

# Proprietà Intellettuale: una questione di fiducia

La fiducia e il tradimento nella società dell'informazione

FRANCESCO GADALETA

5 giugno 2005

Copyright (c) 2005 Francesco Gadaleta.

E' garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della Licenza per Documentazione Libera GNU (ne è proibita quindi la distribuzione commerciale), Versione 1.1 o ogni versione successiva pubblicata dalla Free Software Foundation;

con le Sezioni Non Modificabili *Introduzione, Trusted-Computing - licenza di uccidere la libertà* .

Non è acclusa una copia della licenza, reperibile dal sito di GNU o softwarelibero cercando "Licenza per documentazione libera GNU".

*Il segreto della creatività è  
saper nascondere  
le proprie fonti.  
Albert Einstein*

*A Maria*

*Per rendere la cosa più chiara, dimentichiamo per un momento i calcolatori, i programmi e compagnia: siamo stati condizionati a pensare a queste cose come necessarie, ma difficili; siamo stati abituati, cioè, a rinunciare a formarci un'opinione personale perché, ci viene detto, è troppo complesso, e dobbiamo limitarci a seguire le scelte operate da sedicenti esperti (sulla rivista americana *Byte*, che ha una larga diffusione, c'è anche un logo "Byte, because the expert decide" "Byte, perché decidono gli esperti").*

*Lasciamo un momento questi esperti ai loro intralazzi per andare a vedere che cosa succede nel mondo parallelo dei TecnoCretini in cui un'azienda, chiamiamola MacroPresse, ottiene a poco a poco il controllo assoluto di tutte le tipografie del pianeta.*

*Quest'azienda non controlla direttamente i giornali, ma è lei che li stampa con dei caratteri MacroStampa, di cui è la sola proprietaria.*

*Un bel giorno, dopo una grande campagna pubblicitaria che tesse le lodi di un nuovo insieme di caratteri che permetterà di ottenere dei giornali più moderni, essa comincia a stampare tutto con dei caratteri klingoniani<sup>1</sup> di modo che nessuno riesce più a leggere i nuovi libri o giornali senza ricorrere alla Lente MacroStampa, disponibile alla vendita in tutte le edicole, in cui è distribuita a spese degli editori di giornali.*

*Il pubblico, affascinato dalla meravigliosa novità tecnologica, si adatta e compera la Lente.*

*Incoraggiata dal successo di questa iniziativa, MacroStampa comincia a cambiare i caratteri periodicamente, ogni anno, poi ogni sei mesi: la vecchia Lente non riesce a leggere i nuovi giornali, e quindi occorre rinnovarla a caro prezzo ogni due o tre mesi.*

*Un concorrente di MacroStampa vede lì un'occasione d'oro: produrre una Minilente molto meno cara di quella della MacroStampa e venderla nelle edicole.*

*Ma le edicole hanno un contratto in esclusiva con MacroStampa, e rifiutano di distribuirla.*

*Peggio, MacroStampa cita in giudizio il concorrente, colpevole d'aver analizzato i caratteri klingoniani per costruire una MiniLente, in violazione del copyright di MacroStampa, e vince.*

*Il mondo dei tecnocretini non è così lontano!*

Roberto di Cosmo, 29

Giugno 1998

---

<sup>1</sup>*l'alfabeto dei Klingons nella famosa serie di fantascienza Star Trek*

# Indice

0.1	Introduzione . . . . .	5
0.2	Il legame azienda-cliente . . . . .	7
0.3	Trusted-Computing, licenza di uccidere la libertà . . . . .	9
0.3.1	Che cosa è il TC? . . . . .	9
0.3.2	L'amico Fritz . . . . .	12
0.4	I problemi etici . . . . .	14

## 0.1 Introduzione

Caratteristiche primarie della società dell'informazione sono state, sin dal principio, l'*evoluzione rapida* e imperterrita e la *superficialità*.

E' sempre esistita quella spinta verso il rinnovamento dei sistemi e soprattutto dei principi alla base di quell'informazione da tutti raggiungibile anche senza reali motivazioni.

