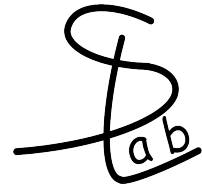




no1984.org  
<http://www.no1984.org>

# Giornata di studio sul Trusted Computing



Università degli Studi di Milano  
Dipartimento di Informatica e Comunicazione  
<http://www.dico.unimi.it>  
Dipartimento di Scienze dell'Informazione  
<http://www.dsi.unimi.it>

# Sicurezza, fiducia e Trusted Computing

**Daniele Masini**

[daniele@no1984.org](mailto:daniele@no1984.org)  
<http://vandali.org/DanieleMasini>

**Copyright © 2006 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

- Concetti di base: sicurezza e fiducia
- Sicurezza in informatica
- Protezione delle informazioni
- 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*?

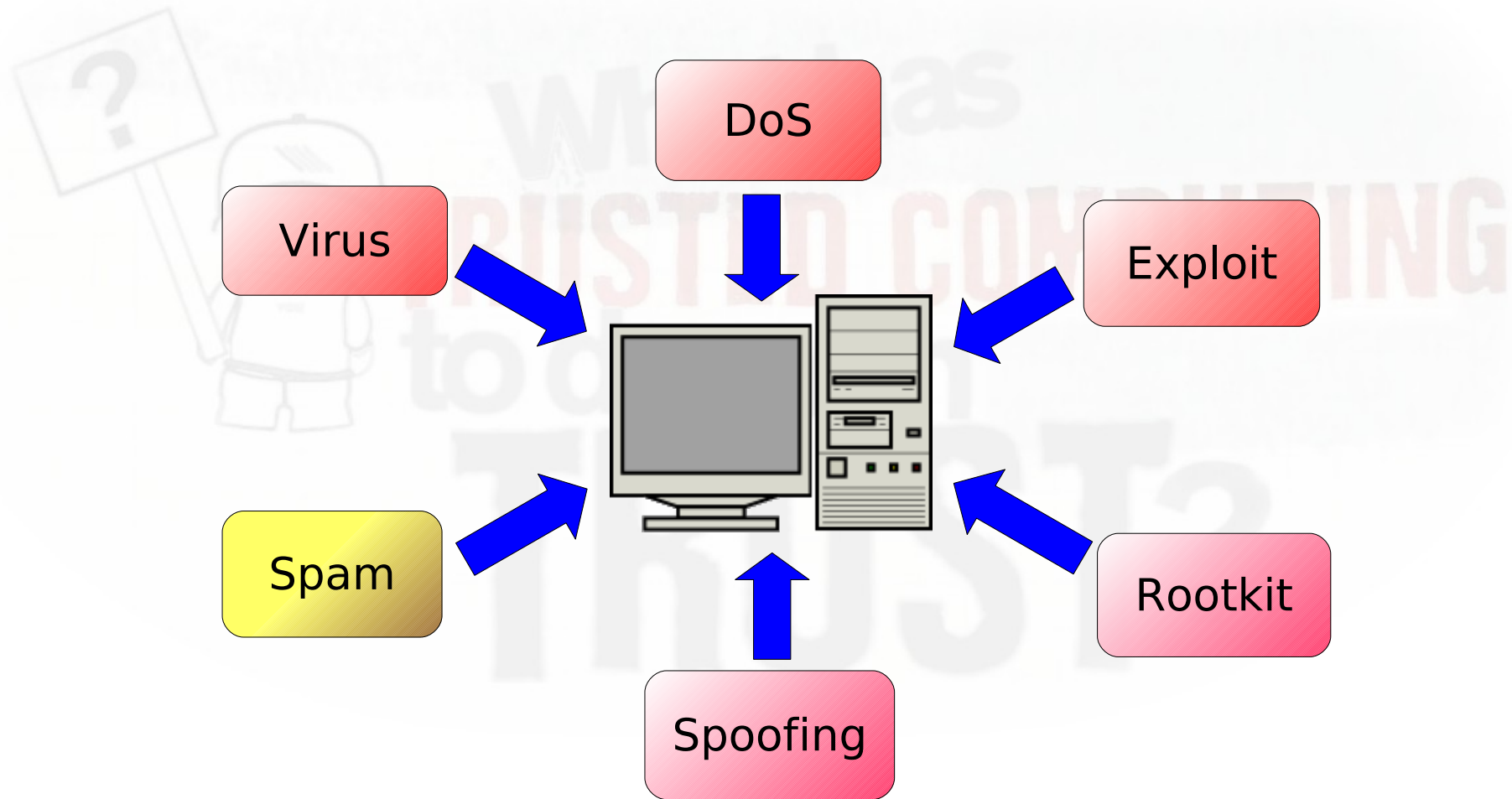
- **Sicurezza**

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

- **Fiducia (*trust*)**

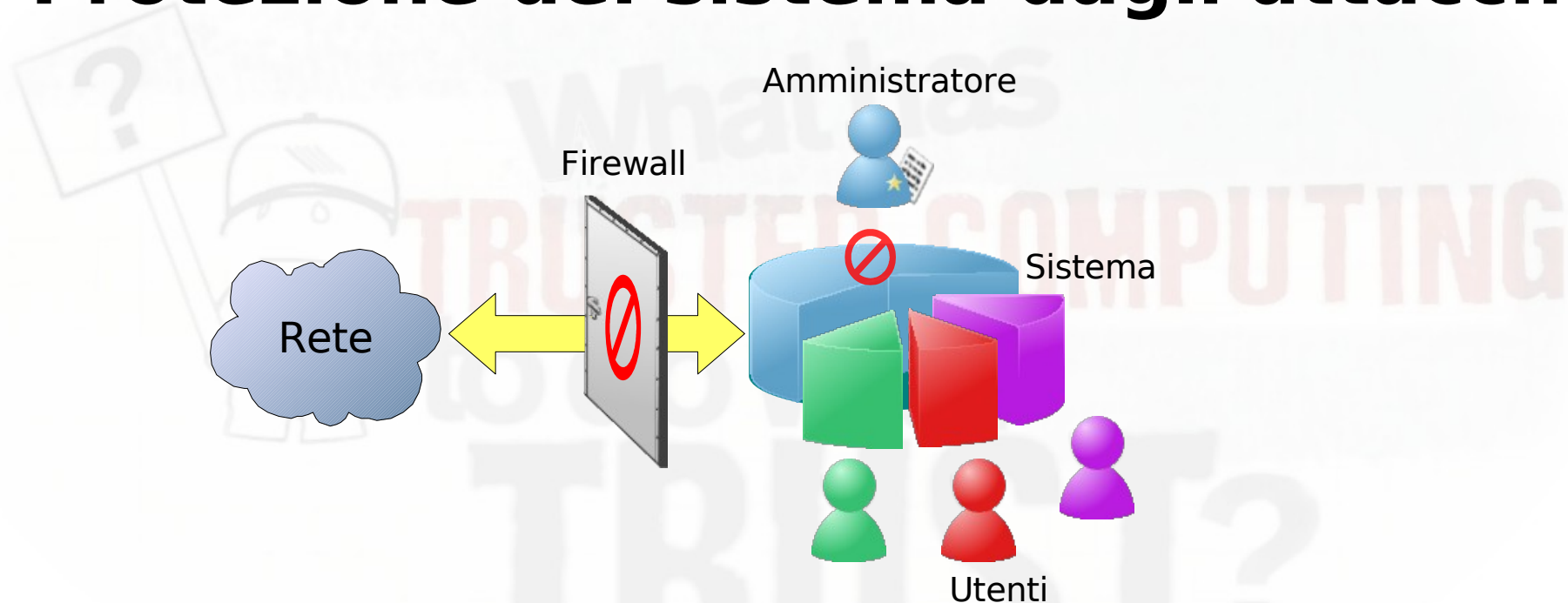
sentimento di *sicurezza* che deriva dal confidare senza riserve in qualcuno o in qualcosa.

# 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?
- Importanza di 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);
}
```

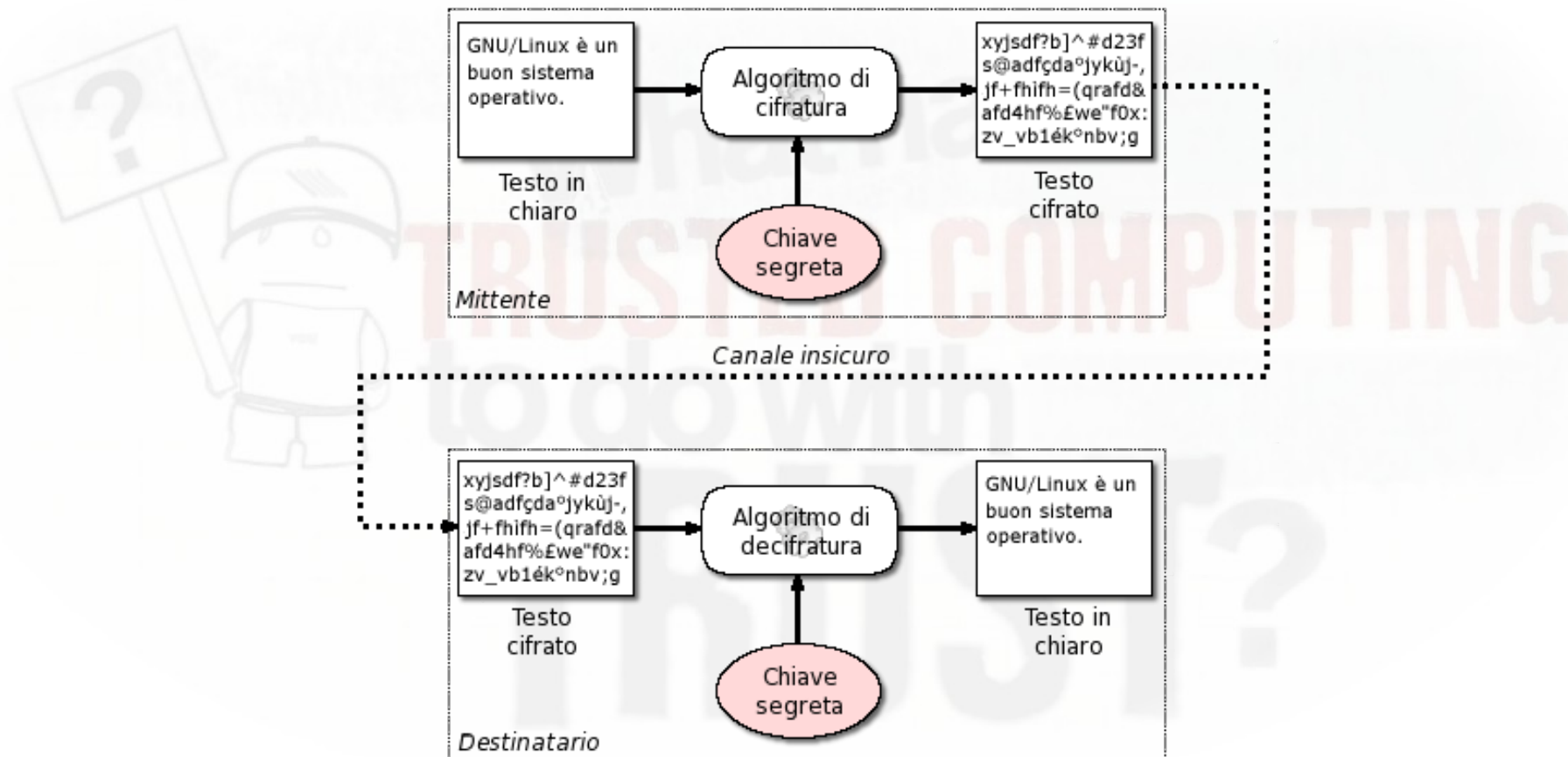
# Sicurezza in informatica

## Protezione delle informazioni

- Cifratura a ***chiave simmetrica***
  - Un'*unica chiave* per la cifratura e decifratura delle informazioni.
