



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

LinuxPerSec 2.0



LUG Verona
<https://www.verona.linux.it>

Trusted Computing miti e realtà

Daniele Masini

daniele@no1984.org

<http://vandali.org/DanieleMasini>

Copyright © 2007 Daniele Masini.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License (<http://www.gnu.org/licenses/gpl.html>) for more details.

Agenda

- La sicurezza
 - Protezione del sistema
 - Protezione delle informazioni
- I sistemi digitali, l'hardware ed il software
- La percezione del software
- Lo stato attuale (legge e tecnologia)
- Il Trusted Computing
- Il DVB
- Possibili scenari



Cosa si intende per ***sicurezza***?

Protezione

Controllo

I dispositivi digitali

L'elettronica digitale ormai ci pervade

- Cellulari
- Fotocamere
- Videocamere
- GPS
- Computer (PC, PDA, ...)
- TV (HD)
- Lettori MP3
- Lettori/masterizzatori DVD
- ...



Problema: la sicurezza

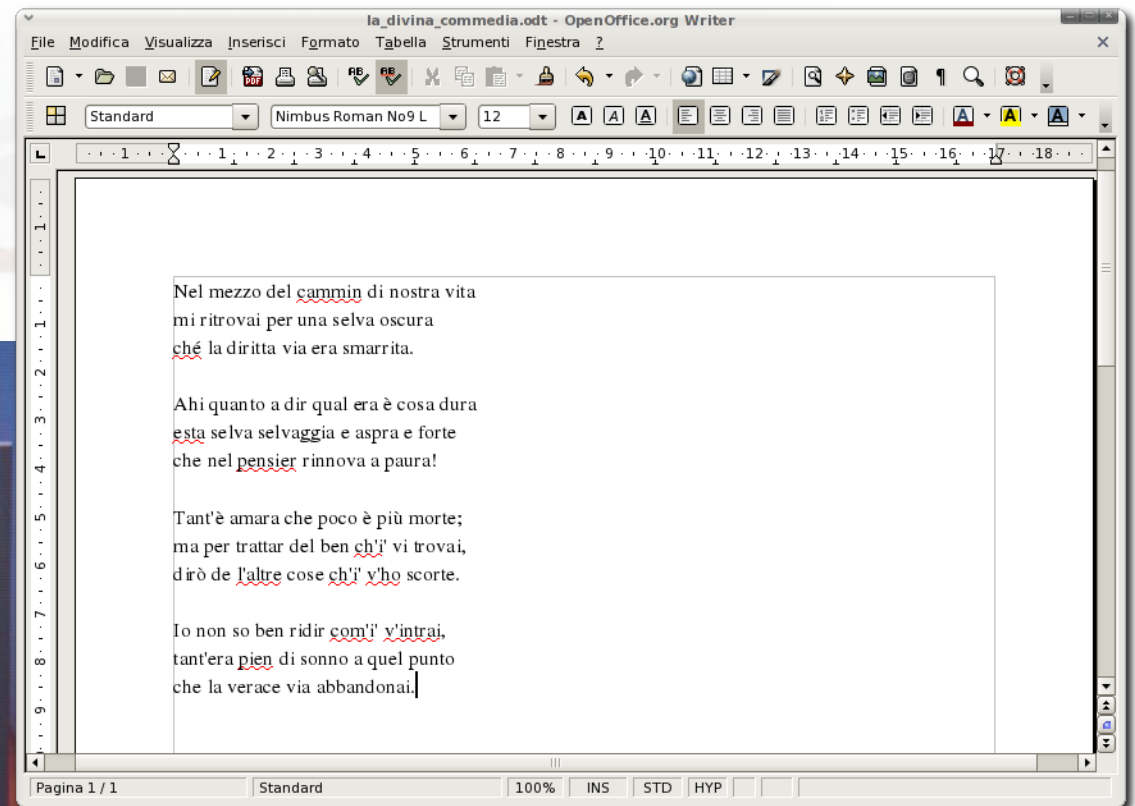
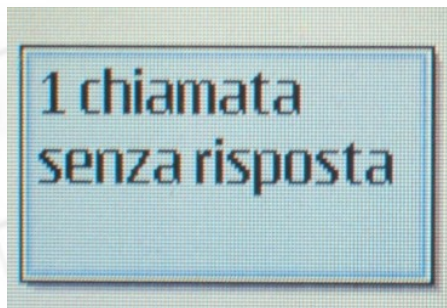
- **Protezione da attacchi**
 - Controllo del software
 - Politiche di accesso, firewall, antivirus, ...
- **Protezione delle informazioni**
 - Accesso ai contenuti
 - Crittografia
 - Protezione dei diritti esercitabili sui contenuti
 - Diritto d'autore e SIAE
 - Brevetti software
 - DRM
 - Altro

