DICE Attestation on AMD SEV-SNP

Ivan Petrov, Juliette Pluto

Google Research

Agenda

1. Project Oak
2. Attestation
3. DICE
4. Demo

Project Oak

github.com/project-oak/oak

Project Oak

Research project aiming to make it possible for **data owners** (including end-users) to reason about **how their data will be used** by the server in ways verifiable by external reviewers

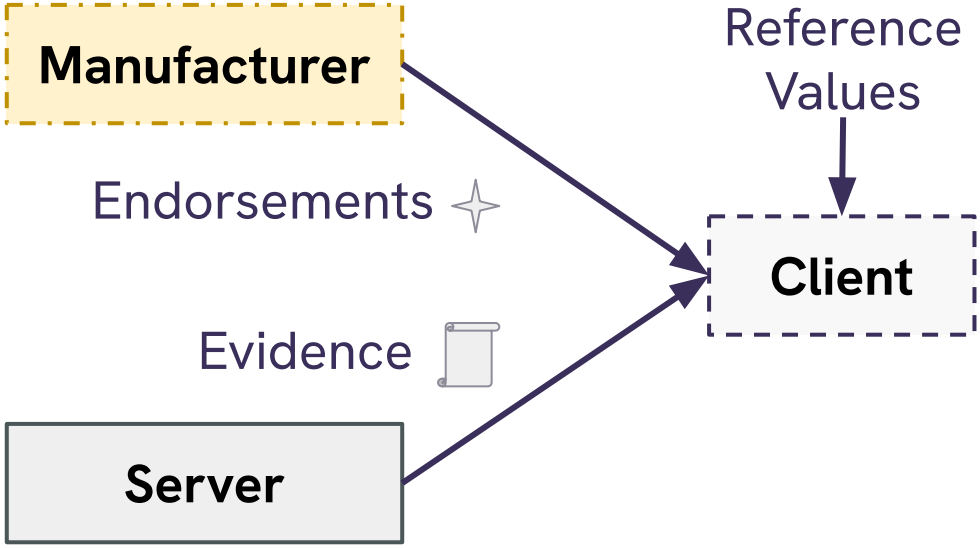
Oak Building Blocks

1. Trusted Execution Environment (TEE)
2. Remote Attestation
3. Transparency
   - *Open-source code*
   - *Reproducible builds*
   - *Verifiable Logs*