  - La chiave deve essere tenuta *segreta*.
  - Scambio delle chiavi attraverso un canale sicuro.
  - Algoritmi: DES/DEA, IDEA, Blowfish, AES, ...



# Sicurezza in informatica



Cifratura e decifratura con *chiave simmetrica*

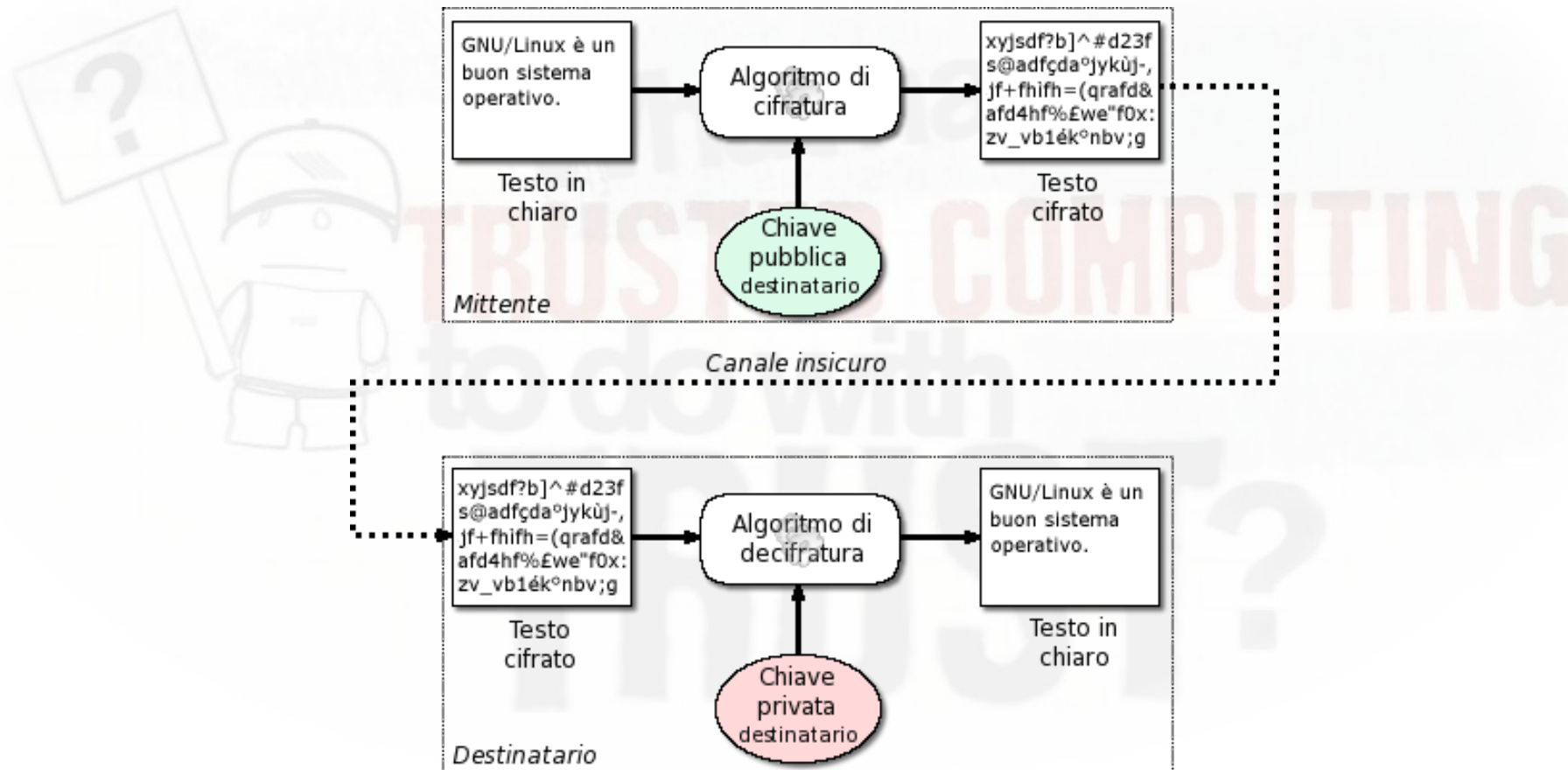


# Sicurezza in informatica

## Protezione delle informazioni

- Cifratura a ***chiave asimmetrica***
  - Due chiavi: ***chiave pubblica*** e ***chiave privata***.