Abbiamo assistito per anni ai cambiamenti che i cosiddetti esperti hanno definito cruciali, per la nostra società.

Quella società che avrebbe dovuto rivelarsi la società equa, nella quale l'informazione sarebbe stata a disposizione di tutti ed in cui il relativismo gnoseologico avrebbe fatto da protagonista, in realtà si è rivelata come la società dei *tecnocretini*.

Obiettivo dei maggiori *vendors*, gli esperti dell'informatica, i pionieri della società del terzo millennio, è stato quello di creare lo standard del decennio per privatizzare algoritmi e protocolli.

Tecnicamente un algoritmo è un insieme di operazioni elementari che un calcolatore può eseguire per la risoluzione di un problema;

il protocollo consiste invece in un insieme di regole alla base di un processo comunicativo quale può essere una chat, una conversazione telefonica ma soprattutto una semplice (semplice lo è solo in questi ultimi anni) trasmissione numerica (scambio di documenti in formato elettronico tra due o più calcolatori).

*Chiudere* un protocollo o un algoritmo è sempre stata un'operazione tanto spregiudicata quanto efficace per impedirne la lettura e comprenderne il funzionamento.

La mobilitazione verso questa politica ha caratterizzato fortemente questi dieci anni di tecnologia tanto esasperata.

L'evoluzione della società dell'informazione non è sempre stata positiva, come spesso si apprende dalle *riviste del settore* oppure dalla televisione in quei *programmi specializzati* in cui l'esperto di turno ha la pretesa di raccontare i dieci anni più complessi della rivoluzione telematica in un'ora scarsa - interrotta ogni quindici minuti dalla pubblicità - ad un pubblico sempre più superficiale.

I due problemi macroscopici, visibili, senza la necessità di studi approfonditi, sono essenzialmente due:

la *non-evoluzione* e la *nascita dei tecnocretini*.

Il primo - sicuramente il più nascosto tra i due - è notoriamente presente nelle realtà aziendali, in particolare i semplici istituti di credito nei quali i calcolatori continuano ad eseguire gli stessi processi di dieci anni or sono senza caduta di prestazioni o instabilità nel calcolo.

L'evoluzione tecnologica ha avuto quell'importanza tanto acclamata solo nelle percentuali, inizialmente piccole ed improduttive, che hanno sostituito il vecchio monopolio e il gioco dell'oca.

Schede video accelerate per il 3D, software sempre più potente per il calcolo dei poligoni che compongono un personaggio tridimensionale,

schede audio che suonano in dolby surround non fanno certo parte delle realtà aziendali che *producono*.

Ma piuttosto di una fetta di mercato, inizialmente di nicchia, che si è sviluppata in seguito proprio per evitare il problema stesso della *non-evoluzione*.

Il problema a mio avviso più grave, che ha letteralmente deteriorato la società moderna è la nascita dei tecnocretini, popolazione, purtroppo, in continuo aumento, progettata nei laboratori di Redmond ed oggi distribuita uniformemente sul pianeta.

L'aspetto più subdolo della rivoluzione telematica consiste in quel processo di controllo mediante cui i signori dell'informazione riescono a vincolare, spiare e sfruttare i cosiddetti end-users cioè i comuni mortali del paradiso telematico, i soldati semplici dell'esercito dell'informazione, coloro a cui non è dato sapere!

Numerosi sono i casi di privati ed imprese che hanno acquistato impianti informatici senza avere idea delle limitazioni e dei controlli a cui si sarebbero sottoposti immediatamente dopo l'acquisto.

Con questo non voglio avere la presunzione di criticare il sistema dell'offshore, ormai d'obbligo per le grandi aziende.

Ma l'atteggiamento, da sempre assunto nei confronti del software è sempre stato, a mio avviso, superficiale.

Quando un medico prescrive un medicinale, il paziente medio si preoccupa di conoscerne il principio attivo perchè ne andrebbe di mezzo la propria salute se dovesse esserne allergico.

