sia disposto ad accettarlo; è il caso delle assicurazioni, con le quali, pagando un certo importo, ci garantiamo che un eventuale impatto, molto più alto, colpirà qualcun altro (la compagnia di assicurazione). Può anche essere però il caso di alcune clausole contrattuali in cui una parte si assume un rischio che altrimenti colpirebbe l'altra parte.

Per capire meglio questi concetti prendiamo un esempio che non riguarda i computer ma i freni di un'automobile. I freni si possono rompere (vulnerabilità), e quindi c'è il rischio che non siano funzionanti quando servono, il mezzo possa sbattere (minaccia) e gli occupanti possano ferirsi o morire (impatto). Per questo, le automobili hanno un freno d'emergenza, il freno a mano: se i freni normali non funzionano, il conducente può ricorrere al freno a mano. E se si rompe anche il freno a mano? Si potrebbe mettere un terzo freno; tuttavia, la sua efficacia sarebbe limitata: il conducente dovrebbe provare i freni, accorgersi che non funzionano, usare il freno a mano, accorgersi che anch'esso è rotto e passare al terzo freno; i casi in cui non andrebbe a sbattere prima di arrivare al terzo freno sarebbero pochi. Per questo ci si limita a due, accettando il rischio residuo. Naturalmente si potrebbe voler comunque mettere un terzo o un quarto freno, ma il costo non è ritenuto giustificabile a causa della poca efficacia. Si vede quindi che in qualche modo, una valutazione economica del rischio che gli occupanti perdano la vita viene comunque fatta, decidendo che non vale la pena di "sprecare" i soldi per un terzo freno (la valutazione è fatta informalmente in base al fatto che la nostra esistenza non è comunque priva di rischi, e che introdurre il terzo freno non modificherebbe significativamente i rischi complessivi della nostra esistenza). Viceversa, quando si tratta ad esempio delle pompe del carburante di un aereo, si può ritenere che una ridondanza di tre

abbia senso, sia perché c'è modo di sfruttarla (maggiore efficacia), sia perché l'impatto dell'incidente sarebbe molto alto (perdita di molte vite umane e danno di immagine per la compagnia aerea), e questo nonostante il costo sia molto maggiore di quello dei freni di un'automobile. Si vede quindi che l'opportunità di una contromisura non può essere vista se non in un contesto specifico in cui è applicata: anche nel caso della sicurezza informatica, non ha senso dire che un certo meccanismo "rende sicuro" un sistema, sia perché rimane sempre un rischio residuo, sia perché l'efficacia del meccanismo varia da contesto a contesto. Nel caso del TC, dobbiamo chiederci quindi se nel contesto specifico in cui verrà utilizzato, il suo costo è giustificato dalla riduzione del rischio che permette di ottenere, tenendo conto dei meccanismi già esistenti nei PC attuali. Dire semplicemente che il TC "rende più sicuro un sistema" non è di alcuna utilità.

I costi, come gli impatti, possono non essere valutabili economicamente, o almeno facili da valutare. Prendiamo come esempio il terrorismo internazionale. La minaccia esiste, l'impatto può essere elevato, quindi è ragionevole ritenere di dover predisporre delle contromisure per ridurre il rischio. Una possibile contromisura potrebbe essere un monitoraggio strettissimo di tutte le attività e comunicazioni dei cittadini, analizzando le relazioni e le anomalie. Una tale contromisura avrebbe certamente una qualche efficacia, ma con un rischio di abuso che comporterebbe un costo molto alto in termini di libertà personali. Queste libertà sono assai difficili da quantificare economicamente, e sono difficili da valutare secondo un qualsiasi metro che non sia soggettivo. In effetti, si avrebbe un rischio per la libertà dei cittadini, che è invece uno dei beni che si vogliono preservare. Si vede quindi che l'introduzione di una contromisura può non solo avere costi più alti dei rischi che si vogliono evitare, ma può addirittura introdurre dei nuovi rischi. Per questo, alcune contromisure non vengono prese. Viceversa, per ridurre un rischio elevato si può accettare l'introduzione di uno più limitato: è la valutazione che permette ad esempio di accettare le intercettazioni telefoniche come mezzo di indagine, purché regolamentate e sottoposte a controlli e autorizzazioni. Tuttavia, scegliendo una contromisura non è sufficiente valutarne la convenienza: questa convenienza deve essere prima confrontata con quella di altre contromisure disponibili, che possono avere la stessa efficacia ma ad un costo più contenuto. Specialmente se una contromisura introduce dei nuovi rischi, è bene chiedersi se sia veramente opportuno utilizzarla: data la generale difficoltà di una corretta valutazione dei rischi infatti, ci si potrebbe trovare in realtà ad aver peggiorato la situazione, anziché averla migliorata.

Infine, un meccanismo molto utile in un contesto può essere quasi inutile in un altro, perché l'impatto o la minaccia che affronta non sono considerati rilevanti (è "la risposta giusta al problema sbagliato"). Ad esempio, un meccanismo che garantisce la riservatezza delle informazioni può essere molto importante per un laboratorio di ricerca ma può essere del tutto inutile per proteggere delle informazioni pubbliche, che invece possono avere bisogno di essere protette dalla manomissione.

Il concetto di "Trust"

Nel campo della sicurezza informatica il concetto di "trust" (*fiducia*) assume alcuni significati specifici, coerenti con quello generale; quello da cui deriva il "Trusted Computing" è focalizzato su problematiche di integrità e di autenticazione, ed è quello che affrontiamo qui.

Il concetto ha assunto particolare rilevanza con la diffusione dei cosiddetti certificati digitali, utilizzati ad esempio nei meccanismi di firma digitale, compresi quelli legati alla firma con valore legale previsti dalla normativa italiana ed europea, o per l'accesso a servizi web "sicuri". A questo tipo di certificati faremo riferimento per spiegare il concetto di trust, che nel seguito indicheremo semplicemente come *fiducia*.

Per prima cosa è necessario spiegare, a grandi linee, cos'è la crittografia asimmetrica o a chiave pubblica⁴. Si tratta di strumenti per cifrare e firmare dati che si basano su coppie di chiavi⁵ legate matematicamente. Ogni coppia di chiavi ha infatti la caratteristica che un dato cifrato con una chiave della coppia può essere decifrato solo con l'altra chiave della coppia. In questo differisce dalla crittografia simmetrica alla quale ci hanno ad esempio abituati i film di spionaggio, in cui un messaggio viene cifrato usando una chiave segreta, e la stessa chiave segreta è necessaria per decifrarlo. La crittografia asimmetrica presenta numerosi vantaggi rispetto a quella simmetrica per molti utilizzi comuni.

In pratica, un soggetto (una persona, un sito web) genera tramite un computer una di queste coppie di chiavi; mantiene privata una delle due chiavi e rende pubblica l'altra⁶. Chi vuole mandargli dei dati riservati (cioè che solo il soggetto possa leggere) li cifra con la chiave pubblica; i dati potranno essere decifrati solo con l'altra chiave della coppia, quella che il soggetto ha mantenuto privata, e quindi solo il soggetto li potrà leggere. Lo stesso tipo di chiavi può essere usato per "firmare" un documento (il meccanismo alla base della firma digitale, che però comprende alcuni ulteriori passaggi che qui non sono rilevanti). Il soggetto infatti può cifrare i dati con la propria chiave privata e consegnarli a qualcun altro. Questi, usando la corrispondente chiave pubblica, può decifrarli⁷ e verificare che sono stati effettivamente cifrati con la chiave privata del soggetto (dato il legame fra le chiavi, se fossero stati cifrati con un'altra chiave, per decifrarli servirebbe la corrispondente chiave pubblica, e non quella del soggetto). Lo stesso meccanismo offre anche una garanzia contro la modifica del dato firmato: se il dato cifrato viene modificato, l'operazione di decifrazione non ha successo e la modifica viene scoperta. Il meccanismo della firma viene utilizzato per la distribuzione di software, ad esempio da Microsoft per gli aggiornamenti dei propri prodotti: Microsoft firma il file che contiene l'aggiornamento con una propria chiave privata (segreta ed estremamente critica); Windows verifica il pacchetto con la corrispondente chiave pubblica di Microsoft, assicurandosi così che il pacchetto sia stato effettivamente prodotto da Microsoft e che non sia stato manomesso durante l'invio. In questo modo i file possono essere distribuiti tramite siti pubblici, senza rischiare che la compromissione di questi siti permetta la distribuzione di aggiornamenti fasulli.

L'intero meccanismo si basa però su un presupposto fondamentale, e cioè che il destinatario del messaggio firmato, che quindi dovrà verificare la firma, sia effettivamente in possesso della chiave pubblica del mittente. Come fa quindi il destinatario ad essere sicuro di essere

⁴ Per maggiori informazioni su questo tema si può fare riferimento al quaderno CLUSIT "Aspetti di Crittografia Moderna: da DES alla Crittografia Quantistica"

⁵ Una chiave è un segreto utilizzato per cifrare o decifrare un dato; solo chi è in possesso della chiave è in grado di svolgere l'operazione.

⁶ Una caratteristica di queste coppie di chiavi è che, anche se le due chiavi sono legate l'una all'altra, conoscendone una non è possibile dedurre l'altra; rendere pubblica una chiave non influisce quindi sulla privacy dell'altra.

⁷ I dati quindi non sono riservati, dato che possono essere decifrati con la chiave pubblica che, per definizione, è accessibile a chiunque

entrato in possesso proprio della chiave pubblica del mittente, e non di una chiave falsa, che permetterà a qualcun altro di impersonare il mittente falsificandone la firma? Una prima possibilità è che il mittente consegni prima “a mano” la chiave pubblica al destinatario. Si tratta però di una soluzione poco pratica, almeno per la maggior parte dei casi. Si è pensato quindi di affidare la distribuzione delle chiavi pubbliche ad un’entità specializzata, l’Autorità di Certificazione (Certification Authority, CA). Compito della CA è verificare l’identità di un soggetto che si presenti con una chiave pubblica, ed emettere un **certificato** per quella chiave pubblica (anche qui il meccanismo sarebbe più complesso, ma per gli scopi di questo documento si tratta di una semplificazione accettabile). Il certificato consiste essenzialmente in un file contenente l’identità e la chiave pubblica del soggetto, firmato con la chiave privata della CA. Apponendo la propria firma, la CA certifica (di qui il nome) che quella chiave pubblica è associata a quell’identità. A questo punto entra in gioco la fiducia; l’intero meccanismo si basa infatti sul fatto che il destinatario del messaggio si fidi del fatto che la CA svolga correttamente il proprio compito di verifica dell’identità dei soggetti ed emissione dei certificati (la CA rientra infatti in una categoria di entità dette, nell’ambito della sicurezza informatica, Terze Parti Fidate, Trusted Third Party). Se la fiducia c’è, allora quando un soggetto riceve un messaggio firmato può:

- Recuperare⁸ il certificato emesso dalla CA che associa l’identità del mittente alla relativa chiave;
- Verificare l’origine e l’integrità del certificato utilizzando la chiave pubblica della CA (associata alla chiave privata utilizzata per firmare il certificato)
- Utilizzare la chiave pubblica così verificata per verificare l’origine e l’integrità del messaggio.

Per fare questo gli serve naturalmente di aver ottenuto in modo sicuro la chiave pubblica della CA. Sembra lo stesso problema di prima, e in effetti lo è, solo che una volta ottenuta per vie sicure (ad esempio di persona) la sola chiave pubblica di una CA, è poi possibile verificare senza difficoltà le chiavi pubbliche di un numero potenzialmente illimitato di soggetti per i quali la CA abbia emesso un certificato.

La base di tutto questo è quindi la fiducia che viene riposta nel fatto che la CA svolga correttamente il proprio compito, ed è questo il concetto di *fiducia* al quale ci riferiamo nel seguito. Se la CA, volutamente o per trascuratezza, emette certificazioni che associano chiavi a identità sbagliate, diventa possibile impersonare altri soggetti, leggere le comunicazioni riservate eccetera, e questo anche senza avere accesso alle chiavi private dei soggetti stessi. Inoltre, se la CA **si rifiuta** di emettere certificati per alcuni soggetti, questi non saranno in grado di comunicare, secondo questo modello, con chi “si fida” di quella CA: chi riceve i messaggi non sarà in grado di verificarne l’origine e li considererà potenzialmente falsi.

Quando la scelta di non emettere certificati sia motivata da altro che la mancata verifica dell’associazione fra identità e chiave, si ha in effetti una sorta di censura (che peraltro, a seconda del contesto di utilizzo, può avere motivazioni più che legittime, come ad esempio il fatto che il soggetto “censurato” non appartiene all’organizzazione all’interno della quale avvengono le comunicazioni). Si vede quindi l’estrema criticità della CA nell’intero meccanismo, e l’importanza della scelta in quali CA riporre la propria “fiducia”. Perché il

⁸ Il certificato, essendo firmato, non può essere manomesso, e quindi può essere distribuito dalla CA o dall’interessato via Internet, senza che il meccanismo perda di efficacia.

meccanismo sia utile inoltre, è necessario che in un contesto siano considerate fidate una o poche CA, alle quali molti fanno riferimento.⁹

Tuttavia, l'uso del termine *fiducia* non deve fuorviare: si tratta di un termine accattivante, ma non bisogna confondere il significato del termine con l'efficacia della tecnologia. Per comprendere i limiti di questi meccanismi è utile analizzare l'uso reale dei certificati e delle CA.

Come primo caso esaminiamo i meccanismi di distribuzione del software, utilizzati ad esempio da Microsoft (ma anche da tool come RPM di Linux). Il software viene firmato con la chiave privata del produttore. Chi lo deve installare verifica la firma, in modo da assicurarsi che si tratti di software originale e non manomesso. Tuttavia, se il software contiene delle vulnerabilità dovute ad errori nella creazione del software, questi errori saranno comunque presenti, la firma è solo una garanzia di origine, non di "sicurezza". In effetti, i casi in cui un sistema diviene vulnerabile in seguito ad una distribuzione manipolata sono attualmente una parte trascurabile rispetto a quelli in cui il sistema diviene vulnerabile per difetti nel software originale.

Tuttavia, per comprendere appieno la differenza fra fiducia e certificati, è utile soprattutto esaminare i cosiddetti "siti web sicuri", ovvero quelli che comportano l'icona di "lucchetto chiuso" sui browser. La comunicazione con questi siti prevede l'uso di un protocollo di comunicazione basato su certificati; lo scopo è garantire al browser di essere in contatto proprio con il sito web desiderato, certificando le chiavi utilizzate per cifrare e firmare le comunicazioni, ovvero associandole all'identità del sito web. In questo caso, è il browser che deve essere sicuro dell'identità della controparte (il sito web), e quindi è lui che dovrebbe scegliere la CA di cui fidarsi. È però il sito web che si fa certificare, ed è quindi in realtà lui a scegliere la CA. Il browser quindi (o meglio, l'utente che lo sta usando), più che fidarsi della CA decide, se di decisione si può parlare, di fidarsi della scelta della sua controparte. Tuttavia, nella pratica e nella maggior parte dei casi, chi utilizza un browser, ad esempio per accedere ad un sito di commercio elettronico, non solo non ha scelto alcuna CA, né deciso di fidarsi di chicchessia: generalmente non sa neppure che cosa sia una CA o un certificato. Come può quindi funzionare il meccanismo di fiducia? In realtà nel browser, ad esempio in Internet Explorer (il browser di gran lunga più utilizzato) sono già presenti i dati necessari per considerare affidabili alcune CA che hanno concluso un apposito accordo con Microsoft¹⁰: se il sito web utilizza certificati di CA che hanno sottoscritto questo accordo, il browser considera affidabile il sito senza bisogno di alcun intervento o decisione dell'utente. Per quanto riguarda il sito web, se vuole accedere al grande pubblico, ad esempio per attività di commercio elettronico, non ha scelta: se sceglie infatti una CA che non sia nell'elenco già installato in Internet Explorer, quando l'utente di conetterà al sito web otterrà un avviso che segnala l'incapacità del browser di verificare l'identità del sito stesso¹¹, e molti utenti sceglieranno, prudentemente, di rivolgersi ad altri; al sito web non resta quindi, se non vuole

⁹ Un'alternativa alle poche CA è la cosiddetta *cross-certification*, che però nella pratica ha trovato poco spazio per ragioni principalmente commerciali

¹⁰ Anche Firefox e gli altri browser principali fanno lo stesso, anche se la loro diffusione sul mercato è minima rispetto a Internet Explorer, vedi ad esempio <http://www.mozillazine.org/talkback.html?article=6485>

¹¹ Bisogna precisare che l'utente può riconfigurare il browser sia per escludere una CA dall'elenco che per aggiungerne di nuove, ma si tratta di un'operazione che l'utente spesso non è in grado di fare (la maggior parte degli utenti non ha nessuna idea del funzionamento del meccanismo), ed è una complicazione che pochi siti web sono pronti ad affrontare; lo richiedono ad esempio alcune banche per l'accesso ai servizi di home banking, avendo la possibilità di istruire preventivamente il cliente all'attivazione del servizio. Non è comunque un'opzione realistica per i grossi siti di commercio elettronico.

perdere clienti, che chiedere di essere certificato da una delle CA che hanno concluso l'accordo con Microsoft. Si vede quindi che non solo la "fiducia" dell'utente è irrilevante, ma anche quella del sito web è generalmente poco importante; quello che conta è il rapporto fra il produttore del browser e la CA. Questo rapporto può naturalmente comprendere anche una verifica sulla "serietà" della CA, come anche qualsiasi altro parametro che sia di interesse per due parti. In effetti, l'utente non sceglie di chi fidarsi: tutto quello che può scegliere è di utilizzare il servizio così com'è oppure di rinunciare.

Si vede quindi come la logica che apparentemente sottendeva al meccanismo non trovi riscontro nella pratica, e che la flessibilità che potenzialmente ci potrebbe essere nella tecnologia è stata di fatto eliminata da meccanismi di mercato (mercato che non è sottoposto a controlli o regolamentazioni specifiche). Va detto peraltro che attualmente non risultano¹² errori particolarmente clamorosi da parte di queste CA, almeno nel senso della certificazione di chiavi non corrette (salvo un caso di certificazione da parte di Verisign di una chiave falsa per la distribuzione di software Microsoft nel gennaio 2001¹³) e il meccanismo sembra nel complesso comunque funzionare: i principali problemi legati agli attacchi al web, compreso il phishing¹⁴, non sono legati alla creazione di certificati falsi.

