UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Edizione italiana a cura di ALSI e Tecnoteca
http://upgrade.tecnoteca.it

Trusted Computing e politiche per la concorrenza – I temi per i professionisti informatici

di
Ross Anderson

(Traduzione italiana a cura di Raffaele Impagnatiello (ALSI – www.alsi.it) dell'articolo
'Trusted Computing' and Competition Policy – Issues for Computing Professionals
pubblicato sul Vol. IV, No. 3, Giugno 2003
della rivista online UPGrade, a cura del CEPIS)

Riassunto italiano: Lo sviluppo strategico più significativo nell'IT nel corso degli ultimi anni è stato il "Trusted Computing" (TC). In questo articolo, l'autore offre una panoramica sul TC, e traccia alcuni dei possibili effetti sul business informatico e sugli operatori del settore.

Parole chiave: antitrust, controllo degli accessi, copyright, DMCA, EUCD, Intel, Microsoft, monopolio, NGSCB, Palladium, politiche per la concorrenza, TCG, TCPA, vincoli.

1. Introduzione

Uno dei problemi più complessi che gli informatici devono affrontare è far fronte alle strategie che i fornitori seguono per estrarre fino all'ultimo centesimo dai loro clienti. I fornitori dominanti, come oggi la Microsoft e l'IBM nella scorsa generazione, cercano di legare i clienti alle loro architetture, in modo da estendere il controllo da un prodotto all'altro. Molti prodotti seguono un ciclo di "entra a buon mercato e poi aumenta"; infatti, dopo che avete impegnato la vostra organizzazione ad usare una particolare smart card, o pacchetto di contabilità, i prezzi – misteriosamente – salgono.

Un'altra strategia è il "vincolo tra prodotti" (*product tying*); un esempio evidente è il caso delle cartucce di inchiostro per le stampanti. Le stampanti sono sussidiate dalle cartucce: questa combinazione permette ai venditori di affrontare con gli stessi prodotti gli utenti aziendali con alti volumi e gli utenti privati attenti al risparmio. Questo livello di sussidiarietà incrociata viene limitato dalle cartucce ricaricabili e da quelle compatibili (third party). Attualmente molte cartucce includono chips che le autenticano rispetto alla stampante, modalità iniziata dalla XEROX N24 nel 1996 (v. [5] per una storia dei chip per le cartucce). In un caso tipico, se la stampante individua una cartuccia compatibile può, senza preavviso, abbassare la prestazione da 1200 dpi a 300 dpi, o anche può rifiutarsi di stampare. Uno sviluppo ancora più recente riguarda la data di scadenza. Le cartucce per la HP BusinessJet 2200C scadono dopo una permanenza di 30 mesi nella stampante, oppure dopo quattro anni e mezzo dalla data di fabbricazione [3], il che ha provocato le proteste dei consumatori [4].

Le "cartucce vincolate" stanno conducendo ad una guerra commerciale tra USA ed Europa. Negli Stati Uniti, un tribunale ha emesso una ordinanza che impedisce al produttore di stampanti Lexmark di vendere cartucce che interoperano con le stampanti della Lexmark stessa. Nel frattempo, il Parlamento Europeo ha approvato una "Direttiva sui rifiuti di apparati elettrici ed elettronici" che ha lo scopo di obbligare gli stati membri a dichiarare illegali, entro il 2006, le attività delle ditte intese ad aggirare le regole della Unione Europea sul riciclaggio, mediante chip nei prodotti che servono ad impedire il riciclaggio stesso [8].

Il controllo post vendita ed il "vincolo tra i prodotti" stanno rapidamente aumentando, tramite ogni sorta di meccanismi. I produttori di telefonini spesso guadagnano di più vendendo le batterie, rispetto al telefonino stesso, e quindi hanno introdotto dei chip di autenticazione che rendono difficile l'uso di batterie dei concorrenti [10]. I produttori di auto usano formati di dati proprietari per impedire ai clienti le riparazioni presso officine indipendenti [12]. E le ditte di videogiochi si sono fatte pagare per anni le royalties per gli sviluppatori software, usandole ora per sussidiare le vendite delle consolle [11].

Queste pratiche sono positive o negative per il mercato? La risposta, secondo gli economisti è "*Dipende*". Hal Varian sostiene che sul vincolo tra cartucce e stampanti non ci sono, da un punto di vista di politica commerciale, troppe obiezioni, perché il mercato delle stampanti è ancora competitivo e quindi vincolare le cartucce con le stampanti porta i venditori a competere più intensamente per vendere le stampanti, portando a prezzi più bassi di mercato [9].

Comunque, se i meccanismi di vincolo sono usati per collegare due mercati per i quali la concorrenza è relativamente bassa – ad esempio il mercato dei sistemi operativi e quello dei web server – ciò può diminuire le opportunità di scelta e far aumentare i prezzi. Questa era una delle obiezioni rispetto al Microsoft Passport, fatta sulla base delle politiche per la concorrenza. Gli intermediari che volevano adottare Passport, erano costretti ad usare anche i web server Microsoft.

