

In Containers We Trust?

Building Trust In Containerized Environments

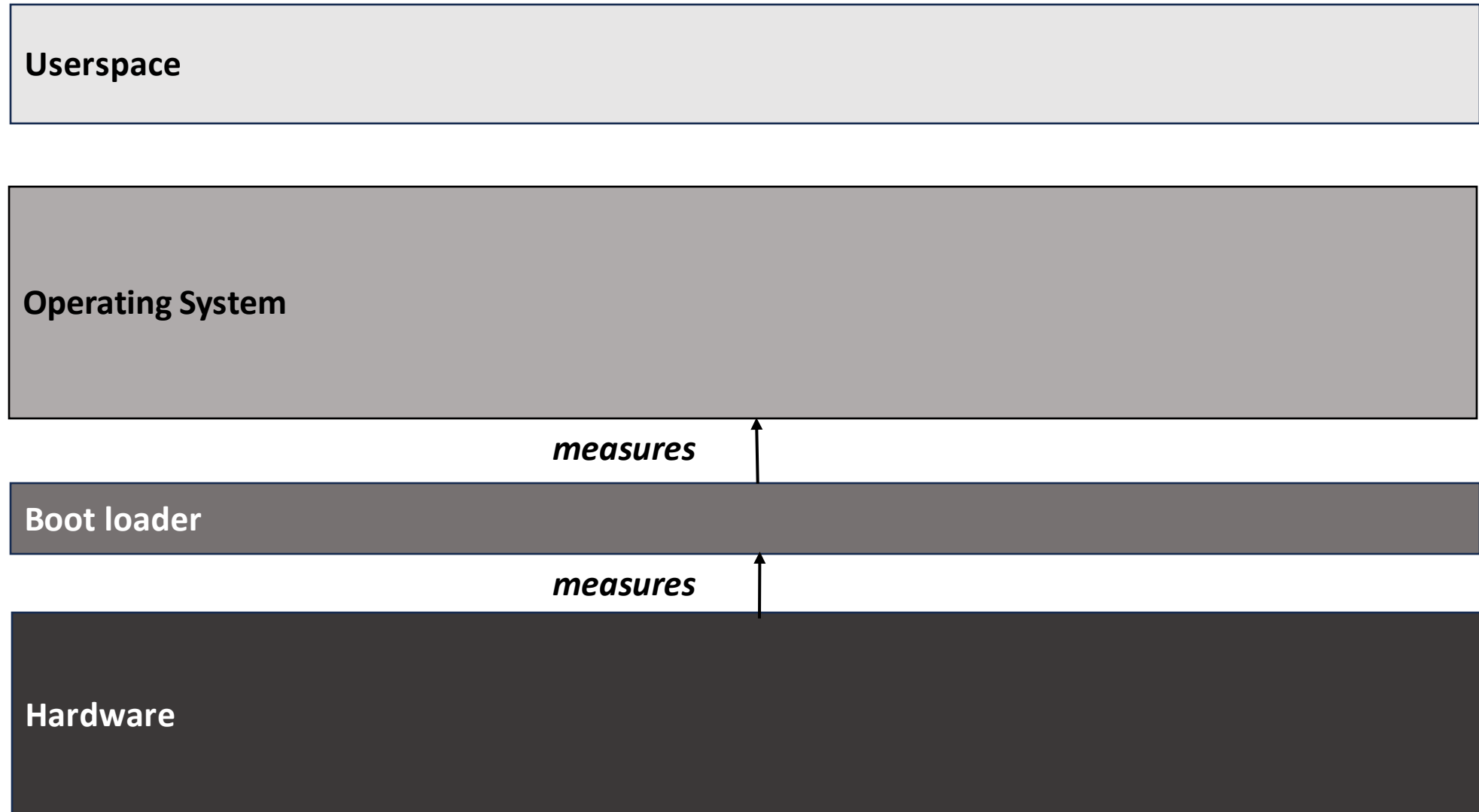
Avery Blanchard¹, Gheorghe Almasi², James Bottomley²
and Hubertus Franke²

