Trusted Computing: tecnologia ed applicazione alla protezione del web

Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

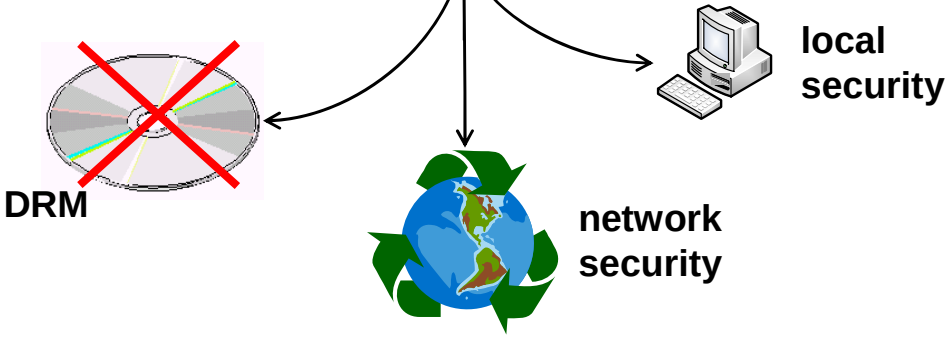
Abbiamo delle certezze?

- nella mia rete sono presenti solo i miei computer?
- i miei computer hanno installato solo il sw che io desidero?
- il sw è configurato nel modo prescelto?
- quando uso Internet invece di una rete privata, sono davvero collegato al nodo desiderato?
- quando sono collegato ad un server, posso sapere se il servizio è quello "buono"o è stato alterato?

TRUST & INTEGRITY

Che cosa è un sistema "fidato" (trusted)?

Chiamasi "fidato" (trusted) un sistema o componente che si comporta nella maniera attesa per uno specifico scopo.



Trusted Computing (TC) – il problema

- **situazione attuale (non-TC):**
  - la mia applicazione è stata infettata da un virus?
  - il mio sistema operativo ospita un cavallo di Troia?
  - il mio hw contiene una "cimice"?
  - posso provare a terzi che il mio sistema è "sano"?
- **molto, molto, molto difficile (impossibile?) da ottenere … a meno di avere:**
  - sicurezza fisica (=isolamento)
  - fiducia nel personale sistemistico
  - nessun collegamento di rete

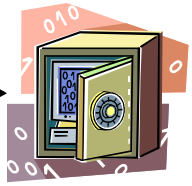
TC – le fondamenta

- garanzia che il SO sia stato caricato correttamente
- richiede che l'hardware non sia stato modificato
- possibile rendere l'attacco difficile (ma non impossibile …) mettendo le funzioni di boot fondamentali in un chip speciale
  - TPM – Trusted Platform Module
- metodi per verificare il processo di boot
  - il verificatore deve essere un elemento hw (core root of trust)
- una volta caricato in modo sicuro il primo elemento sw tutti gli altri (sino alle applicazioni) possono essere verificati in cascata

Verifica dei controlli eseguiti

- memorizzazione dei risultati dei controlli effettuati
- registri hw dedicati (e sicuri) per conservare i valori di hash di tutte le componenti sw eseguite
- valori dei registri usabili per protezione locale e fornibili a terzi per dimostrare lo stato di integrità del sistema

attestation
proof for 3rd parties

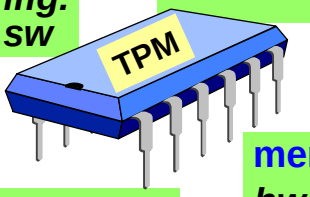


sealed storage
opens only if system is in a specific "state"

Componenti di un sistema TC

isolamento
esecuzione in domini / compartimenti / ambienti distinti

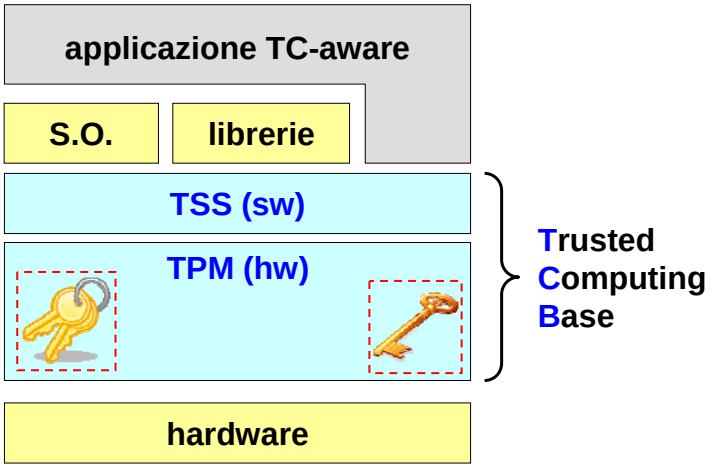
attestazione
garanzia della config. hw e dello stack sw