I venditori ora possono realizzare più facilmente i controlli post-vendita e delle complesse politiche dei prezzi, grazie all'introduzione del "Trusted Computing" (elaborazione fidata).

2. Il Trusted Computing

A giugno 2002 la Microsoft ha annunciato il Palladium, una versione di Windows che realizza il Trusted Computing, il cui rilascio è previsto nel 2004. In questo contesto *trusted* vuol dire che, rispetto al software che è in esecuzione su quel PC, un terzo può *fidarsi*, cioè può verificare che il programma in esecuzione sulla macchina con cui sta comunicando non è stato modificato dal proprietario della macchina. I programmi saranno in grado di comunicare tra loro in modo sicuro e con i loro autori. Questo apre un certo numero di interessanti possibilità.

Una ovvia applicazione è il DRM (Digital Rigths Management – gestione dei diritti sugli oggetti digitali): la Disney sarà in grado di vendervi DVD che si decritteranno su una piattaforma Palladium, ma dei quali non potrete fare delle copie. Le case discografiche saranno in grado di vendervi dei download che non si potranno scambiare. Vi potranno vendere CD che, ad esempio, potrete eseguire solo tre volte, oppure solo alla data del compleanno. Queste applicazioni sono discutibili, altre meno. Per esempio, le piattaforme di trusted computing possono eseguire giochi in cui è difficile barare.

Il sistema Palladium si basa sul lavoro della TCPA (Trusted Computing Platform Alliance) comprendente Microsoft, Intel, IBM e HP come membri fondatori. Si è ora aggiunta la AMD e l'iniziativa è ora rilanciata come TCG (Trusted Computing Group) [13]. Il TCG propone una riprogettazione dell'hardware dei PC, in cui la CPU acquisisce un ulteriore livello di privilegio (che

permette ad alcuni processi di accedere a zone di memorie vietate anche al superuser) ed un componente hardware di sicurezza (il "Fritz chip") che monitorizza quali software e hardware girano sulla macchina. I "Fritz chip" delle macchine possono comunicare tra di loro. Nel sistema ecologico *trusted* il ruolo del Fritz è di assicurare i terzi che la vostra macchina è quella che voi dite che essa sia, e che su di essa è in esecuzione proprio il software che voi affermate che sia in esecuzione.

Non tutti accettano la definizione di "trusted computing" (elaborazione fidata) per questa tecnologia. La Microsoft preferisce chiamarla "trustworthy computing" (elaborazione affidabile): questo perché se voi vi fidate di un sistema, ciò non lo rende affidabile. Ad esempio, se un impiegato della National Security Agency viene visto in un bagno dell'aeroporto di Washington mentre vende materiale critico ad un diplomatico cinese, allora – supponendo che l'operazione non fosse autorizzata – noi possiamo definirlo "trusted but not trustworthy" (fidato – o supposto tale per il suo ruolo - ma non affidabile). Infatti la definizione della NSA di *trusted system* è "un sistema che può violare la politica di sicurezza". Da un altro punto di vista del dibattito, Richard Stallman della Free Software Foundation preferisce la definizione di *treacherous computing* (elaborazione sleale) poiché il vero scopo della tecnologia del Trusted Computing Group è di sottrarre al possessore il controllo pieno del PC [15].

Nel seguito di questo articolo si userà la sigla TC, che il lettore, a seconda delle sue opinioni, potrà pronunciare come *trusted* computing, oppure *trustworthy* computing, oppure *treacherous* computing.

2.1 Il controllo e la Governance

Se il proprietario di un computer non è più in grado di controllarlo completamente, allora il grande interrogativo è dove va a finire questo controllo. Su questa domanda le ditte coinvolte nel TC hanno espresso opinioni diverse in tempi diversi. Le specifiche iniziali (TCPA 1.0) suggerivano una gerarchia di autorità di certificazione, per certificare i vari componenti hardware e software che potevano costituire un sistema di TC. Il controllo sarebbe stato gestito centralmente da un consorzio di industrie.

La posizione attuale delle industrie è che sarà demandato ai venditori di applicazioni TC o dei contenuti usati dalle stesse, di decidere quali combinazioni di hardware e di sistemi operativi sia accettabile. Ad esempio, nel caso della gestione dei diritti di oggetti digitali (DRM) sarà la Disney – o forse la Microsoft in qualità di venditore del Media Player – che dovrebbe certificare le particolari piattaforme adatte alla visualizzazione di Biancaneve. Le regole che una particolare applicazione sarà in grado di stabilire deriveranno alla fine da un server gestito dal fornitore di applicazioni, ad esempio le etichette per i CD commerciali con la specifica "copia vietata", oppure "permessa una sola copia di backup", oppure – per i film diffusi via etere – "registrazione consentita per la visione differita; copia vietata".