Attestation

Remote Attestation on AMD SEV-SNP

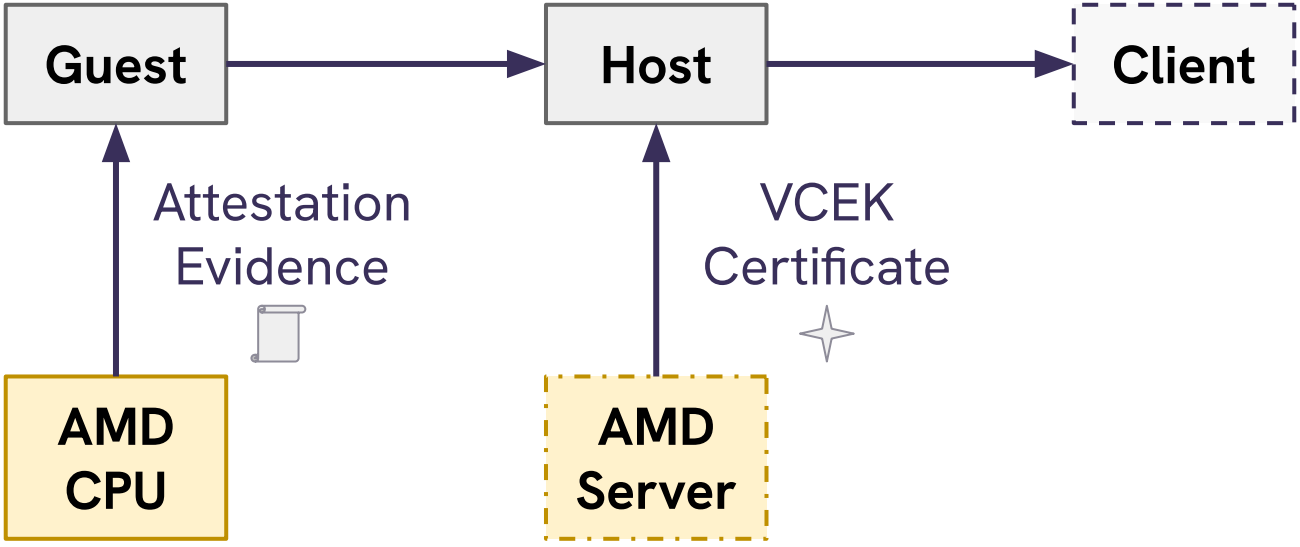
Remote Attestation



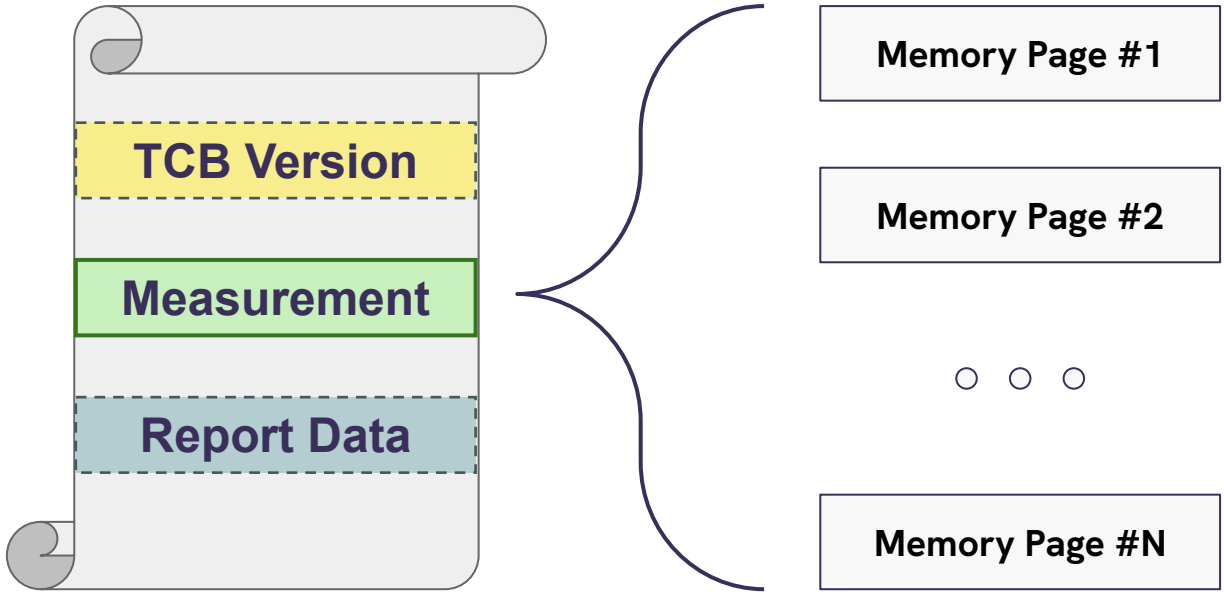
AMD SEV-SNP

- Trusted Execution Environment
- Memory encryption
- Remote attestation
  - *Signed boot measurement*
  - *Chip endorsement certificate authority*