¹ Duke University
² IBM Research

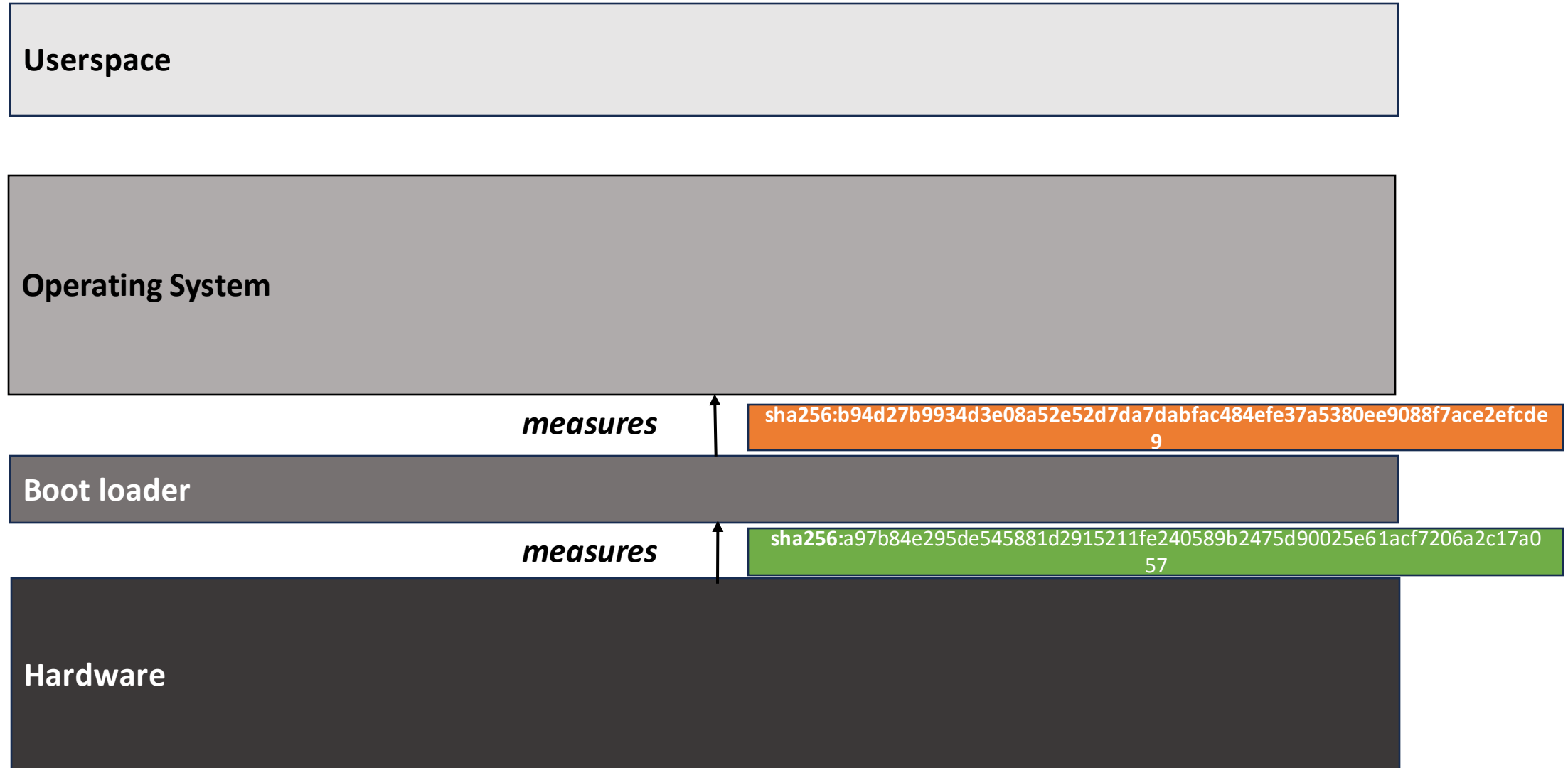
November 13th, 2023

Containers are ubiquitous and blindly
trusted...