3. Valore per gli utenti aziendali e della Pubblica Amministrazione

I server per la sicurezza delle applicazioni possono specificare un ampio spettro di politiche. Ad esempio un sistema TC usato per imporre livelli di protezione per le informazioni governative classificate, può avere una politica centrale per cui le informazioni possono solo muoversi verso l'alto, così che le parti di un file "confidential" possono essere copiate in un file "secret", ma non viceversa. Ma la realizzazione adeguata di controlli di flusso ad una via è difficile[1]; quindi è improbabile che essi siano le killer application per il TC.

L'uso di sistemi di TC per proteggere i segreti aziendali serve per promuovere l'agenda del TC. *"È una cosa singolare"*, ha detto Bill Gates, *"Abbiamo ideato questo pensando alla musica, ma poi abbiamo pensato che le e-mail e i documenti erano campi di applicazioni più interessanti*" [19]. Una prima implementazione dei meccanismi di gestione dei diritti che può essere applicata nei modi suddetti per il controllo di informazioni riservate, al contrario di cose di altro tipo come musica e video, è stata recentemente rilasciata in Windows Server 2003 [16].

Windows Server 2003 consente al creatore di un documento o altro tipo di file di mantenere il controllo su di esse indipendentemente da dove verrà successivamente spostato. Sarà possibile mandare una e-mail con restrizioni, ad esempio che il destinatario non potrà ridirigerla, o stamparla, o potrà leggerla solo se in possesso di apposito nulla osta di sicurezza, oppure che il documento sarà leggibile solo alla fine del mese. Gli utenti di Windows che vogliono il TC devono registrarsi ad un servizio online che – sembra – deciderà se mettere o meno a disposizione una chiave di decodifica all'applicazione. (Ciò è stato appena annunciato alla data di stesura di questo articolo, e i dettagli devono ancora essere chiariti.)

Uno dei punti chiave per vendere questa tecnologia è che una ditta può prescrivere che le e-mail interne diventino illeggibili dopo 90 giorni. La Microsoft ha già questo tipo di regola al suo interno. Viste le tattiche di inchiesta sempre più aggressive usate nelle controversie, può essere comodo per gli uffici legali aziendali il trattare le e-mail come conversazioni telefoniche piuttosto che come lettere.

Ma anche una semplice applicazione può essere complicata nel suo diffondersi nella realtà. Uno studio legale potrà essere riluttante ad accettare istruzioni da un cliente tramite e-mail che solo uno degli avvocati può leggere, che non possono essere stampate, e che diventeranno illeggibili dopo 90 giorni. In che modo lo studio potrà proteggersi da accuse di patrocinio infedele, e che garanzie sono possibili per gli altri partner?

Non è tutto. Le leggi sulle esportazioni di varie nazioni richiedono che le ditte conservino copie delle comunicazioni con le quali viene esportato il software, i documenti ed il know-how di oggetti presenti nella lista di prodotti a duplice uso civile-militare; ciò vuol dire conservare gli e-mail rilevanti per tre anni. Le regole di contabilità possono richiedere la conservazione degli e-mail per sei anni. Si possono prevedere rilevanti dispute tra le politiche che prescrivono la distruzione e quelle che prescrivono la conservazione. Come tutti i manager di sistemi informativi sanno, è un vero campo minato affrontare l'automazione di quelle procedure che prima evitavano i conflitti lasciando abbastanza discrezionalità umana per le questioni difficile da rattoppare.

4. Il valore per i possessori dei contenuti

Le case discografiche e cinematografiche hanno fatto notevoli azioni di pressione a favore di meccanismi di TC, per supportare sistemi più rigorosi di gestione dei diritti di oggetti digitali. Esse hanno già ottenuto una maggiore protezione legale per i sistemi esistenti, e sostengono che le copie di oggetti digitali distruggerebbero i loro affari; questa argomentazione sta perdendo efficacia, dal momento che si è visto che le copie dei CD, semplici da eseguirsi ormai da diversi anni, non hanno avuto un impatto rilevante sulle vendite. Ad una attenta analisi, non è chiaro se un meccanismo più rigoroso della gestione di diritti digitali come quello promesso dal TC possa fornire guadagni sostanziali per i proprietari dei contenuti rispetto allo status quo [20].

Esiste anche un rischio significativo; nel caso in cui i sistemi TC si diffondessero, la controparte potrebbe usarli più facilmente. Gli utenti potrebbero creare delle "reti clandestine" per scambiarsi materiale proibito di vario tipo, e sarebbe più facile creare sistemi "peer-to-peer" come gnutella o mojonation, che sarebbero però molto più resistenti agli attacchi da parte delle case

discografiche, poiché solo i "veri clienti" sarebbero in grado di partecipare. I metodi attuali per attaccare le "reti clandestine", tramite attacchi di service denial che partono da client infettati con Cavalli di Troia, non funzionerebbero più. In tal modo, al realizzarsi del TC, secondo la legge delle conseguenze non volute, le case discografiche potrebbero diventare vittime invece che beneficiarie.

