Crittografia avanzata
Lezione del 4 Aprile 2011

Il trusted computing

- Problema: un apparato è “in mano” a qualcuno che
  - Lo deve utilizzare
  - Non è fidato
- Il “proprietario” vuole assicurarsi che l'apparato sia utilizzato nei modi desiderati

A che livello è fidato?

- Tutti: vuole dire partire dall'hardware
  - Implementazione a livello tale da non poter essere manomessa
    - Modding
    - False smart card
    - …

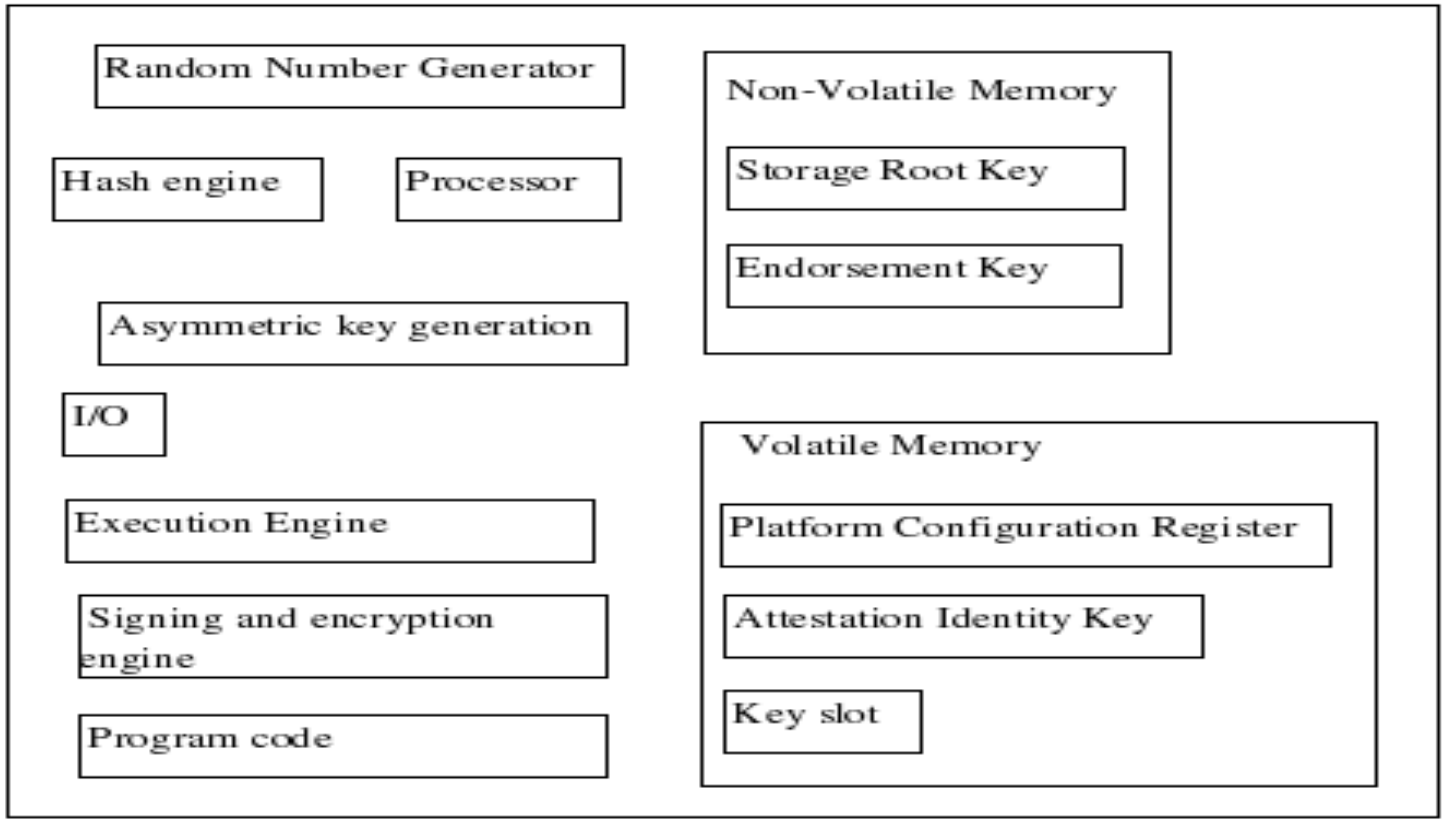
Differenze rispetto ad altre piattaforme