Hardware e software

- **hardware:** i dispositivi digitali (circuiti e meccanismi)
- **software:** la logica di controllo che gestisce il funzionamento dell'hardware (i programmi)

L'hardware *ha bisogno* del software per poter funzionare.

La percezione del software



Il software fa *solo* ciò che l'utente percepisce?

Il software

codice sorgente: elenco delle istruzioni che devono essere eseguite dal sistema, in un linguaggio facilmente comprensibile dal programmatore (essere umano).

codice eseguibile: (linguaggio macchina) insieme di istruzioni comprensibili dalla macchina corrispondenti ad un codice sorgente. Praticamente incomprensibile da un essere umano.

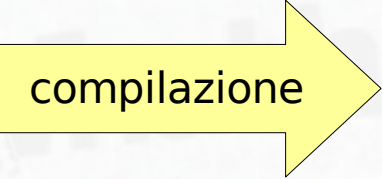
Per lanciare in esecuzione un programma è sufficiente avere il relativo *codice eseguibile*.

Controllo del software

File sorgente: hello_world.c

```
#include <stdio.h>
main()
{
    FILE *fp;
    printf("Salve, mondo!\n");
    return(0);
}
```

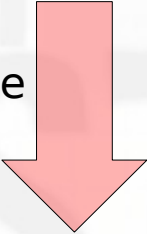
compilazione



File eseguibile: hello_world

```
ELF??4T4
(44?4???????d???d?xx?x????((?(?
Q?td/lib/ld-linux.so.2GNU      ?K??
?)H?  __±?+?_?+??+__  +VTHTFF.??6
IO ?+CRVT+  @      @• P• T• X•
U%åfèf  èÔ  èÿ  ÉÃ  ÿ5H•ÿ%L•
ÿ%P•NL  éàÿÿÿ%T•  éÐÿÿÿ%X•NL
éÄÿÿÿ
lí^%áfäðPTRNL€fNL  fQVNLTfè³ÿÿÿô  U%åSf
iè  [  ÄCR  <"üÿÿÿ...ò+è·ÿÿÿX
...
```

esecuzione



Esempio di esecuzione di hello_world

```
[daniele@dmmobile ~/test]$ ./hello_world
Salve, mondo!
[daniele@dmmobile ~/test]$ ls -l
totale 12
-rwxrwxr-x 1 daniele daniele 4684 20 apr 01:10 hello_world
-rw-rw-r-- 1 daniele daniele  90 20 apr 01:10 hello_world.c
[daniele@dmmobile ~/test]$
```

Controllo del software (2)

File sorgente: hello_world.c

```
#include <stdio.h>
main()
{
  FILE *fp;
  printf("Salve, mondo!\n");
  if ((fp = fopen("hello", "w")) != NULL)
  {
    fprintf(fp, "File creato da helloworld ;-)\n");
    fclose(fp);
  }
  return(0);
}
```

