Convegno Associazione ICT Dottori Commercialisti

Sicurezza in dispositivi hardware a basso costo

(Internet-of-Things per aziende e privati)

Torino, 20 novembre 2023

Relatore: Prof. Antonio Lioy

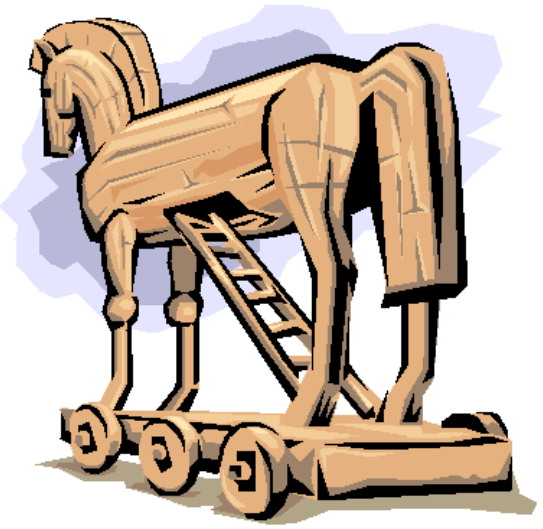
Politecnico di Torino

(antonio.lioy@polito.it)

TaxLawPlanet Webinar

Cavalli di Troia

- ben noti in campo software, ad esempio:
  - un gioco "craccato" a cui è stato aggiunto un "keyboard logger" per registrare password, numeri di carta di credito, …
  - un'estensione di un browser che non sol registra i dati inseriti ma nache copia/altera la visualizzazione dei dati inseriti in un form
  - da MITM (Man-In-The-Middle) … a MATE (Man-At-The-End) o MITB (Man-In-The-Browser)
- … ma ora presenti in campo hardware, ad esempio:
  - report da varie agenzie governative su chip/board manipolate
  - restrizioni sui fornitori di tecnologie 5G/6G
  - il famoso caso CryptoAG – "operazione Rubicone"



