✨Cos’è il Confidential Computing?

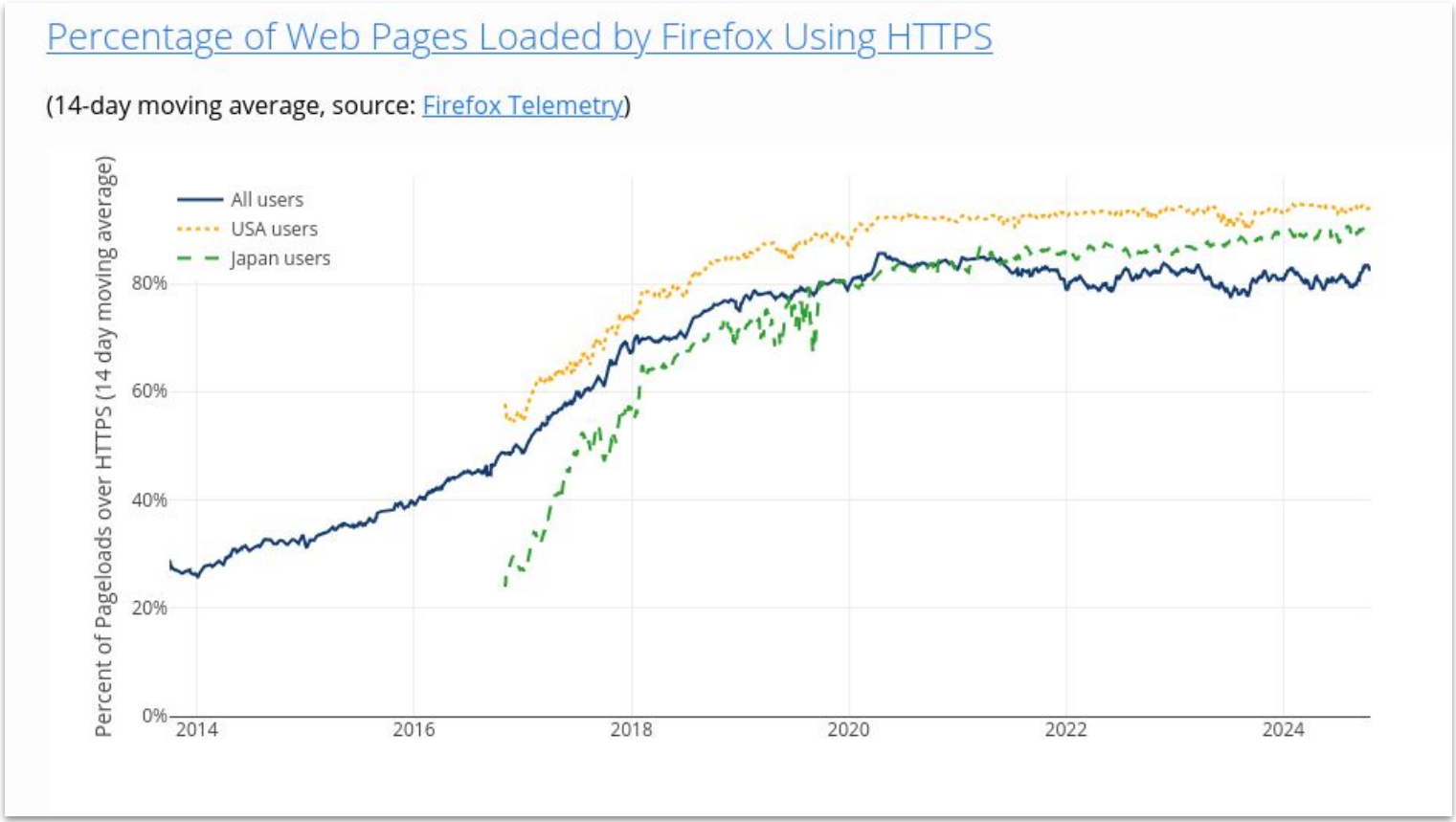
✨Cos’è il Confidential Computing?