compilazione

File eseguibile: hello_world

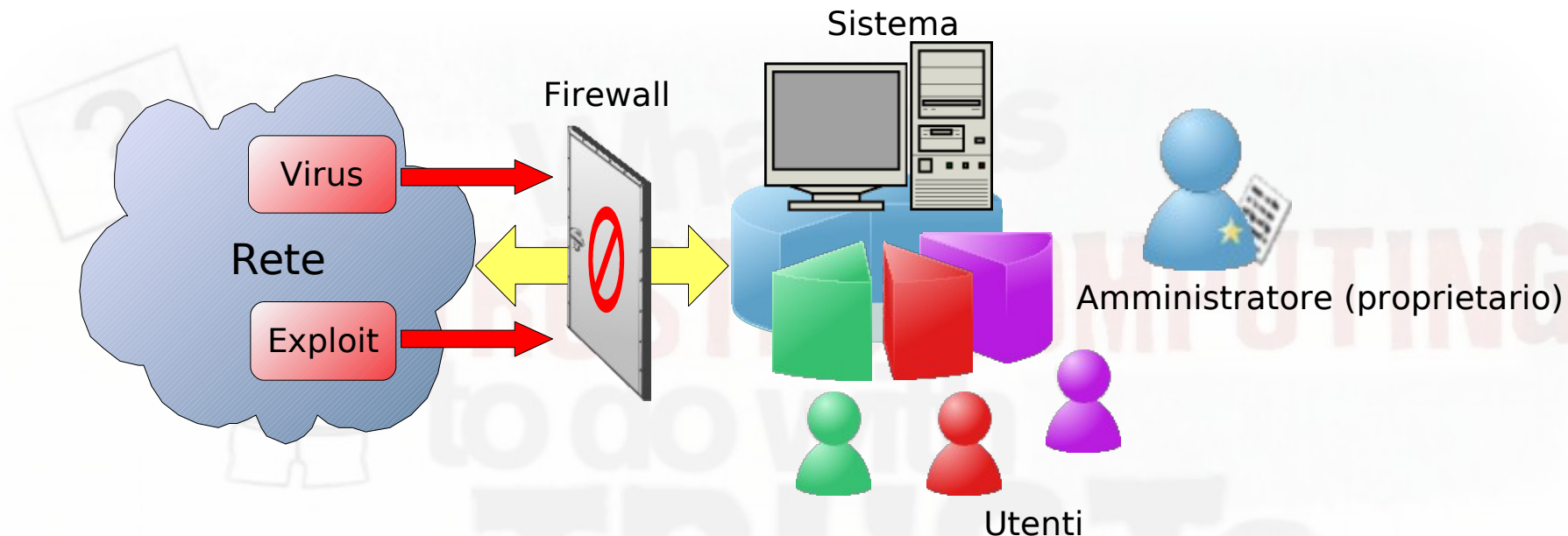
```
ELF??4T4
(44?4???????d???d?xx?x???((?(?
Q?td/lib/ld-linux.so.2GNU
K?? .?)H? ±++? ?+??+
+VTHTFE.???.6 IO ?+CRVT+ @
@• P• T• X• U%åfè£ èÔ èÿ ÉÃ
ÿ5H•ÿ%L• ÿ%P•EUD èàT$ÿÿ%T•
éÐÿÿÿÿ%X•NL éÀÿÿÿ
lí^%áfäöPZRNLEfNL fQVNLTFè³ÿÿÿô U%å
Sfìè [ ÄCR <“üwÿÿ...0+è·ÿÿÿX
...
```

esecuzione

Esempio di esecuzione di hello_world

```
[daniele@dmmobile ~/test]$ ./hello_world
Salve, mondo!
[daniele@dmmobile ~/test]$ ls -l
totale 16
-rw-rw-r-- 1 daniele daniele 30 20 apr 01:14 hello
-rwxrwxr-x 1 daniele daniele 5077 20 apr 01:13 hello_world
-rw-rw-r-- 1 daniele daniele 220 20 apr 01:13 hello_world.c
[daniele@dmmobile ~/test]$ cat hello
File creato da helloworld ;-)
```

Protezione da attacchi



- Politiche di accesso al sistema ed al filesystem
- Firewall, antivirus, IDS

Il sistema è sotto il *controllo* dell'**amministratore**

Protezione delle informazioni

Crittografia

- a *chiave simmetrica*
 - una sola chiave per cifrare e decifrare
- a *chiave asimmetrica*
 - una coppia di chiavi: una chiave *pubblica* ed una *privata*
 - ciò che viene cifrato con una delle due chiavi può essere decifrato solo conoscendo l'altra
- funzioni hash
 - la cifratura one-way
- firma elettronica
 - garanzia dell'autenticità e della paternità dei documenti