5. Il valore per i venditori di hardware

L'esperienza dimostra che i meccanismi di sicurezza spesso favoriscono gli interessi di coloro che pagano per essi, piuttosto che gli interessi dei clienti, a beneficio dei quali si suppone che siano sviluppati [1]. Per esempio, l'introduzione della autenticazione e della cifratura nel telefonini GSM venne propagandata ai clienti come una maggiore sicurezza, in contrapposizione ai telefonini analogici, che erano facili da clonare ed intercettare. Comunque, un'esperienza più maturata mostra che i maggiori beneficiari sono stati i gestori telefonici che hanno investito negli sviluppi per la sicurezza.

Con i vecchi telefonini analogici, chi voleva chiamare gratis, oppure defraudare il sistema tramite i servizi a pagamento, poteva farlo clonando l'apparecchio, e quindi causando una perdita per le aziende telefoniche. Con il sistema GSM, i delinquenti comprano gli apparecchi usando carte di credito rubate (scaricando i costi sulle banche) oppure, sempre di più, usano telefonini presi tramite rapine alle persone (il che è un costo ancora maggiore per il cliente). Per quanto riguarda la privacy, la quasi totalità delle intercettazioni è gestito dai servizi segreti, che in ogni caso riescono ad ottenere la voce in chiaro dalle dorsali telefoniche.

Tali esperienze ci suggeriscono di esaminare il probabile effetto del TC sul business dei suoi promotori.

Nel caso della Intel, l'incentivo a partecipare al TCPA era strategico. Poiché l'Intel ha la maggior parte del mercato dei microprocessori, da cui trae gran parte dei suoi profitti, essa può soltanto crescere se il mercato dei PC cresce. L'Intel ha quindi sviluppato un programma di ricerca per realizzare una "superiorità nelle piattaforme", in cui essa è in testa agli sforzi dell'industria nello sviluppo di tecnologie che rendono i PC più utili, ad esempio il bus PCI e l'USB [23].

Il lato positivo di questa strategia è stato che l'Intel ha fatto crescere il mercato complessivo dei PC; il lato negativo è che ha usato accordi vincolanti di cross-licensing per impedire che i concorrenti potessero raggiungere una posizione dominante nelle tecnologie che avrebbero potuto minacciare il suo controllo sull'hardware dei PC. I cinici sottolineano che l'Intel non poteva permettersi che il bus microchannel dell'IBM prevalesse: esso non era solo un mezzo di connessione della piattaforma hardware dei PC, ma l'IBM non aveva interesse a fornire l'ampiezza di banda necessaria ai PC per competere con i sistemi high-end. In termini di strategia, l'effetto è in qualche modo simile alla pratica degli antichi romani di demolire tutte le abitazioni e tagliare gli alberi ai margini delle loro strade e dei loro castelli. L'approccio della Intel si è evoluto in un modo molto efficace di circoscrivere le leggi antitrust.

6. Il valore per i venditori di software

Il caso della Microsoft è ancora più interessante. Nel suo progetto originale, il TC ha la potenzialità di eliminare direttamente il software senza licenze: una piattaforma TC, che comunica direttamente con un servizio centrale di autorizzazione, potrebbe semplicemente rifiutare di eseguire il software senza licenza. Il meccanismo usato per registrare il software potrebbe essere reso molto difficile da aggirare: il *Fritz chip* mantiene una lista dei componenti hardware e dei componenti del software di sistema di una macchina TC, e si prevede che ciò possa essere verificato ondine.

A seguito di alcune proteste pubbliche, la Microsoft ora afferma che non saranno introdotti meccanismi del tipo "lista nera" – almeno per il livello di sistema operativo [17]. Pare che il Windows 2003 si basi su meccanismi molto più raffinati. Il controllo non sarà più esercitato dal basso tramite l'hardware TC, ma dall'alto, tramite le applicazioni. La Disney sarà libera di decidere in che termini fornire i contenuti ai sistemi costituiti da particolari hardware e software; se la Disney imporrà i prezzi di 12,99$ per la versione DVD di Biancaneve, 9,99$ per un download su un sistema TC/Windows con Media Player, e rifiutarsi del tutto di fornire i contenuti per altre piattaforme, allora la Microsoft potrà affermare alla stampa e alle autorità antitrust che è stata una loro decisione.

Gli incentivi che ne derivano sono fortemente a favore della Microsoft. Se TC/Windows diventa la piattaforma dominante, molti sviluppatori forniranno prima i loro prodotti su Windows e poi su Mac (se mai lo forniranno), nel caso in cui fosse chiaro che il mercato dei PC è sbilanciato nella direzione dell'accoppiata Wintel. Non ci sorprende che la Apple stia cercando di battere la Microsoft in velocità, lanciando il suo servizio di download per i media.

6.1 L'importanza delle applicazioni

Sembra che la Microsoft stia investendo nel corredare la piattaforma del sistema operativo con meccanismi TC, per mietere ricavi attraverso un maggiore introito dalle sue applicazioni. Questo può essere diretto (ad esempio raddoppiando il costo di Office) o indiretto (ad esempio prendendo una percentuale su tutti i contenuti comprati tramite il Media Player). Dal punto di vista della concorrenza, tutto dipenderà da quanto sarà difficile per le altre ditte rendere le loro applicazioni e i loro contenuti interoperanti con le applicazioni e i contenuti Microsoft. È interesse Microsoft rendere questa interoperabilità il più difficile possibile.