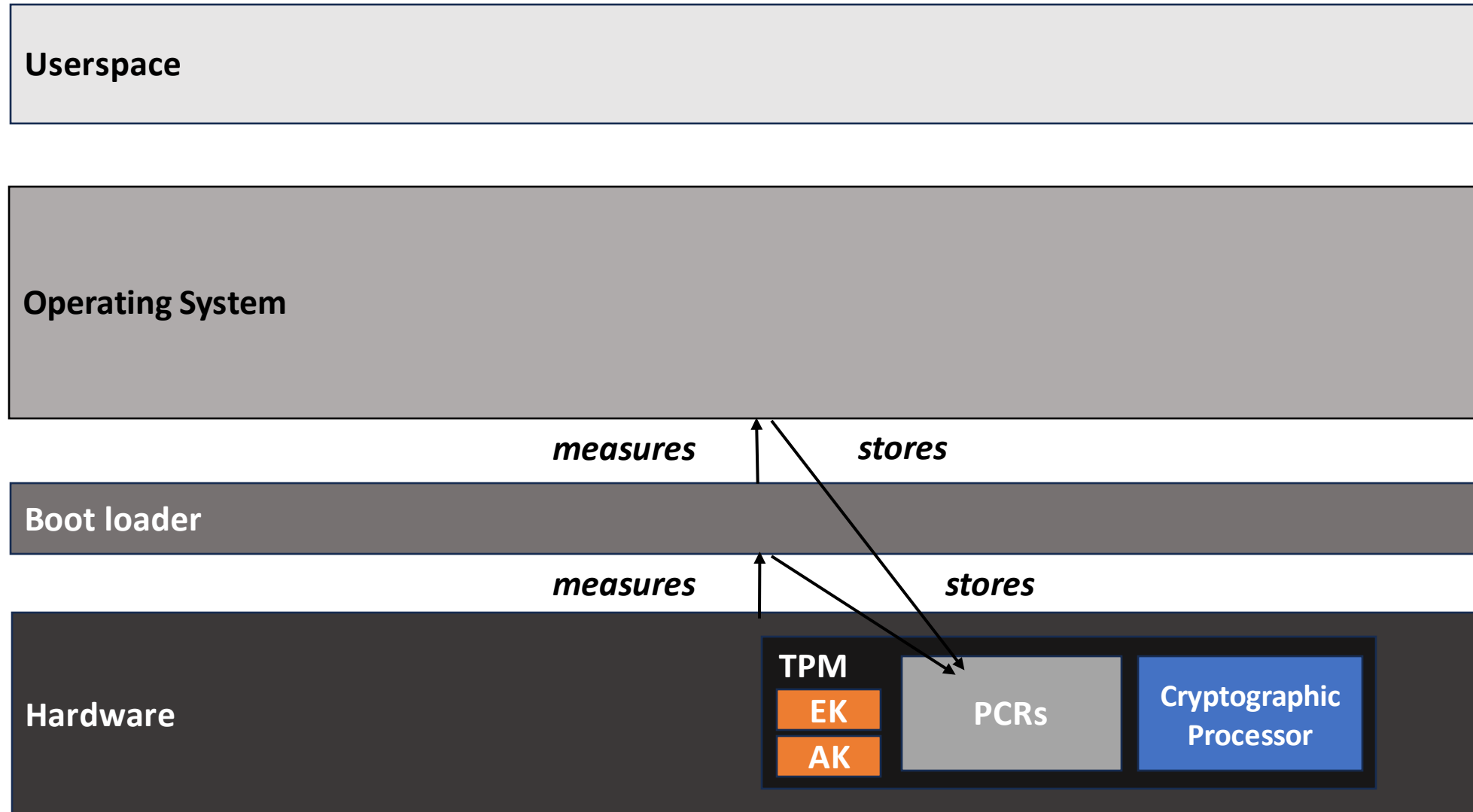
Defining Trust: Measurement