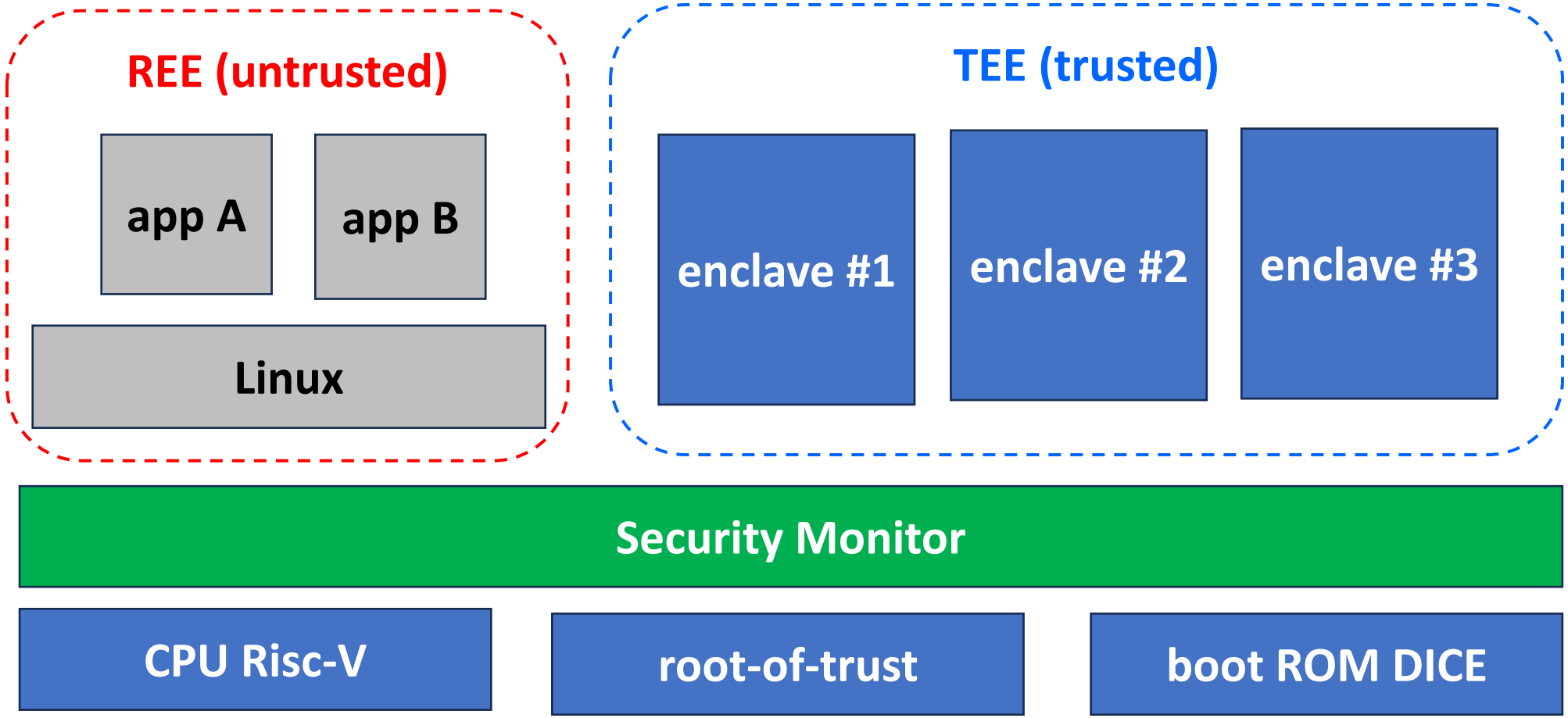
La produzione di chip e board

- design occidentale (US, EU, …)
- ma produzione concentrata in pochi paesi, soprattutto asiatici
  - Taiwan, Corea, Singapore, Cina, …
- molto difficile verificare la corrispondenza tra progetto e realizzazione fisica
  - molti punti di manipolazione nella catena di fornitura (supply chain)
  - non solo per modificare il funzionamento ma anche per renderlo inaffidabile (guasti più frequenti, errori casuali, …)

Open-source hardware

- tutti conosciamo il sofwtare open-source (es. Linux)
- ora arriva anche l'hardware open-source
  - design proprietario (es. Intel, AMD)
  - design coperto da IP (es. ARM)
  - design open (es. RISC-V)
    - implementazione a scelta
    - recente annuncio Qualcomm + Google
- non solo per la CPU … ma anche per la sicurezza
  - Open-Titan
  - progetto H2020 SPIRS