Se i servizi di abbonamento alla musica usano Media Player, e il Media Player alla fine richiederà una piattaforma TC, allora gli abbonati avranno la necessità di migrare su di essa, altrimenti perderanno l'accesso alla musica già memorizzata. Naturalmente, una volta che l'uso di applicazioni TC si diffonde, con molti utenti vincolati ad esse, potranno essere implementati meccanismi di controllo delle licenze che saranno difficili da superare, tanto quanto la tecnologia sottostante sarà difficile da violare. Il modello di business potrebbe quindi seguire quello adottato pionieristicamente dalla Nintendo e da altri produttori di consolle per videogiochi, in cui il software costoso sussidia l'hardware a buon mercato. Le caratteristiche dei sistemi operativi TC saranno allora solo un componente sussidiario di abilitazione la cui funzione vera è di massimizzare il reddito di prodotti costosi come Office, i giochi ed il noleggio dei contenuti.

Se il controllo obbligatorio sugli accessi alle e-mail diventerà una diffusa pratica aziendale nell'ambito di Windows 2003, e questo controllo degli accessi richiederà alla fin fine una piattaforma TC, allora le aziende non avranno altra scelta che migrare. Infatti, esse avranno meno alternative rispetto agli abbonati ai servizi musicali. Gli appassionati di musica possono sempre uscire e comprare nuovi CD, come hanno fatto quando i CD hanno rimpiazzato il vinile; ma se molti documenti arrivano ad essere protetti con chiavi crittografiche, le aziende non potranno fare altro che seguire i meccanismi che proteggono e controllano le chiavi.

6.2. I costi dei vincoli e della conversione

Il ruolo dei costi di conversione nella valorizzazione delle ditte di beni e servizi informatici è stato riconosciuto solo negli ultimi anni. Nel industrie dominate dal vincolo per il cliente (***lock-in***) come l'industria del software, il valore netto attuale del parco clienti è uguale al valore totale dei costi di conversione che essi affronterebbero se passassero al fornitore concorrente [22]. Se il valore

fosse più alto, il concorrente potrebbe invogliare i clienti con bustarelle a passare ai suoi sistemi. Se il valore fosse più basso, la ditta può semplicemente aumentare i prezzi.

Uno degli effetti del TC è di aumentare le possibilità di lock-in. Supponiamo ad esempio che un direttore dei sistemi informativi non voglia più comprare Office, e voglia far usare OpenOffice su GNU/Linux. Attualmente deve affrontare i costi di un addestramento al nuovo software, il suo costo di installazione ed il costo di conversione dei file esistenti. Ci potrebbe essere, in corso d'opera, il costo di occasionali incompatibilità. La teoria economica suggerisce che questi costi sarebbero circa uguali al costo delle licenze di Office.

Comunque, con il TC i costi di conversione dai formati di Office ad altri formati possono aumentare grandemente [24]. Potrebbe non esistere alcun meccanismo o procedura per esportare un contenuto TC ad una piattaforma non-TC, anche se questo fosse pienamente autorizzato dal proprietario dei contenuti. Se esistessero i mezzi per questo tipo di esportazione, potrebbero non essere sufficienti di per sé stessi, se diventassero ampiamente usati i controlli sugli accessi realizzati con il TC. Questo perché la maggior parte dei dati degli archivi aziendali può essere marcata come appartenente agli altri.

Per esempio, uno studio legale può ricevere dai suoi clienti dei documenti confidenziali, riservati all'attenzione solo di alcuni avvocati dello studio. Lo studio legale potrebbe insistere sul diritto di mantenere l'accesso ai documenti per sei anni, nell'eventualità che esso si debba difendere da accuse di patrocinio infedele. Questo tipo di accordo può essere codificato negli attributi per la gestione dei diritti del documento, e imposta usando i meccanismi del TC. Le regole di accesso possono essere cambiate solo dal possessore del documento, cioè della persona che lo ha creato.

In seguito, se lo studio legale volesse migrare da Office e Windows a OpenOffice su una piattaforma TC/Linux, esso dovrebbe ottenere dai loro clienti il permesso di migrare tutti i documenti protetti. Uno studio legale di qualunque dimensione gestisce migliaia di relazioni professionali, alcune delle quali diventano conflittuali; anche se le situazioni logistiche e politiche sono accettabili per chiedere alle controparti il permesso di migrare i documenti, alcuni clienti quasi certamente non sarebbero cooperativi, per vari motivi. Piaccia o no, lo studio legale sarebbe incastrato, nel senso di mantenere un ambiente TC/Windows assieme al nuovo sistema.