Il *controllo* è di chi conosce la chiave di decifratura

Protezione dei diritti

Diritto d'autore

Legge 22 aprile 1941 n. 633 e succ. modificazioni

- **Diritti morali** (paternità dell'opera)
 - Inalienabili
 - Durata: illimitata
- **Diritti di utilizzazione economica**
 - Cedibili
 - Durata: fino a 70 anni dopo la morte dell'autore
 - *Diritto dinastico?*

Protezione dei diritti (2)

SIAE (Società Italiana degli Autori ed Editori)

- Gestisce e amministra i compensi relativi ai diritti d'autore
- *Non chiara ripartizione dei proventi*

Brevetti software

- *Ha senso brevettare le idee?*

DRM (Digital Rights Management)

- Meccanismi per la protezione dei contenuti digitali
 - CSS (DVD), rootkit Sony/BMG (CD)
- Impediscono la fruizione del contenuto se non con specifici programmi o per mezzo di appositi dispositivi
- *Il copyright all'infinito*
- "Se i consumatori soltanto sapessero che esiste un DRM, cos'è e come funziona, noi avremmo già fallito." - P. Lee (*dirigente Disney*)

Protezione dei diritti (3)

DMCA (Digital Millennium Copyright Act) (1998)

EUCD (European Union Copyright Directive) (2001)

- Criminalizzazione dell'utilizzo di sistemi per l'elusione dei meccanismi di protezione delle opere protette dal copyright (DRM) anche senza infrangere il copyright stesso.
- A detta del suo stesso ideatore, Bruce Lehman, *il DMCA ha fallito!*
- *Il copyright dovrebbe supportare la creatività, non foraggiare le aziende dell'intrattenimento.*

IPRED2 (Intellectual Property Restriction European Directive 2) (2007)

- Criminalizzazione della violazione della proprietà intellettuale su scala commerciale. Azione penale senza querela di parte.
- Cooperazione alle indagini da parte di privati. Gli ISP come controllori del traffico.

Protezione dei diritti (4)

Equo compenso (2003)

- È un *sovrapprezzo*, imposto per legge, sull'acquisto di CD, DVD e cassette vergini
- € 0,28 per un CD-R (800 MB) e € 0,87 per un DVD-R (4,7 GB) + IVA
- Nato per compensare il mancato guadagno di autori ed editori dovuto alla *copia privata* dei contenuti
- Il denaro raccolto viene distribuito tra gli iscritti alla SIAE
- € 73.000.000,00 incassati nel 2005 (quasi come per il teatro + cinema)
- La SIAE sta pensando di estenderlo anche a HD e chiavette USB

Protezione dei diritti (5)

Da un'intervista a Giorgio Assumma (pres. SIAE)

pubblicata su "La Stampa" del 12/03/2007

D: Secondo lei è giusto pagare anche per copiare su CD e DVD foto di famiglia o archivi personali, che non sono tutelati dalla SIAE?

R: «Nessuno è riuscito a proporci un sistema valido per differenziare i vari usi del supporto, così la legge applica un criterio che apparentemente presenta discrasie ingiustificate, ma è inevitabile. [...]».

“Presunzione d'innocenza” o “presunzione di colpevolezza”?
Bisogna pagare anche per opere non tutelate dalla SIAE?

D: Oggi chi acquista un brano su internet o su disco versa alla SIAE un compenso, poi un altro se vuole copiarlo su cassetta o masterizzarlo su CD, [...]. Le pare normale?

R: «Il diritto d'autore non è uno solo, ma tanti: leggere, riprodurre, circolare, prestare, dare in noleggio e altri. Non si paga più volte, si pagano più autorizzazioni diverse».

(segue...)

Protezione dei diritti (6)

(... continua dalla pagina precedente)

D: Ma chi compra una canzone per uso privato [...], gli basta poterla ascoltare su tutti gli apparecchi che possiede, è il principio di interoperabilità...

R: «Sono usi differenti, e per ognuno si versa un corrispettivo».

Bisogna acquistare più versioni di un brano per avere il diritto di ascoltarlo con le stesse orecchie ma da riproduttori differenti?