Sarebbe impensabile consultare un medico la cui risposta potrebbe essere "Prenda questo sciroppo e non si preoccupi".

L'analogia con il mondo dell'informatica è immediata se si pensa alla coppia pc-software come al mezzo attualmente più evoluto, efficace e efficiente per conservare i propri dati personali che vanno dalla mail della fidanzata al conto corrente, dalla rubrica telefonica alla banca dati dell'ufficio anagrafe.

I signori dell'informazione hanno capito subito che il mezzo dalle tre 'e', *e*-voluta *e*-fficace *e*-fficiente, sarebbe stato un'ottima fonte di guadagno ma soprattutto di controllo.

L'errore dei *comuni mortali* è stato quello di sottovalutare le potenzialità della coppia pc-software e, parallelamente, sopravvalutare il gioiellino tecnologico del momento, pubblicizzato a palla da quella televisione sempre più vuota di idee e più piena di merda.

Visibilmente la società dell'informazione è in preda alla prostituzione della tecnologia!

Francesco Gadaleta

## 0.2 Il legame azienda-cliente

Lo stravolgimento dell'economia mondiale ha portato le grandi aziende del settore informatico a rivisitare le proprie politiche per la cura del cliente.

L'economia moderna non permette più di valutare un'impresa in base all'ormai classico bilancio annuale ma piuttosto in base al legame più o meno forte con i clienti.

Un legame forte con tanti clienti garantisce, almeno in parte, la sopravvivenza dell'impresa nel nuovo mercato, veloce e binario.<sup>2</sup>

Legare un cliente alla propria architettura vuol dire instaurare un rapporto duraturo con quest'ultimo, alla totale (o quasi) dipendenza dell'azienda e dei suoi prodotti.

Questo nuovo meccanismo di sussistenza ha causato un rafforzamento del legame azienda-cliente, esasperato e per questo contro ogni etica sociale.

I primi esempi di questo fenomeno sono stati i vincoli stampante-cartuccia, cellulare-batteria, ma ancor prima automobile-pezzi di ricambio.

E' ormai consuetudine acquistare stampanti a un minor prezzo rispetto ai prodotti di consumo e batterie appositamente studiate per un particolare modello di telefonino.

Si è instaurata insomma una dipendenza, più che un legame, molto forte tra prodotti.

La politica della dipendenza, alla base dell'economia moderna, circoscritta al mondo dell'informatica è riscontrabile nel legame cliente-software.

Una delle più memorabili è stata la politica di Micro\$oft con il pacchetto MS-Office.

Quando si progettava il software attenendosi alle regole dell'antitrust si pensava alla sua vita, breve, dopo la quale si sarebbe dato spazio ai prodotti di altre software houses.

La politica di Micro\$oft, semplice e spregiudicata, è stata quella di imporsi in un mercato giovane - senza alcuna concorrenza - e vincolare i clienti del suo prodotto, Office.

Una fase iniziale ha visto Micro\$oft imporsi letteralmente sul mercato utilizzando la stessa politica di dipendenza che l'ha portata poi in tribunale.

Lo scacco matto è stato raggiunto mediante una serie di semplici mosse:

legare il cliente ai suoi stessi dati (tipicamente testuali), tramite un

---

<sup>2</sup>Con prodotti diversi cambiano anche i tempi del mercato, definito più volte binario non solo per la natura del prodotto ma soprattutto per la tolleranza zero verso le aziende che non sanno imporsi o per mancanza di fondi o capacità (nel mercato o sei 1 o sei 0 - *dal film Synapsis* ).

software dinamico a cui cambiare periodicamente l'algoritmo di formattazione;

super pubblicizzare il prodotto saturando fiere ed appuntamenti annuali;

far conoscere il prodotto alle istituzioni governative.

Bingo!

Se le leggi dell'antitrust prevedevano un ricambio molto frequente nel mercato dell'informatica, nel quale si reputa obsoleto un software di pochi mesi di vita, dopo lo scacco matto di Microsoft le cose sono profondamente cambiate.