Ci sono conseguenze sia sull'hardware che sul software. Ad esempio, le controversie relative al TC possono accrescere l'incertezza, che a sua volta può portare le aziende ed i consumatori al punto di vista del "meglio il diavolo che conosciamo". Il risultato può essere un incremento dei costi di conversione anche superiore a quello che deriva dalla tecnologia. (I più anziani ricorderanno le controversie sulle parole chiave del marketing IBM "paura, incertezza e dubbio" quando l'IBM, al posto della Microsoft, regnava nel pollaio.)

6.3 I temi dell'antitrust

C'è quindi una chiara prospettiva che il TC si affermi usando un effetto a rete, e che le principali applicazioni TC diventino in pratica impossibili da sfidare da parte di un concorrente, una volta che esse siano diventate dominanti in un particolare settore.

Questo getta nuova luce sulle note argomentazioni nelle dispute antitrust per l'industria informatica. La competizione "per il mercato" è stata ritenuta ugualmente equa da molti economisti, al pari della competizione "all'interno del mercato", specialmente a causa della natura volatile dell'industria e a causa delle opportunità nascenti a intervalli di pochi anni per i concorrenti, dal momento che il progresso insidia i vecchi standard e inventa nuovi settori industriali. Ma se sarà possibile vincolare le grandi e crescenti quantità di dati applicativi che le aziende e i consumatori

memorizzano, in modo che chi ha la posizione dominante del mercato (*incumbent*) diventerà impossibile da sfidare direttamente, allora le argomentazioni di cui sopra dovranno essere rivedute.

In ogni caso, l'incentivo per la Microsoft è chiaro. Il valore dell'azienda dovrebbe corrispondere all'incirca ai costi – diretti e indiretti – che i suoi clienti affronterebbero passando ai concorrenti. Se il passaggio ai concorrenti diventa doppiamente difficile, allora il valore del software business della Microsoft raddoppia.

Ci sono ulteriori punti. Hal Varian ha già sottolineato che il TC può ridurre l'innovazione, diminuendo le opportunità tecniche di modificare i prodotti esistenti [9]; e le cose peggioreranno una volta che i dati delle applicazioni saranno vincolati. Attualmente, molte ditte emergenti di software cercano di ingrandirsi fornendo modalità aggiuntive di usare i grandi insiemi di dati delle applicazioni nei formati più diffusi. Una volta che i fornitori delle principali applicazioni abbracciassero il TC, ci sarebbe tutto l'incentivo per essi a guadagnare tramite l'affitto dei dati. Ciò sembra favorire le grandi ditte rispetto alle piccole, i leader di mercato rispetto agli sfidanti, e in generale sembra soffocare l'innovazione.

Altri produttori di applicazioni software non solo affronteranno la minaccia di essere esclusi dall'accesso ai dati delle applicazioni di altri venditori, ma avranno anche l'aspettativa che se diffondono il loro prodotto ed hanno molti clienti che lo usano per gestire i propri dati, possono usare i meccanismi di TC per vincolare questi clienti in modo più stretto di quanto era possibile con i vecchi sistemi dei formati proprietari dei dati. Questo aprirà la prospettiva di valutazioni molto più alte per le ditte e quindi molti produttori di software avranno forti pressioni per adottare il TC. Il treno in corsa sarà inarrestabile.

Alcuni settori specifici dell'industria potrebbero essere colpiti duramente. Ad esempio i produttori di smart card hanno la prospettiva che molte applicazioni che speravano di colonizzare con i loro prodotti, invece potranno girare sulle piattaforme TC dei PC, dei PDA e dei telefonini. L'industria della sicurezza informatica in generale affronterà uno smembramento, poiché molti prodotti saranno o migrati al TC o abbandonati.

È difficile trovare delle corrispondenti analogie storiche. Forse la più simile è il passaggio dalla navigazione nei canali alle ferrovie, nel 1830 circa. Mentre chiunque con una barca poteva trasportare un carico, le ferrovie sono molto di più di un monopolio naturale, e a quel tempo incontrarono proprio tali obiezioni. Le ferrovie non erano in alcun modo un disastro economico, ma portarono ad una concentrazione di potere economico e di abusi sulla concorrenza che alla fine condussero in alcune nazioni a specifiche leggi anti-trust, e in altre il passaggio in mano pubblica.

È difficile fare previsioni a lungo termine, ma nel breve è ragionevole aspettarsi che gli effetti economici del TC comporteranno probabilmente una tendenza del gioco economico contraria alle piccole ditte e in favore delle grandi; uno slittamento a favore dei leader contro coloro che vogliono entrare nel mercato; maggiori costi e rischi associati alla partenza di nuovi business. Un modo di vedere questa situazione è che l'industria dell'informatica e delle comunicazioni diventerà simile a settori industriali più tradizionali come l'auto e i farmaceutici. Ciò potrebbe rivelarsi tutt'altro che un chiaro beneficio.