A questo punto è opportuno evidenziare l'importanza dei criteri in base ai quali una CA decide di emettere o meno un certificato. La verifica dell'identità del richiedente è il requisito minimo, ma già qui si possono avere parecchie differenze. La verifica può essere più o meno approfondita: da una verifica sostanzialmente nulla (l'utente richiede il certificato e questo viene rilasciato), alla richiesta di un documento di identità, o di una visura camerale. Tuttavia, la CA può avere anche altri criteri, che dovrebbero in generale essere dichiarati nel cosiddetto Certificate Policy Statement (CPS). La CA potrebbe generare certificati solo per chi ha accettato di utilizzare i certificati secondo determinate politiche (ad esempio, usandoli solo per firmare software con determinate caratteristiche), o per chi non ha procedimenti penali in corso, o per chi è residente in un determinato paese, o ancora per chi accetta di operare secondo le normative di un paese o secondo un codice deontologico gradito alla CA stessa. Questi criteri potrebbero anche permettere alla CA di creare certificati falsi nell'ambito di indagini di polizia.

Nel caso dei siti Web, ad esempio, la valutazione coincide sostanzialmente con l'identificazione: chi ha richiesto il certificato è la stessa entità a cui è associato il dominio per il quale è stato richiesto il certificato. Questo ha come effetto un aumento della protezione delle comunicazioni fra browser e sito web, ma non ci dice nulla ad esempio sull'etica del sito al quale ci si connette: questi potrebbe tranquillamente fornirci dello spyware¹⁵ attraverso la connessione sicura, ed in effetti si tratta di evento non raro. Il meccanismo di *fiducia* tuttavia funzionerebbe ugualmente, dal punto di vista tecnico/formale, se la valutazione fosse basata sull'etica dell'entità, o sulla sua capacità economica, o sui partnership commerciali, o sulla sua adesione a politiche di qualsiasi genere. Il fatto è che il concetto di sicurezza è soggettivo di ogni singola organizzazione, mentre la valutazione dell'Autorità di Certificazione è, sperabilmente, basata oggettivamente su alcuni (pochi) criteri dichiarati, che possono anche essere in contrasto con le esigenze di sicurezza di un'organizzazione. Ad esempio, se un'Autorità di Certificazione rilasciasse certificati solo per il software che include

¹² Il fatto che non risultino non vuol dire che non possano esserci stati; nel campo della sicurezza infatti, c'è sempre una grande avversione a rivelare i propri errori, posto che vengano scoperti.

¹³ <http://www.microsoft.com/technet/security/bulletin/ms01-017.msp>

¹⁴ <http://en.wikipedia.org/wiki/Phishing>

¹⁵ <http://en.wikipedia.org/wiki/Spyware>

meccanismi per la “legal interception” (intercettazione legale) da parte del proprio governo, questo tipo di valutazione sarebbe in contrasto con le esigenze di sicurezza di qualsiasi organizzazione criminale, ma anche con quelle delle organizzazioni governative di tutti i paesi stranieri, che rischierebbero che le loro comunicazioni riservate siano intercettate dal governo del paese in cui opera la CA (questo esempio non è stato fatto a caso, come vedremo nel seguito).

Insomma, il fatto che un meccanismo di *fiducia* sia o meno un meccanismo di sicurezza, e in che misura, è di fatto nelle mani della CA e comunque varia come efficacia da utente a utente.

Il Digital Rights Management

È bene fornire qui qualche concetto relativo al Digital Rights Management, dato che molte delle critiche al TC riguardano l'utilizzo in questo ambito.

Il problema di garantire all'autore un equo compenso sulle copie di un'opera nasce sostanzialmente con l'invenzione della stampa. Fino ad allora, la produzione di copie dei testi era una lenta operazione manuale, e l'autore era remunerato, quando era remunerato, per l'opera originale, nella quale si concretizzava sostanzialmente la sua opera d'ingegno; al più era interessato a mantenere la paternità dell'opera in caso di copiatura, ma ad essere remunerato per le copie era normalmente il copiatore, che a volte era anche un vero e proprio artista, ad esempio della miniatura. Con la diffusione della stampa diventò sempre più frequente che chi guadagnava sulla diffusione delle copie, dopo averle stampate con relativamente poco sforzo, non fosse l'autore, che invece guadagnava poco o niente sulla produzione dell'originale. A partire dal diciottesimo secolo, la tutela del diritto d'autore assunse sostanzialmente le caratteristiche che ha conservato fino agli ultimi anni (per quanto queste caratteristiche presentino differenze fra un paese e l'altro). La tutela del diritto d'autore si è basata a lungo essenzialmente sul controllo delle copie fisiche dell'opera. Il primo serio colpo a questo meccanismo è venuto dalla radio: una sola copia fisica permetteva a molte persone non solo di sentire il brano ma, con la diffusione dei registratori, anche di farne facilmente delle ulteriori copie in modo incontrollato. I meccanismi di tutela del diritto d'autore sono andati definitivamente in crisi con la diffusione di Internet e di computer in grado di produrre e distribuire con facilità e in quantità illimitata copie di testi, musica, film e software. Per questo, da tempo sono in corso iniziative volte a contrastare la produzione e diffusione di copie non autorizzate e in generale per mantenere efficaci alcuni attuali meccanismi di mercato. L'attività si svolge a diversi livelli, ed è guidata principalmente dalle grosse case di produzione e distribuzione (case discografiche e cinematografiche, software house, network televisivi, case editrici). Il loro predominio sul mercato potrebbe infatti essere messo a rischio non solo dalla copia non autorizzata (possibilità che comunque è messa in dubbio da più parti) ma anche, e forse soprattutto, da alcune nuove forme di produzione e distribuzione dei materiali multimediali; ad esempio, la distribuzione diretta dell'opera da parte dell'autore, che potrebbe rendere inutili interi rami delle loro attività.

Garantire un pagamento per ogni copia prodotta di un'opera digitale è effettivamente una sfida considerevole dal punto di vista tecnologico, e questo a prescindere dalle modalità di produzione e distribuzione.

Oltre all'attività di lobbying, volta a far approvare norme di legge di contrasto alla pirateria particolarmente severe¹⁶, e ad una campagna che mira a formare nei cittadini un'etica fortemente contraria all'utilizzo di copie illecite, sono stati studiati alcuni strumenti tecnici

¹⁶ <http://www.interlex.it/copyright/urbani5.htm>

che hanno principalmente due scopi: impedire la produzione di copie non autorizzate e, secondariamente, rintracciare l'origine delle copie falsificate. Un esempio di meccanismo di questo tipo, particolarmente diffuso, è il Macrovision®, utilizzato già da tempo per la protezione delle videocassette VHS: se si cerca di registrare con un videoregistratore che implementa il Macrovision (ovvero quasi tutti) un segnale protetto con questo meccanismo, il segnale registrato è distorto in modo da essere in pratica inutilizzabile. È però con le tecnologie digitali e, come detto, con la diffusione di Internet e di PC sufficientemente potenti che il fenomeno della copiatura è esploso. Si cercano quindi di produrre meccanismi adatti ad operare in questo contesto. Se possibile, si vorrebbero nel contempo sfruttare le possibilità di Internet ad esempio in termini di distribuzione autorizzata e di modalità di pagamento, eliminando i costi della produzione e distribuzione dei supporti fisici. Digital Rights Management (Gestione dei Diritti Digitali, DRM) è quindi un termine che si riferisce in generale alla gestione ed il controllo sulle modalità di distribuzione e fruizione di un'opera digitale, comprese la copia, il numero di fruizioni, la diffusione. Si noti che nonostante il termine parli di *rights*, diritti, anche in questo caso non bisogna farsi fuorviare dall'uso dei termini, poiché non è assolutamente detto che questi strumenti gestiscano dei diritti; essendo strumenti, essi gestiscono delle restrizioni, e in effetti c'è chi parla di Digital Restrictions Management; che queste restrizioni corrispondano a quanto è legittimo dal punto di vista legale o etico non è ovvio, specialmente tenendo conto del fatto che, in un mercato globale, gli stessi strumenti vengono comunemente utilizzati in paesi con normative diverse.

Da un punto di vista pratico, le modalità di implementazione di meccanismi di DRM, almeno per quanto può interessare questo documento, si basano essenzialmente:

- sulla cifratura dei contenuti da proteggere;
- sul controllo della distribuzione e dell'utilizzo delle chiavi necessarie per decifrare i contenuti.

Mentre la prima parte è relativamente semplice, la seconda è estremamente difficile da ottenere nella pratica. Infatti, alla fine l'apparato che deve presentare il contenuto all'utente (ad esempio, un lettore di dvd da salotto) deve entrare in possesso della chiave; chiave e algoritmo di decifratura devono quindi essere disponibili in un apparato che è sostanzialmente sotto il controllo dell'utente. Se consideriamo un DVD ad esempio, la chiave di cifratura del film non può che trovarsi sul DVD stesso, seppure "cifrata" in modo che solo un apparato contenente i codici corretti (chiavi e/o algoritmi) la possa decifrare. Dato che però l'apparato è in possesso dell'utente, e ogni produttore di lettori di dvd da salotto deve inserire quegli stessi codici in ogni apparato che produce, di fatto i codici finiscono per non essere segreti. Per vedere (a grandi linee e con molte approssimazioni¹⁷) un meccanismo più sofisticato, possiamo considerare le trasmissioni tv satellitari cifrate. In questo caso, il segnale satellitare di un canale televisivo è unico, cifrato in un modo unico per tutti gli utenti, in base a una chiave che però cambia periodicamente. Ogni utente dispone di una smart card che inserisce nel proprio apparecchio televisivo. Le informazioni necessarie per decifrare il segnale vengono trasmesse periodicamente, ma sono protette in modo da essere recuperate solo grazie alle informazioni presenti in una smart card, che fornisce man mano al ricevitore il flusso di bit necessario per decifrare il segnale. Leggendo le informazioni fra la smart card e il ricevitore (non consideriamo qui attacchi ai meccanismi crittografici utilizzati), è possibile ottenere quindi un'informazione utile per decifrare i dati ricevuti "al momento". Si tratta evidentemente di un meccanismo che sfrutta il fatto che l'interesse è per decifrare le

¹⁷ Per vedere più nel dettaglio il funzionamento di un sistema di questo tipo, si può vedere <http://en.wikipedia.org/wiki/VideoCrypt> e <http://www.cl.cam.ac.uk/~mgk25/tv-crypt/details.txt>

trasmissioni satellitari “sul momento”, più che impedirne la registrazione o la copiatura, e che non è adatto a proteggere invece dvd o documenti.

Inoltre, il segnale in chiaro viene inviato dall'apparato al televisore, o all'amplificatore per quanto riguarda la musica, e quindi, se proprio non si riesce ad accedere al segnale digitale gestito dall'apparato, è possibile accedere in questa fase al segnale analogico, registrando comunque i contenuti in chiaro, seppure con una qualità minore. Si parla in questo caso del cosiddetto “buco analogico”¹⁸ nei meccanismi di DRM. Chiudere il buco analogico richiederebbe di avere una trasmissione cifrata fino all'interno della televisione o del monitor, cosa che peraltro viene effettivamente considerata¹⁹. È chiaro che sarebbe comunque possibile registrare “dall'ambiente” le informazioni (fotografare il monitor, filmare la televisione, registrare l'audio dalle casse), ma la perdita di qualità è comunemente considerata in questi casi un deterrente sufficiente da rendere questa minaccia “sopportabile” almeno per molte aziende interessate al DRM.

Un'ultima considerazione riguarda una difficoltà fondamentale del DRM: in generale, basta che anche una sola copia del prodotto sfugga ai meccanismi di controllo, per rendere possibile la produzione di un numero potenzialmente illimitato di copie non autorizzate, vanificando ogni sforzo.

¹⁸ http://en.wikipedia.org/wiki/Analog_hole

¹⁹ <http://punto-informatico.it/p.aspx?id=1580540>

SEZIONE IV

IL TRUSTED COMPUTING

Cos'è il Trusted Computing

Quanto segue è una descrizione semplificata e sommaria dell'architettura, necessaria per comprendere questo documento ma che può presentare alcune imprecisioni, non rilevanti comunque in questo contesto. Per una comprensione completa della tecnologia è opportuno fare riferimento ad esempio al documento "TCG PC Specific Implementation Specification vers. 1.1"²⁰ ed eventualmente all'ulteriore documentazione disponibile sul sito del Trusted Computing Group.

Il TC è una tecnologia che mediante strumenti hardware, software e protocolli di comunicazione, vuole garantire che diversi componenti di un sistema (ad esempio un PC) siano in uno stato corretto e autorizzato. Per ottenere questo risultato, il TC si basa sulla possibilità di poter verificare alcune caratteristiche del sistema; in particolare:

- se i componenti presenti sono *fidati*, ovvero se sono fra quelli ritenuti adatti a svolgere il compito desiderato;
- se i componenti del sistema sono stati modificati o comunque non sono nello stato ritenuto opportuno per svolgere quel compito;
- punto importante, si vuole poter riferire in modo autentificato anche a componenti esterni al sistema sullo stato del sistema stesso.

Per esempio, supponiamo che in un'azienda un dipendente voglia accedere a dei dati riservati; prima di concedergli l'accesso a quei dati, l'azienda può voler verificare che il programma con cui l'utente visualizzerà quei dati sia quello autorizzato dall'azienda, che non ci siano altri programmi attivi che potrebbero ad esempio leggere i dati per inviarli a terzi, e che il programma autorizzato non sia stato manomesso. Già da questo esempio si capisce un concetto fondamentale per il TC, e cioè la differenza fra **owner** (*proprietario*) del PC e **user** (*utente*) del PC o della risorsa. Nella logica del TC è il *proprietario*, e non l'*utente*, che stabilisce quali sono gli usi consentiti della risorsa, e una parte del PC, ovvero la **Trusted Computing Platform, TCP**, è lo strumento attraverso il quale il *proprietario* verifica che l'*utente* non sia in grado di sfuggire a questo controllo. L'esempio fatto è abbastanza semplice: il *proprietario* del PC è l'azienda, l'*utente* è il dipendente. Per gestire questo semplice caso (che pure nella realtà è ben lontano dall'essere gestito facilmente) non servirebbero, in teoria, meccanismi molto complessi. Più difficile è il caso in cui ad accedere ai dati è un dipendente di una società esterna di consulenza, che utilizza un PC portatile fornito dalla propria azienda: in questo caso, il proprietario dei dati è uno, il *proprietario* del PC è un altro (la società di consulenza), l'*utente* non coincide con nessuno dei due (sarà il dipendente della società di consulenza) e il proprietario dei dati non si fida necessariamente della gestione della sicurezza da parte del *proprietario* del PC. È per gestire questi casi complessi che sono principalmente necessari i meccanismi di *fiducia* già descritti in una sezione precedente di questo documento. Un altro caso di non facile gestione è quello del PC domestico dal quale si vuole ad esempio vedere un film scaricato via Internet: nella logica del TC, la cosa potrebbe essere modellata con il *proprietario* del PC che coincide con l'*utente*, e

²⁰ https://www.trustedcomputinggroup.org/groups/pc_client/TCG_PCspecificSpecification_v1_1.pdf

il distributore del film come proprietario dei dati. In pratica, come vedremo, un punto importante di questi meccanismi è che dovrebbero permettere un controllo sullo stato del sistema a chi non ne ha il controllo fisico.

Per ottenere questo risultato devono essere disponibili nella TCP almeno tre funzionalità:

- un'area di memoria protetta, nella quale possano essere memorizzate ad esempio le chiavi di cifratura necessarie per le attività della TCP (come vedremo, il TC si appoggia a meccanismi di firma);
- un meccanismo che possa fare delle "misure di integrità" sul sistema (ad esempio verificare che il player video autorizzato non sia stato modificato);
- un meccanismo per comunicare i risultati di queste misure al *proprietario* o comunque ai meccanismi interessati; è tuttavia previsto che l'interazione da remoto non si limiti passivamente alla ricezione di rapporti sullo stato del sistema, ma possa anche intervenire sullo stato del sistema stesso.

Per ottenere questo risultato, i meccanismi devono essere profondamente integrati nell'hardware del sistema (processore, chipset della scheda madre ecc.), mediante un componente detto **Trusted Platform Module** (TPM) che contiene la memoria protetta e le funzionalità protette necessarie per i controlli di integrità. In effetti, in [2] (sezione 4.3.3) si dice esplicitamente che il TPM deve essere protetto fisicamente dalla manomissione, e che devono essere adottate misure che permettano di rilevare all'ispezione fisica l'eventuale manomissione. Per capire la necessità di un'integrazione con l'hardware consideriamo il seguente esempio.