Curiosità

- Supporti e contenuti legalmente acquistati
 - *Non duplicabili*
 - Contenuti fruibili solo per mezzo di *opportuni lettori*
- Supporti e contenuti illegali
 - *Duplicabili*
 - Contenuti fruibili per mezzo di *qualunque lettore*

Soluzione: Trusted Computing

- Traduzione: “informatica fidata”.
- Alias: TCPA, Palladium, NGSCB, LaGrande Technology, Presidio, ...
- Trusted Computing Group (TCG)
 - Consorzio no-profit nato nel 2003 per la stesura di specifiche *hardware* e *software* relative al TC.
 - Promotori: AMD, hp, IBM, Infineon, Intel, Microsoft e Sun.
 - Affiliati: tutti i maggiori *produttori hardware e software* mondiali (e non solo...).
 - Scopo dichiarato: **miglioramento della *sicurezza dei sistemi***.

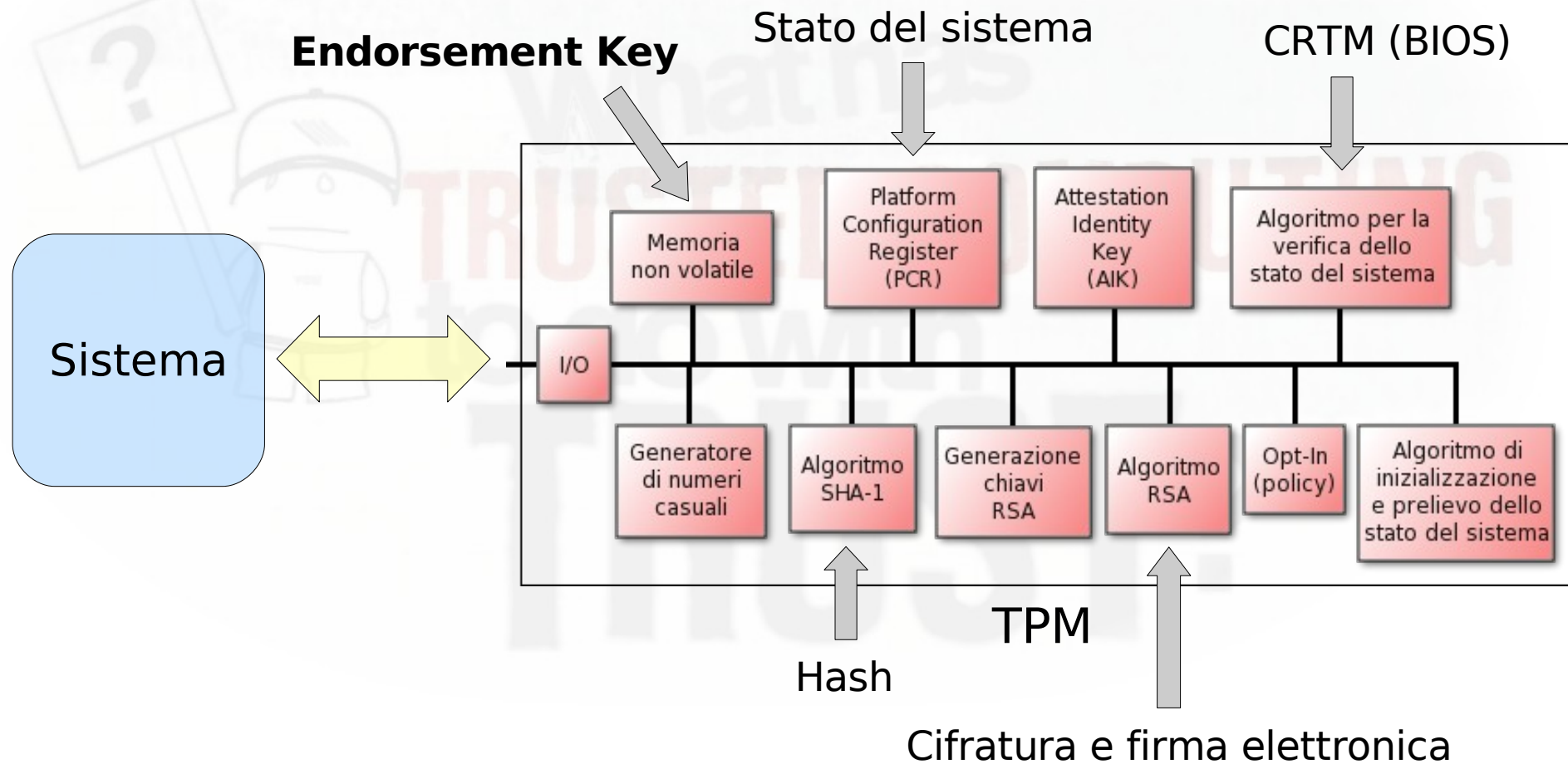
Cos'è il Trusted Computing?