Camilla Conte

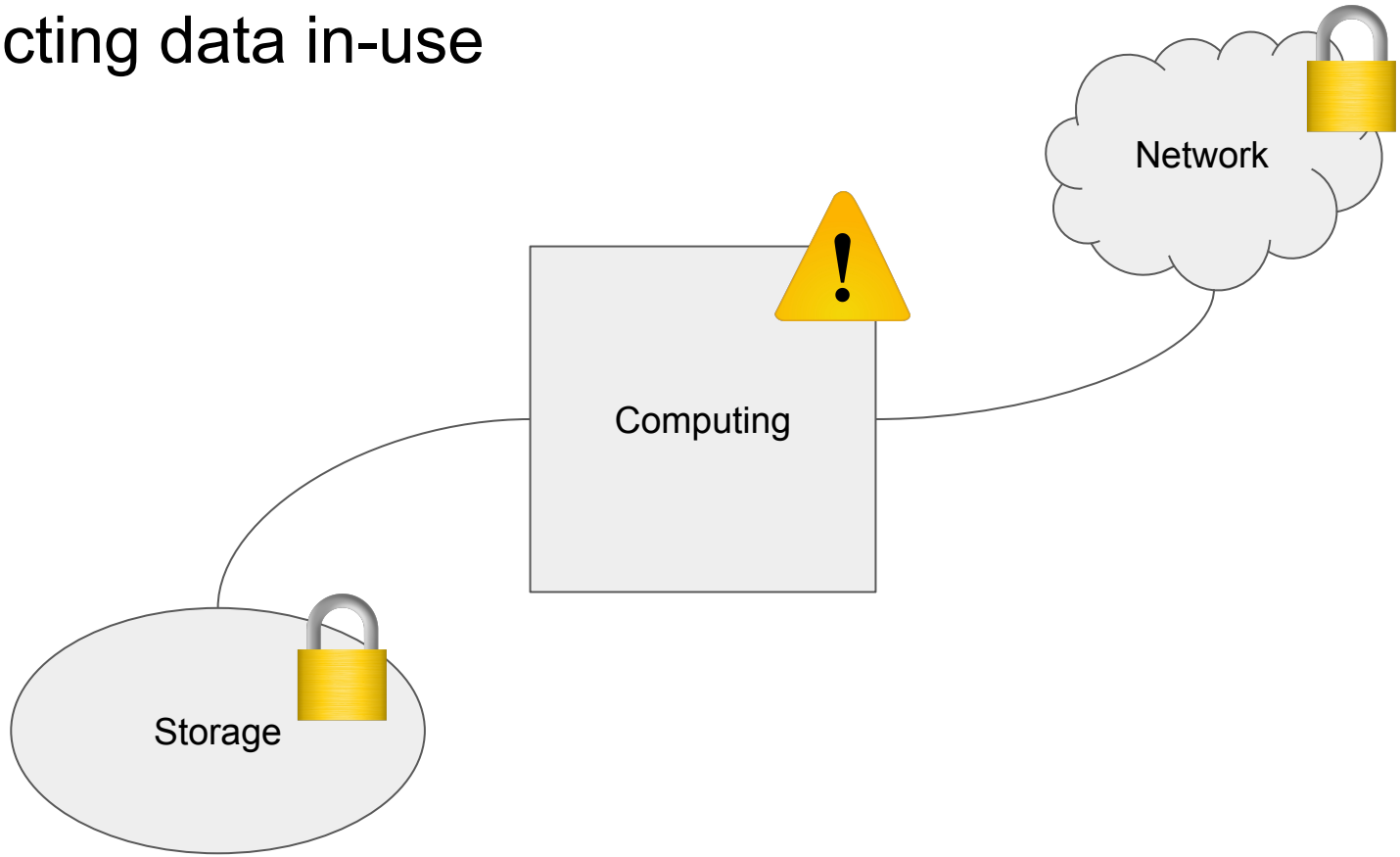
1. Introduzione
2. Encrypted Memory
3. Attestation
4. Hardware Root of Trust