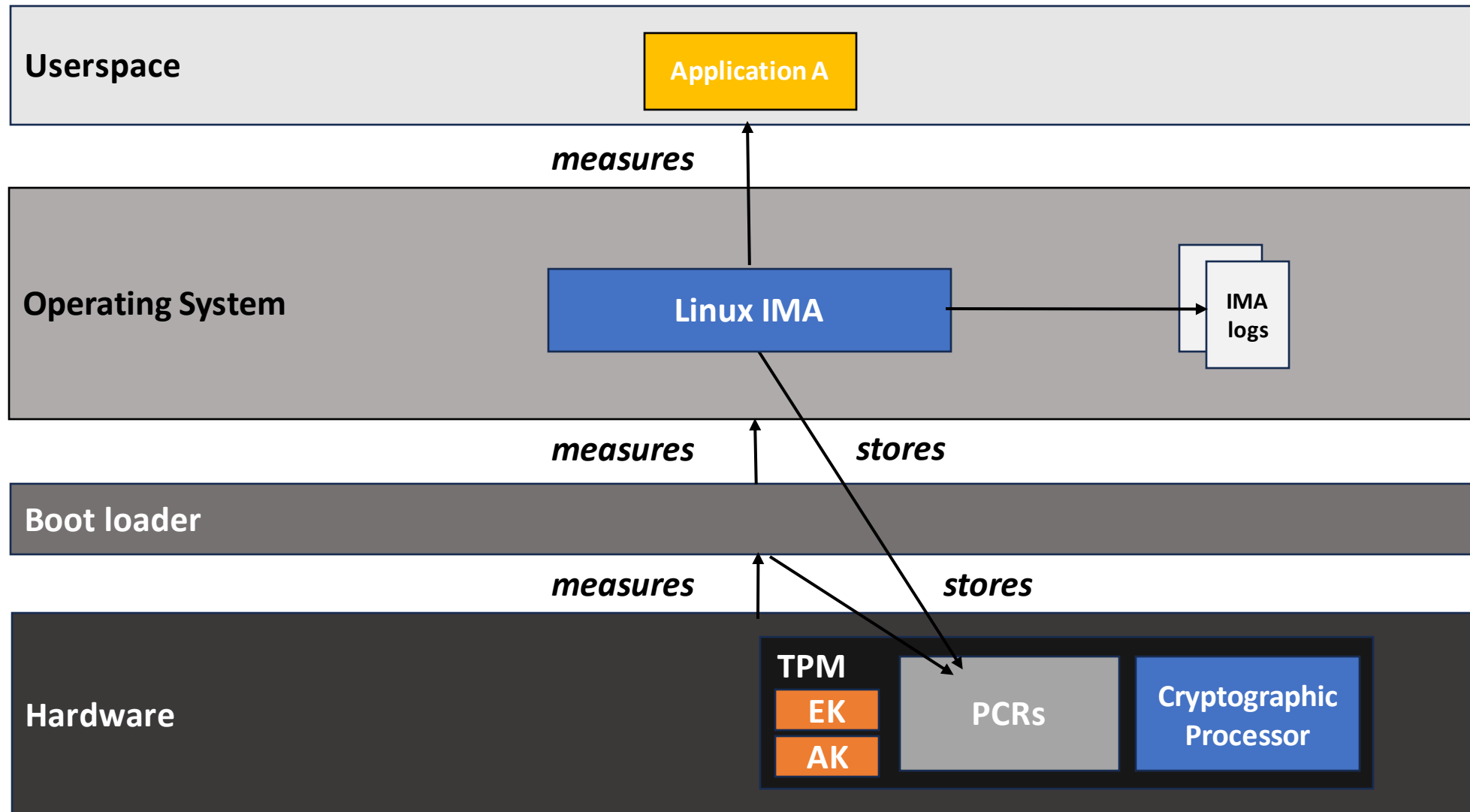
Defining Trust: Measurement



