Linux Day 2006

Firenze, 28 Ott 2006

no1984.org
http://www.no1984.org

FLUG
http://www.firenze.linux.it

Sicurezza, fiducia e Trusted Computing

Daniele Masini

daniele@no1984.org
http://vandali.org/DanieleMasini

Agenda

- Sicurezza in informatica
- Fiducia nel software
- Cenni di crittografia
- Il Trusted Computing
- Specifiche del Trusted Computing Group
- Il Trusted Platform Module
- Il Digital Rights Management
- Pro e contro del Trusted Computing

Definizioni di base

Cos'è la *sicurezza*? E la *fiducia*?

- **Sicurezza**

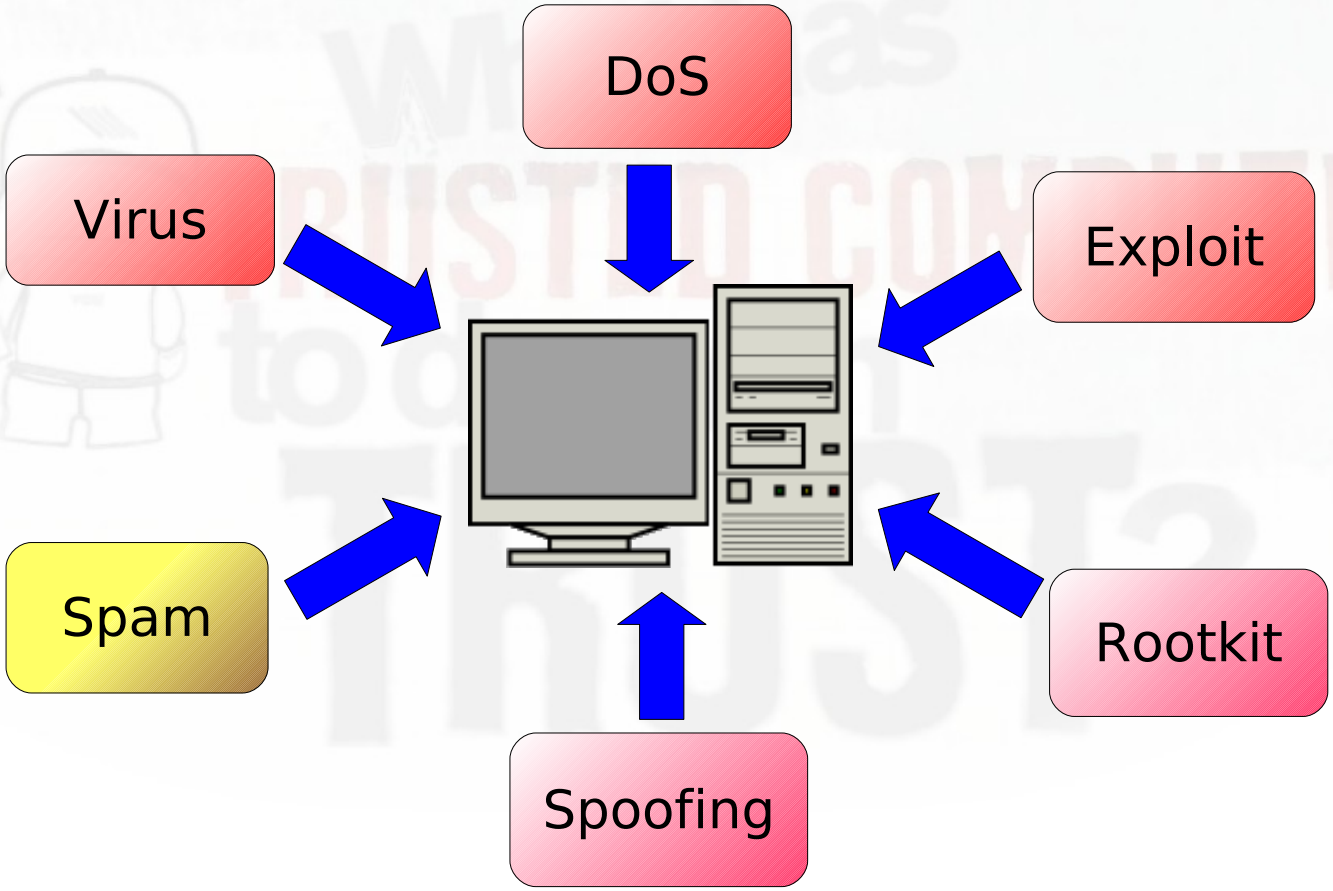
  l'essere esente da pericoli, condizione di ciò che è sicuro.