Non è più possibile fare le affermazioni di qualche anno fa che consideravano un software *vecchio* dopo poco tempo dando spazio ad altre software houses per produrne uno migliore ed aggiornato.

Oggi vi è un legame nei confronti del documento creato con il software, in modo che cambiando il software il documento non risulti più leggibile.

Quindi non interessa più l'applicazione per generare il documento ma l'informazione generata da quell'applicazione e cioè il documento stesso.

L'interesse primario del comune mortale non ricade sull'applicazione ma sulla possibilità di trattare i vecchi documenti con il nuovo software di videoscrittura.

La diffusione fuori norma di Microsoft Windows, il sistema operativo con la s e la o minuscole, ha annientato la concorrenza, facilitando il piazzamento sul mercato dei fratelli Office e Internet Explorer<sup>3</sup>.

A diffusione avvenuta, per i principi di dipendenza esposti finora è facile intenderne il valore commerciale.

Microsoft Word è, a tutti gli effetti, una forma primitiva di dipendenza cliente-prodotto; solo il precursore meno evoluto di un fenomeno, molto più pericoloso, che si sta sviluppando in questi ultimissimi anni: il Trusted-Computing.

---

<sup>3</sup>Tengo a ricordare che la morte di Netscape e moltissime altre piccole società di cui semplicemente non si ha notizia, è stata causata dalla distribuzione scorretta, secondo le norme dell'antitrust, del browser per Internet letteralmente regalato con il sistema operativo Windows.

La concorrente Netscape vendeva il proprio prodotto Netscape Navigator a poco meno di 100\$.

Annientata!

## 0.3 Trusted-Computing, licenza di uccidere la libertà

Il TC<sup>4</sup> ha ereditato la politica di Microsoft, sfruttando a pieno le nuove tecnologie.

Obiettivo principale è sempre lo stesso: controllare i clienti dopo la vendita del prodotto.

Questo, come precedentemente affermato, è il maggiore cambiamento dell'assetto economico relativo alla società dell'informazione: dopo la vendita il rapporto con il cliente non è ancora terminato.

Anzi comincia!

Le grandi società hanno già provveduto a giustificare la necessità del TC richiamando l'antico bisogno di maggior sicurezza.

Ai più acuti, in realtà si è rivelato subito un affare ancora più redditizio del fenomeno Word che, per le ragioni che vedremo vincolerà ancora di più il cliente finale.

### 0.3.1 Che cosa è il TC?

Ma che cosa è il trusted computing?

Visto da vicino appare come l'ennesima trovata innovativa che giustifica l'eccesso di tecnologia.

Frutto di un'alleanza di Microsoft, Intel, IBM, HP e AMD - che nulla hanno mai fatto per garantire i diritti del piccolo programmatore essendo loro i massimi vendors da sempre sul pianeta - il trusted computing ha come obiettivo la sicurezza in ambito informatico.

Si apre un dualismo di opinioni nel quale i puristi della sicurezza si considerano soddisfatti.

Molto meno gli utilizzatori finali delle piattaforme che vedrebbero annullato il controllo delle proprie macchine.

Infatti, mediante il trusted computing sarebbe possibile controllare - nel vero senso del termine - quasi completamente le macchine su cui viene installato software trusted.

I signori dell'informazione hanno capito che la nostra società sta diventando sempre più *cablata*.

Cablata, dal loro punto di vista, vuol dire portare ogni persona ad utilizzare fortemente i nuovi mezzi per la comunicazione digitale (anche se sovradimensionati per il tipo di informazione da comunicare) di cui hanno attualmente il pieno controllo.

Esempi di città cablata venivano fatti da Carlo Massarini nel programma MediaMente [4] su RaiTre che mi appassionava tenendomi incollato al televisore dopo le 5 ore di lezione al Liceo.

Era il 1996 e parole come privacy, etica, diritto, tutela non erano entrate nel nuovo vocabolario della rivoluzione telematica.