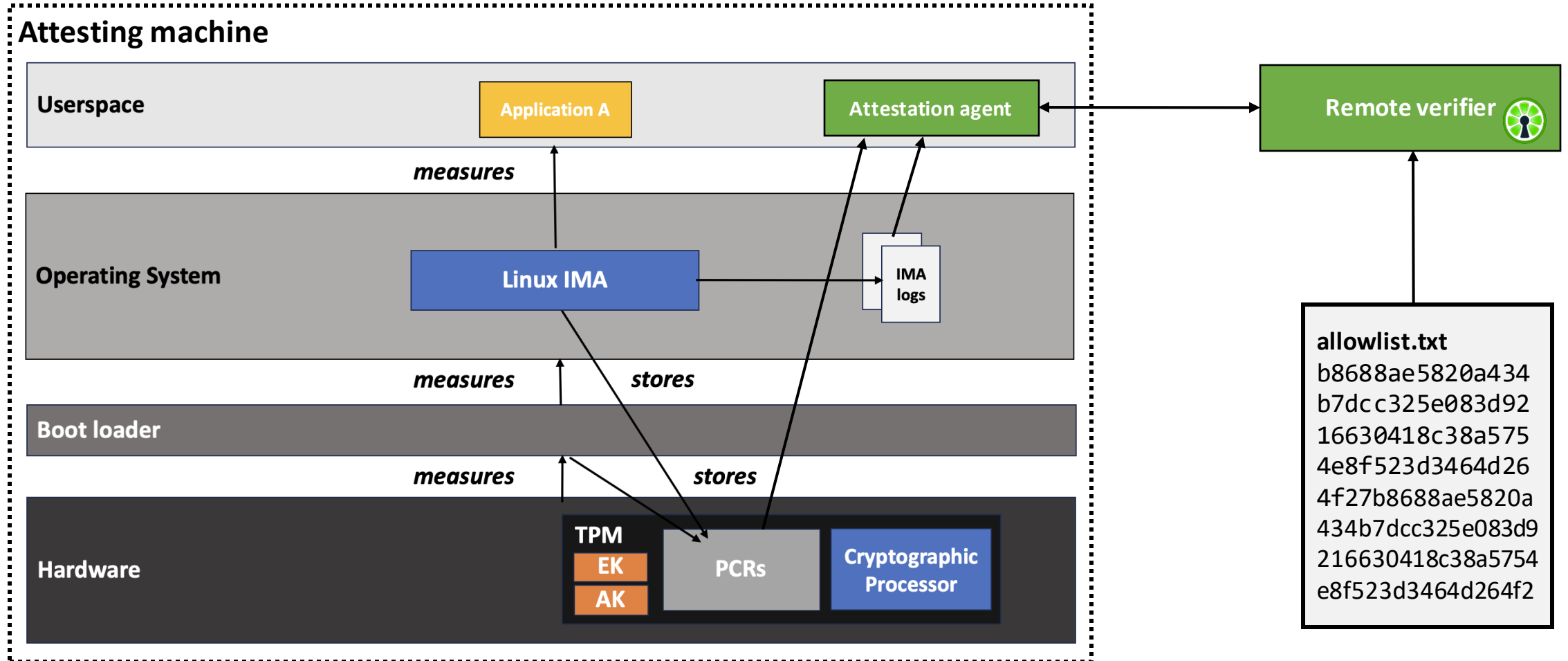
Building Trust from Hardware