- **Fiducia (*trust*)**

  sentimento di *sicurezza* che deriva dal confidare senza riserve in qualcuno o in qualcosa.

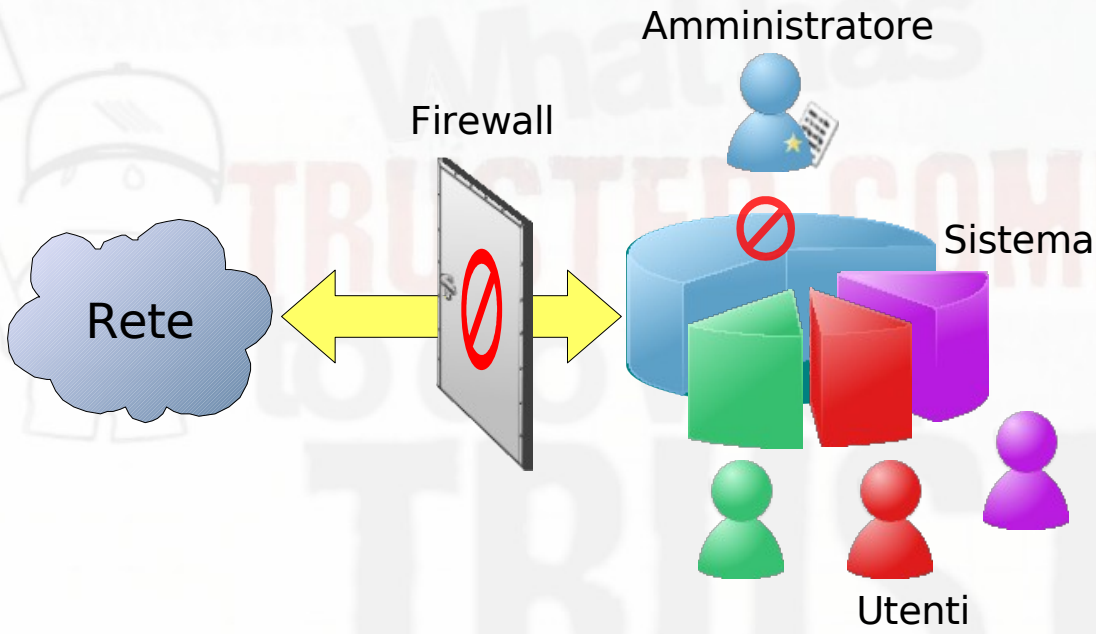
  La fiducia è un sentimento reciproco che non può essere forzato (imposto).

Gli “attacchi informatici”



Sicurezza in informatica

Protezione del sistema dagli attacchi



– L'amministratore deve avere il *controllo* del sistema
  - Politiche di gestione di accesso al sistema ed al filesystem
  - Politiche di firewalling

Sicurezza in informatica

Fiducia nel software

- Il software fa *solo* ciò che l'utente percepisce?
- È importante avere a disposizione il *codice sorgente.*

(un semplice esempio: `helloworld`)

```
#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);
}
```