Introduzione

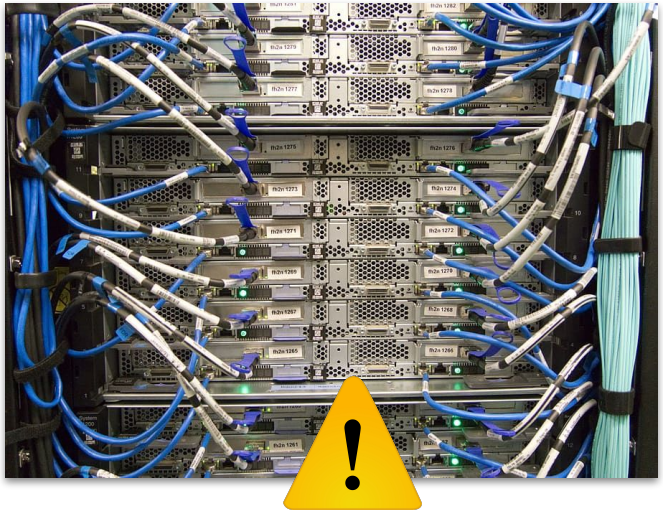
“Confidential Computing is HTTPS for hardware”



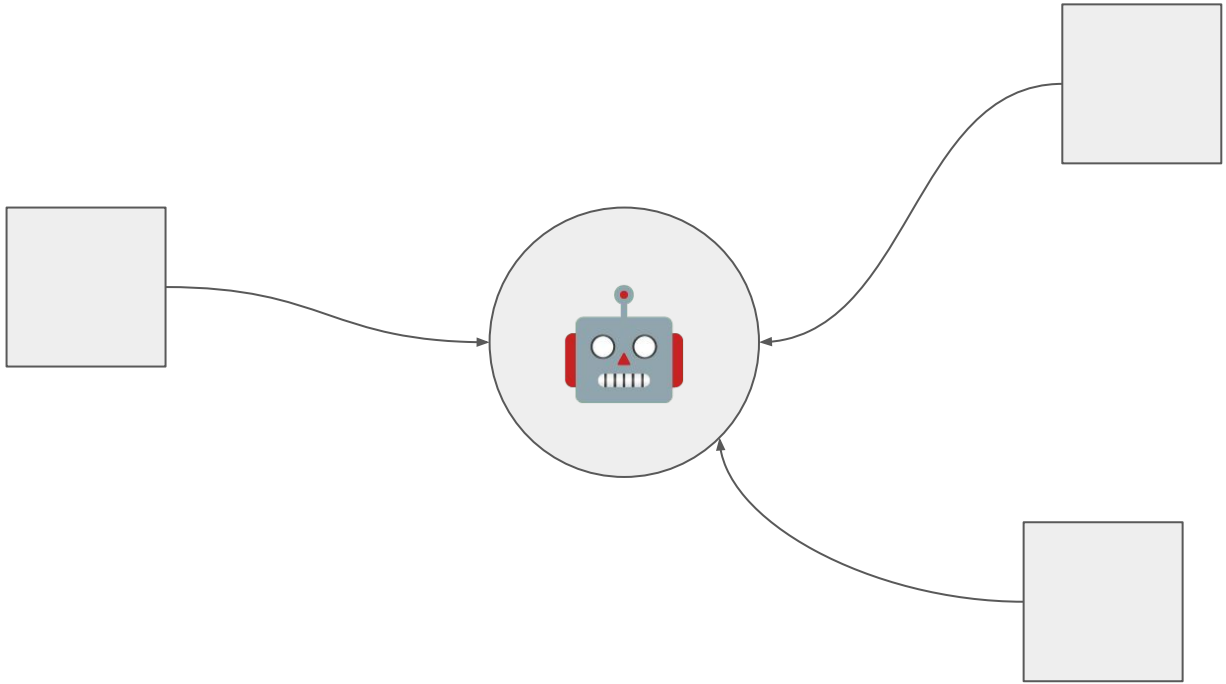
Protecting data in-use



Protecting data in-use

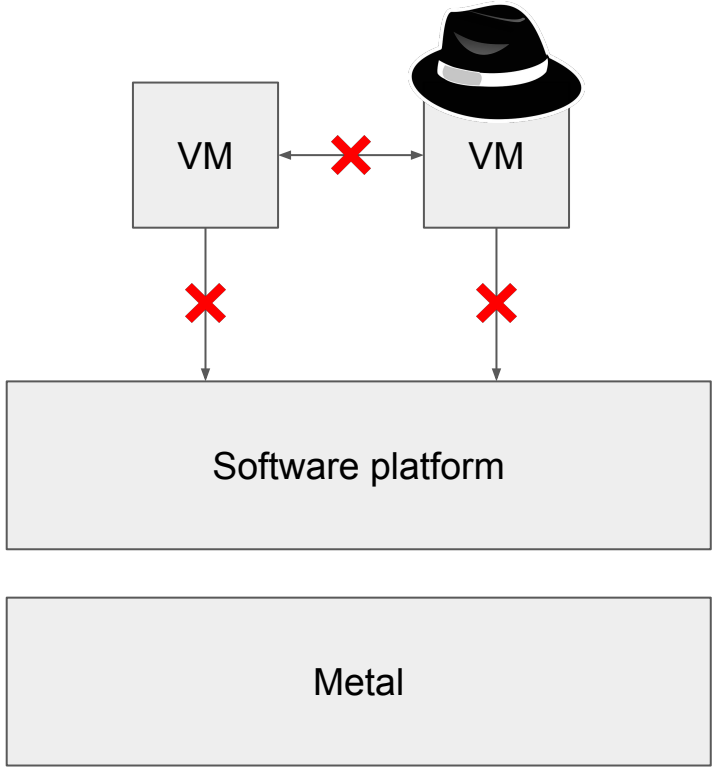