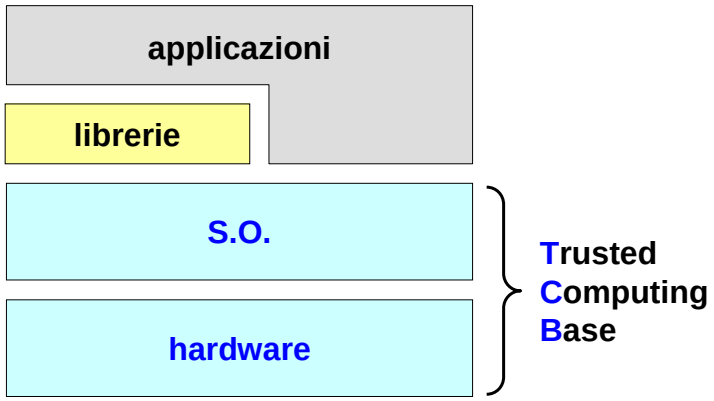
memoria protetta
hw key container
cifratura dati
data sealing

I/O sicuro
verso l'utente
tra le varie componenti

TC – architettura software e TCB



TCB in un sistema tradizionale



TC – gli attori

- **TCG (TC group)**
  - www.trustedcomputinggroup.org
- **Microsoft**
  - NGSCB (Next Generation Secure Computing Base) e Vista
- **vari progetti open-source**
  - es. Open-TC (www.opentc.net)
- **produttori di hw:**
  - Intel (CPU “LaGrande”) e AMD (CPU “Presidio”)
  - Infineon (chip TPM)
- **vari governi (Francia, Germania, Cina, …)**

TC – componenti tecniche (I)

- **EK (Endorsement Key)**
  - chiave RSA 2048 bit
  - generata una volta sola alla fabbricazione del TPM
  - usata per fare le attestazioni (TPM “genuino”)
- **remote attestation**
  - certificazione stack sw in uso in un certo istante
  - possibile anche in forma anonima (DAA)
- **memory curtaining**
  - isolamento completo (anche dal SO) di alcune aree di memoria
  - accessibili solo da uno specifico programma

TC – componenti tecniche (II)

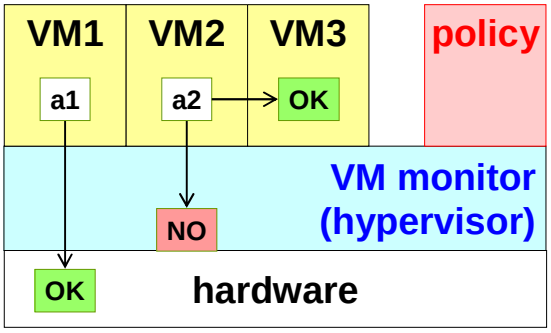
- **sealed storage**
  - dati cifrati con una chiave derivata dalla combinazione di hw+sw usato
  - dati decifrabili solo dalla stessa combinazione
  - chiavi “migrabili”
    - indicazione esplicita dell’utente
    - indicazione esplicita del TPM destinatario
- **I/O sicuro**
  - canali protetti tra utente e dispositivi (=impossibile intercettare o cambiare i dati)

Troppo controllo?

- **le tecniche di TC suscitano dubbi su:**
  - chi governa realmente il sistema
  - chi è il proprietario dei dati
- **in realtà noi vogliamo protezione ma anche:**
  - trasparenza su chi controlla le varie parti/dati del sistema
  - mantenere il controllo del sistema