Sicurezza in informatica

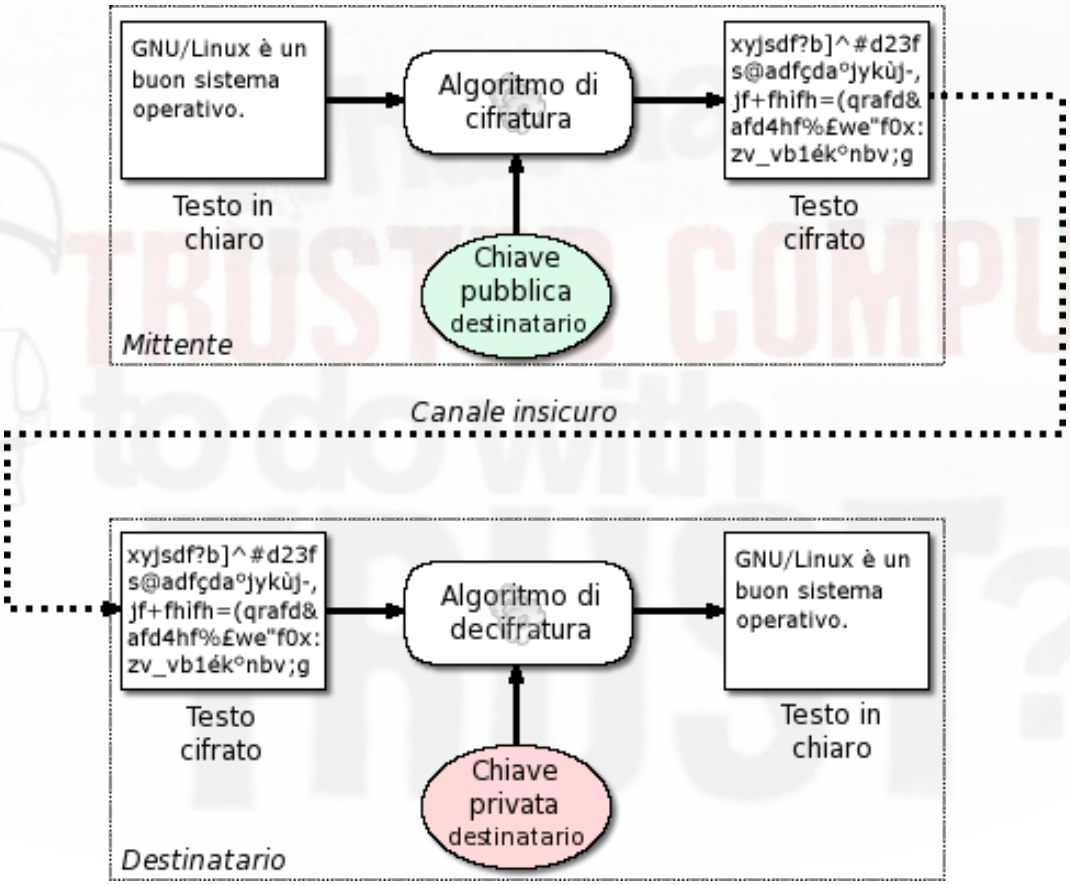
Protezione delle informazioni

È possibile *proteggere* le informazioni, utilizzando dei **meccanismi crittografici**, che permettono camuffarle e renderle fruibili soltanto se si è a conoscenza di un segreto detto ***chiave***.

È possibile *verificare* che certe informazioni siano state scritte da chi si dichiara esserne l'autore, se quest'ultimo ha apposto sulle stesse la propria **firma elettronica**.

- **Cifratura a *chiave asimmetrica***
  - Due chiavi: ***chiave pubblica*** e ***chiave privata***.

Sicurezza in informatica



Cifratura e decifratura con *chiave asimmetrica*

Sicurezza in informatica

- **Gli strumenti per la gestione della sicurezza esistono già!**
  - Permessi utenti/gruppi
  - Quota
  - Firewall (Netfilter)
  - Proxy (Privoxy)
  - IDS (Snort)
  - Crittografia (GnuPG)
  - Anonimizzazione (Tor)
- ***Esperienza***

Trusted Computing (TC)

- Traduz.: “informatica fidata” o “calcolo fidato”.
- 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.
  - Tra i promotori: AMD, hp, IBM, Intel, Microsoft e Sun.
  - Affiliati: tutti i maggiori *produttori hardware e software* mondiali (e non solo...).
- Scopo dichiarato: **miglioramento della *sicurezza* dei sistemi**.