7. Quali implicazioni per i professionisti IT ?

Per molto tempo, gli esperti della sicurezza si sono lamentati che né i produttori di hardware, né quelli di software ponevano molto interesse nell'incorporare protezioni nei loro prodotti. Alcuni lavori preliminari nel campo dell'economia della sicurezza ora mostrano qual'era il motivo [25]. I costi fissi alti, il basso costo marginale, gli elevati costi del passaggio alla concorrenza e l'effetto a

rete incontrato da molte aziende della IT, hanno condotto a ditte dominanti grazie ai vantaggi di essere entrate per prime nei mercati. Il time-to-market è critico, e la filosofia Microsoft del decennio 1990 *"lo spediremo mercoledì e funzionerà correttamente con la versione 3"* era perfettamente razionale.

Inoltre, quando si è in competizione per un mercato a rete, le ditte devono far ricorso a venditori di beni e servizi complementari. Così i produttori di sistemi operativi hanno pochi incentivi a fornire meccanismi complessi di controllo degli accessi, poiché questi se li ritrovano gli utenti nelle applicazioni. Lo scarso potere contrattuale degli utenti finali, se raffrontato a quello dei produttori di beni e servizi complementari, ha portato le aziende ad adottare tecnologie (come la PKI) che consentono ai produttori di applicazioni di scaricare sugli utenti i costi della sicurezza e della amministrazione. Il controllo delle interfacce delle applicazioni è critico per il produttore della piattaforma, e quindi è meglio che l'interfaccia sia proprietaria, complicata, estensibile e quindi piena di errori. Inoltre, data l'assenza di una conoscenza diffusa sulla sicurezza, l'effetto "bidone" ha causato comunque la cacciata dei prodotti buoni da parte dei prodotti scadenti.

Cosa ha fatto improvvisamente cambiare l'orientamento della Microsoft?

I commentatori cinici potrebbero sostenere che la recente composizione del caso antitrust da parte del Ministero della giustizia degli Stati Uniti obbliga la Microsoft a condividere le informazioni sulle interfacce ed i protocolli, ad eccezione dei casi che coinvolgono la sicurezza. Quindi c'è l'incentivo a ridefinire tutto ciò che la ditta produce come critico per la sicurezza. La Microsoft ha anche sostenuto che il recente pubblicizzare i diversi tipi di attacchi alla rete è stato un incentivo per questa politica. Ma sicuramente un *worm* o due all'anno non possono giustificare un cambiamento così significativo di politica e di orientamenti.

In questo articolo sosteniamo che un altro fattore importante della recente decisione Microsoft di spendere somme a nove cifre per la sicurezza informatica, dopo averla virtualmente ignorata per decenni, è la prospettiva di vincolare a sé sempre di più i clienti. (Si noti che Intel, AMD, IBM e HP stanno facendo investimenti significativi nel TC, anche se non ci sono minacce di interventi antitrust.)

Ci sono molti altri temi sollecitati dal TC, dalla censura alla sovranità nazionale, al destino del "digital commons" e al futuro del movimento per il software libero e open source. Ma gli uomini d'affari avveduti vedranno probabilmente il TC attraverso le lenti delle politiche sulla concorrenza. La domanda cruciale è "In che modo tutto ciò permetterà alla Microsoft di spillarmi più soldi?". La risposta, abbastanza semplicemente è questa: "Vincolandoti ancora più strettamente ad usare piattaforme Microsoft, come ad esempio Office".

Cosa potrebbero fare i legislatori e le Autorità indipendenti? Forse alcuni precedenti possono essere trovati nelle leggi sui brevetti. Per anni, se un contratto nel Regno Unito aveva vincoli illeciti, causava la non validità di un brevetto; ad esempio se io ho il brevetto per un processo di molitura, e concedo la licenza ad un altro, a condizione che egli compri tutto il grano da me, allora con quel tipo di contratto ho reso il mio brevetto non valido nei confronti del contraente (e di tutti gli altri). Alla fine, si potrebbe ipotizzare che le protezioni legali apparentemente fornite dalla DMCA, dalla EUCD (direttiva europea sul diritto d'autore) e dai meccanismi di TC che pretendono di far rispettare il diritto d'autore, dovrebbero essere considerate inefficaci nel caso in cui siano usati per scopi anti-concorrenza, come ad esempio il controllo degli accessi oppure i crescenti vincoli per il consumatore.

Come alternativa, noi suggeriamo che il test che il legislatore può fare è se i meccanismi TC aumentano o diminuiscono il surplus per il consumatore. Questo è lo stesso tipo di test che

suggerisce la letteratura sulla risoluzione dei conflitti sui brevetti abusivi [26]. Data l'argomentazione che il TC creerà valore per i consumatori, e la netta aspettativa che lo creerà anche per i venditori, e tutto il polverone di accesi argomenti sui torti e ragioni della gestione dei diritti di oggetti digitali, forse se il test per i consumatori finirà bene o male può essere il modo più semplice e pratico per arrivare a degli indirizzi politici consistenti e forti.

Riferimenti

[1] R.J. Anderson, 'Security Engineering – a Guide to Building Dependable Distributed Systems', Wiley (2001), ISBN 0– 471– 38922– 6.

[2] R.J. Anderson, "TCPA/Palladium FAQ". <http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>.