Secure multi-party computation and Federated learning

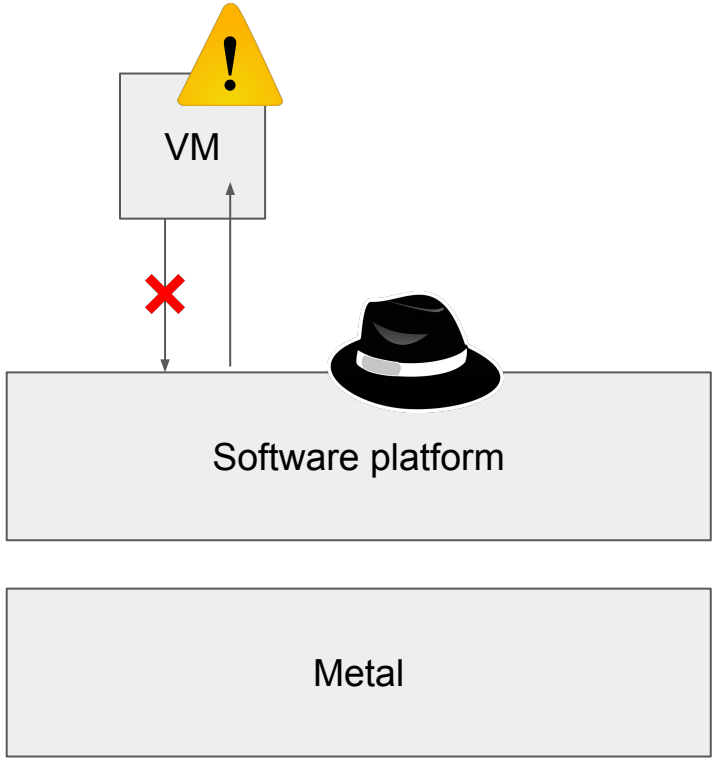


Encrypted Memory

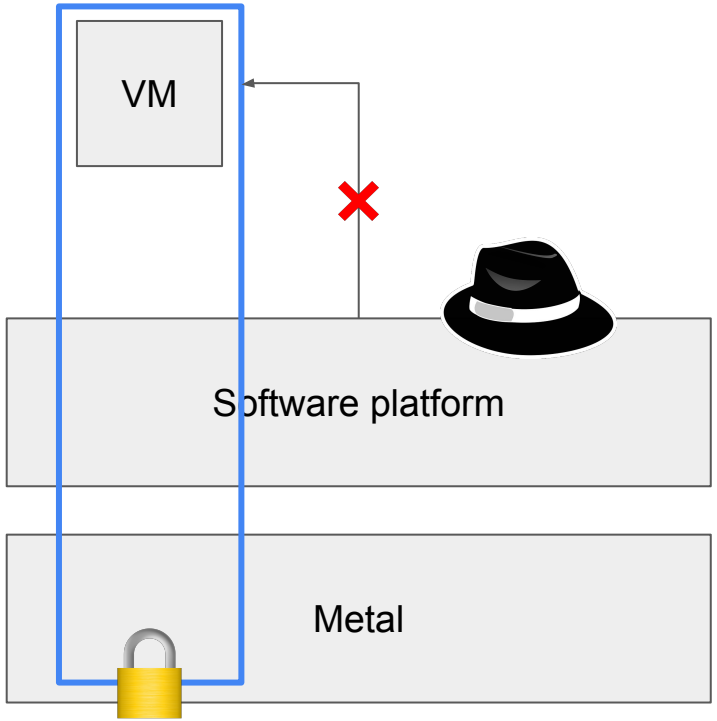
Virtual Machines



Virtual Machines