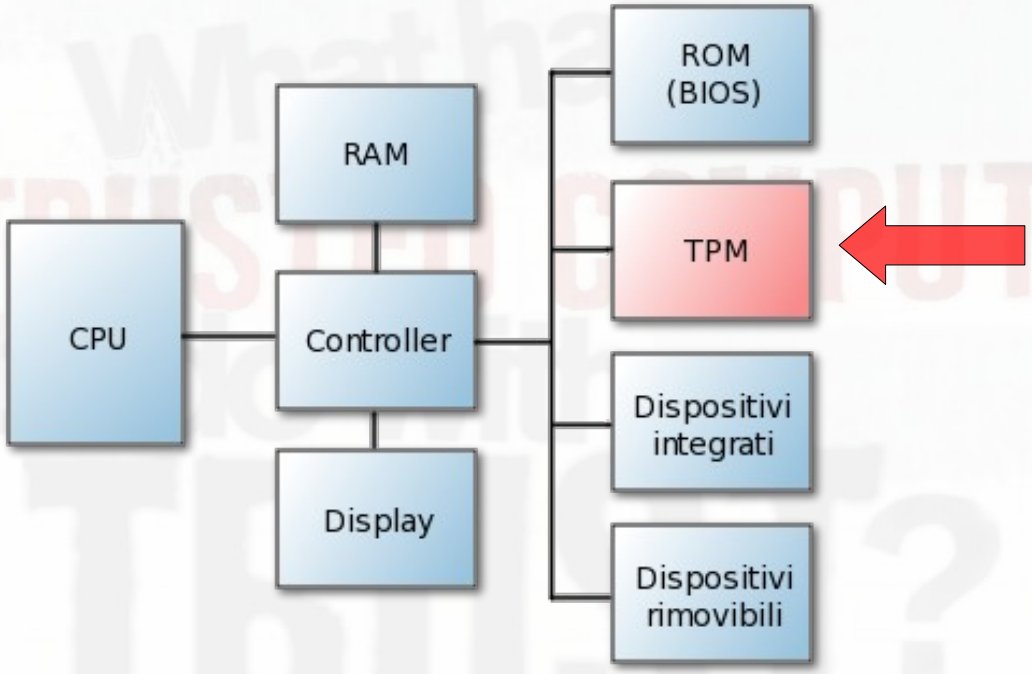
Il TC ed i dispositivi

- Il TC è una piattaforma tecnologica che fa uso di *meccanismi crittografici*, 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, lettori MP3, lettori DVD, telecamere, ...).