Supponiamo che un utente acquisti la possibilità di vedere una e una sola volta un film scaricato via Internet. Si può ipotizzare ad esempio che il file venga fornito all'utente in forma cifrata, che il programma player abilitato si connetta quindi al sito Internet, scarichi la chiave per decifrare il file, la utilizzi per mostrare un'unica volta il film e poi la cancelli. Il problema è che per poter visualizzare il film, il player deve contenere il codice per decifrare il film, e deve entrare in possesso della chiave, seppure per poco tempo. Trattandosi di software, è possibile modificarlo, oppure studiarlo, analizzare il sistema di decifratura e scrivere un altro programma analogo che scarichi la chiave ma, una volta riprodotto il film, salvi il file in chiaro eliminando ogni protezione, o ancora salvi la chiave in modo che questa possa essere riutilizzata per vedere nuovamente il film. Senza entrare ulteriormente nel dettaglio, per impedire che tutto ciò avvenga sarebbe necessario che il sistema operativo impedisca l'esecuzione di questo codice modificato, permettendo solo l'esecuzione di player che sono stati verificati (e certificati) come *fidati*, ovvero che rispettano i vincoli di utilizzo del film imposti dal distributore. Tuttavia, lo stesso sistema operativo è software e può essere modificato o sostituito; ad esempio, l'utente potrebbe utilizzare un sistema operativo che non si appoggia a meccanismi di *fiducia*, o potrebbe aggiungere dei certificati che gli permettono di accettare i player modificati. Per rendere inefficace tutto questo, l'unico sistema è agire ad un livello ancora più basso del sistema operativo, ovvero a livello dell'hardware: componenti hardware che verificano che il codice eseguito, sistema operativo compreso, sia *fidato*. Tuttavia, ancora non basta: il film verrebbe comunque trasmesso in chiaro alla scheda video, e da qui al monitor; per evitare che il film possa essere salvato in questa fase, anche la scheda video e le comunicazioni fra scheda e processore devono utilizzare componenti *fidati*. Si garantisce insomma che tutti i componenti hardware e software che possono trattare il film non cifrato siano fra quelli *fidati*, escludendo quelli che potrebbero copiare il film o permetterne la visione, nel nostro caso, più del numero di volte previsto. In effetti, specifiche che vanno nella direzione della compatibilità con il TC sono state recentemente proposte, ad

esempio, per il PCI Express, lo standard recente per la comunicazione fra processore e periferiche veloci come appunto la scheda video^{21 22}.

Vediamo ora, molto a grandi linee, con quali meccanismi il TPM riesce a svolgere il proprio compito, e come entrano in gioco i meccanismi di *fiducia*. Un componente di cui è facile comprendere l'utilizzo è lo spazio di memorizzazione protetto: è un'area di memoria utilizzata dal TPM per memorizzare i dati necessari per il proprio funzionamento, ad esempio alcuni tipi di chiave; deve essere protetto perché la manomissione di questi dati permetterebbe di aggirare completamente le funzionalità del TPM. I meccanismi di "misura di integrità" possiamo immaginarli, con un caso certamente semplificato ma realistico, come dei meccanismi che ad esempio verificano mediante checksum crittografiche²³ (una sorta di "impronta digitale" matematica di un file) il codice di un programma e confrontano il risultato con quello previsto per il programma stesso: se la verifica ha successo, il programma può ad esempio accedere a dati riservati (ad esempio, alla chiave con cui un file è stato cifrati); in caso contrario l'accesso sarà negato, e questo indipendentemente dai controlli di accesso implementati o meno dal sistema operativo. Infine, il risultato della verifica potrebbe essere comunicato via rete al *proprietario*, che potrà quindi rilevare se il sistema si trova nello stato previsto o se invece l'utente ha provato a manipolare il programma.

Ci si pongono a questo punto due problemi: come fa il TPM a sapere qual è il codice corretto e originale di un programma? Una soluzione è quella di utilizzare gli stessi meccanismi già descritti per la distribuzione degli aggiornamenti software: il software viene firmato, in modo che eventuali manomissioni possano essere rilevate perché la verifica della firma fallisce.

Il secondo problema è più complesso: come fa il *proprietario* a sapere che i rapporti che gli vengono inviati sono stati effettivamente generati dal PC? È chiaro che questi rapporti devono essere in qualche modo firmati dal PC, e che la chiave utilizzata per firmarli non deve essere accessibile ad altri che al TPM. Si potrebbe pensare quindi che il *proprietario* possa caricare una propria chiave nel TPM, ma questo può funzionare nel caso di un'azienda proprietaria di dati e PC; che fare ad esempio quando a fidarsi della verifica deve essere il proprietario di un film, che non ha controllo sul PC? Non può fidarsi di una chiave gestita dal *proprietario* del PC, perché questi potrebbe a quel punto comunicare quello che vuole, ad esempio che il software è *fidato* quando non lo è, allo scopo di poter creare delle copie del film. Alla base del meccanismo, che prevede l'utilizzo di diverse chiavi, c'è quindi una **Endorsement Key (EK)**, una coppia di chiavi asimmetriche che viene generata nella fase stessa di produzione del TPM ([2] sez. 4.2.5.4.1) e poi viene univocamente legata all'hardware, ad esempio in fase di assemblaggio della scheda madre. L'associazione fra Endorsement Key e hardware viene creata dal produttore dell'hardware mediante certificati digitali, certificando la chiave pubblica dell'EK. Associate a questo tipo di certificazione sono anche le **Conformance Credentials** (credenziali di conformità), con cui una CA, ritenuta *fidata* da chi le dovrà utilizzare, certifica che un certo tipo di hardware (ad esempio un modello di scheda madre) è conforme ai requisiti. Si noti anche che nell'ambito delle specifiche del TCG viene dato spazio alla certificazione secondo i Common Criteria²⁴. Altre chiavi vengono generate per

²¹ Trusted Configuration Space for PCI Express, PCI-SIG Engineering Change Notice, March 2005, http://www.pcisig.com/specifications/pciexpress/specifications/ECN_Trusted_Configuration_Space_1jul2005.pdf

²² Si è discusso molto dei costi che protezioni di questo tipo possono comportare per i produttori di schede video, e quindi indirettamente per gli utenti. Si può vedere http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html

²³ <http://it.wikipedia.org/wiki/Hash>

²⁴ I Common Criteria sono uno standard di certificazione di sicurezza di sistemi e prodotti informatici, http://en.wikipedia.org/wiki/Common_Criteria

diversi motivi internamente al TPM, ma alla base delle verifiche sull'origine e l'autenticità di queste chiavi c'è sempre l'EK, di cui si capisce quindi la criticità. Alcune delle chiavi necessarie per il corretto funzionamento dei meccanismi sono **non migratable** (*non migrabili*) nel senso che nascono su un PC e non possono essere trasferite su un altro. Esistono invece chiavi dette **migratable** (*migrabili*), che possono essere trasferite su altri sistemi: sono ad esempio chiavi generate per la cifratura di dati che può essere necessario leggere altrove, come quelle utilizzate per generare backup cifrati.

Per completare la panoramica del sistema bisogna a questo punto chiedersi quanto controllo abbia il *proprietario* del PC sul TPM. Esiste un comando, TPM_TakeOwnership, con il quale il *proprietario* prende inizialmente il controllo del sistema definendo il "segreto" (una chiave) con il quale si presenterà al sistema. Lo stato di *proprietario* permette all'amministratore di eseguire tutti i comandi previsti dal TPM, compreso generare una nuova EK internamente al TPM (si noti che questa nuova chiave non sarà stata certificata dal produttore, né sarà associabile alle Conformance Credentials originali), tuttavia non gli consente di manomettere il funzionamento del TPM stesso; in particolare, non gli permette di accedere alla chiave privata dell'EK o delle altre chiavi *non migrabili*, né di decidere quale chiave verrà generata dal TPM. L'associazione fra EK e PC rimane quindi univoca, e quindi lo è anche quella fra PC e dati prodotti dal TPM, utilizzati poi per comunicare le misure sull'integrità del sistema (questa operazione è detta *attestation*).

Infine, è utile segnalare anche il Trusted Network Connect, un protocollo che permette ad esempio di verificare remotamente caratteristiche di identità di un utente e integrità di una piattaforma appoggiandosi ai meccanismi offerti dal TPM (quindi *fidati*), utilizzabile anche per meccanismi di controllo dell'accesso alla rete (appoggiandosi a protocolli come 802.1x).

Possiamo quindi descrivere a grandi linee come può svolgersi l'avvio e l'utilizzo di un PC con il supporto per il TC attivo.

All'accensione, il TPM si attiva prima del caricamento del BIOS, e utilizzando una porzione di codice immutabile presente anch'esso sulla scheda madre, il "Core Root of Trust for Measurement". Si tratta almeno del Bios Boot Block (è così possibile aggiornare il resto del BIOS con i meccanismi abitualmente utilizzati a questo scopo, senza interferire con l'integrità dei meccanismi del TC). Questo codice verifica l'integrità del rimanente codice del BIOS prima di eseguirlo (da qui in poi, con verifica di integrità del codice si intende sostanzialmente la verifica di una firma del codice; se una delle verifiche fallisce, il codice non viene eseguito oppure il PC passa a uno stato "*non fidato*"). Il BIOS a sua volta verifica l'integrità del boot loader, che verifica l'integrità del kernel del sistema operativo prima di eseguirlo. Quest'ultimo verifica l'integrità di ogni componente, driver o applicazione di terza parte prima di eseguirla. Tutte queste verifiche vengono fatte appoggiandosi al TPM, che implementa appunto le funzioni necessarie. L'integrità di questa "catena di fiducia" (chain of trust) garantisce che alla fine del processo, il PC si trovi in uno stato *fidato* e con il sistema operativo attivo. Supponiamo adesso che l'utente voglia acquistare la visione di un film su Internet. L'utente si connette al sito del fornitore di contenuti, che richiede al PC di autenticarsi e dichiarare la propria integrità, usando la remote attestation, secondo un tipico meccanismo di autenticazione a chiave pubblica. La chiave privata utilizzata per l'autenticazione e la remote attestation si trova all'interno del TPM (dal quale non esce): il sistema operativo fornirà al TPM i dati che questi firmerà al proprio interno. Avvenuta con successo l'autenticazione e l'attestazione di integrità del sistema, il sito remoto potrà ad esempio fornire al PC il film insieme ai vincoli di DRM, il tutto cifrato con una chiave simmetrica, a sua volta cifrata con la chiave pubblica del TPM. Il sistema operativo riceve film e chiave cifrata, e passa quest'ultima al TPM. Dato che il sistema è in uno stato *fidato*, il

TPM decifra la chiave simmetrica e la fornisce al sistema operativo (anche in questo passaggio, nessuna chiave del TPM viene fatta uscire dal TPM stesso, e non può quindi essere intercettata sul bus). Il sistema operativo la passa a un media player *fidato*, che nel rispetto delle indicazioni di DRM riproduce il film una volta e poi lo cancella. I dati vengono inviati alla scheda video, eventualmente anch'essi cifrati sul bus, e nel caso più estremo sono cifrati anche quelli dalla scheda video al monitor, *fidato* anch'esso, che quindi deve comprendere anche l'hardware necessario per autenticarsi e decifrare le immagini prima di riprodurle. Si vede quindi come i dati vengono protetti dal sito Internet fino alla riproduzione sul monitor.

Quali sono gli obiettivi del Trusted Computing?

Quali sono quindi gli obiettivi del TC? E bene chiarire subito che il TCG non presenta il TC come un meccanismo di DRM; in effetti, l'identificazione fra TC e DRM è alla base di molte posizioni "anti TC". Il TC è invece una tecnologia che implementa principi di *fiducia* a partire dai componenti hardware. È l'uso che di questi meccanismi verrà fatto che stabilisce l'effetto che il TC avrà sui sistemi: un aumento della sicurezza, l'implementazione di meccanismi robusti di DRM o addirittura una diminuzione della sicurezza. Per quanto l'obiettivo dichiarato dal TCG sia l'aumento della sicurezza e non specificamente la realizzazione di meccanismi di DRM, di fatto saranno i produttori di software e hardware TC-compliant a stabilire quali usi ne saranno fatti, secondo le proprie priorità, le proprie politiche commerciali e i vincoli che saranno loro eventualmente imposti²⁵. Come abbiamo visto nel caso delle CA e dei certificati per i siti web, non bisogna infatti confondere le potenzialità delle tecnologie con quelli che sono gli utilizzi che ne verranno fatti. Questi utilizzi sono generalmente un sottoinsieme limitato delle potenzialità, del quale il mercato e gli interessi dei principali attori determinano il successo (questi interessi possono coincidere in alcuni casi con quelli degli utenti).

Come esempi di utilizzo, sono comunemente presentati l'amministrazione remota dei sistemi all'interno di un'organizzazione e le prove di identità e integrità nell'accesso a siti di home banking o commercio elettronico.

Quale sicurezza fornisce?

Per valutare la sicurezza offerta dal TC, è necessario individuare:

- quali meccanismi offre: come visto, una tecnologia non offre "sicurezza", ma meccanismi che in uno specifico contesto permettono eventualmente di soddisfare i requisiti di sicurezza;
- quali sono le differenze rispetto ai meccanismi ed alle tecnologie già disponibili;
- le minacce che le novità introdotte dal TC sono in grado di contrastare;
- i costi introdotti, anche in termini di rischi; questo ultimo aspetto, data la natura di questo documento, sarà trattato a parte.

Come abbiamo visto, il TC offre dei meccanismi che permettono di garantire la presenza di determinati componenti hardware/software, la loro integrità, di comunicare questo stato ad altri componenti o all'esterno del sistema e quindi, nel complesso, di prendere delle decisioni sull'accesso a risorse in funzione dei risultati di queste verifiche sullo stato del sistema. Un aspetto importante è che le caratteristiche hardware/software del TPM e del suo collocamento nel sistema garantiscono che il meccanismo non possa essere aggirato né manomesso neppure

²⁵ <http://punto-informatico.it/p.asp?i=57362>

da chi controlla fisicamente il sistema, e che solo il *proprietario* possa gestirne lo stato (ma comunque non manometterlo).

Se esaminiamo l'architettura di un PC attuale (senza TC) vediamo che, contrariamente a quanto spesso si crede, in realtà esistono già meccanismi hardware all'interno del processore²⁶ che hanno lo scopo di proteggere alcune funzionalità del sistema critiche per la sicurezza. Ad esempio, da circa vent'anni i processori utilizzati nei PC implementano **livelli di privilegio o ring**: alcune attività critiche per la sicurezza e la robustezza del sistema, come la gestione della memoria, possono essere effettuate solo al cosiddetto ring 0, ovvero nella modalità di protezione più elevata, accessibile solo ad alcuni componenti essenziali e fidati (in senso generale) del sistema operativo. In modo analogo sono gestite le segnalazioni che permettono ad esempio l'interazione con i dispositivi hardware. Per contro, processi degli utenti (ad esempio le applicazioni) sono eseguite al livello meno privilegiato, il ring 3, e non sono quindi in grado di manomettere quanto viene gestito al ring 0²⁷. La modalità privilegiata non va confusa con i diritti di Amministratore del sistema: le attività dell'amministratore sono comunque eseguite in modalità non privilegiata. Semplificando la distinzione, l'amministratore non può comunque aggirare i meccanismi di controllo degli accessi imposti dal sistema operativo; tuttavia, questi sono configurati per concedergli poi di operare su qualsiasi file o risorsa; con una diversa configurazione, potrebbero impedire l'accesso anche all'amministratore²⁸. Il sistema operativo ha almeno un componente, il kernel, che viene eseguito a livello privilegiato²⁹. Questo componente è in grado effettivamente di controllare l'accesso dei processi alle risorse, e potrebbe implementare le funzionalità previste da una TPM, ovvero la memoria protetta e i meccanismi di misura e comunicazione sull'integrità del sistema, in modo protetto dall'azione degli altri processi³⁰.

Quello che principalmente distingue le potenzialità del TC da un'implementazione delle stesse funzionalità basata su questo meccanismo già esistente è la resistenza del TC alla manomissione fisica, anche da parte del *proprietario*³¹. Una seconda differenza non trascurabile è che gli attuali sistemi operativi eseguono in realtà una quantità considerevole di codice al ring 0, e difetti e vulnerabilità in questo codice, che oltretutto deve essere occasionalmente aggiornato, permetterebbero di aggirare le protezioni. Viceversa, le

²⁶ Si tratta in realtà di meccanismi hardware/firmware, come del resto è anche il TPM. Il concetto fondamentale è che la loro manomissione richiederebbe comunque una manomissione dell'hardware, o la complicità di componenti considerati fidati e quindi eseguiti in modalità privilegiata
http://en.wikipedia.org/wiki/Protection_ring

²⁷ Per quanto riguarda questo documento, è sufficiente considerare i ring 0 e 3, che sono quelli effettivamente utilizzati all'interno dei PC.

²⁸ Da tempo i processori Intel della famiglia x86 sono utilizzati per sistemi valutati ai livelli più elevati di sicurezza, e questo anche in seguito ad analisi che ne hanno evidenziato i limiti, vedi ad esempio "An Analysis of the Intel 80x86 Security Architecture and Implementations", IEEE Transactions on Software Engineering, SE-22, 4, May 1996.

²⁹ I livelli di privilegio 1 e 2 non sono attualmente utilizzati.

³⁰ Se esaminiamo l'attuale architettura PC e soprattutto l'uso che ne viene fatto, si vede che in realtà un altro punto debole è il fatto che l'intero sistema operativo, compreso il kernel, si trova sull'hard disk, dove può essere modificato facilmente dall'Amministratore del sistema. Si tratta comunque di limiti dell'utilizzo attuale, non del meccanismo in sé.

³¹ Il modello delle minacce del TC comprende quindi anche fra le minacce chi controlla fisicamente il sistema, ritenendo invece fidate delle entità remote.

funzionalità offerte dal TMP non sono aggirabili da difetti del sistema operativo, anche se, come vedremo, difetti nel sistema operativo ne possono ridurre notevolmente l'efficacia.

La prima riflessione necessaria è che però i sistemi attuali non sono vulnerabili alla sola manomissione fisica, ed anzi sono vulnerabili a molti problemi che non dipendono da funzionalità del kernel e che potrebbero essere contrastati efficacemente dall'attuale modello di processore con livelli di privilegio il quale, oltre a poter implementare le funzionalità del TPM al ring 0, potrebbe implementare un insieme molto più ampio di controlli³². Infatti, se le chiavi fossero in un'area di memoria accessibile solo al kernel del sistema³³, esse non sarebbero accessibili all'utente ed ai suoi processi se non manomettendo il sistema, ad esempio accedendo fisicamente al disco, o naturalmente avviando un diverso sistema operativo, privo di protezioni. È quindi necessario a questo punto chiedersi come mai, se le queste e altre funzionalità potrebbero essere realizzate appoggiandosi ai meccanismi di privilegio, questa potenzialità dei processori non sia stata sfruttata a fondo, fino al punto da generare la convinzione diffusa che le protezioni di un sistema siano solo software. Bisogna infatti capire se le stesse difficoltà potrebbero presentarsi per un'efficace applicazione delle potenzialità del TC. Si tratta ancora una volta della differenza fra le potenzialità di un modello e i limiti della sua applicazione pratica.