  - La chiave *privata* deve essere tenuta *segreta*.
  - La chiave *pubblica* può essere distribuita su un canale insicuro.
  - Algoritmi: RSA, ElGamal, DSA, ...

# Sicurezza in informatica

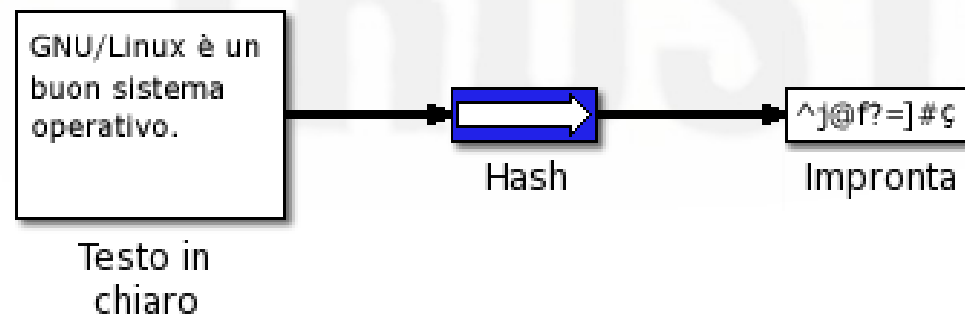


Cifratura e decifratura con *chiave asimmetrica*

# Sicurezza in informatica

## Protezione delle informazioni

- Funzioni *hash*
  - Cifratura *one-way*, creazione dell'**impronta** (*digest*).
  - Nessuna chiave.
  - Algoritmi: MD5, SHA, RIPEMD, ...



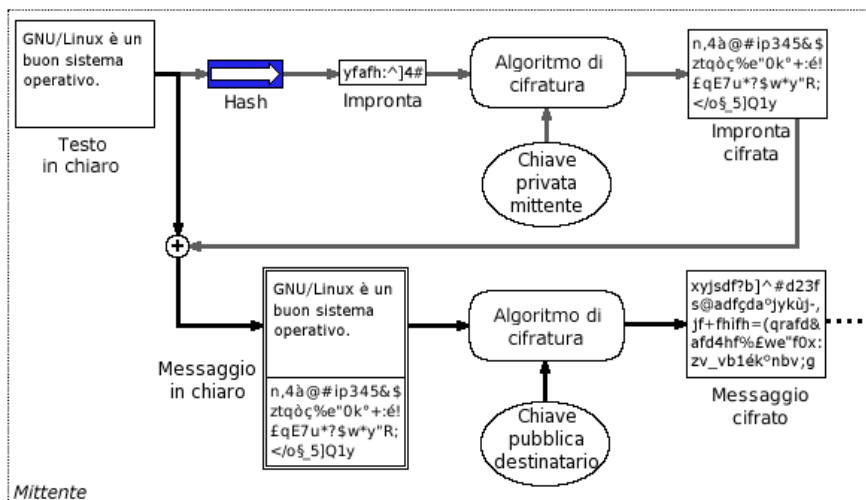
# Sicurezza in informatica

## Protezione delle informazioni

- ***Firma elettronica***

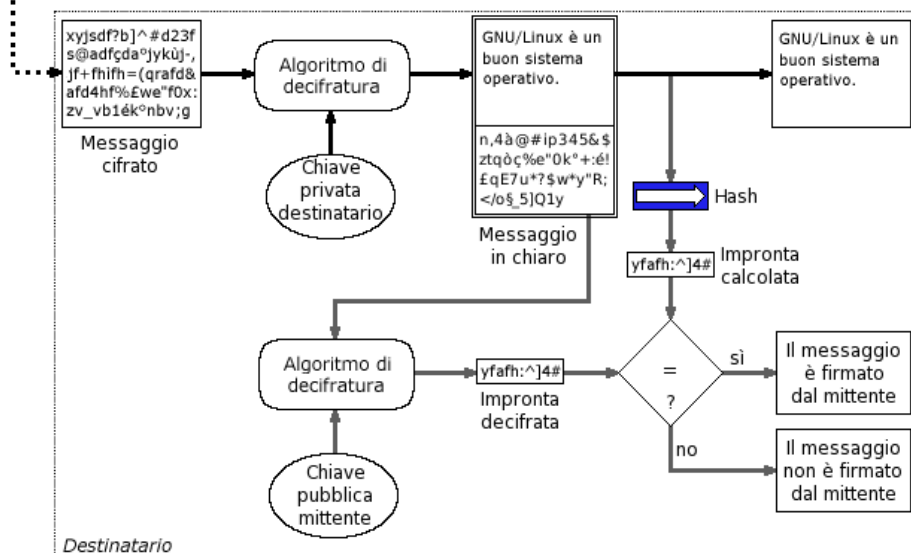
- Creazione dell'*impronta* dell'informazione con una funzione hash.
- Cifratura asimmetrica dell'impronta con la propria chiave *privata*.