---

<sup>4</sup>Trusted-Computing, da ora TC

Eppure quelli erano gli anni del boom, in tutto il mondo!

Si badava ai numeri: “ Si stendono cinquanta chilometri di fibra per connettere tre nodi strategici ... si riducono così i costi della rete mantenendo costante la banda a 155 Megabit...” erano discorsi all’ordine del giorno.

Nessuno ha mai parlato dei problemi che una cablatrice di massa avrebbe portato se fosse stata controllata in modo sbagliato.

Insomma quello che Noam Chomsky aveva previsto riguardo al fenomeno della televisione e di programmi disarmanti per alimentare il gregge disorientato - da non istruire per tenerlo lontano da ogni decisione - a tutti gli effetti si è verificato, in modo meno evidente, nella creazione di servizi online per il pubblico.

Non vorrei apparire come un tragicomane paranoico.

Ma sembra che si siano gettate le basi per beneficiare degli effetti collaterali, inaspettati e ovviamente difficilmente prevedibili.

Il cuore del trusted computing è infatti il mezzo che oggi usiamo più del telefono e dei libri messi insieme: **la rete**.

Analizzo qualche aspetto tecnico per permettere al lettore una sommaria comprensione sull’argomento.

Dal punto di vista hardware i trusted computers saranno dotati di un chipset dedicato (approfondimenti in 1.3.4) alla cosiddetta sicurezza e di una memoria separata dalla CPU centrale<sup>5</sup>.

La presenza di una chiave hardware o di una smartcard saldata sulla motherboard di un calcolatore sarà in grado di reperire informazioni sulla macchina sin dal bootstrap, la sequenza di avvio che precede il loading del sistema operativo.

La chiave hardware sarà ovviamente affiancata a un apparato software complesso quanto basta: un kernel di sicurezza in ciascuna applicazione trusted ed ovviamente l’interlocutore di tale kernel, costituito da uno o più server di back-end gestito dai vendors stessi.

In modo molto banale - per smentire la tanto acclamata innovazione tecnologica - il chip hardware altro non fa che memorizzare le caratteristiche della macchina corrente (tipo di hardware a bordo, versione del sistema operativo, licenze del software installato eccetera) e generare una hash, chiave univoca.

A questo punto se il bootstrap termina in uno stato approvato, il chipset di sicurezza renderà disponibili le chiavi per decifrare le applicazioni e i dati trusted.

In caso contrario tutto il materiale protetto non sarà accessibile.

Il kernel del sistema operativo, appositamente modificato rispetto ad un comune kernel, fa da tramite fra chipset di sicurezza e server di back-end: controlla se tutto il materiale presente sul calcolatore sia registrato legalmente, se i numeri seriali di qualche applicazione sono stati revo-

---

<sup>5</sup>L’utilizzo di una memoria separata da quella centrale è indispensabile per impedire ai debuggers di visionare - debuggare in gergo - il codice macchina e, mediante reverse engineering di copiare il software di controllo.

cati e se ci sono cambiamenti non trascurabili nell'hardware dovrebbe ri-registrare la macchina sul server di back-end.

Inoltre servendosi della memoria separata dalla CPU, il kernel impedirà ad un'applicazione trusted di leggere dati generati da applicazioni non trusted.

Alla faccia della compatibilità!

Dal punto di vista del business il trusted computing risulta terribilmente vantaggioso per coloro che oggi sono già i grandi vendors.

Un esempio eclatante che spiega le potenzialità del TC, è quello della Disney.

Sarà possibile infatti che il server di Disney ci consenta di visionare un film *Disney* solo se dotati di un particolare hardware *Disney*, oppure di un software chiamato *Disney Media Player* acquistabile nei migliori negozi *Disney*.

Sarà possibile affittare applicazioni oppure regalare un mp3 alla fidanzata che suoni solo il giorno del suo compleanno oppure darle un'immagine visionabile solo ed esclusivamente dal suo personal trusted computer, oppure...