È convinzione diffusa che il motivo principale per cui le potenzialità di protezione degli attuali processori non è stata sfruttata appieno sia un problema di complessità e, per alcuni aspetti limitati (come la quantità di codice che viene eseguita con privilegi elevati), anche di prestazioni³⁴. Una tipica installazione di un PC comprende infatti qualche decina di migliaia di file; un controllo granulare su quali programmi possono accedere a quali file e in quali condizioni sarebbe estremamente complesso, non solo in fase di installazione, ma soprattutto durante le modifiche al sistema (installazione di nuove applicazioni, aggiornamenti, creazione di nuovi file, compresi programmi). Il problema diventa facilmente ingestibile se si tiene conto delle diverse esigenze dei diversi utenti e contesti e della varietà di applicazioni che possono essere installate su un PC. Al contrario, attualmente la granularità del controllo si limita sostanzialmente all'utente: se un utente ha accesso ad un file, allora tutti i suoi processi possono accedere a quel file³⁵. Altri problemi si presenterebbero con il controllo della condivisione di file fra applicazioni o fra utenti (ad esempio, l'invio di file per posta elettronica). In effetti lo sviluppo dei sistemi e delle applicazioni è andato verso un aumento della complessità e delle funzionalità, a discapito della capacità di controllo (ad esempio con una distinzione sempre più labile fra programmi e dati) e quindi della sicurezza. Per quanto ci sia ultimamente un'attenzione leggermente maggiore alla sicurezza, il processo continua

³² Attualmente sono implementati meccanismi di sicurezza basati su diversi modelli a seconda del sistema operativo, vedi http://en.wikipedia.org/wiki/Comparison_of_operating_systems ; un esempio di meccanismo hardware presente nei processori moderni è descritto in http://en.wikipedia.org/wiki/NX_bit

³³ analogamente alla tabella dei descrittori dei processi o alle tabelle per la gestione della memoria virtuale

³⁴ Ad esempio, in molti sistemi operativi i driver dei componenti hardware del sistema sono eseguiti al ring 0 per migliorare le prestazioni, e questo è sempre stato uno dei principali motivi di instabilità dei sistemi, ancor più che fonte di vulnerabilità; tuttavia, la tendenza a sacrificare la stabilità alle prestazioni integrando funzionalità nel kernel, forse anche grazie all'aumento delle prestazioni nei sistemi recenti, sembra destinata a invertirsi: <http://www.techworld.com/opsys/news/index.cfm?NewsID=5002>

³⁵ Meccanismi come il Role Based Access Control offrono una granularità data dai diversi ruoli che un utente può avere, ma anche con questi meccanismi, nell'ambito dello stesso ruolo, un processo per la riproduzione di file audio può ad esempio accedere anche a documenti di uno spreadsheet, anche se ragionevolmente l'utente non ha alcuna necessità che ciò sia possibile.

sostanzialmente ad andare verso una maggiore complessità, facilitando l'instaurarsi di nuove situazioni di rischio³⁶.

Non si vedono motivi per cui lo stesso problema non dovrebbe presentarsi qualora si tentasse di utilizzare i meccanismi del TC in modo esteso e granulare sul sistema. È invece assai più probabile invece un utilizzo mirato alla protezione di alcune attività e di alcuni dati ritenuti più critici, o di maggior valore. Il valore aggiunto del TC sarà quindi principalmente che le sue specifiche funzionalità, utilizzate su un insieme limitato di dati, saranno efficaci indipendentemente da chi possiede fisicamente il PC.

Ci possiamo chiedere a questo punto quali sono i problemi di sicurezza che il TC non è destinato a risolvere (lo stesso TCG afferma chiaramente che il TC non è nato per risolvere tutti i problemi di sicurezza). Un tipo di problema che difficilmente si può vedere risolto è quello dei difetti di un programma che permettano comportamenti inattesi. Ad esempio, se un mailer (integro) presenta una vulnerabilità per cui gestendo il contenuto di un messaggio di posta elettronica può essere indotto a prendere gli indirizzi della sua rubrica ed inviare a tutti gli indirizzi contenuti un virus, il TC non è lo strumento che lo può impedire. In effetti, molti problemi di sicurezza comuni rientrano in questa categoria: sono quelli per i quali più spesso vengono prodotti aggiornamenti di sicurezza.

Analizzando le vulnerabilità più comuni ed i problemi di sicurezza dichiarati dalle aziende, la quantità di problemi di sicurezza che non è minimamente interessata dal TC è considerevole.

Un'altra categoria di problemi è quella che potrebbe avere una soluzione basata sul TC, ma ha anche soluzioni non basate sul TC che però per diversi motivi non sono state realizzate e che eventualmente potrebbero essere di più semplice realizzazione del TC. Consideriamo ad esempio un problema di phishing in cui un sito fasullo riesce a farsi consegnare dall'utente di un servizio di home banking la propria password di accesso. Un meccanismo basato sul TC potrebbe riconoscere ad esempio che l'accesso non è effettuato dallo stesso PC che l'utente ha autorizzato per la connessione. Una maggiore efficacia si otterrebbe però con un'autenticazione del client basata su meccanismi a chiave pubblica, già implementati all'interno dei browser. In questo caso, il TC potrebbe proteggere la chiave privata permettendone l'uso solo all'applicativo di home banking; tuttavia, questo tipo di protezione potrebbe essere implementata altrettanto efficacemente con i normali meccanismi software di controllo degli accessi che si appoggiano sulle funzionalità hardware del processore, e con la chiave privata conservata su una smart card; l'associazione fra utente e autorizzazione sarebbe data dal possesso del PC ma da quello della smart card, soluzione decisamente più flessibile. Il problema, a detta di molti, è attualmente che i sistemi di home banking generalmente utilizzano una semplice password, anziché l'autenticazione a chiave pubblica del client o della transazione, a prescindere dal fatto che quest'ultima sia implementata con il TC, le smart card o anche solo meccanismi interamente software.

³⁶ Una pratica diffusa ad esempio fra i rivenditori è consegnare agli utenti domestici i nuovi PC con Windows XP configurato con un unico utente, a cui sono assegnati i privilegi di amministratore. Questo semplifica (banalizza) attività come l'installazione di applicazioni, ma fa sì che errori dell'utente possano condizionare la sicurezza e la stabilità dell'intero sistema. Non c'è motivo in realtà per cui i privilegi di amministratore debbano essere disponibili se non in pochi contesti e per attività limitate: installazione di nuovo software/hardware, aggiornamento del sistema e poche attività di configurazione. In effetti, questo errato comportamento dei rivenditori non dovrebbe semplicemente essere consentito dal sistema.

In pratica, per molti problemi di sicurezza il TC potrebbe costituire solo un meccanismo di base, alternativo o integrativo rispetto a quelli già presenti nei processori. Tutta l'attività di implementazione e integrazione necessaria per sfruttare questi meccanismi nei sistemi operativi, nelle applicazioni e nei servizi, dovrebbe però essere comunque realizzata; questa attività rappresenta un onere considerevole, e spesso i problemi di sicurezza derivano più da carenze nell'affrontare questa parte che da limiti nei meccanismi di base.

Bisogna dire peraltro che l'insicurezza dei sistemi operativi più diffusi, che per vari motivi non hanno sfruttato appieno le potenzialità dei meccanismi offerti dai processori, ha minato la fiducia che utenti ed aziende possono avere nei meccanismi già esistenti, ed è quindi comprensibile che possano essere attirati da soluzioni hardware che si presentino come "diverse e migliori" di quanto già disponibile.

Se vogliamo cercare quali sono gli utilizzi che richiedono realmente il TC, dobbiamo quindi esaminare le sue specificità. Una prima caratteristica riguarda il fatto di non essere implementato nel kernel del sistema operativo, e quindi di non poter essere disabilitato in caso di vulnerabilità del kernel stesso. Tuttavia, dato il ruolo del kernel nel sistema (ad esempio, l'assegnazione della memoria ai processi), attualmente è difficile immaginare che un kernel integro ma vulnerabile possa essere contrastato efficacemente. La caratteristica più rilevante sembra rimanere quindi l'impossibilità per l'*utente* e per il *proprietario*³⁷ di manomettere il meccanismo (il *proprietario* lo può disabilitare o riconfigurare). Vediamo quindi tre applicazioni che sembrano essere adatte per le specificità del TC, e che sono effettivamente fra quelle maggiormente pubblicizzate.

Un primo esempio riguarda il controllo sullo stato di un sistema prima di consentirne la connessione alla rete aziendale. Che si tratti del portatile di un dipendente o di quello di un consulente, l'azienda vuole essere sicura che il sistema abbia alcune protezioni attive: aggiornamenti di sicurezza installati, antivirus attivo e aggiornato e così via. Il TPM può quindi effettuare queste verifiche (appoggiandosi a componenti del sistema operativo di cui ha già verificato l'integrità) e comunicare il risultato all'*access point*, che ne terrà conto, insieme alle credenziali *utente*, prima di concedere l'accesso alla rete. Lo scopo è evitare che possano essere introdotti ad esempio virus nella rete a causa di sistemi mal gestiti. In questo caso si comincia a vedere un'utilità per un meccanismo non manomissibile da parte del *proprietario*: anche se questi, ad esempio per motivi di urgenza, volesse connettere una macchina non aggiornata alla rete, violando le politiche di sicurezza, il meccanismo sarebbe in grado di impedirglielo.

Un esempio più interessante riguarda la riservatezza dei dati. Supponiamo ad esempio che un'azienda debba concedere ad un consulente di esaminare dei documenti riservati, ma non voglia che questi ne possa fare delle copie. In questo caso il consulente, e non l'azienda, ha il controllo fisico del proprio portatile. Grazie al TC, sarebbe possibile assicurarsi che i documenti siano visualizzati solo con un'applicazione *fidata*; ad esempio, cifrando i documenti, "consegnando" la chiave per la decifrazione al TPM che a sua volta fornirà la chiave solo all'applicazione *fidata*, che chiaramente non permetterà di salvare copie del

³⁷ Si noti che attacchi di social engineering, che mirano a "convincere" l'utente a violare la sicurezza del sistema per conto dell'attaccante, ad esempio consegnando password o installando software, riguardano generalmente l'utente, appunto, e non l'owner.

documento³⁸. Questa forma di gestione dei diritti di accesso ai documenti aziendali è indicata a volte come Enterprise Rights Managements, ed è sostanzialmente una forma di DRM interno all'azienda.

Infine, il TC può essere utilizzato in maniera analoga in un contesto di DRM per evitare la copia dei dati protetti, ad esempio di un film scaricato da Internet.

Un ulteriore uso del TC può essere assicurarsi che un sistema rubato non possa essere riutilizzato (tuttavia, per quanto riguarda i dati contenuti, la cifratura dei dati su disco è ritenuta sufficiente per la quasi totalità dei contesti, se correttamente realizzata).

Insomma, quando il comportamento dell'*utente*, o anche del *proprietario*, è considerato rischioso, la soluzione naturale è togliergli il controllo sul sistema, almeno per quanto riguarda le risorse che si vogliono proteggere, e questo è quanto il TC permette di fare. Infatti:

- le caratteristiche del software *fidato* sono (o possono essere) valutate e certificate in modo indipendente dal *proprietario*;
- il TPM può verificare se le caratteristiche del software corrispondono a quelle certificate senza che il *proprietario* o l'*utente* possano influire sulla correttezza della verifica; al massimo la possono impedire o far fallire;
- i risultati della verifica possono essere comunicati a terzi (l'*access point*, l'azienda proprietaria dei dati protetti) senza che il *proprietario* possa influire sul contenuto della comunicazione: di nuovo, al massimo la può impedire, facendo comunque fallire la verifica.

Si noti nuovamente che l'effettiva esigenza del TC si manifesta principalmente quando ci si aspetta la volontà esplicita dell'*utente* di manomettere fisicamente il sistema pur di accedere alle risorse protette.

Una volta che il TC sia disponibile, ci si può anche aspettare che funzioni di sicurezza che potrebbero comunque essere ottenute con altri strumenti vengano invece realizzate appoggiandosi al TPM. In particolare, funzionalità di protezione dei dati che potrebbero essere realizzate via software si appoggeranno probabilmente al TC, specialmente se questo darà la sensazione di una maggiore "sicurezza". Un esempio può essere la protezione di chiavi di accesso a servizi come quelli di home banking o quelli offerti dalle Pubbliche Amministrazioni al cittadino.

³⁸ L'intero meccanismo si appoggia quindi su una sinergia fra TPM, sistema operativo e applicazione: il TPM riporta sullo stato del sistema, compreso il fatto che è in esecuzione uno specifico sistema operativo. La chiave viene resa disponibile solo all'applicazione prevista tramite il TPM e il sistema operativo

SEZIONE V

I RISCHI DEL TRUSTED COMPUTING

Per valutare correttamente i rischi descritti nel seguito (è bene ricordare che parliamo di rischi, non di certezze), è importante chiarire un altro punto: ci sono alcune cose che sono garantite da TC, altre che sono permesse. Che quanto è permesso sia effettivamente implementato dipende dalle politiche di chi sviluppa un prodotto. Allo stesso modo, una caratteristica che non è richiesta dal TC può comunque essere implementata se non è in contrasto con le specifiche del TC stesso.

Per chiarire questo concetto facciamo due esempi. Il TC *permette* l'implementazione di alcune funzionalità in modo anonimo, permettendo quindi ad esempio il rispetto della privacy in alcune attività. Tuttavia, il TC non richiede che le funzionalità siano implementate in modo anonimo (non *garantisce* l'anonimato), e quindi sta all'implementatore, in base alle proprie politiche, decidere se intende rispettare o meno la privacy degli utenti. Ci dobbiamo quindi porre il problema del rischio di violazione della privacy nell'uso di queste funzioni. La valutazione dovrà tenere conto sia della probabilità che le funzioni siano implementate in modo non anonimo, sia dell'impatto che questa violazione della privacy avrebbe.

Allo stesso modo il TC non richiede l'uso di CA esterne, tuttavia lo *consente*, ed essendo probabile che i meccanismi di mercato portino in quella direzione, allora non è sbagliato discutere i rischi dell'associazione di CA esterne al TC.

Come già detto, i rischi vanno confrontati con la situazione "senza TC": se ad esempio il rischio di violazione della privacy è simile, con o senza TC, non è corretto considerarlo una particolarità del TC. Viceversa, se il rischio è direttamente riconducibile a funzionalità che senza TC non sarebbero disponibili, o da queste è incrementato in modo significativo, allora il rischio è riconducibile al TC.

Alcune delle considerazioni che seguono riguardano possibili "condizionamenti del mercato". Si potrebbe ritenere inopportuno che il CLUSIT si esprima al riguardo, occupandosi di sicurezza informatica. Tuttavia, un mercato sano è una condizione per lo sviluppo di prodotti di qualità. Se alcuni attori possono condizionare il mercato, allora non saranno più adeguatamente stimolati a curare la qualità dei propri prodotti, e l'esperienza insegna che quando la qualità dei prodotti diminuisce, la sicurezza è la prima a risentirne. Dato che il TC non è sicuramente in grado di risolvere tutti i problemi di sicurezza, è comunque importante che la sua introduzione non influenzi negativamente il mercato dell'hardware e del software.

Per proseguire in questa analisi è necessario a questo punto ricordare a grandi linee alcune caratteristiche del mercato dell'informatica e del suo probabile sviluppo futuro.

Lo scenario

Per quanto riguarda l'utente domestico, ci sono due tendenze principali che, secondo le previsioni più comuni, influenzeranno il suo rapporto con il PC.

La prima è lo svolgimento di attività rilevanti dal punto di vista economico ed anche sociale, attraverso il PC: lo sviluppo dell'e-government, l'offerta sempre maggiore di servizi di commercio elettronico, la convergenza con i sistemi di telefonia o di videofonia, l'eventuale utilizzo di sistemi di voto elettronico, renderanno il PC domestico un punto di riferimento critico per la sicurezza sotto tutti gli aspetti, primo fra tutti quello della privacy.

La seconda è la convergenza con le diverse piattaforme di comunicazione e per la fruizione di contenuti audio/video, sia in termini di intrattenimento che di informazione. Microsoft XP Media Center Edition³⁹ è un esempio di questa tendenza, che con soluzioni di TV via Internet o di offerte anche più innovative farà sì che il PC sostituisca o integri televisione, radio ed altri strumenti analoghi (gli attuali ricevitori satellitari e registratori di DVD più evoluti, dotati ad esempio di hard disk, sono anch'essi un passaggio verso l'integrazione completa).

Si noti che la convergenza non è solo tecnologica, ma anche di interessi economici e di capitali; ne sono la prova i sempre più numerosi annunci di accordi fra software house, case cinematografiche, gestori di tv satellitari ed altri ancora⁴⁰. Al centro di questi interessi c'è principalmente l'offerta all'utente domestico. È chiaro quindi che se già adesso c'è interesse per il DRM, questo scenario lo rende ancora più interessante, e il TC sembra lo strumento ideale per gestirlo. Mentre per le aziende si possono immaginare altri utilizzi per il TC, è probabile che questo diventi l'utilizzo dominante per l'utente domestico.

Per completare lo scenario, è necessario ricordare che attualmente il mercato dei PC presenta, per alcuni componenti fondamentali, una situazione in cui ci sono pochi attori dominanti. Questo è vero particolarmente per i PC domestici: nel mercato dei processori (CPU), dove Intel occupa la maggior parte del mercato e AMD copre la quasi totalità del rimanente; in quello dei sistemi operativi, dove la quasi totalità dell'installato è Microsoft; in quello degli strumenti di Office Automation, dei web browser, dei mailer e dei "media player", dove Microsoft è ancora una volta dominante⁴¹. Di questo sarà necessario tenere conto nel valutare la capacità del mercato di resistere ad eventuali forzature o condizionamenti.

Gli effetti certi

Nel momento in cui i membri del TCG decidessero di diffondere capillarmente il TC, data la loro forza sul mercato, saranno certamente in grado di imporlo come unica piattaforma; i rimanenti produttori di hardware non potranno che adeguarsi all'utilizzo della tecnologia, e lo stesso vale per i produttori di applicazioni e sistemi operativi. Quello con cui ci dobbiamo confrontare quindi, per la valutazione dei rischi⁴², è un mercato in cui non ci sono alternative a piattaforme TC-compliant, sia per produttori che per gli utenti, non più di quanto ci siano adesso alternative reali a piattaforme per PC con processori Intel o AMD.