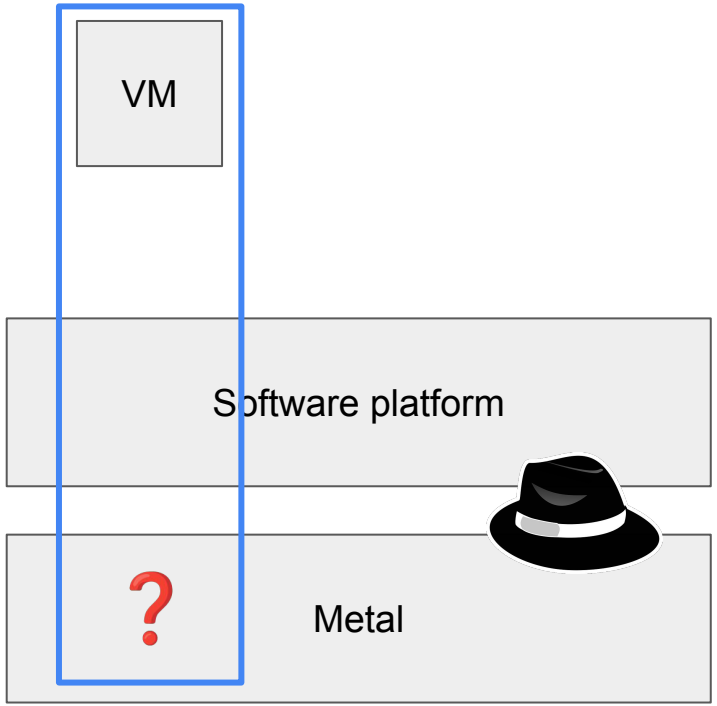


Confidential Computing: Encrypted Memory

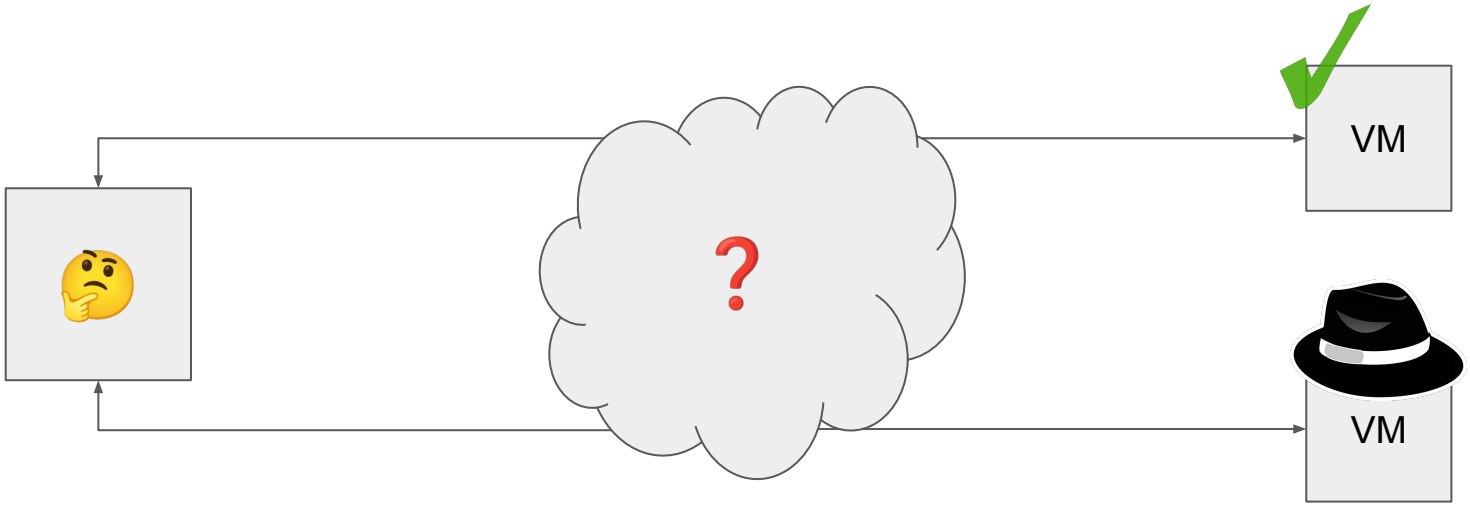


Attestation ✓

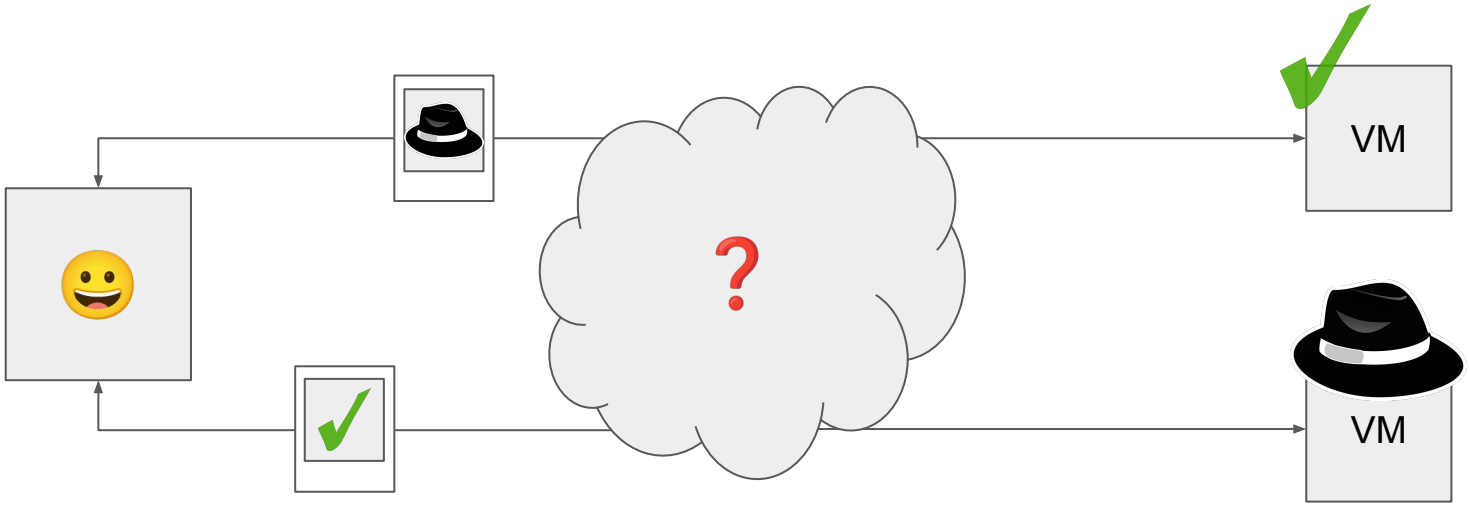
Untrusted environment