[3] M. Magee, "HP inkjet cartridges have built-in expiry dates – Carly's cunning consumable plan", The Inquirer, 29 April 2003. <http://www.theinquirer.net/?article=9220>.

[4] "Ink Cartridges with Built-In Self-Destruct Dates", Slashdot. <http://slashdot.org/articles/03/04/30/1155250.shtml>.

[5] "Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future", Static Control, Inc. <http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm>.

[6] "Lexmark invokes DMCA in Toner Suit", Slashdot. <http://slashdot.org/article.pl?sid=03/01/09/1228217&mode=thread&tid=123.

[7] "Prepared Statements and Press Releases", Static Control, Inc. <http://www.scc-inc.com/special/oemwarfare/lexmark_vs_scc.htm>.

[8] M. Broersma, "Printer makers rapped over refill restrictions", ZDnet Dec 20 2002. <http://news.zdnet.co.uk/story/0,,t269– s2127877,00.html>.

[9] H.R. Varian, "New Chips Can Keep a Tight Rein on Customers", New York Times July 4 2002. <http://www.nytimes.com/2002/07/04/business/04SCEN.html>.

[10] "Motorola Announces Availability of New Wireless Phone Batteries for Increased Performance and Safety, Featuring New Hologram Design", Motorola Press Release, July 23, 1998; eliminato dopo essere stato citato in [2]; ora reperibile in <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/mototola_battery_auth.html>.

[11] D. Becker, "Sony loses Australian copyright case", on CNN.com, July 26 2002. <http://rss.com.com/2100– 1040– 946640.html?tag=rn>.

[12] N. Pickler, "Mechanics Struggle With Diagnostics", AP, June 24 2002; previously at radicus.net; eliminato dopo essere stato citato in [2]; ora reperibile in <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/car-diagnostics.html>.

[13] Trusted Computing Group, <http://www.trustedcomputinggroup.org/>.

[14] J. Lettice "Bad publicity, clashes trigger MS Palladium name change", The Register, Jan 27 2003. <http://www.theregister.co.uk/content/4/29039.html>.

[15] R. Stallman, “Can you trust your computer?”. <http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19>.

[16] Microsoft Corp., “Windows Server 2003”, Feb 20, 2003. <http://www.microsoft.com/windowsserver2003/rm>.

[17] J. Manferdelli, “An Open and Interoperable Foundation for Secure Computing”, in Windows Trusted Platform Technologies Information Newsletter March 2003.

[18] A. Huang, “Keeping Secrets in Hardware: the Microsoft Xbox Case Study”, May 26, 2002. <http://web.mit.edu/bunnie/www/proj/anatak/AIM–2002–008.pdf>.

[19] P. Thurrott, “Microsoft’s Secret Plan to Secure the PC”, WinInfo, June 23, 2002. <http://www.wininformant.com/Articles/Index. cfm?ArticleID=25681>.

[20] S. Lewis, “How Much is Stronger DRM Worth?” at Second International Workshop on Economics and Information Security. <http://www.cpppe.umd.edu/rhsmith3/index.html>.

[21] S.E. Schechter, R.A. Greenstadt, M.D. Smith, “Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment”, at Second International Workshop on Economics and Information Security. <http://www.cpppe.umd.edu/rhsmith3/index.html>.

[22] C. Shapiro, H Varian, ‘Information Rules’, Harvard Business School Press (1998), ISBN 0-87584–863–X
(traduzione italiana: C. Shapiro, H. Varian, ‘Information rules: le regole dell’economia dell’informazione’, ETAS, Milano, 1999)

[23] A. Gawer, M.A. Cusumano, “Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation”, Harvard Business School Press (2002), ISBN 1–57851–514–9.

[24] J. Brockmeier, “The Ultimate Lock-In”’, Yahoo News. Mar 12, 2003. <http://story.news.yahoo.com/news?tmpl=story2&cid=75&ncid=738&e=9&u=/nf/20030312/tc_nf/20982>.

[25] R.J. Anderson, “Why Information Security is Hard – An Economic Perspective”, in Proceedings of the Seventeenth Computer Security Applications Conference IEEE Computer Society Press (2001), ISBN 0–7695–1405–7, pp 358–365. <http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf>.

[26] C. Shapiro, “Antitrust Limits to Patent Settlements”, preprint. <http://faculty.haas.berkeley.edu/shapiro/settle.pdf>.

Ross Anderson guida il security group del Computer Laboratory della Università di Cambridge, Regno Unito. È Fellow dell’ Institution of Electrical Engineers e dell’Institute of Mathematics and its Application. Ha prodotto documenti molto noti sui temi delle politiche di sicurezza, dalla riservatezza in medicina ai sistemi bancari, e anche sulle tecnologie connesse come la crittografia e l’impedimento delle intercettazioni. È autore del libro “Security Engineering – a Guide to Building Dependable Distributed Systems”. Presiede la Foundation for Information Policy Research.
<Ross.Anderson@cl.cam.ac.uk>