Nel momento in cui il TC verrà effettivamente utilizzato per gestire problematiche di DRM, diventerà praticamente impossibile non utilizzarlo, sia per gli utenti domestici che per quelli

³⁹ <http://www.microsoft.com/italy/windowsxp/mediacenter/default.mspx>

⁴⁰ <http://punto-informatico.it/p.asp?i=57170&r=PI>

⁴¹ Per la normativa italiana, essere dominante in un mercato è assolutamente lecito (può essere indice di maggiori capacità o di migliori prodotti rispetto alla concorrenza). Quello che non è consentito è abusare di una posizione dominante, ad esempio per impedire l'accesso di nuovi concorrenti al mercato.

⁴² Il caso in cui il TC è solo un'opzione, oltre ad essere molto meno probabile (si parla anzi di integrazione del TPM direttamente nel processore), presenta decisamente meno rischi, e quindi è meno significativo per questo documento.

aziendali, a meno di voler rinunciare a un numero considerevole di servizi. A meno che gli utenti non sviluppino un'avversione per il TC, al momento molto difficile da ipotizzare, saranno sempre più i servizi offerti attraverso controlli di DRM basati sul TC, ed anche altri servizi sfrutteranno queste funzionalità per controllare ad esempio lo stato dei clienti. Il fatto che le funzionalità possano essere realizzate con altri strumenti diventerà a quel punto irrilevante, e in pratica disabilitare il TC, possibilità offerta dalle specifiche, non sarà più un'opzione realistica per la maggior parte degli utenti.

I rischi

L'analisi del TC evidenzia come TC stesso non sia solo un meccanismo di fiducia nel TPM e in eventuali CA⁴³: è anche un meccanismo di sfiducia nei confronti dell'utente. La valutazione sul corretto stato del sistema viene infatti tolta all'utente e condivisa fra il TPM, la CA e il proprietario della risorsa da proteggere, sia esso azienda o detentore di diritti su proprietà intellettuale. Mentre questo rientra negli interessi ed eventualmente nel diritto di questi ultimi soggetti, la posizione dell'utente è decisamente meno ovvia. Ci riferiamo per ora all'utente domestico, quindi non al dipendente o al consulente. L'utente domestico non ha nessun interesse a perdere il controllo sul proprio sistema, a meno di accettare l'idea di non essere in grado di capirne e gestirne la sicurezza (questa posizione è per altro piuttosto diffusa sia fra gli utenti che fra i fornitori di soluzioni di sicurezza), e di essere quindi disposto a "consegnarne le chiavi" a qualcuno che, almeno su alcuni aspetti, decida per lui. Tuttavia, è probabile che ben presto si trovi con la necessità di attivare il TC sul proprio PC⁴⁴, indipendentemente dal fatto che lo ritenga o meno nel proprio interesse.

Nel momento in cui il TC sarà sufficientemente diffuso, è probabile ad esempio che i produttori di contenuti inizino a richiederne le funzionalità per consentire la fruizione dei loro prodotti.

Il mercato del software

Il rapporto fra TC, DRM e software può diventare preoccupante per gli equilibri del mercato. Per il produttore di contenuti infatti, sarà naturale richiedere, tramite il TC, la presenza di strumenti che soddisfino le sue esigenze di DRM, non solo in termini di funzionalità, ma anche di vincoli imposti sull'utilizzo. Anziché porsi il problema di quali siano le funzionalità richieste infatti, potrebbe essere molto più semplice indicare esplicitamente uno o due media player che devono essere utilizzati, consegnando di fatto il mercato a questi prodotti. Questo tipo di problema si vede già in parte, per altri motivi, con i siti web: nonostante esistano degli standard, molti siti web richiedono invece l'utilizzo di uno specifico browser (Internet Explorer) o al più due (includendo allora Netscape/Mozilla/Firefox). La logica è che se un browser è assolutamente dominante sul mercato, e il browser soddisfa le necessità del sito web, allora è inutile preoccuparsi di compatibilità con altri strumenti. Nel caso dei media player l'effetto potrebbe essere enormemente più macroscopico, dato che l'esigenza che l'utente utilizzi uno strumento adeguato è, in termini di DRM, ancora più stringente: se venisse infatti accettato anche un solo media player che permette la realizzazione di copie, l'intero meccanismo potrebbe diventare inutile. C'è quindi il rischio che per visualizzare determinati contenuti venga richiesto esclusivamente Microsoft Windows con Windows Media Player, data la sua attuale dominanza sul mercato e una probabile propensione a

⁴³ L'uso di CA è la soluzione naturale qualora si voglia usare il TPM per controlli non condizionabili da parte dell'owner, come è il caso del DRM ma anche quello del controllo di dati riservati acceduti da consulenti

⁴⁴ Prima ancora, naturalmente, si troverà a dover pagare il costo dell'intera infrastruttura composta da hardware, software, CA, certificazioni

supportare meccanismi stringenti di DRM⁴⁵ (Microsoft è infatti in prima linea nella lotta alla pirateria). Questo potrebbe condizionare fortemente il mercato: un produttore di un media player, seppure disposto a supportare le politiche di DRM più stringenti, non riuscirebbe di fatto ad accedere al mercato, perché il suo player non sarebbe fra quelli indicati. Di fatto il mercato potrebbe essere completamente bloccato. Inoltre, non si tratterebbe necessariamente di un abuso di posizione dominante da parte di chiacchessia (tantomeno da parte di Microsoft), dato che non sono necessari accordi fra il produttore del media player e quelli dei contenuti multimediali perché l'effetto si manifesti, esattamente come ora non ci sono accordi fra Microsoft e i siti web che supportano solo Internet Explorer.

Un problema analogo si potrebbe avere con altri strumenti software, per i motivi più disparati. Ad esempio, se una grossa azienda sceglie un certo prodotto per visualizzare i propri documenti, allora i suoi fornitori potrebbero essere obbligati ad utilizzare lo stesso prodotto, sullo stesso sistema operativo, e non semplicemente uno in grado di leggere file nello stesso formato. Dato che, come abbiamo visto, per molti strumenti esistono produttori fortemente dominanti nei rispettivi settori, questo porterebbe ad un fortissimo irrigidimento del mercato, che resisterebbe all'introduzione di prodotti alternativi. Infine, l'esistenza o meno di formati standard aperti diventerebbe ininfluenza per il mercato del software, dato che quello che conta in questo contesto non è solo la capacità di un prodotto di leggere i dati, ma soprattutto l'autorizzazione a farlo.

Uno scenario meno catastrofico è quello in cui non viene richiesto un player specifico, ma solo un player che abbia le caratteristiche gradite al proprietario dei contenuti, ad esempio implementi i meccanismi di DRM richiesti. Questa caratteristica potrebbe essere oggetto di una valutazione, ad esempio secondo i Common Criteria (standard ISO/IEC 15408⁴⁶), e poi di una certificazione da parte di una CA. Si noti che il fatto che questo scenario sia meno catastrofico non lo rende più probabile, quantomeno perché un numero più elevato di player vuole dire una probabilità più elevata di vulnerabilità che permettano di violare i vincoli di DRM.

Si può subito evidenziare come si tratti, almeno per quanto riguarda l'ottenimento della certificazione secondo i Common Criteria, di un processo lungo e costoso. Questo naturalmente andrebbe a discapito dei produttori più piccoli. Inoltre, renderebbe più difficoltosa la sperimentazione "sul campo", ovvero con dati reali, dato che un prodotto non certificato non avrebbe certamente accesso ai contenuti commercializzati; d'altra parte un prodotto ancora sperimentale difficilmente verrebbe certificato. Lo sviluppo di nuovi prodotti potrebbe diventare quindi vincolato ad accordi con i produttori di contenuti e difficilmente sarebbe un'attività autonoma. Come detto, fra produttori di software e di contenuti sono già in corso accordi e alleanze, ed anche questo potrebbe bloccare l'ingresso di nuovi attori che possano contrastare le attuali posizioni dominanti.

⁴⁵ In effetti, già adesso, senza il TC, molti siti offrono i propri contenuti multimediali in formati fruibili solo con una, o al massimo due applicazioni, tipicamente Windows Media Player, Macromedia Shockwave o Real Realplayer; il predominio di questi prodotti sul mercato è tale che per molti siti non è di nessun interesse considerare alternative, anche senza che ci siano accordi di alcun genere fra i gestori dei siti e Microsoft, Adobe o Real. Un problema simile, ampiamente dibattuto in questo periodo, riguarda il formato dei file distribuiti per iPod.

⁴⁶ Si tratta di uno standard per la certificazione delle caratteristiche di sicurezza di sistemi e prodotti informatici, <http://www.commoncriteriaportal.org/>

Oltre a questo, è possibile che per sviluppare prodotti TC-compliant siano necessarie licenze detenute ad esempio da qualcuno dei membri del TCG. Non si tratta infatti di uno standard prodotto da un organismo di standardizzazione, ma del risultato dell'attività di alcune aziende. Mentre molti organismi di standardizzazione cercano di assicurare, per quanto possibile, che gli standard sviluppati non consegnino il mercato ai detentori di uno o più brevetti, lo stesso non è garantito per il TC. L'accesso ai brevetti, oltre ad essere un maggiore costo, può essere un ulteriore strumento di controllo del mercato. In effetti, il TCG non indica se alcune delle tecnologie legate al TC siano coperte da brevetti, né chi eventualmente li detenga.

L'interesse del CLUSIT per queste problematiche, come già detto, è che in assenza di concorrenza, la qualità dei prodotti come è noto tende a scendere (ed il costo a salire), e quando la qualità dei prodotti scende la sicurezza è la prima a risentirne; inoltre, gli utilizzatori dei prodotti, non avendo reali alternative, non hanno a disposizione i tipici strumenti di mercato con cui fare pressione sui fornitori per un miglioramento della qualità dei prodotti.

L'Italia dovrebbe essere particolarmente sensibile a problematiche di condizionamento del mercato a favore di poche grosse aziende. Il significato strategico dell'informatica in un gran numero di settori e di attività è evidente, come anche è evidente la quasi totale dipendenza dell'Italia dall'estero. La produzione italiana di software è minima, destinata al mercato interno e non copre nessun componente di ampia diffusione; ad esempio, sostanzialmente tutto il software presente su un PC domestico è importato. La situazione dell'Europa è di poco migliore, con alcune grosse aziende di rilevanza mondiale ma con prodotti destinati a settori specifici. In alcuni paesi europei, ad esempio in Germania, c'è una forte attenzione verso l'Open Source, che al momento ha sviluppato in alcuni settori le poche alternative credibili ai prodotti degli attori principali, senza tuttavia intaccare in modo rilevante il mercato dei PC domestici; l'Open Source, almeno per come è sviluppata attualmente la maggior parte dei prodotti, sembra particolarmente sensibile a costi di sviluppo imposti e vincoli come la necessità di certificazioni o di licenze.

Qualsiasi meccanismo che tenda a rafforzare la posizione degli attuali grossi attori del mercato dell'informatica rafforza la dipendenza dell'Italia dall'estero, riduce la possibilità di sviluppo di prodotti nazionali e soprattutto riduce la capacità dell'Italia, delle sue aziende e dei suoi cittadini di decidere quali strumenti e quali funzionalità devono essere presenti sui propri sistemi.

Il rischio di inefficacia sostanziale delle norme

Un'obiezione che si potrebbe fare al rischio di eventuali storture del mercato o abusi delle tecnologie è che, qualora il mercato non riesca a correggersi autonomamente, esistono o possono essere emanate delle norme che possono riportare nei binari dell'etica e della legalità i comportamenti scorretti. Un esempio possono essere le normative relative all'abuso di posizione dominante, con l'Authority per la Concorrenza, e quelle sul trattamento dei dati personali. Nel campo dell'informatica si pone però con una certa facilità il rischio di inefficacia sostanziale delle norme, ovvero l'impossibilità pratica di imporre il rispetto di norme esistenti, o di comminare sanzioni in caso di mancato rispetto.

Esistono numerosi fattori che possono limitare fortemente l'efficacia delle norme nel settore dell'informatica. Per comprenderle, è necessario tenere conto di due fatti:

- il mercato dell'informatica è globale; le strategie delle grosse aziende del settore sono basate principalmente sul mercato degli Stati Uniti, ed eventualmente su grossi mercati emergenti con grandi potenzialità, come quello della Cina; mentre il mancato

rispetto di normative di questi paesi può avere un impatto notevole, il mancato rispetto di normative italiane, o in alcuni casi anche europee, sembra avere impatto molto più limitato sulle scelte di queste aziende, e può essere affrontato anche con azioni correttive quando e se necessario;

- nel mercato dell'informatica i tempi sono estremamente accelerati; per contro, i tempi della Legge sono notoriamente lenti, e quelli italiani lo sono ancora di più; un intervento a posteriori può quindi arrivare con un ritardo tale da essere assolutamente inefficace dal punto di vista del ripristino di un mercato corretto.

Ci chiediamo quindi se l'introduzione del TC possa aggravare, almeno in alcuni settori dell'informatica, il rischio di inefficacia sostanziale delle norme.

A titolo esemplificativo, possiamo esaminare il problema dello spam e la capacità delle norme italiane di contrastarlo in quanto trattamento abusivo di dati personali. Giova ricordare che la prima normativa italiana sul trattamento dei dati personali è del 1996, ovvero più di dieci anni fa. Il problema dello spam allora era limitato e si riferiva sostanzialmente a quello in lingua inglese proveniente dall'estero. Da allora, non solo lo spam è aumentato enormemente, ma si è diffuso anche quello interamente italiano, sul quale in teoria ci dovrebbe essere una maggiore capacità di repressione, e si è sviluppato quello mediante chiamate telefoniche automatiche e, ultimamente, quello via SMS. Nella pratica quindi, l'esistenza di una normativa che dovrebbe controllare l'abuso dei dati personali, non solo non è riuscita a impedire il protrarsi di un abuso effettuato dall'estero, ma non è riuscita neppure a impedire la nascita e la diffusione di un abuso praticato in Italia. Forse nei prossimi anni un'applicazione più rigorosa della norma potrà aiutare ad arginare il fenomeno, ma comunque i costi sostenuti nel frattempo in termini di risorse e tempo sprecati da parte di cittadini ed aziende sarà enorme. Si può notare come in questo caso sia palese la differenza fra le normative di diversi paesi, e la difficoltà nell'applicare le norme di un singolo Stato, di fronte alla globalità del problema.

Per quanto riguarda i tempi della Giustizia, è interessante esaminare il procedimento COMP/37.792 - MICROSOFT/ W2000⁴⁷ e la decisione IP/04/382 della Commissione Europea. Si tratta di un procedimento di notevole rilevanza per il mercato del software, di cui si è ampiamente e pubblicamente discusso, ed è quindi forse il genere di procedimento che ci si potrebbe aspettare in caso di abuso da parte di una grossa azienda delle possibilità offerte dal TC. Il procedimento viene aperto ufficialmente nel 2000 con un'indagine relativa a un possibile abuso di posizione dominante legato alla distribuzione di "software middleware" allegato a Windows 2000. Nell'agosto 2000 viene avviato un procedimento per abuso di posizione dominante e "discriminatory licensing". Nell'agosto del 2001 la Commissione Europea inizia un ulteriore procedimento per abuso di posizione dominante, legato al problema, ampiamente noto e dibattuto, della distribuzione di Windows Media Player insieme a Windows, cosa che lo mette in una posizione molto forte rispetto ai media player concorrenti. Nel 2004 la Commissione Europea conclude l'indagine indicando "rimedi e multe": *"The European Commission has concluded, after a five-year investigation, that Microsoft Corporation broke European Union competition law by leveraging its near monopoly in the market for PC operating systems (OS) onto the markets for work group server operating systems(1) and for media players(2). Because the illegal behaviour is still ongoing, the Commission has ordered Microsoft to disclose to competitors, within 120 days, the interfaces(3) required for their products to be able to 'talk' with the ubiquitous Windows OS. Microsoft is also required, within 90 days, to offer a version of its Windows OS without*

⁴⁷ http://europa.eu/comm/competition/antitrust/cases/index/by_nr_75.html#i37_792

Windows Media Player to PC manufacturers (or when selling directly to end users). In addition, Microsoft is fined euro 497 million for abusing its market power in the EU.”

Al momento quello che ci interessa evidenziare è che il solo procedimento ha richiesto più di quattro anni di attività ufficiale. A questo si aggiunge il tempo necessario perché il problema venisse rilevato e la Commissione Europea decidesse di avviare un'indagine. È chiaro che si tratta di tempi lunghissimi se confrontati con quelli dell'informatica. Nel frattempo infatti, se le conclusioni della Commissione Europea sono corrette, Microsoft ha avuto quasi cinque anni in cui ha potuto continuare ad abusare della propria posizione. È chiaro che eventuali concorrenti presenti nel 2000, specialmente nel caso di piccole imprese di informatica (il tipo di azienda certamente più diffuso in Europa in questo settore) difficilmente potevano essere ancora sul mercato nel 2004 per trarre giovamento dalle conclusioni della Commissione Europea. Vale inoltre la pena di dire che alcuni grossi produttori e distributori di PC ebbero modo di dichiarare che loro avrebbero comunque continuato a distribuire la versione di Windows con Media Player (in effetti, non è dai distributori di PC che ci si può aspettare un interesse a distribuire un prodotto “menomato”). La vicenda tuttavia, non è ancora conclusa; dopo l'opposizione di Microsoft, le stime danno generalmente per probabile una decisione definitiva entro l'inizio del 2007. Nel frattempo, Windows 2000 è uscito di produzione, e dopo Windows XP, con l'inizio del 2007 è iniziata la distribuzione di Microsoft Vista: intere generazioni di prodotti sono nate e saranno uscite di produzione prima della sentenza definitiva.