- Piattaforma tecnologica basata su
 - Componenti hardware (chip)
 - Componenti software (driver e programmi)
 - Specifiche tecniche
- Dispositivi coinvolti
 - PC e derivati (server, desktop, laptop, palmari, navigatori satellitari, ...)
 - Elettronica di consumo (cellulari, Hi-Fi, TV, lettori DVD, telecamere, ...)

Caratteristiche del TC

- **I/O sicuro**: cifratura delle informazioni che transitano sui bus di sistema (*Endorsement Key*).
- **Memory curtaining**: protezione hardware della memoria.
- **Sealed storage** (memoria sigillata): accesso alle informazioni consentito soltanto se il sistema si trova in un determinato stato (dipende dal software e dall'hardware).
- **Remote attestation** (attestazione remota): lo stato della propria macchina è rilevabile da altri.

Trusted Platform Module



Transitive trust

- Quand'è che il sistema è fidato?
 - È in uno stato fidato.
 - Proviene da uno stato fidato (transitive trust).
- L'avvio del sistema
 1. CRTM (BIOS) – partenza fidata
 2. Boot loader
 3. Sistema operativo
 4. Applicazioni

Ad ogni passo, prima di essere lanciato in esecuzione, il codice del passo successivo viene “verificato”.

Osservazioni sul TC

- È una tecnologia attuale
 - Il TPM è **già presente** in vari dispositivi in commercio!
- Protezione della memoria
 - Problemi nel debug del software (neanche il S.O. può accedere a certe zone di memoria)
- Attestazione remota
 - Si perde il beneficio della non conoscenza del software che gira sulle altre macchine (la non conoscenza limita il controllo che si può avere sugli altri)
- Sealed storage
 - I dati salvati da un programma saranno fruibili da altri programmi?
 - Possibili pratiche anticompetitive

Osservazioni sul TC (2)

- L'*implementazione* delle specifiche del TC è lasciata ai produttori!
- Chi ci assicura che non esistano *backdoors* o funzionalità *non* documentate?
- *Chi* stabilisce quale software può essere eseguito dal sistema?
- Il *legittimo proprietario* di un dispositivo è considerato un possibile *nemico* del dispositivo stesso!
- Se i produttori non si fidano del legittimo proprietario del sistema, perché quest'ultimo dovrebbe *fidarsi* dei produttori?

DVB

- Digital Video Broadcasting = Trasmissione video digitale
- La trasmissione digitale diverrà (in Italia dal 2009) l'unico sistema per la diffusione di programmi televisivi
- Standard definiti dal DVB Project (<http://www.dvb.org>)
 - Nato nel 1993
 - Consorzio chiuso di circa 260 aziende (comunicazioni, trasmittenti televisive, sviluppo software, produttori hardware, ...)
 - Praticamente il 99% delle aziende produttrici di apparecchi televisivi del mondo
 - DVB-S, DVB-C, DVB-T, DVB-H, DVB-IPTV, ...
 - DVB-CPCM (protezione dei contenuti)

DVB (2)

CPCM (Content Protection and Copy Management)

- Divieto di *registrazione* delle trasmissioni
- Divieto di *copia* di contenuti digitali anche per uso personale
- Divieto di *trasferimento* di una trasmissione da un ricevitore ad un altro
- Divieto di *condivisione* dei contenuti con altri che risiedono nello stesso appartamento
- Obbligo dell'*aggiornamento* del dispositivo (altrimenti diventa obsoleto e non funzionerà più)
- Oscuramento delle trasmissioni in chiaro