Un'azienda chiamata Microsoft sta applicando una politica aziendale tramite la quale tutte le email interne vengono distrutte dopo sei mesi.

Mediante il TC sarà possibile estendere questa magnifica trovata a tutte le aziende che utilizzano prodotti Microsoft.

Tutte quelle aziende che potenzialmente erano in grado di nascondere informazioni imbarazzanti sui loro bilanci troverebbero qualcuno che risolve il problema.

In effetti il logo pubblicitario non dice niente di diverso: *Microsoft. Your potential. Our passion.*

Un effetto immediato del TC è l'annientamento totale della concorrenza. Dove per concorrenza si intende soprattutto la piccola azienda, nuova nel mercato, con grandi potenzialità ma inizialmente con pochi mezzi.

TC sarà un vantaggio solo per le aziende con un presenza forte nel mercato che orienteranno gli utenti sugli applicativi di loro produzione, molto facilmente.

Mediante TC, Microsoft potrebbe ad esempio incrementare esageratamente i costi per passare dai prodotti Microsoft a prodotti di concorrenza.

Oggi infatti uno studio legale che voglia passare a OpenOffice<sup>6</sup> dovrebbe installare il software, formare i dipendenti e convertire i file esistenti (con le ultime versioni di OpenOffice è assolutamente automatico in quanto c'è quasi totale compatibilità).

Con il TC le cose si complicheranno perchè per convertire i documenti esistenti, lo studio legale dovrà avere il permesso (tramite certificati digitali) da ogni singolo cliente con cui ha avuto rapporti e scambi di documenti in passato.

---

<sup>6</sup>Il clone opensource della suite MS Office, reperibile su <http://www.openoffice.org>

Praticamente impossibile visti anche gli inevitabili rapporti conflittuali (tipici di uno studio legale) !

### 0.3.2 L'amico Fritz

Questo articolo non vuole avere la pretesa di spiegare un argomento complesso come la crittografia, in poche pagine.

Ma avvicinare i non addetti ai lavori, all'argomento.

Il chip alla base della piattaforma crittografica dei trusted computers ha un nome: *Fritz*.<sup>7</sup>

Inizialmente si è pensato di saldare il chip sulle schede madri, il componente fondamentale di un personal computer, a cui connettere tutti gli altri componenti (altrettanto importanti) come scheda video, audio, schede di rete, ma anche tastiera e mouse.

Successivamente si penserà di includerlo direttamente nelle CPU.

Il funzionamento del chip Fritz è schematizzato nella figura 1, descritta nelle righe che seguono.

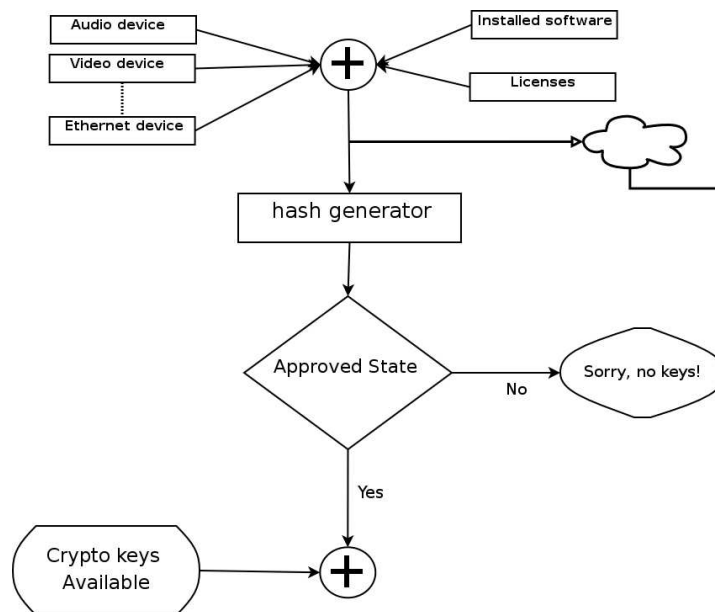


Figura 1: dettagli del chip Fritz

Tutti i dispositivi presenti sulla macchina (scheda audio, video, rete eccetera...) ma anche il software installato (numero di versione, intestario, data di installazione eccetera) e le licenze relative vengono date in

---

<sup>7</sup>dal nome del senatore Ernest "Fritz" Hollings, il quale ha condotto campagne per la difesa della proprietà intellettuale nell'era digitale negli USA, *massimo esportatore di democrazia nel mondo*.