Caratteristiche del TC

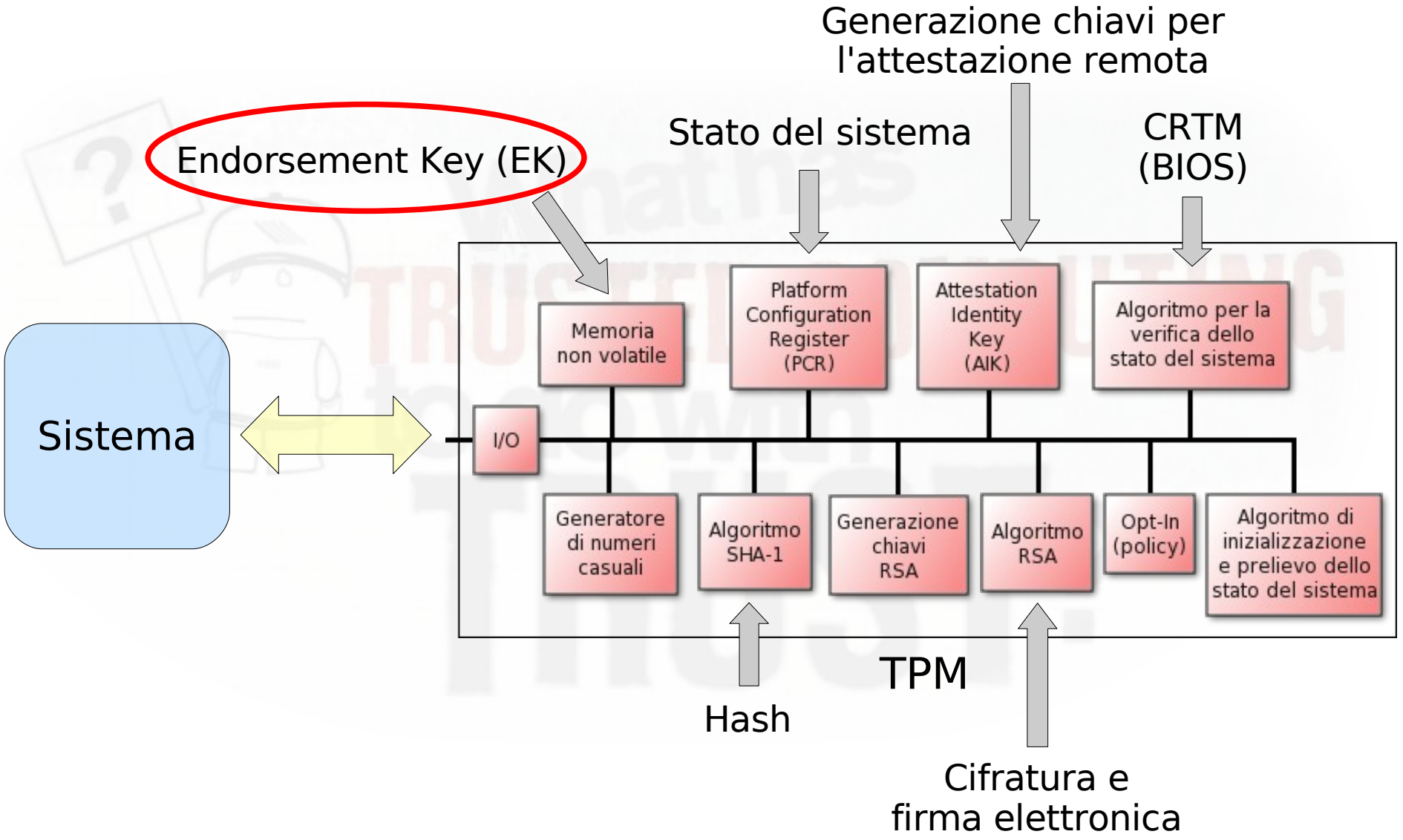
- **I/O sicuro**: cifratura delle informazioni che transitano sui bus di sistema.
- **Memory curtaining**: (separazione della memoria) protezione hardware delle informazioni in RAM.
- **Sealed storage** (memoria sigillata): accesso alle informazioni consentito soltanto se il sistema si trova in un determinato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

Architettura TC



Architettura di un sistema TC

TPM (Trusted Platform Module)



Transitive trust

- Quand'è che il sistema è fidato?
  - È in uno stato fidato (*trusted*).
  - Proviene da uno stato fidato e il software per passare allo stato successivo è ritenuto fidato (*transitive trust*).
- **L'avvio del sistema ed il *transitive trust***
  1. CRTM (BIOS) – partenza fidata.
  2. Boot loader.
  3. Sistema operativo.
  4. Applicazioni.

  Ad ogni passo, prima di essere lanciato in esecuzione, viene “verificata” l'affidabilità del codice del passo successivo.

Osservazioni sul TC

- 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: possibili pratiche discriminatorie per l'accesso ai servizi.
- Sealed storage
  - I dati salvati da un programma non possono essere utilizzati da altri programmi: possibili pratiche *anticompetitive*.

Osservazioni sul TC

- Key escrow: chi ci assicura che *non esistano* ***backdoors*** per il TPM?
  - Funzionalità *non* documentate.
  - Meccanismi *nascosti* di accesso alle chiavi private.
- Come viene riconosciuto il software “buono” dal malware?
- ***Chi*** **stabilisce quale software può essere eseguito dal sistema?**

Osservazioni sul TC

- Il TCG riconosce le potenzialità della tecnologia descritta, ma **lascia ai produttori l'*implementazione* delle specifiche**.
- Il legittimo proprietario di un dispositivo è considerato un possibile *nemico* del dispositivo stesso (non ha il controllo della EK).
- Se i produttori *non si fidano* del proprietario del sistema, perché quest'ultimo *deve fidarsi* dei produttori?