Possibili scenari

- **I legittimi proprietari *non* avranno più il pieno controllo dei propri dati e dei propri dispositivi**
- Censura dei contenuti digitali (“scomodi”): siti web, documenti, ...
 - v. SIAE contro www.homolaicus.com (filmati su YouTube)
 - v. vicenda della contro-analisi di Shelley Batts (<http://www.doxaliber.it/quando-il-termini-copyright-potrebbe-essere-tradotto-semplicemente-in-censura/514>)
- Fidelizzazione forzata degli utenti/clienti
- Crollo degli standard per l’interscambio delle informazioni
- Impossibilità di cambiare canale TV per “saltare” la pubblicità
 - Tecnologia di Philips (v. <http://punto-informatico.it/p.aspx?i=58938>)

... L'importanza dei termini

• Furto

- Si riferisce alla sottrazione di un bene ad un'altra persona.
- Si adatta bene alle cose materiali. Es. Bob ruba una mela ad Alice. Bob ha la mela ma Alice non ce l'ha più.
- Per il software è più corretto parlare di *copia*.

• Proprietà intellettuale

- Spinge a considerare *copyright*, *brevetti* e *marchi* in analogia alla proprietà sugli oggetti, ma essi sono cose diverse tra loro.
- Copyright, brevetti e marchi sono regolamentati da leggi diverse ed ognuno ha caratteristiche specifiche.



“Chi è disposto a rinunciare alle proprie libertà fondamentali in cambio di briciole di sicurezza, non merita né la libertà né la sicurezza.”

- *B. Franklin*

Cosa fare?

- Informarsi
- Divulgare l'informazione
- Acquistare dispositivi digitali con cautela e con coscienza:
 - se non si vogliono il TC o i DRM si eviti di acquistare la tecnologia che li supporta
 - Noi siamo i clienti: senza il nostro “consenso” i produttori non vendono
- Aiutare i gruppi e le associazioni che fanno informazione (es. www.no1984.org)



What has
TRUSTED COMPUTING
to do with
TRUST?

Domande?

Link utili

No1984.org

<http://www.no1984.org>

Wikipedia – Trusted Computing

http://it.wikipedia.org/wiki/Trusted_Computing

D. Masini – Trusted Computing

<http://vandali.org/DanieleMasini/notc.php>

A. Bottoni – La spina nel fianco

<http://www.laspinanelfianco.it>

R. Stallman – Puoi fidarti del tuo computer?

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

R. Anderson – Trusted Computing FAQ

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

Trusted Computing Group

<https://www.trustedcomputinggroup.org>

Microsoft NGSCB FAQ

<http://www.microsoft.com/technet/archive/security/news/ngscb.msp>

B. Schneier – Trusted Computing Best Practices

http://www.schneier.com/blog/archives/2005/08/trusted_computi.html

S. Schoen – Trusted Computing: Promise and Risk

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

M. Russinovich – Sony, Rootkits and Digital Rights Management Gone Too Far

<http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>

Punto Informatico – Il DMCA ha fallito

<http://punto-informatico.it/p.aspx?id=1935461>

La Stampa – Assumma: Studiamo una tassa SIAE sui contenuti internet

http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=1962&ID_sezione=&sezione

Punto Informatico - Il DRM da oggi rischia in Europa

<http://punto-informatico.it/p.aspx?id=1959066>

M. Ryan – Trusted Computing and NGSCB

<http://www.cs.bham.ac.uk/~mdr/teaching/TrustedComputing.html>

Punto Informatico – Untrusted

<http://punto-informatico.it/cerca.asp?s=%22alessandro+bottoni%22&o=0&t=4&c=Cerca>

A. Bottoni – Le Mani sulla Televisione Digitale

http://www.partito-pirata.it/liberate_la_TV_digitale.html

DVB Project

<http://www.dvb.org>

Zeus news – Vietato disinstallare Vista dai nuovi portatili HP

<http://www.zeusnews.it/index.php3?ar=stampa&cod=5665&numero=999>

Come disporre liberamente di un proprio acquisto

http://www.aduc.it/dyn/comunicati/comu_mostra.php?id=178001

V. Ciarumbello – Sviluppo tecnologico e libero arbitrio, due concetti in antitesi

<http://www.zeusnews.it/index.php3?ar=stampa&cod=5664&numero=999>