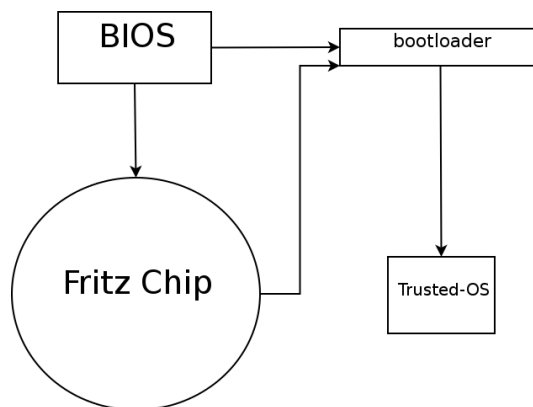
pasto ad un *hash generator* (generatore di hash) che genera appunto una chiave univoca di  $N^8$  bit.

A questo punto il sistema verifica la chiave generata e se questa porta ad uno *Approved State*, cioè se l'hardware installato rispetta la volontà di chi eroga il servizio (Disney per esempio) e soprattutto se il software è stato rigorosamente acquistato in negozio (licenza registrata e non scaduta) vengono rilasciate le chiavi per decifrare i dati presenti sulla macchina (tra questi sono compresi anche i dati che noi stessi abbiamo generato con le applicazioni installate, anche un semplice file di testo).

L'*Approved State* può essere fornito direttamente da un server remoto a cui il chip Fritz si collega comunicando la chiave hash generata in precedenza.

Si intuisce quindi quanto complesso sarebbe violare un sistema cifrato di questa tipologia.

Facendo un passo indietro schematizzo l'avvio del sistema trusted, il *trusted bootstrap* nella Figura 2.



**Figura2: interazione del chip Fritz con il bootloader**

Il primo chip che si occupa di controllare i dispositivi hardware installati sul sistema è il BIOS.

In un sistema trusted il BIOS sarebbe collegato direttamente al chip Fritz.

Compito fondamentale del BIOS è quello di far partire il bootloader il quale a sua volta si occupa di caricare il sistema operativo.

Come è facile intuire tutto il meccanismo di loading del sistema operativo verrebbe controllato indirettamente dal chip Fritz il quale sarebbe

---

<sup>8</sup>Il numero di bit della chiave dipende da quanto complesso si vuole il sistema. Un numero di bit molto grande ha il vantaggio di memorizzare molta più informazione e quindi di fare controlli più efficaci su tutte o quasi le caratteristiche della macchina. Ovviamente aumentando le dimensioni dell'hash aumenta la complessità del sistema di cifratura. Ma questo è un compromesso che si accetta volentieri pur di conoscere quanta più informazione possibile di un utente.

in grado di bloccare il processo in qualsiasi momento secondo le direttive del server remoto.

Ignorare il chip Fritz significherebbe non disporre delle chiavi per decifrare e quindi, ancora una volta risulterebbe impossibile usufruire dei dati che lo stesso possessore della macchina avrebbe generato.

Il criterio che non solo permette al chip Fritz di funzionare, ma soprattutto di farlo a insaputa dell' utilizzatore della macchina è molto semplice: si gestisce memoria dedicata, separata dal contesto globale.

Cioè parte della memoria disponibile viene dedicata al chip Fritz.