AMD SEV-SNP Attestation



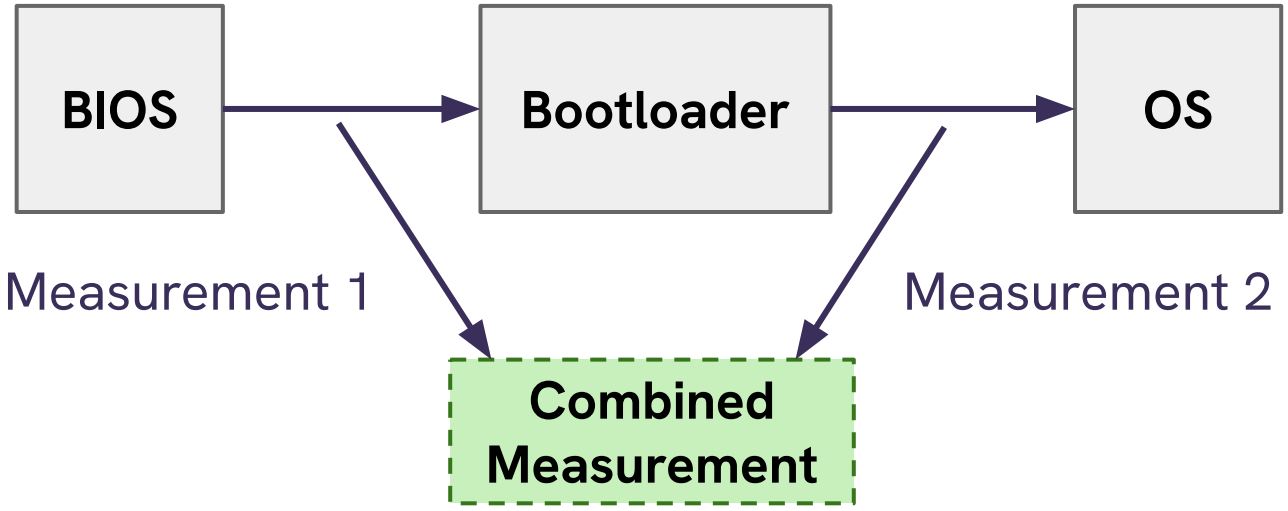
Attestation Report



Challenge

- Only the **initial state** of the VM is measured
- How do we measure the **complete workload**?