# Sicurezza in informatica



Mittente

Canale insicuro



Destinatario

Cifratura e decifratura con *firma elettronica*

# Gli strumenti

- **Gli strumenti esistono già!**

- Permessi utenti/gruppi.
- Quota.
- Firewall (Netfilter).
- Proxy (Privoxy)
- IDS (Snort).
- Crittografia (GnuPG).
- Anonimizzazione (Tor).

- ***Esperienza***

# Trusted Computing (TC)

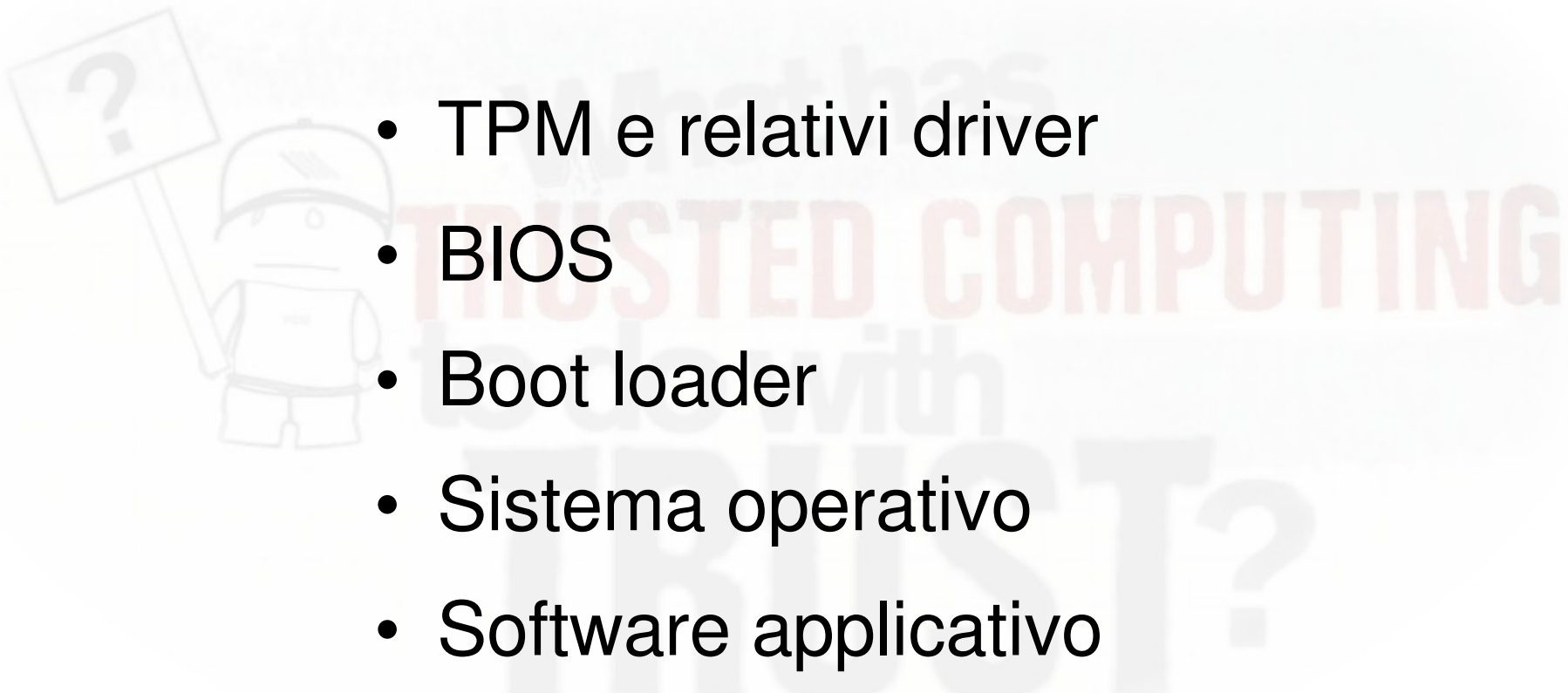
- Traduzione: “informatica fidata”.
- Alias: TCPA, Palladium, NGSCB, LaGrande Technology, Presidio, ...
- Trusted Computing Group (TCG)
  - Consorzio no-profit nato nel 2003 per la stesura di specifiche *hardware* e *software* relative al TC.
  - Promotori: AMD, hp, IBM, Infineon, Intel, Microsoft e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



# Cos'è il TC

- 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, VCR, lettori DVD, telecamere, ...)

# Componenti di un sistema TC

- 
- TPM e relativi driver
  - BIOS
  - Boot loader
  - Sistema operativo
  - Software applicativo

# Features del TC

- Cifratura on-the-fly delle informazioni (documenti, comunicazioni, ...).
- Memorizzazione delle proprie chiavi in un posto sicuro.
- Firme elettroniche e verifica delle stesse.
- Protezione dal malware.
- Verifica da parte di altri dello stato del sistema.