In questo modo, caricando il sistema operativo su uno spazio di indirizzamento diverso da quello di Fritz sarebbe:

- Impossibile fare debug e quindi scoprire i dettagli della computazione all'interno del chip.
- Impossibile modificare il software durante la sua esecuzione poichè esso risiede in uno spazio di indirizzamento sconosciuto dal punto di vista del sistema operativo (e quindi dell'utente che lo utilizza<sup>9</sup>).
- Impossibile fare reverse engineering per gli stessi motivi di cui sopra.

Quindi tutto l'apparato informatico si trasforma nella cosiddetta black box, di cui all'utente non è dato sapere!

## 0.4 I problemi etici

Una lista delle situazioni tragicamente possibili dopo la diffusione spudorata del Trusted Computing:

- Tutti gli mp3 finora scaricati potrebbero non essere più leggibili poichè la macchina trusted potrebbe rifiutarsi di suonare tutti gli mp3 che non hanno un header approvato dal server remoto.
- Uno studio legale afferma di possedere tutti i documenti necessari per la causa di Lunedì prossimo ma dal momento che in studio si è deciso di utilizzare un software di trattamento testi diverso, anche perchè più economico, non è più possibile presentarsi in tribunale con i suddetti documenti.
- Come mai questo dvd non si vede più sul questo computer? Ah adesso ricordo! L'ho visto già 5 volte.

---

<sup>9</sup>Cosa non sempre chiara all'utente finale: cio' che utilizziamo di un calcolatore è l'applicazione la quale tramite il sistema operativo richiede risorse hardware come memoria, disco, rete eccetera. L'utente non utilizza mai il sistema operativo. Perchè esso non esegue nulla di interessante se non allocare risorse per le applicazioni.

Come è facile intuire, non ci sono limiti all'immaginazione.

Tutto quello che in questo momento si teorizza potrebbe divenire una realtà dura da accettare nel momento in cui il trusted computing verrà diffuso in modo globale, per esempio riducendo i prezzi delle macchine trusted rispetto all'hardware *normale*.<sup>10</sup>

Ciò che oggi è definito trusted computing, ieri si chiamava Microsoft Word.

Alla base di entrambi c'è il desiderio di controllare l'utente in ogni momento cercando di prevenire l'utilizzo di software libero, piuttosto che curarlo.

Le differenze?

Dal punto di vista etico, nessuna: immorali entrambi.

Dal punto di vista tecnologico, drammaticamente migliore il Trusted Computing!

Se oggi si riesce a convivere con il virus *Word* tramite il vaccino *Openoffice* - visto che stiamo semplicemente convivendo con la malattia! - liberarsi dal retrovirus TC sarà molto più difficile e, forse, una battaglia persa in partenza vista la struttura di controllo enormemente più complessa e quindi più efficace.

Non si risolvono problemi di natura etica semplicemente delegando ad altri le scelte del software necessario per il nostro lavoro.

Nè si potranno mai risolvere, rifiutando di esplorare le alternative, nascondendosi dietro le presunte incompatibilità o scelte burocratiche del sistema.

Solo gli individui hanno un senso di responsabilità. – Nietzsche

---

<sup>10</sup>Un pò come si è fatto con i cellulari marchiati con il logo del gestore. Molti utenti hanno infatti preferito acquistare il telefonino marchiato per risparmiare una dozzina di euro.

# Bibliografia

- [1] Roberto di Cosmo Presente e futuro della società dell'informazione  
29 giugno 1998 - Riflessioni Trappola nel Cyberspazio
- [1] <http://www.mywiseowl.com/articles/Fritz-chip>
- [2] <http://www.eff.org/>
- [3] <http://www.mediamente.rai.it/home/bibliote/intervis/f/ferrero.htm>
- [4] <http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19>  
- articolo di Richard Stallman
- [5] <http://www.loftesness.com/radio/categories/trustedComputing/>
- [6] Noam Chomsky - I cortili dello zio Sam - *What Uncle Sam really wants* 1992
- [7] <http://www.biblio-net.com/filosofia/nietzsche.htm>
- [8] The World as I see it - Albert Einstein