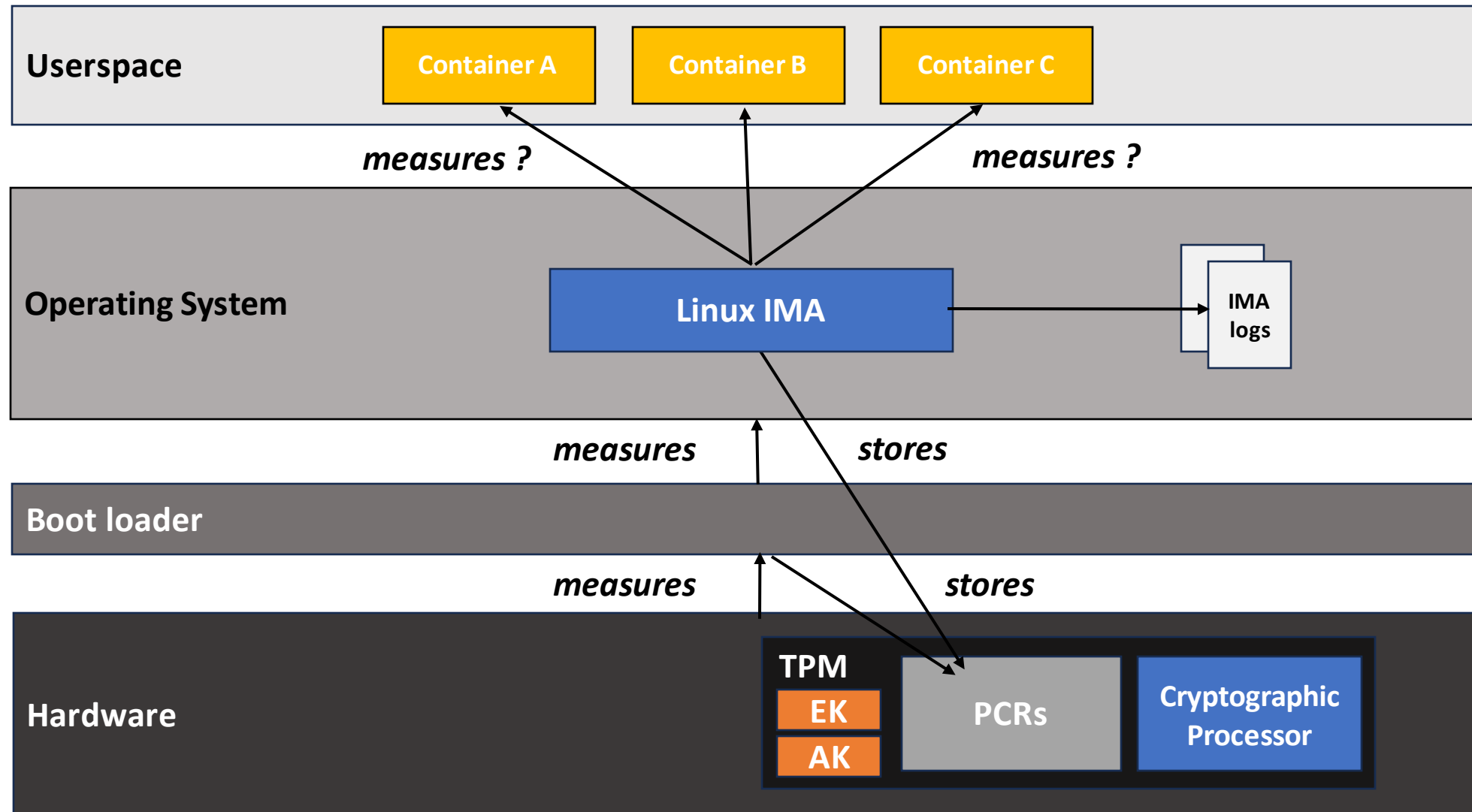
Extending Integrity Measurements in Runtime



