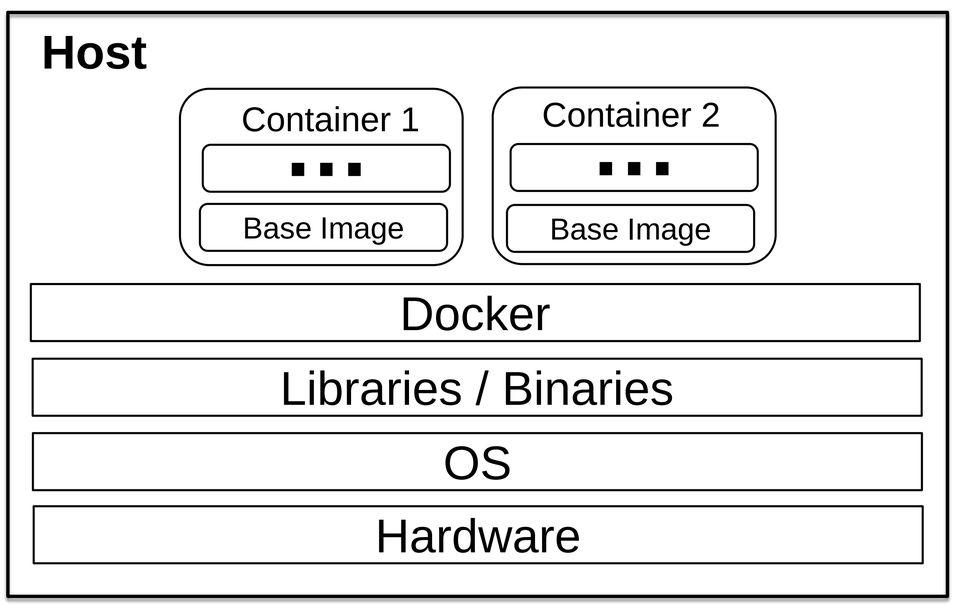
Platform Security

Secure Systems Group, Aalto University

Jorden Whitefield, Lachlan J. Gunn, N. Asokan

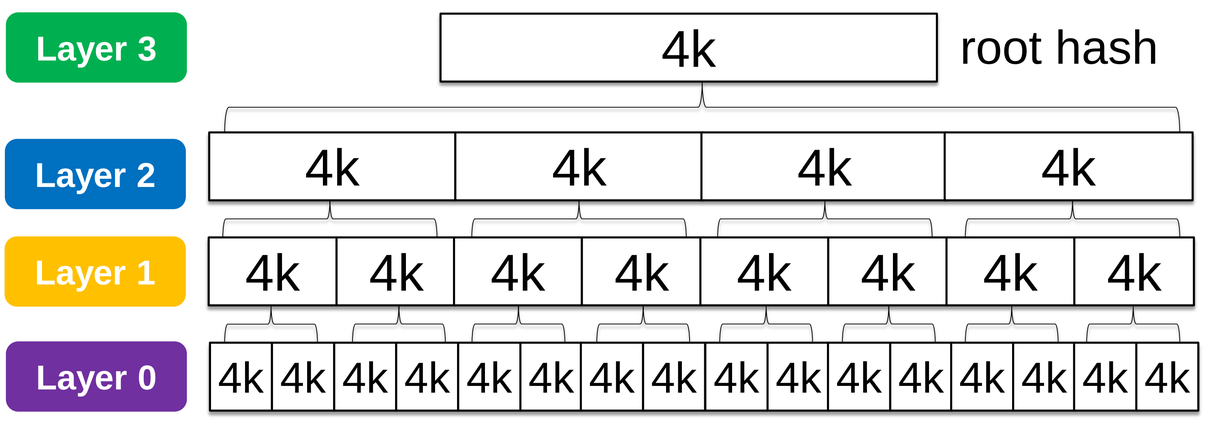
APOC: Attesting Properties of Containers

- Binary attestation requires tracking and re-measuring an entire system when updated
- Measure properties of a container, e.g., software, configuration. Reduces complexity
- **Challenge:** Can two running containers be shown to be functionally equivalent?
- Our system, **APOC**, aims to attest properties of containers to establish trust



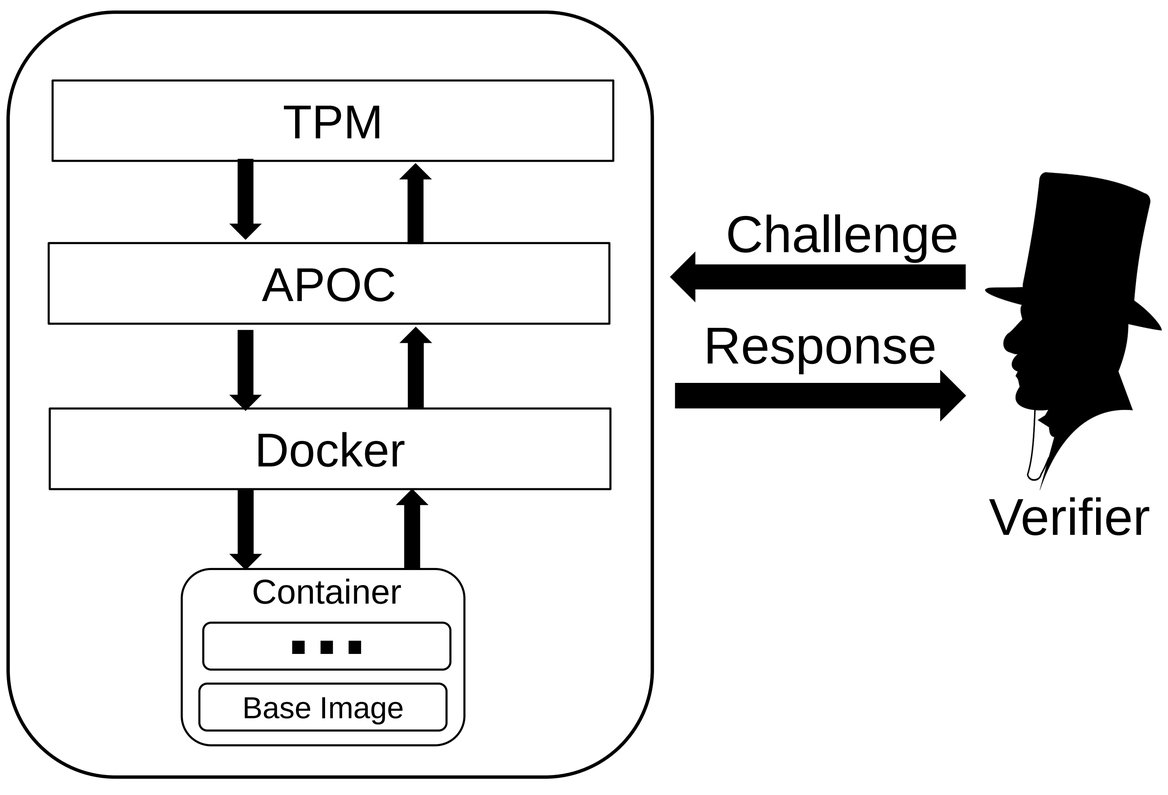
Containers

- Isolated execution environment
- Protects
  - System from applications
  - Applications from one another
- Based on namespaces and cgroups
  - No VMs, very low overhead



Host System Measurements

- Measured boot using TPM and Intel TXT
- dm-verity to measure the Host OS image
- Remote Attestation using TPM



APOC

- Host can inspect container contents
- Measurements of rich properties:
  - Hashes of executables
  - Package versions
  - Configuration of running services