Secondo le logiche del mercato, un abuso di posizione dominante, riducendo la concorrenza, può fra l'altro causare un aumento dei prezzi e bloccare la nascita di nuovi prodotti innovativi. L'aspetto interessante è che, anche dopo la decisione della Commissione del 2004, non solo è cambiato poco per quanto riguarda il mercato, ma non sono apparentemente cambiati i rapporti neppure con le Pubbliche Amministrazioni e con le Istituzioni, almeno con quelle italiane. Esiste quindi il rischio che l'intervento a posteriori di un'autorità di garanzia possa avere un'efficacia limitata sia per quanto riguarda la correzione dell'irregolarità, sia soprattutto per rimediare ai danni causati prima che l'irregolarità venisse evidenziata e nel corso del procedimento. Si può anche ipotizzare che l'efficacia di un intervento a livello nazionale, anziché europeo, sia ancora minore.

Come ultimo esempio prendiamo la normativa italiana sul diritto d'autore, come modificata dal Decreto Legislativo 9 aprile 2003, n. 68.

L'art. 71 sexies prevede al primo comma: "È consentita la riproduzione privata di fonogrammi e videogrammi su qualsiasi supporto, effettuata da una persona fisica per uso esclusivamente personale, purché senza scopo di lucro e senza fini direttamente o indirettamente commerciali, nel rispetto delle misure tecnologiche di cui all'articolo 102-quater". Uno degli scopi principali della creazione di copie private, almeno fra quelli ritenuti generalmente parte del cosiddetto “fair use”, è di utilizzare poi le copie, non esponendo quindi il supporto originale ad usura ed eventuali danneggiamenti (cosa che costringerebbe ad acquistarne un'altra copia, pagando nuovamente i diritti già pagati con la prima). Le misure tecnologiche di cui all'art. 102-quater sono le tecnologie utilizzate per la protezione delle opere. Tuttavia, al comma 4, dice che: “*Fatto salvo quanto disposto dal comma 3, i titolari dei diritti sono tenuti a consentire che, nonostante l'applicazione delle misure tecnologiche di cui all'articolo 102-quater, la persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto, ovvero vi abbia avuto accesso legittimo, possa effettuare una copia privata, anche solo analogica, per uso personale, a condizione che tale*

possibilità non sia in contrasto con lo sfruttamento normale dell'opera o degli altri materiali e non arrechi ingiustificato pregiudizio ai titolari dei diritti.”

In base a quest'ultima disposizione, visto il diritto in capo alla persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto di effettuare una copia privata, le misure tecnologiche applicate non potrebbero essere così restrittive da impedire l'esercizio di questo diritto salvo che la possibilità di effettuare una copia privata: 1) non sia in contrasto con lo sfruttamento normale dell'opera e 2) **non arrechi ingiustificato pregiudizio ai titolari dei diritti.**

Vero quanto detto, la formulazione di quest'ultima è stata contestata da numerosi interpreti vista la sua indeterminatezza e difficoltà di applicazione e molti hanno altresì richiesto la sua sostanziale riformulazione. E' indubbiamente un dato di fatto che il diritto dei possessori legittimi di effettuare una copia privata dell'opera è sempre più spesso vanificato dall'applicazione da parte dei titolari dei diritti di misure tecnologiche di protezione che impediscono qualsiasi forma di riproduzione. Tali misure spesso vengono giustificate dai titolari dei diritti dalla necessità di porre un argine concreto all'enorme diffondersi della pirateria musicale ed audiovisiva senza tenere in alcuna considerazione il diritto legislativamente stabilito dell'effettuazione delle copie private. Inoltre vi è al momento l'assenza di pronunce giurisprudenziali che abbiano fornito una chiave interpretativa dell'articolo 71 sexies l.d.a e che soprattutto abbiano valutato la legittimità delle misure tecnologiche che impediscono l'effettuazione di copie private.

Ad esempio, esistono da tempo sistemi per la protezione delle videocassette. Uno di questi è il Macrovision^{®48}, già citato nella sezione sul DRM. È chiaro quindi come i titolari dei diritti d'autore possono far valere il loro diritto ad utilizzare misure tecnologiche per la protezione delle opere. Meno chiaro è come ci si aspetta che il consumatore venga nella pratica tutelato; allo stato attuale ad esempio, bisognerebbe che un consumatore si assumesse l'onere di una causa nei confronti almeno di un distributore di videocassette, causa che certamente si protrarrebbe a lungo, fino ai gradi più alti di giudizio e con costi notevoli, assumendosi il rischio di dover pagare almeno le spese processuali nel caso risultasse che l'uso del Macrovision è legittimo. Quello che è certo è che a più di due anni di distanza dall'approvazione del decreto, e con un interesse diffuso e riconosciuto da parte dei consumatori per la realizzazione di copie private, strumenti come Macrovision continuano ad essere diffusi e non esiste una giurisprudenza che testimoni un'attività a favore dei diritti sanciti dal quarto comma.

Tuttavia, è utile porsi un'ulteriore domanda, e cioè: nell'ipotesi che l'applicazione di tecnologie come il Macrovision sia in contrasto con la normativa, come sarebbe possibile agire nei confronti di chi lo utilizza? Si potrebbero arrivare a immaginare misure draconiane come il ritiro delle videocassette dal mercato. Si tratta però di misure applicabili solo ai supporti fisici. Nel momento in cui le opere fossero distribuite attraverso Internet, possibilmente da siti esteri, delle opere in violazione del quarto comma dell'art. 71 sexties, la capacità di intervento sarebbe decisamente ridotta.

⁴⁸ Si tratta ad esempio della protezione abitualmente utilizzata per le videocassette Walt Disney

Possiamo a questo punto tornare al TC. Come abbiamo visto, il TC fornisce uno strumento con cui è possibile controllare quali sistemi operativi, applicazioni e dati possono essere utilizzati su di un sistema. Abbiamo visto inoltre alcuni meccanismi con cui aziende o gruppi possono trarre vantaggio dal TC in modo anche illecito. Tuttavia si possono immaginare facilmente altre possibilità, offerte ad esempio dalle politiche di certificazione delle CA, che possono facilmente escludere aziende dal mercato semplicemente ostacolando l'ottenimento dei certificati necessari (un'azione di questo tipo sarebbe per certi versi simile al "discriminatory licensing").

L'introduzione del TC potrebbe quindi rendere ancora più impraticabile per i singoli Stati l'applicazione di normative nel settore dell'informatica (e, conseguentemente, delle comunicazioni, dell'intrattenimento e dell'informazione). Esso fornirebbe un potente strumento con cui imporre regole e vincoli con strumenti tecnici, controllati da soggetti privati il cui primo interesse è necessariamente quello dei propri azionisti; per contro il riconoscimento e la correzione degli abusi sarebbe una lenta, continua e faticosa "rincorsa" da parte degli organi preposti.

Accordi internazionali, oltre ad essere lunghi e laboriosi da predisporre, potrebbero facilitare l'applicazione a livello internazionale solo di quei principi unanimemente condivisi, mentre scelte specifiche dei singoli Stati potrebbero essere sostanzialmente ininfluenti.

La privacy

Uno dei rischi più comunemente evidenziati per il TC è quello della raccolta di dati personali dell'utente, a sua insaputa e/o senza il suo consenso. Le informazioni potrebbero poi essere trasmesse in modo cifrato, protette in modo tale che né il *proprietario* né l'*utente* siano in grado di riconoscerle o bloccarle.

Da questo punto di vista, sembrerebbe però che l'unica particolarità aggiunta dal TC allo stato attuale, per quanto riguarda l'utente domestico, sia l'impossibilità di disabilitare il meccanismo (sempre, a meno di disabilitare l'intero meccanismo di TC e quindi rischiando di perdere buona parte delle funzionalità e dei servizi offerti attraverso il PC). Infatti, già adesso un gran numero di applicazioni, e più ancora lo stesso Windows, utilizzano protocolli proprietari per comunicare con la casa madre, raccogliendo e trasferendo informazioni relative al sistema allo scopo di individuare gli aggiornamenti necessari.

Queste comunicazioni avvengono per lo più attraverso canali cifrati; generalmente le case produttrici dichiarano, con forme diverse, che non sono raccolti dati personali e/o che i dati sono trattati in forma anonima. Tuttavia, molte applicazioni prevedono una fase di registrazione opzionale o addirittura una fase di attivazione obbligatoria, in cui la licenza viene generalmente collegata ad una persona. La definizione di "dati personali" si riferisce inoltre presumibilmente alla normativa statunitense: difficilmente l'informativa corrisponde ad un adattamento della procedura alle norme locali, ma è invece semplicemente una traduzione in italiano di quella in inglese. Comunque sia, cosa effettivamente venga raccolto e come venga trattato non è generalmente noto se non attraverso le dichiarazioni delle aziende stesse: se queste volessero raccogliere illecitamente e segretamente dati personali, ad esempio per attività di "profiling", sarebbero di fatto già in grado di farlo⁴⁹.

⁴⁹ La cifratura di questi dati è generalmente giustificata con la protezione dell'utente stesso, evitando di trasmettere in chiaro via Internet dati relativi al PC. Si tratta di una giustificazione tecnicamente molto debole, in quanto la chiave temporanea con la quale sono cifrati i dati e la struttura dei dati trasmessi potrebbero essere

Gli utenti domestici che sono coscienti del potenziale problema sono una minima parte, e meno ancora sono in grado di intervenire tecnicamente; l'intervento richiederebbe oltretutto di disabilitare o bloccare le funzionalità di aggiornamento automatico, rendendo più difficile o impraticabile l'aggiornamento del sistema. La prima domanda da porsi sarebbe quindi se si ritiene che allo stato attuale l'utente sia sufficientemente tutelato. Se la risposta è sì, allora difficilmente il TC può aumentare significativamente il rischio. Se viceversa si ritiene che gli attuali protocolli costituiscano un rischio, ci si può chiedere cosa viene fatto o cosa può essere fatto per affrontarlo: si tratta probabilmente di un buon esercizio per la comprensione del rischio di inefficacia sostanziale delle norme sopra descritto. Infatti, il contesto internazionale rende nuovamente improbabile che l'Italia sia realmente in grado di controllare cosa viene effettivamente raccolto e forse anche all'Europa sarebbero necessari procedure e tempi attualmente improponibili. In quest'ottica, il TC può rappresentare un significativo aumento del rischio stesso, nel senso che l'applicazione di eventuali controlli può essere ancora più ardua. Non sembra però rappresentare allo stato attuale un aumento significativo del rischio per la privacy della maggior parte degli utenti.

Diversa è invece la situazione per le grandi aziende e le pubbliche amministrazioni. Queste infatti generalmente non consentono comunicazioni dirette fra le applicazioni sui singoli PC e relativa casa madre, ma gestiscono in proprio il riconoscimento e l'installazione degli aggiornamenti necessari. Tuttavia, queste stesse organizzazioni dovrebbero consentire comunicazioni per la gestione del DRM, quelle con le CA per le verifiche e quant'altro richiedessero gli strumenti e i servizi che si appoggiassero al TC per il proprio corretto funzionamento. Si esporrebbero quindi al rischio di consentire comunicazioni incontrollate, e presumibilmente cifrate, fra i loro sistemi e altre entità. È utile a questo punto ricordare un caso interessante, legato agli effetti collaterali inaspettati delle misure di sicurezza sul software imposte dal paese di produzione.

Fino al 1996 circa, la regolamentazione statunitense richiedeva che la robustezza dei meccanismi di crittografia dei prodotti esportati venisse deliberatamente indebolita. In particolare, la lunghezza massima delle chiavi di cifratura era di 40 bit, quando internamente agli Stati Uniti gli stessi prodotti utilizzavano tipicamente 56 o anche 128 bit⁵⁰. I vincoli vennero gradatamente ridotti, e anche se l'esportazione non è ancora completamente deregolamentata, adesso possono essere esportati strumenti con protezioni ritenute, per quanto è dato sapere, adeguate. Durante gli anni di transizione, si parlò per un certo tempo di key

accessibili all'utente stesso senza alcun rischio, permettendo all'utente di verificare i dati effettivamente trasmessi.

⁵⁰ Il vincolo di 40 bit per gli algoritmi simmetrici (512 per quelli asimmetrici, in pratica con lo stesso grado di robustezza) non è mai stato ufficializzato, ma l'esportazione di prodotti che fanno uso di crittografia era regolamentata e soggetta ad autorizzazione. In pratica, era noto che 40 bit fosse il limite per ottenere l'autorizzazione all'esportazione. Dalla lunghezza della chiave dipende numero massimo di tentativi necessario per scoprire la chiave stessa, ovvero in pratica il tempo massimo necessario per "forzare" un messaggio cifrato. Attualmente, una chiave di 40 bit costituisce una protezione praticamente nulla, ma dieci anni fa richiedeva ancora risorse di calcolo consistenti, seppure abbondantemente alla portata di diverse grosse aziende e dell'agenzia di controspionaggio statunitense (NSA). Già nel 1999, Deep Crack, un sistema realizzato a scopo dimostrativo appositamente per forzare chiavi di 56 bit (circa 65.000 volte più difficili da forzare delle chiavi di 40 bit) costò 200.000 dollari, e avrebbe forzato una chiave di 40 bit in circa quattro secondi.
http://en.wikipedia.org/wiki/40-bit_encryption

escrow⁵¹ e della possibilità che strumenti che lo implementavano potessero essere esportati con più facilità. Nel 1997, secondo il giornale Svenska Dagbladet, la versione di Lotus Notes utilizzata fra l'altro dai parlamentari svedesi, conteneva questo tipo di funzionalità, il che permetteva potenzialmente al governo statunitense di accedere ai documenti cifrati⁵². Questo esempio mostra come una funzionalità introdotta in prodotti ampiamente diffusi possa arrivare a colpire, magari involontariamente, anche le attività più riservate di un governo. Nel caso del TC, non si tratterà presumibilmente di funzionalità volute dal Governo degli Stati Uniti, ma di funzionalità gestite da soggetti privati mediante comunicazioni cifrate⁵³.

La censura

Un altro rischio presentato da più parti è quello della censura, nel senso più ampio del termine: esattamente come è possibile che dei dati possano essere visualizzati con un solo programma, il TC può essere utilizzato per fare sì che un programma impedisca la visualizzazione di certi dati. Sarebbe inoltre possibile non solo escludere l'accesso a dati e programmi dal PC, ma anche cancellare quelli esistenti sul PC stesso. Si parla già di meccanismi di DRM che potrebbero riconoscere file "pirata" e non solo impedirne l'esecuzione, ma anche cancellarli. Anche in questo caso, la decisione di cosa cancellare sarebbe presa da chi controlla il meccanismo di DRM, e non necessariamente riguarderebbe file sui quali ha diritti. È bene precisare che si tratterebbe di una funzionalità di applicazioni di DRM che si appoggia al TC, e non di una funzionalità del TC stesso. Ad esempio, un governo che chiedesse alle aziende che operano sul suo territorio di censurare alcuni contenuti troverebbe un canale perfetto (è noto che molte grosse aziende collaborano ad esempio con la Cina nella sua attività di censura, nel rispetto delle norme locali⁵⁴). Mentre la censura dovuta alle leggi locali può essere considerata legittima (ogni stato ha la sua normativa sulla censura, in costante evoluzione⁵⁵), il problema si pone quando la censura può arrivare da altri paesi, in grado di esercitare pressione sui grandi produttori di software per PC, o dalle aziende stesse, secondo i propri principi ed interessi. A titolo esemplificativo, possiamo considerare il caso del rapporto U.S.A. sul caso Calipari⁵⁶. Per un banale errore tecnico, è stato possibile eliminare le censure apposte al documento; indipendentemente dai contenuti, è stato certamente interessante per l'Italia esaminare il documento completo, evitando le ambiguità di interpretazione che sempre derivano dalle parti censurate. Corrispondentemente, è altamente probabile che gli Stati Uniti sarebbero stati interessati a "ritirare" il documento, non solo dai siti Internet, ma da ogni singolo computer. Con uno strumento come il TC, sarebbe stato possibile, o almeno sarebbe stato possibile ritirarlo dai sistemi su cui fossero attivi ad esempio

⁵¹ Si tratta di un meccanismo grazie al quale la cifratura dei dati è sufficientemente robusta nei confronti di tutti, tranne di chi conosce un particolare segreto (la chiave o una parte di essa, o un altro segreto che permette di scoprire con facilità la chiave). Questo segreto doveva essere consegnato ad un'autorità (nel caso specifico, del Governo degli Stati Uniti). In questo modo, i dati sarebbero stati protetti, ma chi avesse avuto accesso al segreto avrebbe avuto la possibilità (e, nella logica del meccanismo, il diritto) di decifrare i dati.

⁵² <http://catless.ncl.ac.uk/Risks/19.52.html#subj1> L'episodio non fu molto pubblicizzato, e tuttora si trovano pochi riferimenti, fra i quali un articolo di "The Guardian" del marzo 1999 in cui si riporta la conferma da parte di Lotus che la funzionalità era presente nel 1997 in tutte le copie di Notes esportate dagli Stati Uniti <http://technology.guardian.co.uk/online/story/0,3605,305360,00>.

⁵³ Naturalmente questi stessi soggetti potrebbero essere sottoposti a pressioni per rendere accessibile il meccanismo a uno o più governi

⁵⁴ http://www.repubblica.it/2005/f/sezioni/scienza_e_tecnologia/cinaweb/cinaweb/cinaweb.html

⁵⁵ <http://punto-informatico.it/p.asp?i=56927>

⁵⁶ <http://www.repubblica.it/2005/d/sezioni/esteri/niccal3/rror/rror.html>

meccanismi di DRM controllati da aziende degli Stati Uniti disposte a collaborare (o comunque un qualsiasi meccanismo basato sul TC che offrisse un canale di controllo accessibile). Tuttavia, sarebbero state possibili soluzioni di DRM più evolute e meno “chiassose”⁵⁷. Una soluzione flessibile potrebbe ad esempio associare comunque ad ogni documento prodotto il vincolo che non ne possano essere fatte copie non protette dal DRM, comprese copie stampate o modificate. Questo permetterebbe di intervenire a posteriori in caso di problemi, introducendo vincoli più restrittivi che le applicazioni abilitate all’accesso dovrebbero rispettare; queste restrizioni potrebbero appunto ridurre il numero di applicazioni che possono visualizzare il documento (escludendo ad esempio quelle che non ne rispettano le censure), ma potrebbero anche escludere tutte le applicazioni, rendendo di fatto inaccessibile il documento stesso. Il meccanismo di DRM potrebbe costringere anche a richiedere la chiave dal sito del produttore ad ogni nuovo accesso, permettendo quindi di tracciare la diffusione e l’utilizzo del documento stesso. Mentre si può ritenere questo comportamento legittimo in alcuni casi (compreso eventualmente quello del rapporto Calipari), ci si può ragionevolmente chiedere che effetto avrebbe uno strumento di questo genere sulla libertà di stampa o sulla disponibilità di prove in ambito processuale, quando un’entità avesse la possibilità di rendere inaccessibile a posteriori un documento che gli sia sgradito.