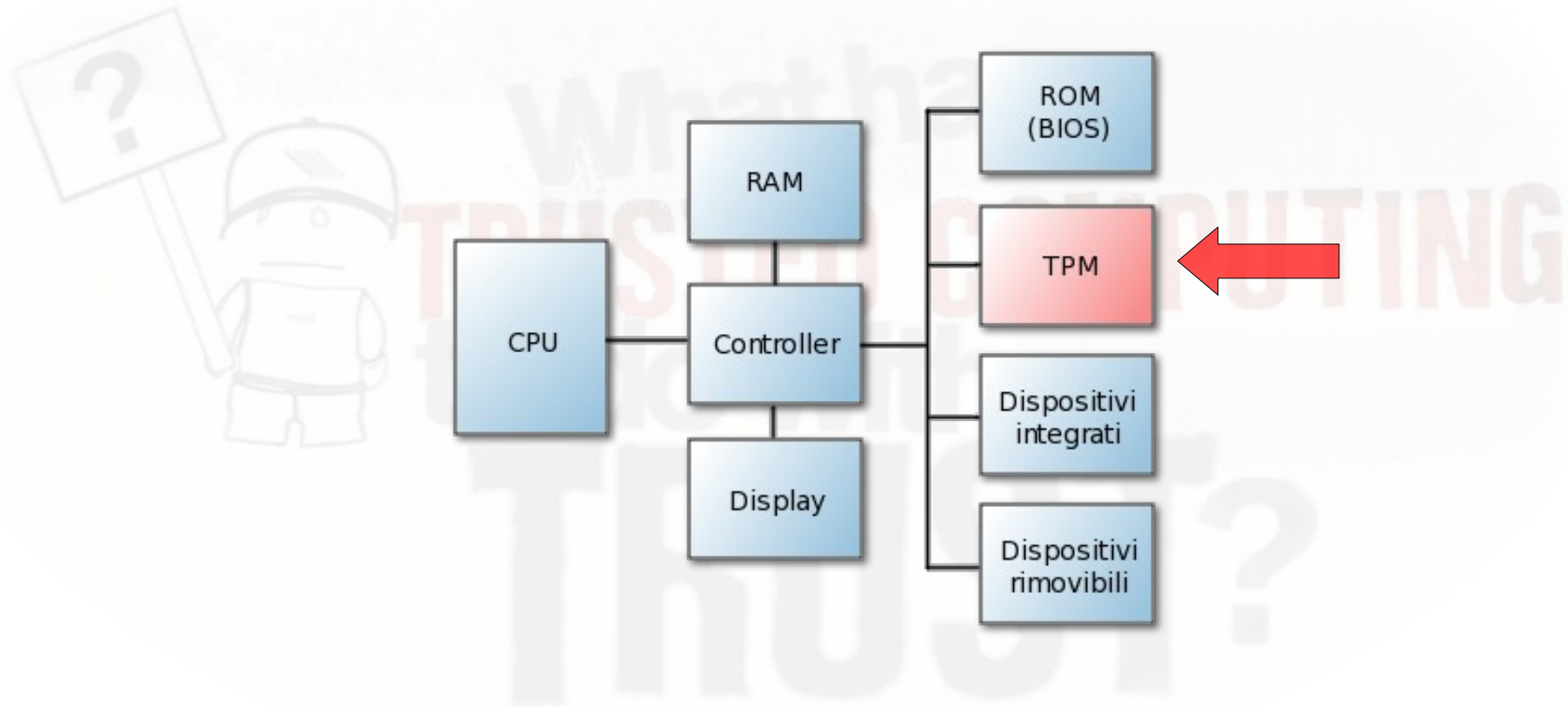
# Caratteristiche del TC

- **I/O sicuro:** cifratura delle informazioni che transitano sui bus di sistema.
- **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.

# Le sorgenti della sicurezza

- **Roots of Trust** (sorgenti di sicurezza)  
Componenti che *devono essere ritenuti fidati* per definizione.
  - Root of Trust for Measurement (RTM)  
Algoritmo per la verifica dell'integrità del sistema.  
Radice del *transitive trust* (CRTM).
  - Root of Trust for Storage (RTS)  
Algoritmo per la gestione delle *impronte* sullo stato di integrità del sistema.
  - Root of Trust for Reporting (RTR)  
Algoritmo per la fornitura delle informazioni gestite dal RTS.