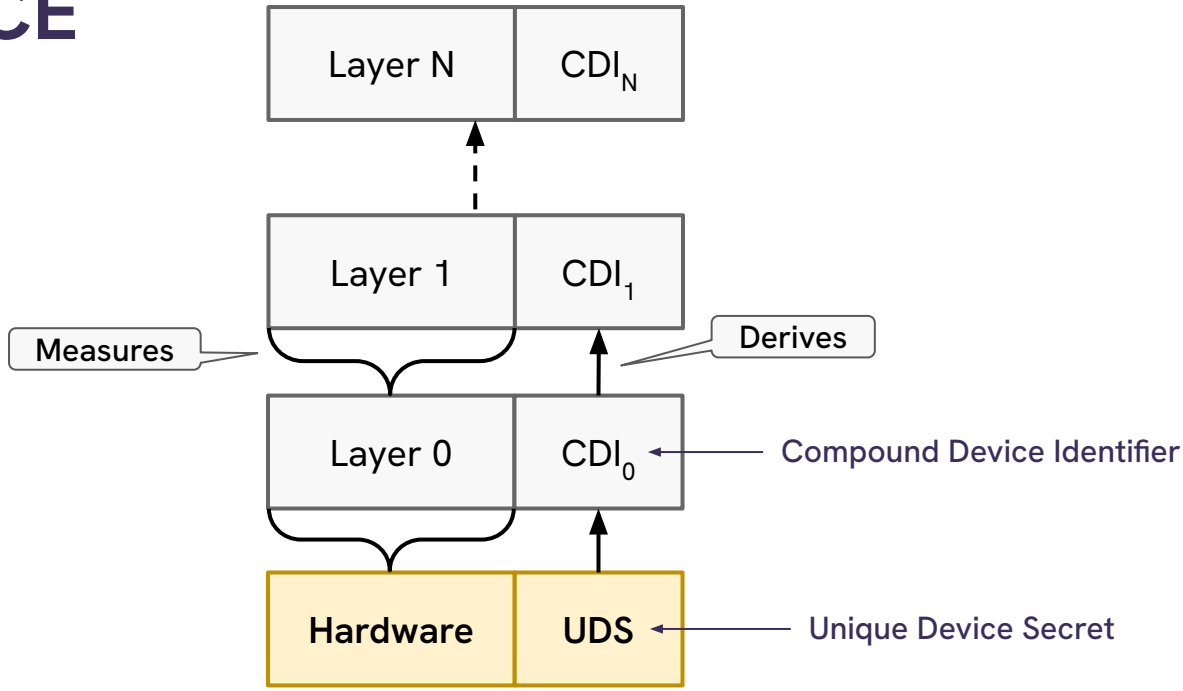
Measured Boot



DICE

DICE implementation for AMD SEV-SNP

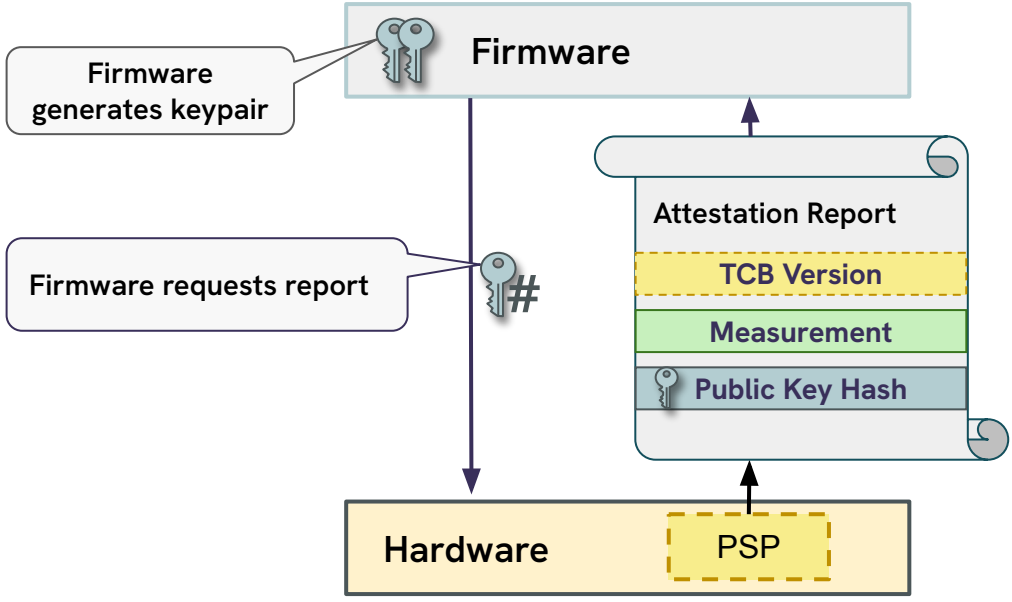
DICE


Layer N
CDI_N
Layer 1
CDI_1
Measures
Derives
Layer 0
CDI_0
Compound Device Identifier
Hardware
UDS
Unique Device Secret