- Pay TV/Satellite: basta proteggere la master key
- HDTV/DRM: simile, ma apparati specializzati
  - Fino a un certo punto...
  - Molti produttori => poca robustezza
- Cellulari
  - Interessa proteggere soprattutto la SIM, che “si protegge da sè”
- Per i PC
  - l'uso deve rimanere “general purpose”
  - Poco controllo sui componenti software

Soluzione: TPM

- Trusted Platform Module
  - Integrato nel package della CPU
    - Ma non controllato dalla CPU
  - Surface mounted sulla mainboard
- Capacità:
  - PRNG
  - Memoria protetta
  - Capacità elaborativa (algoritmi crittografici, “misure”, in pratica hash)
- In sostanza, una smart card che è sotto il controllo del proprietario

Componenti


Random Number Generator
Hash engine
Processor
Asymmetric key generation
I/O
Execution Engine
Signing and encryption engine
Program code
Non-Volatile Memory
Storage Root Key
Endorsement Key
Volatile Memory
Platform Configuration Register
Attestation Identity Key
Key slot

Endorsement Key

- Chiave “madre” RSA creata nel TPM al momento dell'inizializzazione **in fabbrica**
- La chiave pubblica, esportata, identifica univocamente il TPM e quindi il PC
  - È sotto il controllo esclusivo del TPM
  - È associata al PC su cui è installato il TPM
- È utilizzata anche per “firmare” altre chiavi generate dal TPM e da utilizzare nelle diverse attività legate al TC
- È utilizzata in autenticazioni challenge/response firmando nonce

Conformance Credentials

- Una terza parte fidata “certifica” che un certo hardware associato al TPM è conforme alle specifiche e quindi il TPM
- Questo certificato può essere usato per decidere se quel TPM/PC potrà avere accesso a dei dati/servizi

Memoria protetta

- Memory curtaining
  - Memoria protetta anche dal S.O.
  - Può essere a bordo del TPM
  - Può essere memoria del PC con dati cifrati in modo da essere accessibili solo al TPM
- Sealed storage
  - Dati che è previsto siano accessibili solo da una specifica combinazione di hw/sw (un pc in una certa configurazione)

Storage Root Key

- Chiave RSA usata per cifrare/decifrare le chiavi di cifratura di dati/memoria
- Può cambiare al momento del “Take ownership”
  - Meccanismo fondamentale per trasferire dati/backup da un sistema all'altro
- Usata per cifrare/decifrare chiavi per la protezione di dati
- Migrabili/non migrabili: posso essere o meno estratte dal PC e portate su un altro

Il processo di bootstrap

- Core Root of Trust Measurement: Boot block del BIOS (trusted, immutabile)
  - Che permette di verificare l'integrità del Trusted BIOS
  - Che permette al BIOS di (chiedere di) verificare l'integrità dell'hardware e del bootloader
  - Che permette al bootloader di verificare il kernel
  - Che permette al S.O. di (chiedere di) verificare l'integrità delle applicazioni (es. JVM, macchina virtuale...)
- Tutto questo permette al TPM di attestare che il sistema è in uno stato Trusted

Misure

- PCR: Platform Configuration Register
  - Utilizzati per mantenere hash (SHA-1?) di applicazioni
  - Sono in numero limitato, quindi si usa un'operazione di hash chaining per conservare misure di più applicazioni (PCR extend)
  - Le singole misure sono anche conservate in un log che permette di “ricostruire” la storia o rilevare la manipolazione
  - Solo dopo che la misura è scritta nel PCR il controllo può essere passato all'entità misurata
- http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_ima.measurements.html

Remote attestation

- Si firma lo “stato” (PCR) e si invia insieme a SML ad un sistema remoto, che in base a questo decidono se dare l'accesso a dati e servizi
  - I dati arrivano cifrati per quel TPM
- Per non esporre l'EK e mantenere un certo “anonimato”, il TPM può generare delle Attestation Identity Keys e concederne l'uso ad applicazioni quando il sistema è in stato trusted
- Le AIK saranno in generale certificate da una CA, e solo questa le linkerà all'EK, mentre chi riceve l'attestazione le legherà a un'identità diversa per ogni AIK
  - Problemi come la firma “al volo” delle AIK e il ruolo della CA