# Architettura TC



Schema dell'architettura di un sistema TC

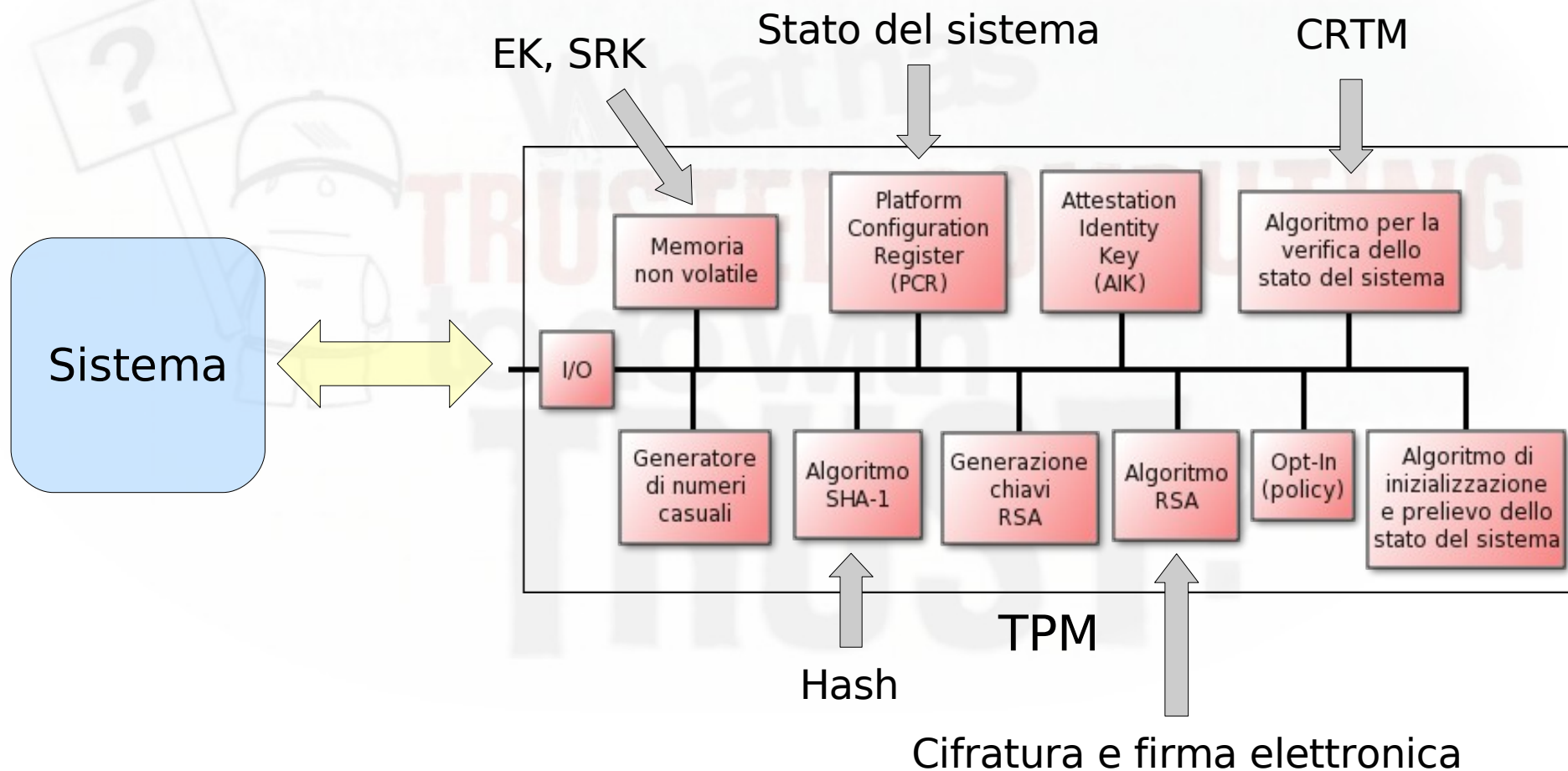
# TPM

## Trusted Platform Module

- Detiene la *Endorsement Key* (EK) – che lo *identifica univocamente*.
- Effettua la cifratura delle informazioni.
- Detiene informazioni sullo *stato del sistema* nei Platform Configuration Register (PCR).
  - $PCR[n] \leftarrow \text{SHA-1}(PCR[n] + \text{informazioni prelevate})$
- Genera e gestisce le *Attestation Identity Key* (AIK).
- Genera e detiene la *Storage Root Key*.
- Effettua la protezione della memoria.
- Opt-in policy: possesso, abilitazione, attivazione.



# TPM



# 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

- Protezione della memoria.
  - Problemi nel debug del software (neanche il S.O. può accedere a certe zone di memoria).
- L'AIK, firmata con l'EK, viene utilizzata nel protocollo di attestazione remota.
  - Riconoscimento della macchina.
- Il TPM può essere disattivato dal proprietario.
  - Alcune funzionalità rimangono comunque inalterate.
- Il TCG riconosce le potenzialità della tecnologia descritta, ma **lascia ai produttori l'implementazione delle specifiche.**

# Osservazioni sul TC

- Specifiche fumose e per certi versi troppo generiche.
  - Cosa si intende per “sicurezza”? Che i prodotti vengano sicuramente utilizzati come vuole il *produttore* e non come desidera il *proprietario* della macchina?
  - Chi sono le entità sconosciute o non autorizzate dalle quali il TCG vuole “proteggere” gli utenti?
- **Chi stabilisce quale software può essere eseguito dal sistema?**

# Attestazione remota

- *L'attestazione* certifica che in un certo istante sul computer è in esecuzione una certa combinazione di programmi. *L'attestazione remota* comunica ad altri questa informazione.
- Si perde il beneficio della **non conoscenza del software** che gira sulle altre macchine.

*La non conoscenza del software in esecuzione sui sistemi remoti è un beneficio perché limita le possibilità di controllo sugli altri.*

# Interoperabilità

- Possibilità per un fornitore di un servizio di controllare se sulle macchine client gira un programma a lui gradito oppure no.
- I dati salvati da un programma saranno recuperabili da altri programmi?
  - Possibili pratiche *anticompetitive*.
- Scarsa possibilità allo sviluppo di software per la comunicazione tra piattaforme diverse (es. Samba).
- I virtualizzatori non funzioneranno con il TPM.

# Key escrow

- Chi ci assicura che non esistano backdoors?
  - Funzionalità non documentate.
  - Meccanismi nascosti di accesso alle chiavi private.
- L'hardware è generalmente più difficile da verificare rispetto al software.
- I governi potrebbero richiedere ai produttori di ottenere un accesso privilegiato sui sistemi (v. clipper chip).