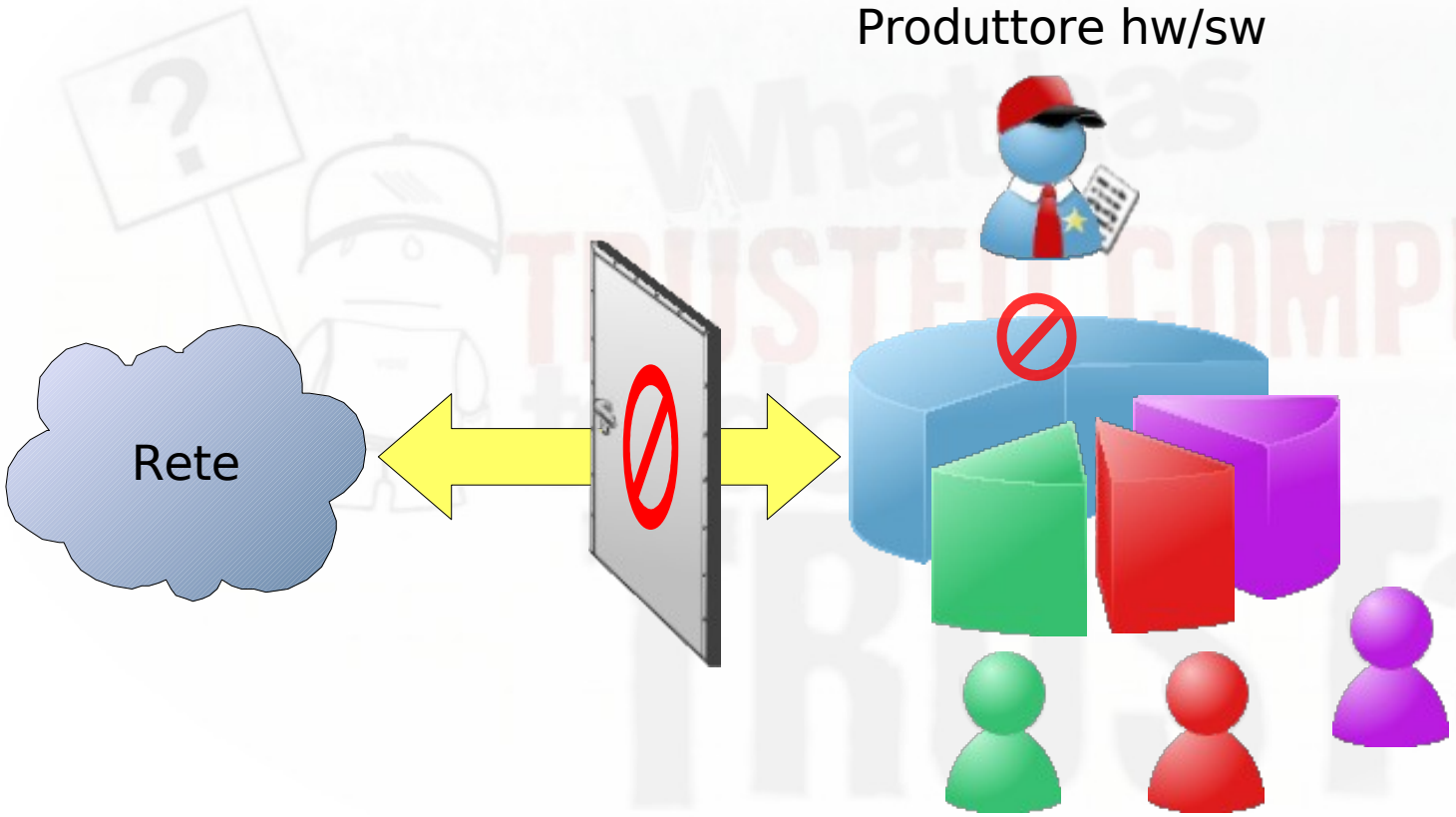
DRM (Digital Rights Management)