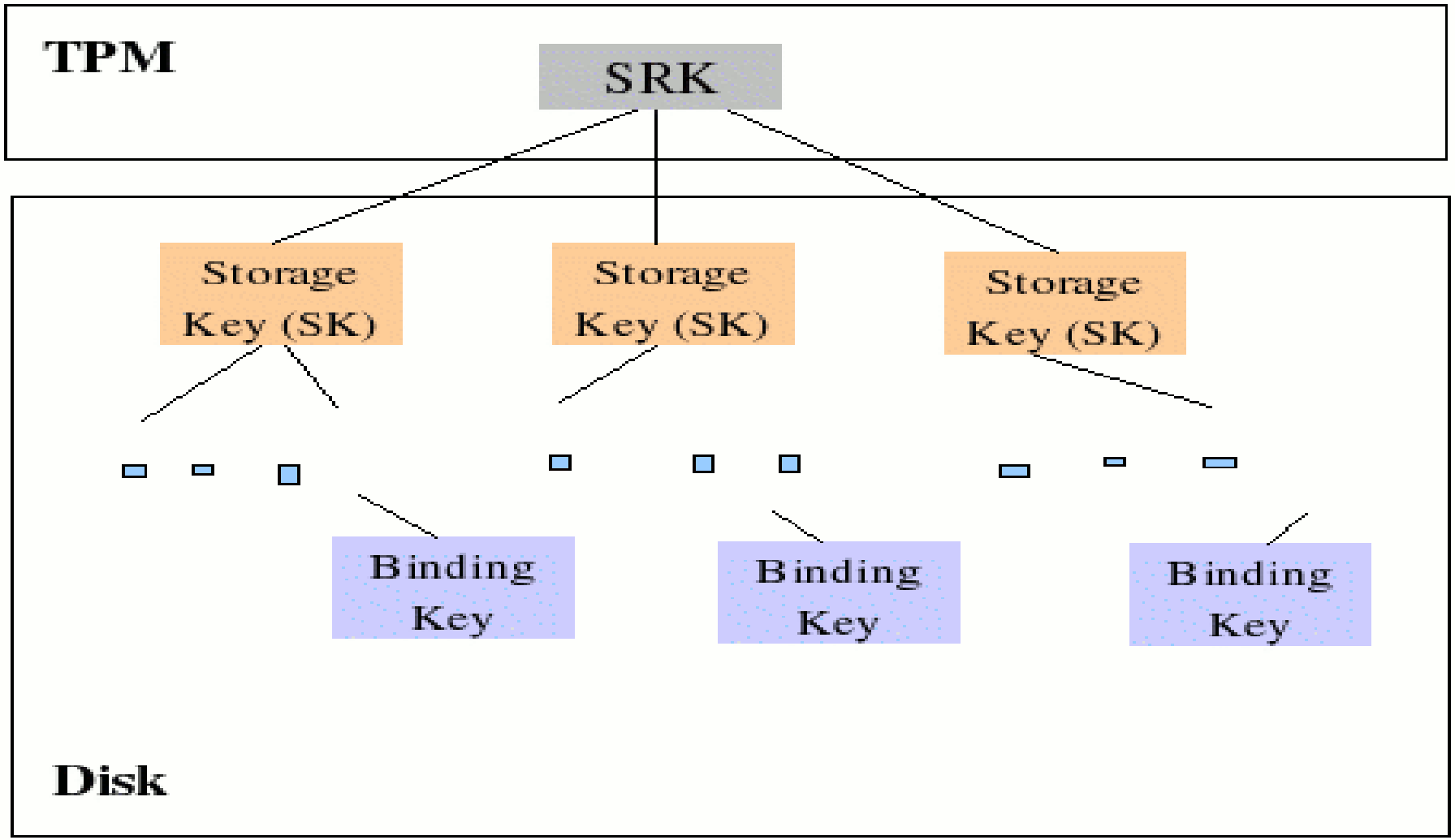
Direct Anonymous Attestation

- Lo vedremo un altro giorno

Protected Storage

- Si usa una gerarchia di chiavi
  - Per aumentare la flessibilità
  - Per ridurre il carico al TPM
  - Per gestire la portabilità dei dati da un sistema all'altro
- Storage Keys: usate per cifrare chiavi di storage
  - Cifrate con la age Root Key
- Binding keys
  - Usate per cifrare chiavi simmetriche, usate per cifrare i dati
  - Sono migrabili
- Sealing: usa chiavi non migrabili, PCR e dati