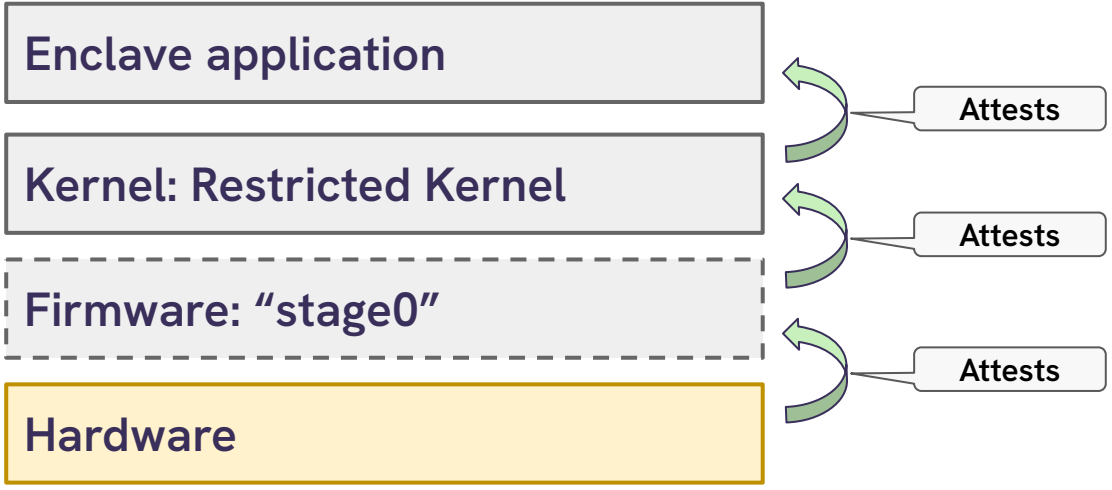
DICE + TEE

- ***Challenge:***
  - UDS value cannot be used to derive keys
- ***Proposal:***
  - Generate ephemeral keys instead of CDIs
  - Use Attestation Report as a root certificate
- ***Inspiration:***
  - Talk by Peter Gonda (Google Cloud) youtube.com/watch?v=SitfZLoEFww

Attestation Report instead of UDS



Restricted Kernel Dice Layers



Firmware: “stage0”

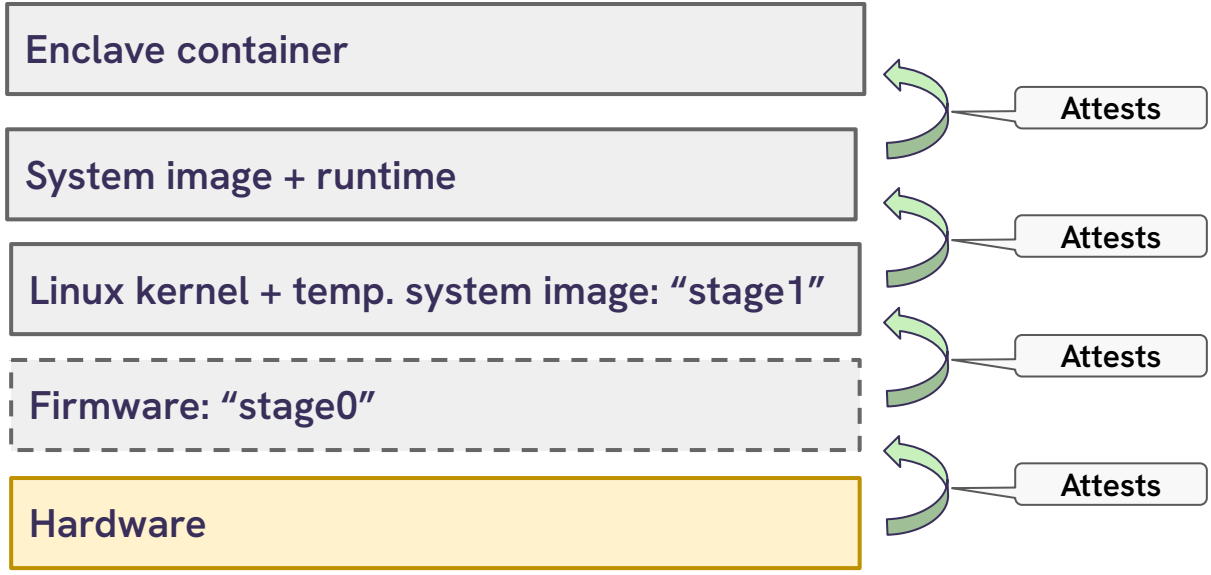
- Custom vBIOS & Bootloader
- Minimal *[~10K Lines of code]*
- Written in Rust
- Dependencies reviewed
- SEV-SNP & DICE enlightened

Kernel: “Restricted Kernel”

- Custom
- Minimal *[~15K lines of code]*
- Written in Rust
- DICE enlightened

Learn more: youtube.com/watch?v=1wZczK4X-VI

DICE adapts to different layers



Demo (see recording)

Verifying endorsed DICE evidence

github.com/project-oak/oak/tree/demo_oc3_2024/demo_oc3_2024

Summary

- DICE attestation for AMD SEV-SNP
  - *Provides measurements of the full workload*
- Minimal TCB for the workload
- Client verification logic

Contact us!

Repo

github.com/project-oak/oak

Demo

github.com/project-oak/oak/tree/demo_oc3_2024/demo_oc3_2024