- Le specifiche del TCG non sono ufficialmente pensate per il DRM, ma gli si adattano particolarmente bene!
  - È possibile fare in modo che un certo contenuto digitale sia fruibile solo dopo l'attestazione.
  - Infinite possibilità di *controllo* sulle modalità di fruizione dei contenuti digitali.
- Il rootkit di Sony/BMG.
- *"Se i consumatori venissero a conoscenza che esiste un DRM, cos'è e come funziona, noi avremmo già fallito."* - P. Lee (dirigente Disney)

I prodotti

- Prova di Intel: l'identificativo dei PIII.
- Windows Vista è pronto per il TC.
- Molti sistemi (PC) **già sul mercato** includono i chip TPM. Il TPM verrà presto integrato all'interno delle CPU.
- *Cartello di mercato*: presto diverrà impossibile per i consumatori riuscire a trovare sistemi e componenti non TC-compliant.

Trusted Computing



È questo il futuro dei dispositivi digitali?

Possibili scenari

- **Gli utenti *non* avranno più il pieno *controllo* dei propri dati e dei propri dispositivi.** Il *controllo* sarà nelle mani di chi gestisce il TC.
- *Censura* dei siti web e dei contenuti digitali.
- Controllo dell'accesso ad Internet.
- DRM iper-pervasivi ed intrusivi.
- *Fidelizzazione forzata* degli utenti (clienti).
- Crollo degli standard per l'interscambio delle informazioni.

Software libero

- Linux 2.6.12 supporta al suo interno un driver per l'utilizzo del TPM.
  - Pilota chip di National Semiconductor e Atmel, che si trovano sui ThikPad IBM.
- Trousers.
  - Libreria per GNU/Linux (sviluppata da IBM) per il TSS (TCG software Stack).

Poiché il software libero è *modificabile* da chiunque, le possibilità di farlo funzionare con il TPM nel mondo reale sono molto basse.

TC

~~**Trusted Computing**~~

~~(informatica fidata)~~

Threacherous Computing

(informatica infida)

No1984.org

- È un gruppo di volontari.
- Nato nel settembre 2005 come mailing list tc@no1984.org.
- Sito web: http://www.no1984.org.
- Scopo: fare informazione sul Trusted Computing e comunque contro qualsiasi sistema di controllo centralizzato che tende a limitare le libertà del singolo.
- Il nome deriva dal celebre romanzo di G. Orwell “1984”.

Cosa fare?

- **Informarsi** sul Trusted Computing.
- **Divulgare l'informazione** sul Trusted Computing.
- Acquistare dispositivi digitali *con coscienza*.
- Aiutare **no1984.org** ;-)

Se nessuno fa niente, i produttori hw/sw avranno la strada spianata verso il TC.

Noi siamo i clienti: senza il nostro “consenso” i produttori non vendono i loro prodotti.

Link utili

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

Against-TCPA
http://www.againsttcpa.com

Trusted Computing Group
https://www.trustedcomputinggroup.org

Microsoft NGSCB FAQ
http://www.microsoft.com/technet/archive/security/news/ngscb.mspx

Wikipedia – Trusted Computing
http://it.wikipedia.org/wiki/Trusted_Computing

Daniele Masini – Trusted Computing
http://vandali.org/DanieleMasini/notc.php

Alessandro Bottoni – La spina nel fianco
http://www.laspinanelfianco.it

Linux in Italia – Intervista a Riccardo Tortorici
http://linuxinitalia.spaghettilinux.org/modules/news/article.php?storyid=101

R. Anderson – Trusted Computing FAQ
http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html

R. Stallman – Can you trust your computer?
http://www.gnu.org/philosophy/can-you-trust.html

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

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

Wikipedia – DRM
http://it.wikipedia.org/wiki/Digital_Rights_Management

Defective by design
http://www.defectivebydesign.org

Open TC
http://www.opentc.net

Domande?