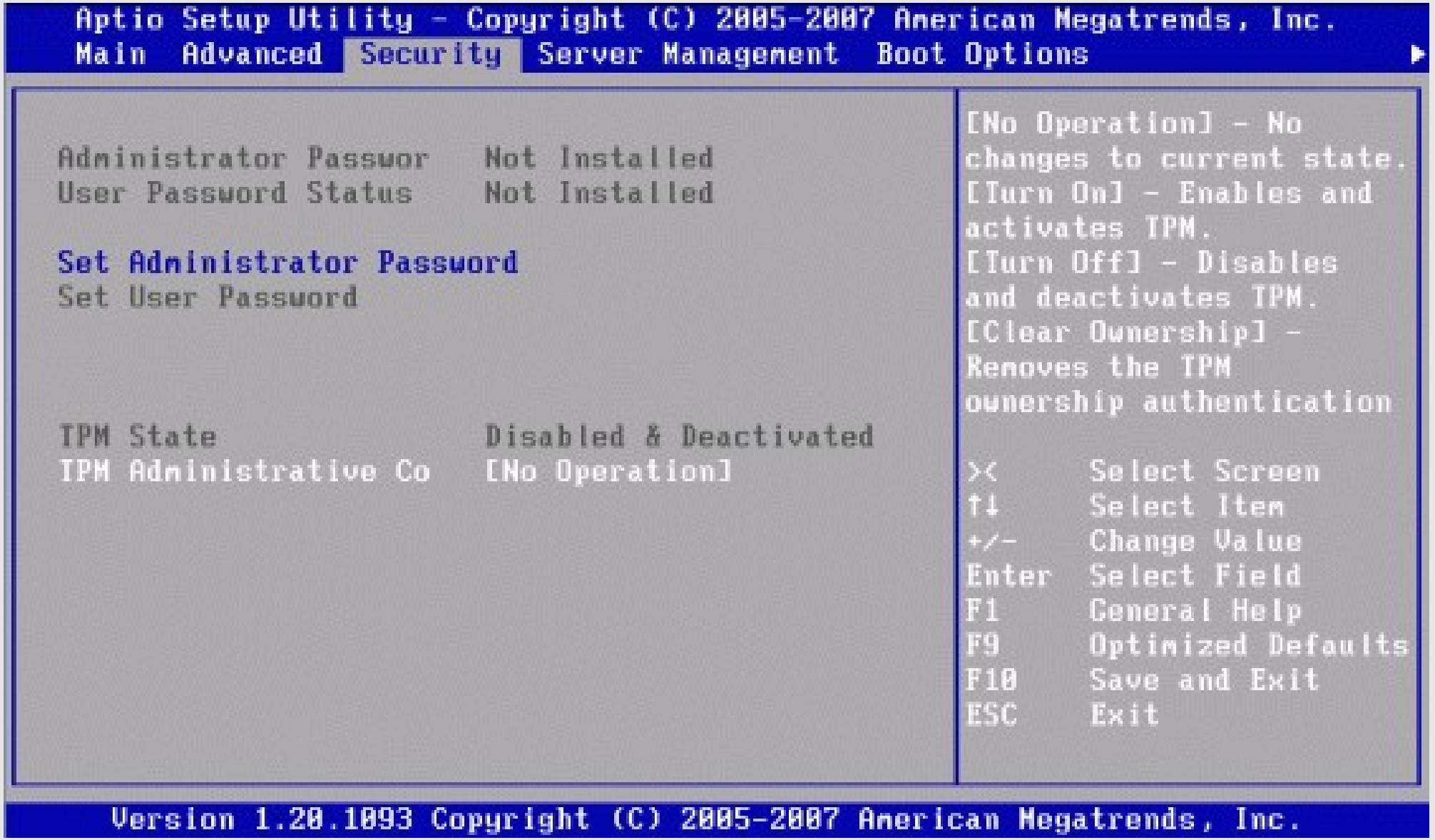
Chiavi per lo storage



Owner/user

- Owner: configura (non controlla!) il TPM
  - es. lo abilita/disabilita
- User: usa il computer senza poter interferire con il TPM
- L'Amministratore del PC è in generale uno user
- Take ownership: operazione specifica che rende “owner” inserendo una chiave
- Operazione gestita generalmente a livello BIOS

Attivazione TPM



TC: non solo tecnologia

- Rischi del TC: vedi quaderno Clusit
- Opportunità in molti contesti chiusi o specialistici in cui si pone il problema dell'hardware
- BitLocker

Cifratura sul bus

- I dati possono dover essere protetti anche in transito verso le periferiche
  - Soprattutto verso la scheda video...
- Contrattazione/gestione di chiavi con le periferiche e cifratura sul bus es. PCI
- Problema analogo a quello di HDCP (High-bandwidth Digital Content Protection) per DVI