TC e virtualizzazione

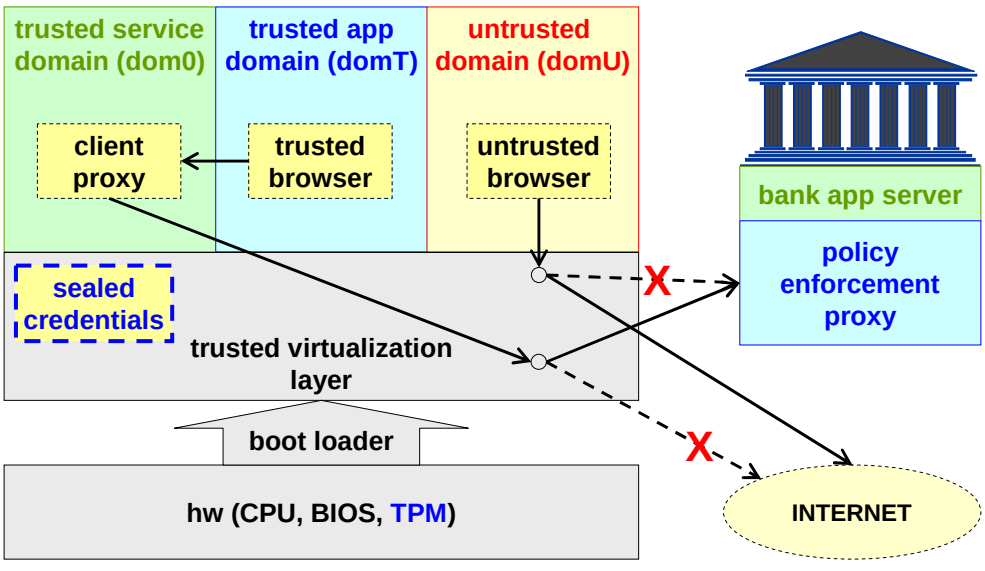
- **uso di uno stesso computer per:**
  - attività lecite e protette
  - attività “pericolose” o non previste



Esempio: Private Electronic Transactions

- **phishing**
  - si accede a un server web falso
  - … che cattura le credenziali dell'utente
  - … e poi le usa sul vero server web
- **vulnerabilità software lato utente**
  - SO o browser bacato o vulnerabile
- **malware**
  - cavali di troia, key logger, …

PET : architettura



PET : contromisure

- **compartimenti isolati (trusted/untrusted) sul client**
  - differente visualizzazione dei compartimenti
- **autenticazione del server web**
  - root CA + certificati del server = all'interno del compartimento trusted
- **mutua attestazione remota tramite proxy**
  - cliente: attestazione remota alla banca
  - banca: autenticazione al cliente
- **firewall sul compartimento trusted**
  - blocca tutte le connessioni in ingresso
  - ridirige tutto il traffico in uscita al proxy del client
- **protezione delle credenziali in memoria "sigillata"**

TC e open-source

- **TSS (TC Software Stack) open-source:**
  - C
  - Java
- **progetto Europeo Open-TC (www.open-tc.net)**
  - versione di Linux che usa TPM 1.2 per funzioni di sicurezza
  - uso di L4 o XEN per creare macchine virtuali assolutamente protette
    - virtualizzazione dei server
    - VM sul client per operazioni "rischiose"

TC – possibili applicazioni (I)

- **utenti generici**
  - operazioni critiche (es. firma digitale)
    - certezza di non manipolazione del sw e dei dati
- **industrie e fornitori di servizi (in outsourcing)**
  - attività “trusted” e “auditable”
    - nella gestione di impianti critici
    - per fornire prove certe ai clienti o a terzi

TC – possibili applicazioni (II)

- **banche e finanza per transazioni B2C**
  - il cliente non può ripudiare la transazione
  - le credenziali (es. password) non possono essere rubate facilmente
  - il cliente può fidarsi del server (evitando così il phishing)
  - client può verificare identità e stato del server
  - server può verificare lo stack sw del client

TC – possibili applicazioni (III)

- **virus e spyware**
  - protezione delle applicazioni
  - protezione dei programmi antivirus e dei loro dati
- **protezione dati biometrici**
  - accessibili solo ad applicazioni “trusted” (una password si può cambiare, un’impronta no …)
- **grid computing**
  - integrità sw dei vari nodi, da cui deriva l’integrità dei risultati (qualcuno potrebbe falsare i risultati …)
- **evitare i bari nei giochi on-line**
  - persone che modificano il proprio client

Conclusioni

- **chip TPM e CPU con TPM sono già in produzione:**
  - IDC stima che entro il 2010 tutti notebook e la maggioranza dei desktop avranno il TPM
  - il DOD dal 2008 compra solo notebook con TPM
- **è quindi molto probabile che il nostro prossimo PC abbia il TPM:**
  - cerchiamo di usarlo per i nostri fini
- **come al solito, non è la tecnologia in sè ad essere buona o cattiva ma l’uso che noi ne facciamo**