La vulnerabilità dei sistemi

Come già detto, le funzionalità del TC permettono di concedere l’accesso ad un documento solo ad un’applicazione non manomessa, ma non proteggono in generale da eventuali difetti dell’applicazione stessa. Supponiamo ad esempio un produttore di contenuti multimediali si appoggi al TC per garantire che solo un certo media player possa accedere ai suoi documenti, e questo media player implementi dei meccanismi che impediscono la copia dei file. Una vulnerabilità nel codice potrebbe comunque consentire la copia dei file, anche con un media player originale e integro e quindi *fidato* secondo il TC⁵⁸. Supponiamo che un utente ritenga che i vincoli imposti dal produttore non siano adeguati (non corrispondono alle normative locali, all’etica dell’utente o semplicemente non sono convenienti). L’utente sarebbe in questo caso invogliato a mantenere vulnerabile il proprio sistema, in modo da poter usufruire delle “funzionalità” offerte dalla vulnerabilità. Questo è una conseguenza diretta del fatto che il TC sottrae il controllo del PC all’utente, e la vulnerabilità, apparentemente, glielo riconsegna in parte: in realtà lo riconsegna a lui e a chiunque sia in condizioni di sfruttarla. Non è interesse di questo documento affrontare le problematiche etiche di questi comportamenti. È bene comunque sottolineare di nuovo che ridurre il tutto a una problematica di pirateria è probabilmente troppo semplicistico, e che si potrebbe invece avere il caso in cui una percentuale cospicua di cittadini, o anche di aziende e persino di Pubbliche Amministrazioni, abbia la vulnerabilità del proprio sistema come unica strada per poter usufruire di un diritto garantito dalle normative locali, e che si trovi a dover rinunciare di fatto a quel diritto a favore della sicurezza dei propri sistemi (basta pensare alle problematiche di censura appena descritte). Quello che è interessante notare è che si potrebbe creare la situazione, apparentemente paradossale, in cui l’utente è interessato a mantenere vulnerabile il proprio PC, anziché a proteggerlo. Una tale situazione creerebbe un ambiente decisamente

⁵⁷ Si ricorda che un meccanismo semplice di DRM che si appoggi al TC sarebbe quello di distribuire il documento in formato cifrato, concedendo poi la chiave di decifratura solo ai sistemi che, tramite le verifiche del TC, siano in grado di dimostrare che aprirebbero il documento con uno strumento abilitato e rispettoso dei vincoli imposti. La chiave verrebbe concessa mediante comunicazioni on-line protette.

⁵⁸ In realtà, sarebbe possibile impedire al media player di scrivere file in senso assoluto, appoggiandosi a un sistema operativo *fidato*. Tuttavia, una vulnerabilità nel sistema operativo potrebbe permettere di aggirare anche questa protezione. Se questo può sembrare improbabile, bisogna considerare che ogni mese vengono pubblicati aggiornamenti per risolvere vulnerabilità di questo tipo.

sfavorevole alla sicurezza di Internet nel suo complesso e all'offerta di servizi attraverso di essa. Un comportamento simile, seppure in forma assai più lieve, si è già visto nell'aggiornamento del firmware di apparati, quando l'aggiornamento elimina delle "funzionalità" non previste, come la possibilità di rendere "region free" un lettore di DVD⁵⁹.

Per contro, alcune entità, in particolare quelle che traggono vantaggio dall'efficacia del TC, potrebbero essere maggiormente interessate a favorire o a forzare l'aggiornamento dei sistemi, eventualmente attraverso un maggiore controllo sulle versioni del software presente sui sistemi stessi; sembra difficile prevedere quale delle due tendenze potrebbe prevalere.

L'abuso da parte di terzi

Quanto visto finora prevede che uno dei soggetti coinvolti decida di abusare dei meccanismi messi a disposizione dal TC. Tuttavia, bisogna anche porsi il problema dell'accesso da parte di terzi al meccanismo, ad esempio attraverso debolezze nel meccanismo stesso o nei siti delle aziende che vi hanno legittimamente accesso.

A questo scopo possiamo considerare il caso del rootkit Sony, che ha suscitato molto scalpore negli ultimi mesi⁶⁰. Il tutto comincia nell'ottobre 2005 con la scoperta che alcuni CD prodotti da Sony, quando eseguiti su un PC, installavano sul PC stesso un programma che risultava poi invisibile e completamente integrato nel sistema, interponendosi fra il driver del lettore di CD e il driver originale. Tutto questo, senza avvertire l'utente, né tantomeno chiederne il permesso. Lo scopo erano funzionalità di raccolta e comunicazione di dati a Sony per la gestione del DRM. La rimozione di questo cosiddetto rootkit rendeva inutilizzabile il lettore di CD, salvo reinstallazione di componenti di Windows. Alla scoperta ne è seguita un'altra, e cioè che il programma apriva le porte a possibili worm e virus, che sono prontamente comparsi⁶¹. Infine, e ironicamente, il rootkit sembra utilizzasse componenti Open Source senza dichiararlo, violandone quindi la licenza d'uso. La vicenda, che ha avuto risonanza mondiale⁶², ci interessa qui per il fatto che la vulnerabilità introdotta da Sony ha favorito la diffusione di worm e virus. Il rootkit aveva caratteristiche analoghe a quelle che ci si potrebbero aspettare da un utilizzo del TC per la gestione del DRM: nascosto e non rimovibile dall'utente senza danneggiare il sistema, controllava le attività svolte attraverso il lettore di CD e comunicando con Sony; il rootkit è stato trovato anche su alcuni sistemi del Dipartimento della Difesa degli Stati Uniti. Il rischio nell'aver strumenti di questo tipo diffusi capillarmente su tutti i sistemi, controllato certamente da più soggetti (ad esempio, ognuno per i diritti sul proprio materiale), è che se la gestione della sicurezza da parte uno di

⁵⁹ Nel valutare la possibilità che l'utente o il cittadino medio facciano ricorso a tecniche di questo tipo, apparentemente troppo sofisticate, è sempre utile ricordare la diffusione che aveva raggiunto in Italia alcuni anni fa l'uso di schede riprogrammabili per accedere gratuitamente ai canali satellitari cifrati di D+/Tele+, con la diffusione di programmatori di EPROM fra persone che mai si erano interessate di elettronica, e con una scarsa riprovazione sociale riguardo a questo comportamento illegale. Non dobbiamo dimenticare che i PC domestici diventeranno presto la piattaforma multimediale attraverso cui fruire dei più diversi contenuti, compresi quelli attualmente forniti via tv satellitare.

⁶⁰ Un riassunto della vicenda, con molti link utili e alcuni interessanti commenti, si può trovare qui: http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

⁶¹ <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ryknos.b.html>

⁶² La vicenda, ha favorito la discussione sull'opportunità di limitare le funzionalità del DRM, vedi ad esempio <http://punto-informatico.it/p.asp?i=57362> In Italia, un'azione come quella di Sony potrebbe violare l'art. 615-quinquies C.P. "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"; è unanime certamente la valutazione dell'operato di Sony come analogo, negli strumenti e nei modi, a quello degli scrittori di virus e worm.

questi soggetti non sarà adeguata, i danni causati attraverso il TC potrebbero essere assai più gravi e diffusi di quelli, tutto sommato limitati, causati dal rootkit Sony.

Il rootkit mostra anche quanto possono essere aggressive le politiche di alcune aziende nell'applicazione di meccanismi di DRM per la tutela dei propri interessi.

Infine, è interessante esaminare i tentativi di portare Linux su Xbox⁶³, la console per videogame di Microsoft. Questo caso mostra infatti quanto impegno è stato messo per mantenere il controllo del software eseguibile sulla Xbox e non solo di quello utilizzato in violazione dei diritti d'autore. Si possono anche notare le analogie con il TC dal punto di vista dei meccanismi, ma soprattutto si può notare che errori implementativi e di progettazione hanno di fatto permesso di violare il meccanismo: nello specifico, permettendo di usufruire pienamente dell'hardware; tuttavia, ci si può chiedere quali sarebbero le conseguenze di un errore di questo tipo nel caso di un TPM al quale si appoggino molte funzionalità di sicurezza di un'azienda. Se è vero infatti che l'hardware è più difficile da manomettere, è anche vero che in caso di vulnerabilità, queste sono assai più difficili da correggere, se non aggiornando (cioè sostituendo) l'hardware stesso.

Altri rischi

Esistono altri rischi che vengono a volte associati al TC, che sono raccolti in questa sezione perché meno rilevanti o di più semplice trattazione.

Realizzazione difforme dalle specifiche. Uno dei rischi paventati è che chi deve poi implementare le specifiche del TCG realizzi i propri prodotti hardware o software in modo difforme dalle specifiche, introducendo ad esempio backdoor⁶⁴ o ulteriori meccanismi di controllo. La cosa è senz'altro possibile, ma non c'è bisogno del TC per farlo; chi ha questa preoccupazione dovrebbe averla anche per i prodotti attuali, di qualsiasi tipo. Ad esempio, è noto che molti BIOS hanno avuto delle password di default che permettevano di aggirare le eventuali password definite dall'utente, tipicamente con la motivazione di facilitare l'assistenza tecnica. Il rischio non è quindi riconducibile al TC, nè sembra che il TC lo debba particolarmente aumentare.

Revoca delle chiavi. Uno dei meccanismi fondamentali nella gestione delle infrastrutture di certificazione è quello della revoca dei certificati. Tuttavia, se il certificato associato a una EK viene revocato, non è chiaro come possa essere ricertificata la stessa chiave, o come ne possa essere certificata un'altra generata internamente al TPM (in generale, è difficile verificare che la nuova chiave provenga effettivamente dal TPM). Il rischio quindi è che in questi casi l'hardware divenga inservibile e debba essere sostituito. Una valutazione di questo rischio richiederebbe però uno scenario molto più chiaro su quali saranno gli utilizzi effettivi del TC.

⁶³ http://www.xbox-linux.org/wiki/17_Mistakes_Microsoft_Made_in_the_Xbox_Security_System

⁶⁴ <http://it.wikipedia.org/wiki/Backdoor>

SEZIONE VI

MA ALLORA, IL TRUSTED COMPUTING È UN PROBLEMA?

Il rischio è reale?

Da quanto esposto, dovrebbe essere chiaro che esistono dei rischi associati al TC. Del resto, è quanto conferma anche il TCG in ([1], pag. 13). Tuttavia, anche se ogni meccanismo di sicurezza può presentare dei rischi, la probabilità e l'impatto associati ai diversi rischi variano, e alcuni rischi sono certamente più concreti di altri: ogni lettore di questo documento avrà considerato più probabili alcuni dei rischi descritti, ed altri meno probabili o addirittura fantasiosi o paranoici. Non ci sono però ragioni tecniche per cui gli scenari esposti non si possano realizzare, e questo è senz'altro un punto importante. Tuttavia, questa è una piccola parte del problema. I punti più discutibili e meno chiari sono certamente molto più di natura economica e sociale. Sicuramente un ruolo importante lo gioca l'etica delle aziende che avranno la possibilità di influenzare l'utilizzo del TC: in qualche caso, i rischi sono direttamente riconducibili alla possibilità per queste aziende di acquisire guadagni o controllo del mercato in modo più o meno legittimo. Su queste problematiche il CLUSIT non si può esprimere, e non è suo compito farlo: compito del CLUSIT è presentare gli aspetti tecnici, in modo che chi vuole o deve gestire questi rischi abbia le informazioni necessarie per comprenderli, ed anche confrontarli con i vantaggi che il TC può fornire nella soluzione di alcuni problemi di sicurezza. La valutazione del rischio deve quindi passare da una discussione aperta che coinvolga tutte le parti interessate: aziende, amministrazioni pubbliche e cittadini, affrontando il problema in un contesto non puramente tecnologico. Un concetto che diventa quindi fondamentale è quello di sicurezza multilaterale, che consiste nel considerare requisiti di sicurezza di parti diverse; questi requisiti possono essere in contrasto fra di loro, rendendo quindi necessario trovare un equilibrio fra le esigenze delle diverse parti. Difficilmente la sicurezza multilaterale viene affrontata correttamente quando la definizione delle specifiche è in mano ad una sola delle parti, che dovrebbe quindi rinunciare volontariamente ad alcune delle proprie tutele a vantaggio di altri. Nel caso del TC, non è chiaro quale o quali delle parti siano rappresentate dal TCG; uno dei problemi generalmente riconosciuti nelle specifiche del TCG è infatti una definizione fumosa e ambigua di quale sia la "sicurezza" che si vuole ottenere, e chi ne tragga vantaggio.

Cosa si può fare per gestirlo?

Se si ritiene che uno o più dei rischi indicati siano eccessivi, è necessario mitigarli.

Anche da questo punto di vista, le soluzioni non possono essere cercate solo nella tecnica informatica: a meno di modificare la natura stessa del meccanismo, questo è pensato per resistere alle interferenze, ed eventuali soluzioni tecniche non possono che limitarne le funzionalità. In questa sezione ci limitiamo ad indicare o a commentare alcune possibili soluzioni, ed a evidenziare alcuni dei limiti delle diverse strade che possono essere percorse. Di nuovo, non è possibile fornire soluzioni "preconfezionate"; l'individuazione di quali siano i rischi da mitigare e quindi di quali siano le soluzioni adatte per mitigarli può scaturire solo da una discussione ampia e non strettamente tecnica del problema.

Soluzioni tecniche

Consistono essenzialmente nell'introduzione di modifiche alle specifiche prodotte dal TCG. L'applicabilità di queste soluzioni è limitata dalla necessità di indurre il TCG e gli

implementatori ad accettare le modifiche. Se con “indurre” si vuole intendere convincere, ci si scontra con la difficoltà nel riconoscere quali siano gli interessi difesi dal TCG, e quindi quali siano le vie corrette per convincerlo a modificare le specifiche. Se invece con “indurre” si fa riferimento ad un obbligo, ci si scontra con lo status del TCG: non è un ente normatore, né l'adesione ai suoi standard è obbligatoria, quindi è difficile trovare una ragione legittima per intervenire sugli standard emessi. Si può forse più facilmente agire sulle implementazioni, ma in questo caso si tratterebbe di imporre dei vincoli almeno a colossi come Intel, AMD e Microsoft; un obiettivo certamente fuori dalla portata dell'Italia, e che anche la Comunità Europea avrebbe difficoltà a raggiungere. Si tratterebbe comunque di una prova di forza che richiederebbe una determinazione notevole a raggiungere lo scopo di modificare le specifiche. In ogni caso, dovrebbe trattarsi di modifiche alle attuali specifiche emesse dal TCG; allo stato attuale non sembra che Intel, AMD e Microsoft siano interessate a modifiche radicali o a specifiche alternative a quelle già in parte implementate nei loro prodotti.

La soluzione tecnica probabilmente più discussa è quella proposta dall'Electronic Frontier Foundation, ovvero il cosiddetto **owner override**⁶⁵: la capacità cioè da parte del *proprietario* di poter *attestare* (nel senso del TC) a terzi lo stato del proprio sistema indipendentemente dai controlli effettuati dal TPM. Questa soluzione riporta in sistema in parte sotto il controllo del *proprietario*, ma ad un costo: lo stato del sistema non è più garantito ai terzi, e questo limita alcuni degli utilizzi del TC. D'altra parte, è proprio questo limite che permette di ridurre alcuni dei rischi. Vediamo quindi più nel dettaglio quali sono le conseguenze.

Prima di tutto, questo meccanismo non cambia i rapporti fra il *proprietario* e l'*utente* del PC. Questo vuole dire che un *utente* non è in grado ad esempio di utilizzare applicazioni non autorizzate dal *proprietario* (e quindi eventualmente di fare copie di documenti aziendali riservati). In generale, eventuali meccanismi che si appoggino a verifiche dello stato del sistema (antivirus ecc.) ma che non si appoggino all'attestazione remota continuano a funzionare. Si tratta senz'altro di una parte considerevole degli utilizzi interessanti del TC. Quello che in parte smette sicuramente di funzionare è il supporto a meccanismi di DRM. Il *proprietario* è infatti in grado di attestare uno stato del sistema diverso da quello reale, inducendo quindi ad esempio un server remoto a fornire le chiavi di decifratura di un file protetto ad un'applicazione che ne potrà fare una copia. Si intende che anche in questo caso, il meccanismo di DRM può essere aggirato solo dal *proprietario*, non dall'*utente*. Nel caso dell'utente domestico, queste due figure coincidono. Nel caso di un'azienda o di una pubblica amministrazione tuttavia, questa è comunque in grado di impedire determinate attività ai dipendenti; in realtà, per l'azienda può essere assai complicato limitare i rischi del TC sui propri sistemi anche in presenza di funzionalità di *owner override*, dato che queste probabilmente dovrebbero essere utilizzate dal *proprietario* di volta in volta sulle singole macchine, e in effetti si può dubitare dell'usabilità e dell'efficacia dell'*owner override* in questi contesti. Un altro caso in cui l'efficacia del TC verrebbe limitata è il rapporto con i consulenti: il *proprietario* dei loro sistemi sarebbe infatti anch'esso in grado di produrre false attestazioni, e di acquisire documenti in applicazioni che ne permettono la copia. Tuttavia, spesso il problema di fiducia non si pone nei confronti del proprietario, ovvero dell'azienda che fornisce il servizio di consulenza, bensì nei confronti dei singoli *utenti*, che potrebbero essere infedeli o eventualmente poco accorti (facendosi rubare il portatile con i dati riservati dei loro clienti). In questi casi, anche in presenza di *owner override* il TC continuerebbe a fornire le garanzie richieste. Questa soluzione ridurrebbe inoltre i rischi di condizionamento del mercato

⁶⁵ http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php

del software, dato che non sarebbe più possibile verificare la presenza di uno specifico software su un sistema. Allo stesso modo, azioni di censura o simili sarebbero molto più difficili da mettere in pratica.