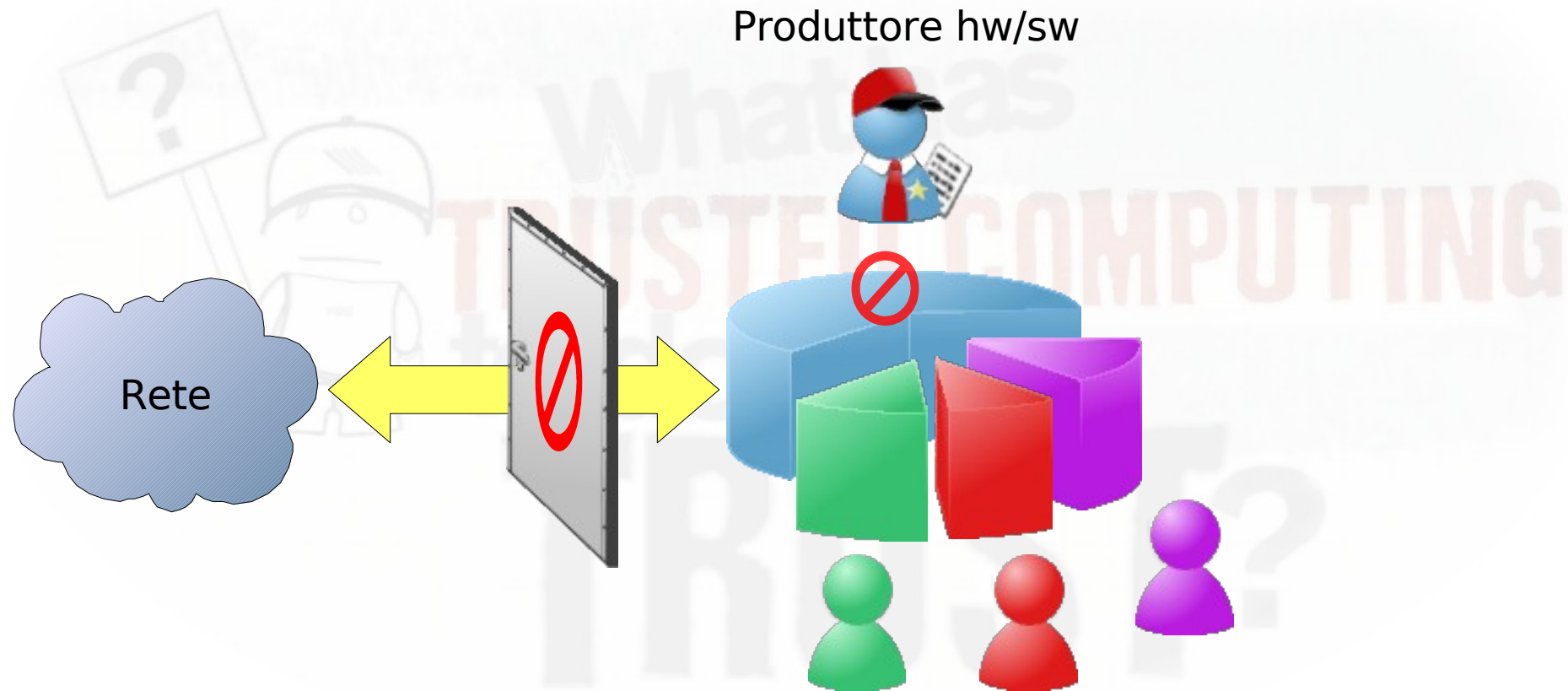
# DRM

- Digital Rights Management = gestione dei diritti digitali.
- 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.
  - Caso DVD DeCSS.
  - Caso rootkit Sony/BGM.

# I produttori hw/sw

- Prova di Intel: l'identificativo dei PIII.
- Windows Vista è pronto per il TC.
- Molti sistemi **già sul mercato** includono i chip TPM. Il TPM verrà integrato all'interno delle CPU.
- Il TC non sarà solo per i computer, ma per tutti i dispositivi digitali.
- Cartello di mercato: diverrà impossibile per i consumatori trovare componenti non TC.

# 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 proprietario di un dispositivo è un possibile “nemico”.
- Censura dei siti web.
- Censura dei contenuti digitali.
- Fidelizzazione forzata degli utenti.
- Crollo degli standard per l’interscambio delle informazioni.

# Owner override

- Proposta di EFF
  - L'utente non è un nemico e deve poter gestire i meccanismi di TC a proprio piacimento.
  - AIK a disposizione dell'utente.
  - Possibilità di inviare una falsa attestazione di integrità.
- Conseguenze
  - Il TC non può essere utilizzato per il DRM.
  - Non tutti i problemi vengono risolti (sealed storage e memory curtaining).

# 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 ThinkPad 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.
- Trusted Computing o *Threacherous Computing*?

TC

~~Trusted Computing~~  
(informatica fidata)



**Threacherous Computing**  
(informatica infida)



# Cosa fare?

- Informarsi sul Trusted Computing.
- Divulgare l'informazione sul Trusted Computing.
- Acquistare dispositivi digitali con cautela.
- Aiutare [www.no1984.org](http://www.no1984.org) ;-)
- Se nessuno fa niente i produttori hw/sw avranno la strada spianata.
- Noi siamo i clienti: senza il nostro “consenso” i produttori non vendono.

# 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.msp>

Wikipedia – Trusted Computing

[http://it.wikipedia.org/wiki/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](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](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>



What has  
TRUSTED COMPUTING  
to do with  
TRUST?

# *Domande?*