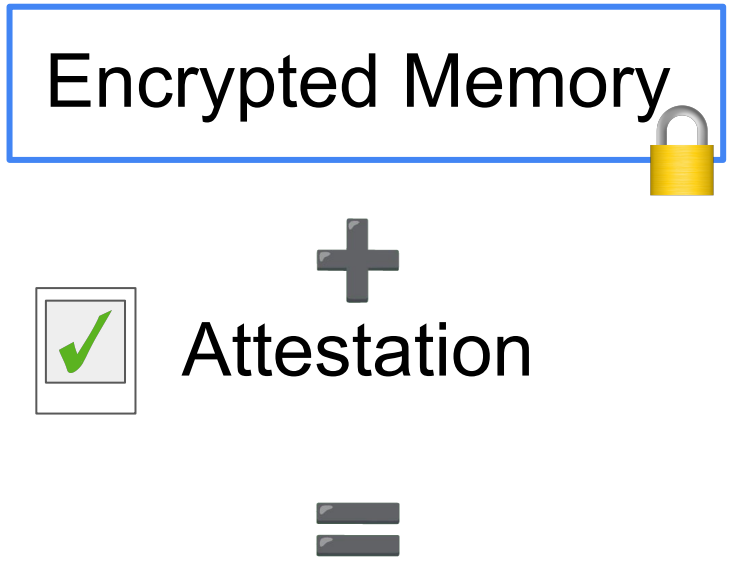


Untrusted environment



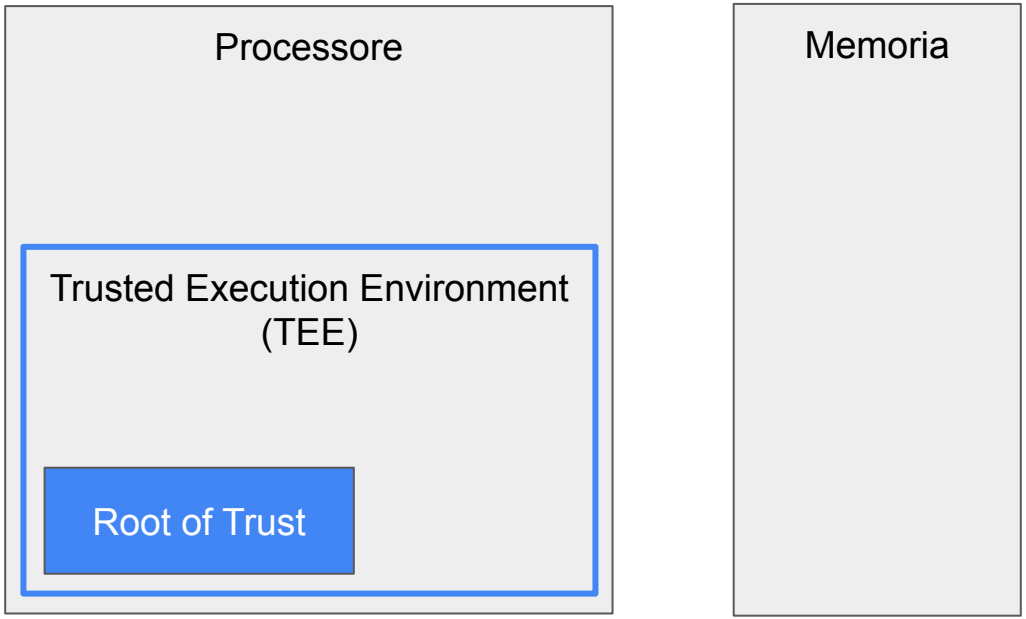
Confidential Computing: Attestation




Encrypted Memory
Attestation
Confidential Computing

Hardware Root of Trust

Hardware Root of Trust



Approfondire

- Confidential computing - Wikipedia
- What Is Confidential Computing? | NVIDIA Blogs
- Confidential computing primer - Red Hat Blog
- Confidential Containers · GitHub
- Scrivimi: cconte@redhat.com