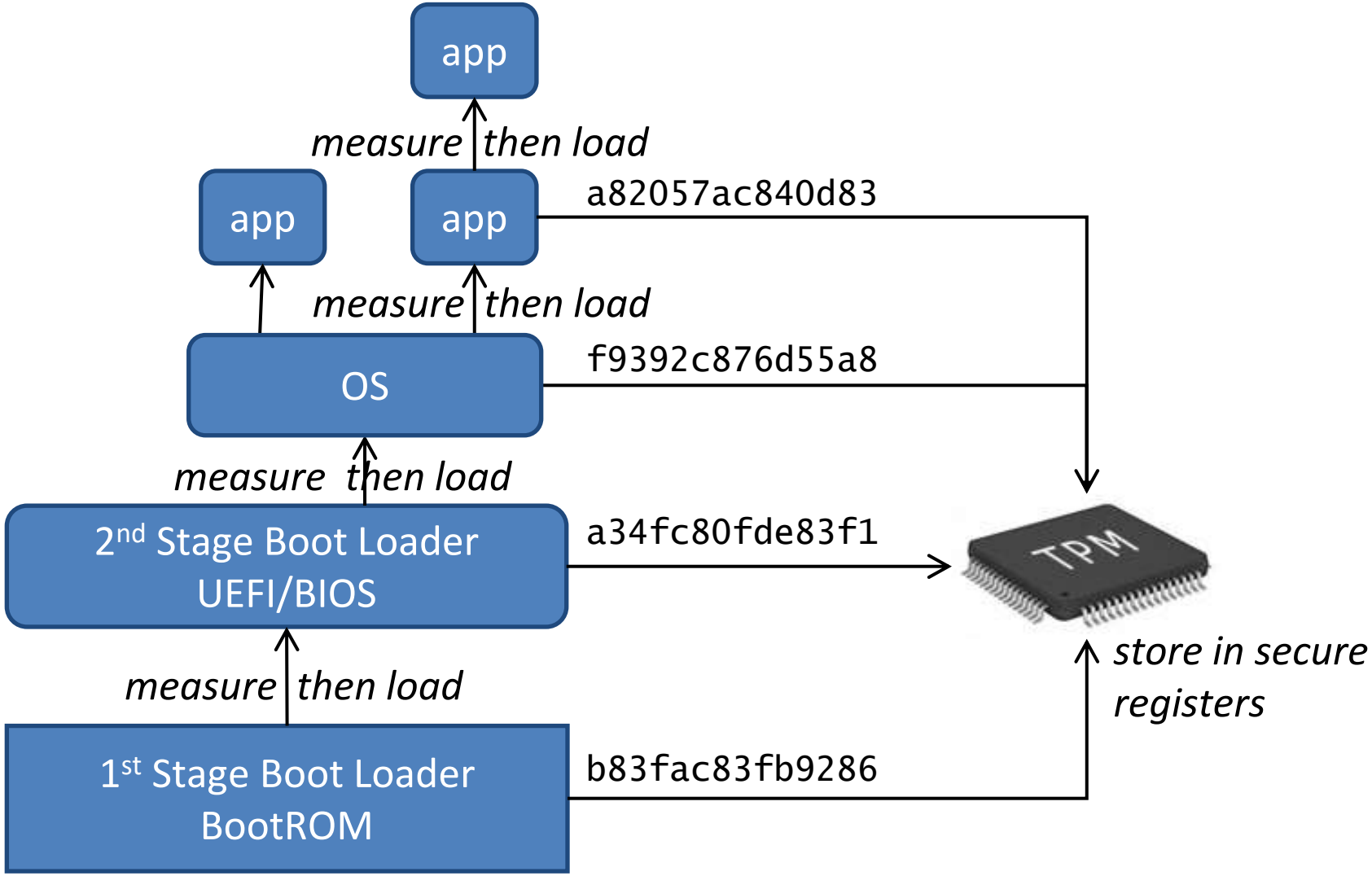
Architettura SPIRS



SPIRS: implementazione

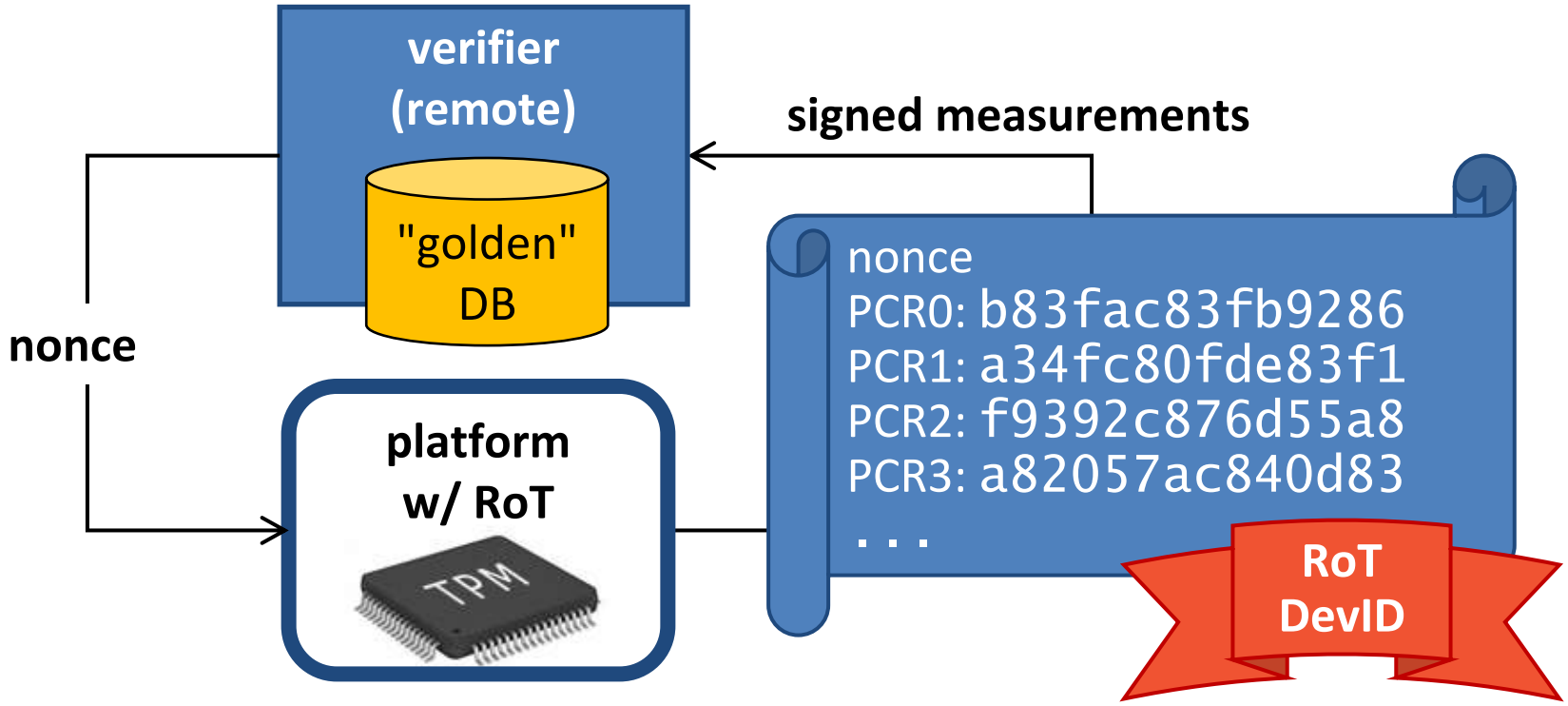
- hardware open-source
  - RISC-V
  - acceleratori crittografici (AES, ECDSA, SHA-3)
- software open-source
  - Keystone TEE (Trusted Execution Environment)
  - Linux
  - DICE
- implementazione "trusted"
  - FPGA (per piccole quantità, basse prestazioni)
  - chip (grandi quantità, altre prestazioni)

Measured boot (and execution)



SPIRS: attestazione

- permette di verificare il software e l'hardware di un nodo di rete
- ogni componente sw eseguito viene riportato al verificatore (esterno)
- confronto con componenti autorizzati



SPIRS: applicazioni

- nodi sicuri per implementare terminatori di rete 5G/6G
- automazione di fabbrica
  - sistemi di monitoraggio della produzione
  - sistemi di controllo della produzione