Anche l'*owner override* tuttavia affronta solo in parte il problema dell'identificatore unico costituito dall'EK; si tratta di un problema legato infatti più ai meccanismi di certificazione che all'accesso alle chiavi. Se una Certification Authority certifica solo le chiavi installate dal produttore, allora l'attestazione fatta mediante *owner override* si dovrebbe appoggiare ad una EK generata dal produttore, e quindi il sistema verrebbe comunque identificato. I rischi legati alla privacy non vengono quindi risolti.

In effetti, questi rischi sono più legati alle infrastrutture di certificazione che ai meccanismi hardware. Per aggirare questo meccanismo, sarebbe necessaria una modifica ancora più radicale dell'*owner override*, come ad esempio l'accesso da parte del proprietario alla chiave privata. Mentre questo potrebbe in teoria affrontare correttamente il problema, l'accesso diretto alla chiave porterebbe probabilmente spesso ad un'esposizione della chiave stessa in contesti tali da rendere in pratica inefficace il TC nel suo complesso.

Una soluzione intermedia potrebbe essere quella di registrare la chiave privata non direttamente sul TPM, bensì su una smart card che sia accessibile direttamente al TPM mediante un canale hardware protetto (non è *fidato* nel senso del TC, perché questo richiederebbe la verifica mediante la chiave, che però è accessibile sulla smart card solo dopo che dell'hardware ci si è già fidati). Il TPM dovrebbe conservare al proprio interno una chiave di accesso alla smart card, sottraendone l'accesso all'*utente* ma non al *proprietario*⁶⁶. Questo uso di smart card, che implementa anche implicitamente l'*owner override*, permette di separare l'utente dal PC, e può permettere all'utente di possedere più smart card per servizi diversi. L'adeguatezza di una soluzione di questo tipo non può essere valutata di per sé, ma deve essere vista nell'ottica della sicurezza multilaterale, che in realtà è il primo problema da affrontare. Ad esempio, il canale di comunicazione fra smart card e TPM dovrebbe essere protetto se si vuole garantire che solo il proprietario possa utilizzare l'*owner override*, e non chiunque abbia accesso fisico al sistema, come l'utente. Un aspetto senz'altro positivo sarebbe la possibilità di sviluppare prodotti di questo tipo senza dover modificare il sistema operativo (Windows), e potenzialmente con poche modifiche anche all'architettura hardware dei PC dotati di TPM. In effetti, che un TPM conservi le informazioni internamente o su una smart card ad esso direttamente connessa, potrebbe essere del tutto trasparente al sistema. Una soluzione di questo genere avrebbe il vantaggio di poter rendere disponibili al TPM chiavi specifiche per diversi servizi, prime fra tutte le smart card che si iniziano a diffondere per l'accesso a servizi di E-Government.

Soluzioni di mercato

Intendiamo qui riferirci alle soluzioni grazie alle quali i meccanismi di autoregolamentazione del mercato permettono di mitigare eventuali rischi. Un esempio estremo sarebbe quello in cui i cittadini, ritenuti eccessivi i rischi del TC, non acquistano PC con quella tecnologia, forzando quindi i produttori a rendere disponibili PC che non la implementano. Soluzioni di questo tipo si basano molto sulla capacità dei cittadini di valutare in proprio i rischi del TC e

⁶⁶ Anche nel caso dell'utente domestico, *utente* e *proprietario* è bene che rimangano figure distinte, per quanto possano poi coincidere nella stessa persona fisica, per lo stesso motivo per cui è opportuno che un utente non svolga le proprie normali attività con i privilegi di amministratore, ovvero evitare che programmi malevoli o errori possano approfittare di quei privilegi per danneggiare il sistema.

di agire di conseguenza, in un mercato fortemente dominato da pochi produttori. Perché soluzioni di questo tipo siano praticabili, serve innanzitutto che gli acquirenti di PC siano adeguatamente informati, e che i prodotti che implementano il TC siano riconoscibili. Al momento, la presenza di funzionalità di TC nei prodotti non è generalmente pubblicizzata né riconoscibile. Se questa tendenza rimane, sistemi dotati di TPM si diffonderanno senza che gli utenti se ne rendano conto; nel momento in cui le funzionalità del TC cominciassero ad essere utilizzate (ad esempio unilateralmente da produttori di contenuti per tutelare anche illegittimamente i propri interessi), sarebbe molto più difficile per il proprietario del PC opporsi, se non rinunciando ai servizi basati sul TC.

Interventi correttivi a posteriori basati sulle norme

Una possibilità è quella di lasciare che il TC si diffonda e venga utilizzato, salvo poi intervenire in caso di comportamenti illeciti. In effetti, questa potrebbe sembrare una soluzione corretta; in assenza di comportamenti illeciti infatti, non è ovvio perché si dovrebbe intervenire. Tuttavia, questa scelta si scontra con il già citato rischio di inefficacia sostanziale delle norme. Una volta che il TC sia diffuso, i tempi necessari per eventuali procedimenti e la capacità correttiva di eventuali sanzioni potrebbero essere inadeguati. Vale la pena qui di ricordare che la richiesta fatta a Microsoft di fornire versioni di Windows senza Microsoft Media Player non ha avuto nessun effetto significativo, perché i principali produttori di PC non hanno avuto interesse a distribuire questa versione “menomata”, indipendentemente da quelli che potessero essere gli interessi del mercato del software. Allo stesso modo, la possibilità di disabilitare il TC non avrebbe probabilmente un impatto rilevante se chi offre servizi comunque lo richiede.

Inoltre, come già detto, non sempre le eventuali storture sarebbero facilmente riconducibili ad un illecito. Di nuovo possiamo prendere come esempio il problema frequente di siti web realizzati in modo da essere fruibili solo con Internet Explorer: la nascita di questo problema non è certamente riconducibile ad un accordo di cartello, ma semplicemente alla presenza di un prodotto dominante sul mercato.

Interventi normativi preventivi

Si tratta di utilizzare norme esistenti o di crearne di nuove, in modo da prevenire l'insorgere di situazioni illecite e di rischio eccessivo, anziché tentare di correggerle a posteriori. Potrebbe essere la soluzione migliore, ma anche in questo caso, si pone il problema della praticabilità di questa strada. I tempi disponibili infatti non sono lunghi (i primi sistemi dotati di TPM sono già in vendita), mentre sia la valutazione dei rischi che l'individuazione di contromisure efficaci non sembrano vicini; ogni ritardo può portare le eventuali iniziative a divenire correttive anziché preventive. In effetti, la discussione sul TC è ancora confinata ad ambiti ristretti, e l'interesse delle istituzioni a questo tema non è ovvio. Inoltre, al momento la produzione normativa sembra orientata più alla tutela delle esigenze di DRM dei produttori di contenuti multimediali che alla limitazione della loro capacità di intervenire sui sistemi degli utenti. Infine, la capacità di imporre norme si scontra anche qui con un rischio di inefficacia in un mercato internazionale. Di nuovo, solo l'Europa, e non certo l'Italia, potrebbe avere la forza di imporre norme efficaci. Tuttavia, quali possano essere queste norme non è evidente. Un appiglio può essere la presenza dell'EK come identificatore unico del sistema, riconoscibile attraverso i meccanismi di *attestazione*, che può facilmente portare a violazioni delle normative sulla privacy, pur non costituendo la sua presenza una violazione di per sé. Da più parti è stato proposto di rendere obbligatoria l'indicazione della presenza di TPM nei sistemi,

in modo da facilitare la scelta informata da parte degli utenti; questa misura, di efficacia comunque limitata, può essere messa in pratica rapidamente e probabilmente con poco sforzo. Si tratta comunque di una misura che ha un senso solo se contestualmente i cittadini vengono adeguatamente informati sulle potenzialità e sui rischi del Trusted Computing.

SEZIONE VII

GLOSSARIO

Per approfondimenti sui termini legati alla crittografia, si rimanda al Quaderno CLUSIT “Aspetti di Crittografia Moderna”. Un glossario dei termini relativi al Trusted Computing è disponibile su <https://www.trustedcomputinggroup.org/groups/glossary/>

Access Point: apparato di rete che permette la connessione di sistemi alla rete mediante tecnologie wireless, ad esempio Wi-Fi

Applet: programmi che possono essere caricati ed eseguiti nel contesto di un altro programma; ad esempio, un applet Java può essere inviato da un server Web ad un browser in risposta ad una richiesta, ed essere quindi eseguito dal browser

Attestazione: nel contesto del Trusted Computing, garanzia sulla correttezza di un'informazione, ottenuta attraverso meccanismi di firma digitale

Backdoor: funzionalità nascosta di un programma che permette a chi ne conosca l'esistenza ed il funzionamento l'accesso al programma (e al sistema)

CA, Certification Authority: entità il cui compito è verificare l'identità di soggetti, ed associarla a chiavi pubbliche mediante l'emissione di certificati digitali

Certificato digitale: documento digitale che associa un'identità ad una chiave pubblica; l'associazione è certificata da una Certification Authority mediante firma digitale della coppia identità/chiave

Chiave privata: nella crittografia asimmetrica, è la chiave, parte di una coppia, che viene mantenuta privata, e che viene utilizzata per decifrare i messaggi riservati o per firmare i messaggi

Chiave pubblica: nella crittografia asimmetrica, è la chiave, parte di una coppia, che viene resa pubblica, e che tipicamente viene certificata da una Certification Authority

Chiave segreta: chiave utilizzata nella crittografia simmetrica: la stessa chiave usata per cifrare i messaggi è usata per decifrarli

Common Criteria: Standard (ISO/IEC 15408) per la certificazione delle caratteristiche di sicurezza di un sistema o prodotto informatico

Conformance credentials: credenziali (identità e certificato) che certificano la conformità di un TPM alle specifiche del Trusted Computing Group

Crittografia asimmetrica, algoritmi asimmetrici o a chiave pubblica: insieme di algoritmi crittografici (e loro utilizzo) caratterizzati dal fatto che per la cifratura/decifratura dei messaggi vengono utilizzate due chiavi, generate insieme e legate matematicamente: i messaggi cifrati con una chiave possono essere decifrati (solo) con l'altra

Crittografia simmetrica, algoritmi simmetrici: insieme di algoritmi crittografici (e loro utilizzo) caratterizzati dal fatto che la chiave utilizzata per cifrare i messaggi è la stessa utilizzata per decifrarli

EK: Endorsement Key; coppia di chiavi pubblica/privata, conservata nel TPM e utilizzata per riconoscere da quale TPM è stata prodotta un'informazione, ad esempio in un processo di attestazione.

Firma digitale: da un punto di vista strettamente informatico, si tratta di un'operazione mediante la quale viene calcolato un hash crittografico di un documento, e questo hash viene

cifrato con la chiave privata di una coppia chiave privata/pubblica. L'hash garantisce l'integrità del documento ed è possibile verificare la firma mediante la chiave pubblica (generalmente associata all'identità del firmatario mediante un certificato digitale)

Funzioni di hash crittografico: funzione che, dato un documento di lunghezza arbitraria, ne calcolano un'*impronta* (hash) di lunghezza fissa; ogni modifica al documento comporta una differenza nel valore dell'hash che viene calcolato; questa proprietà viene utilizzata per rilevare modifiche ai documenti: dati infatti un documento ed il relativo hash, non è computazionalmente praticabile l'individuazione di un secondo documento che abbia lo stesso valore di hash.

Infrastruttura di certificazione: infrastruttura che ha lo scopo di permettere alla Certification Authority di ricevere le richieste di certificazione, identificare gli utenti, distribuire i certificati emessi e gestirne la revoca

Key Escrow: meccanismo attraverso il quale gli utenti di uno strumento di cifratura forniscono obbligatoriamente ad un'autorità le informazioni necessarie per accedere con facilità ai dati cifrati (ad esempio, una parte consistente della chiave di cifratura) pur senza indebolire la protezione dei dati nei confronti di terzi

Livelli di privilegio di un processore: meccanismo attraverso il quale viene limitato l'utilizzo delle istruzioni di un processore critiche per il controllo delle risorse del sistema; i livelli di privilegio sono un insieme ordinato di stati del processore: ai livelli più elevati di privilegio, accessibili solo ai processi critici del sistema, corrisponde un insieme più ampio di istruzioni eseguibili

Lotus Notes: Insieme di strumenti software collaborativi e client/server prodotti da Lotus Software, del gruppo IBM

Macrovision: sistema di protezione dalla copiatura per cassette VHS e DVD prodotto dall'omonima società, ottenuto mediante l'aggiunta al segnale video di un segnale che, se ricevuto da un apparato di registrazione compatibile (ad esempio quasi tutti i videoregistratori) in fase di registrazione, disturba e riduce la qualità della registrazione fino a renderla inutilizzabile

Mailer: più propriamente Mail User Agent (MUA) programma personale per la gestione della posta elettronica, come ad esempio Microsoft Outlook o Mozilla Thunderbird

Migratable keys: nel Trusted Computing, chiavi che possono essere trasferite da un TPM ad un altro, a differenza di chiavi, come l'Endorsement Key, che sono legate ad uno specifico TPM e sono dette non-migratable

Open Source Software: software la cui licenza soddisfa i requisiti stabiliti dall'Open Source Initiative, www.opensource.org

Owner: nel Trusted Computing, la figura che può gestire le funzionalità di un TPM e che conosce le chiavi necessarie per farlo

Phishing: tecnica di ingegneria sociale utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli (od anche tramite altre tecniche della suddetta ingegneria sociale), opportunamente creati per apparire autentici. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare informazioni quali numero di conto corrente, nome utente e password, numero di carta di credito ecc.

Profiling: profilazione, analisi di dati relativi ad una persona allo scopo di creare un suo profilo, ad esempio comportamentale

Revoca dei certificati: un certificato garantisce l'associazione fra un'identità e una chiave pubblica; tuttavia, se l'associazione non è più garantita (ad esempio perché qualcun'altro è entrato in possesso della corrispondente chiave privata) è necessario revocare il certificato, ovvero rendere pubblicamente noto che il certificato non è più valido, ad esempio mediante la pubblicazione in una Certificate Revocation List (CRL, Lista di Revoche di Certificati) pubblica

Ring 0: nell'architettura della famiglia dei processori Intel x86, corrisponde al livello più alto di privilegio, al quale possono essere eseguite tutte le istruzioni del processore

Rootkit: insieme di programmi utilizzati da malintenzionati una volta acceduto ad un sistema, allo scopo di cancellare le proprie tracce, nascondere la propria presenza e attività sul sistema, garantirsi un accesso (backdoor) ed eventualmente raccogliere informazioni interessanti sulle attività svolte sul sistema, utili ad esempio per compromettere altri sistemi

Social Engineering, ingegneria sociale: la pratica di manipolare gli utenti (di un sistema informatico) allo scopo di convincerli a violare a vantaggio dell'attaccante le politiche di sicurezza del sistema, ad esempio rivelando informazioni riservate o concedendo l'accesso al sistema

Spyware: tipo di [software](#) che raccoglie [informazioni](#) riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite [Internet](#) ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di [pubblicità](#) mirata.

TCG: Trusted Computing Group; il Trusted Computing Group è un'associazione senza scopo di lucro nata per sviluppare, definire e promuovere standard aperti per “hardware-enabled trusted computing and security technologies” (uso dei computer e tecnologie di sicurezza resi fidati mediante meccanismi hardware)

TCP, Trusted Computing Platform: Un sistema in grado di riportare informazioni sul proprio stato in modo fidato, nel significato utilizzato dal Trusted Computing Group

TPM: Trusted Protection Module; modulo che implementa le funzionalità di base del Trusted Computing (aree di memoria protette, generazione e conservazione di chiavi, generazione di numeri casuali ecc.); in un Personal Computer al momento si tratta tipicamente di un chip saldato sulla scheda madre

User: nel Trusted Computing, la figura che può utilizzare le funzioni di un TPM, ma non gestirlo

Xbox: Console per videogiochi prodotta da Microsoft.

SEZIONE VIII

RIFERIMENTI

Riferimenti principali:

Il sito del Trusted Computing group: <http://www.trustedcomputinggroup.org>

In particolare i documenti:

[1] TCG: Design, Implementation, and Usage Principles, ver. 2.0, Dec. 2005

[2] TCG Specification Architecture Overview, rev. 1.2, Apr. 2004

I membri del TCG: <https://www.trustedcomputinggroup.org/about/members/>

Prodotti: <https://www.trustedcomputinggroup.org/kshowcase/view>

Wikipedia (contiene anche un ampio elenco di riferimenti):

http://en.wikipedia.org/wiki/Trusted_computing

Il consorzio OpenTC: <http://www.opentc.net/consortium>

Critiche e opposizione al Trusted Computing:

Ross Anderson: <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

Bruce Schneier su ZDnet:

<http://opinion.zdnet.co.uk/comment/0,1000002138,39215921,00.htm>

Richard Stallman (trad. in italiano): “Puoi fidarti del tuo computer?”

<http://www.gnu.org/philosophy/can-you-trust.it.html>

The Trusted Systems Project: <http://trusted-systems.info/>

No1984.org <http://www.no1984.org/>

Detective by Design: <http://www.defectivebydesign.org/en/about>

Utilizzo su sistemi Microsoft:

Next Generation Secure Computing Base:

<http://www.microsoft.com/resources/ngscb/default.mspx>

NGSCB technical FAQ:

<http://www.microsoft.com/technet/archive/security/news/ngscb.mspx?mfr=true>

A Cost Analysis of Windows Vista Content Protection:

http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html

BitLocker® http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption

Utilizzo del TC su sistemi Dell:

<http://www.wave.com/csc/ets-support/introduction.htm>

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