Building Trust in Remote Environments

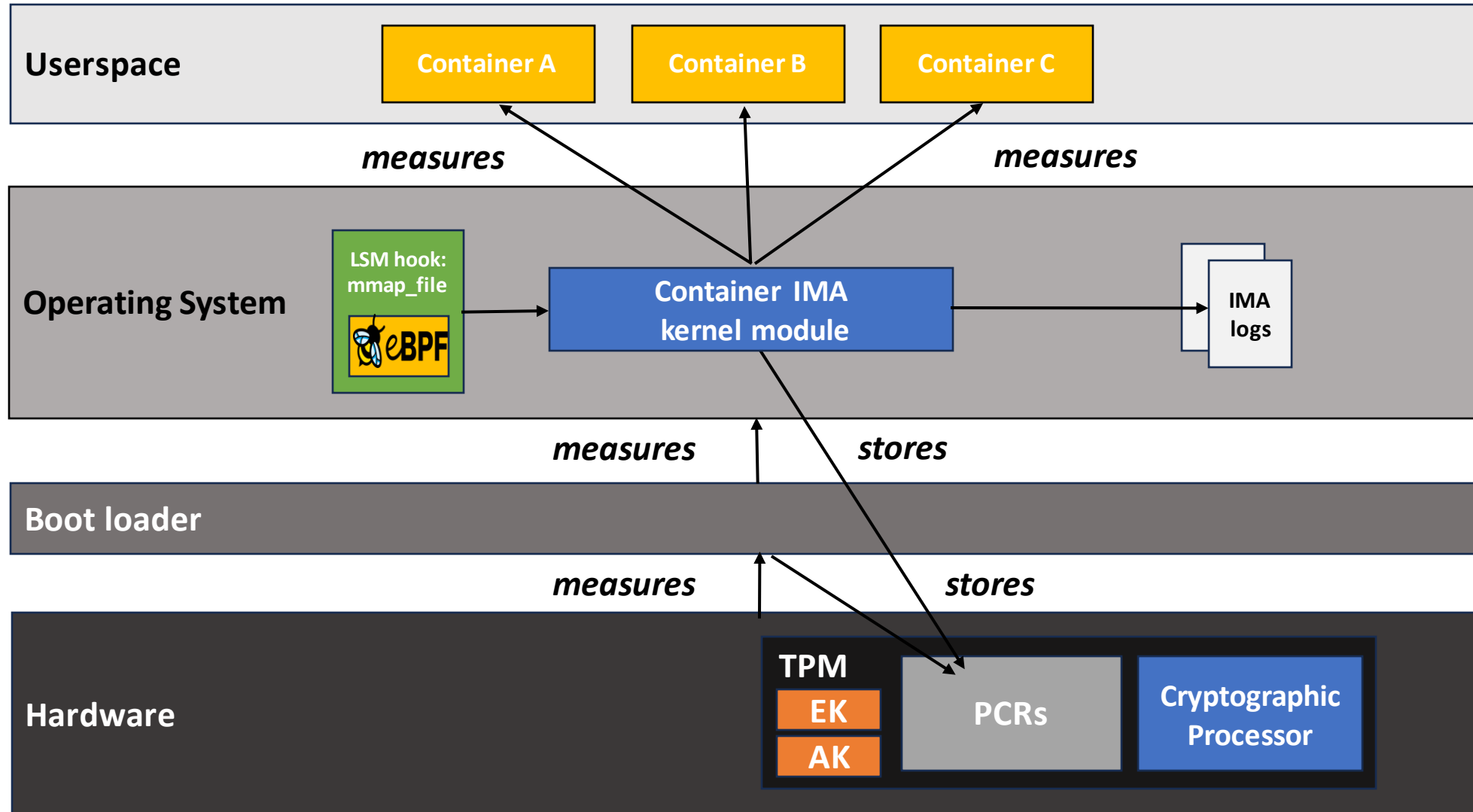


Container Present a Gap in Trust and Integrity

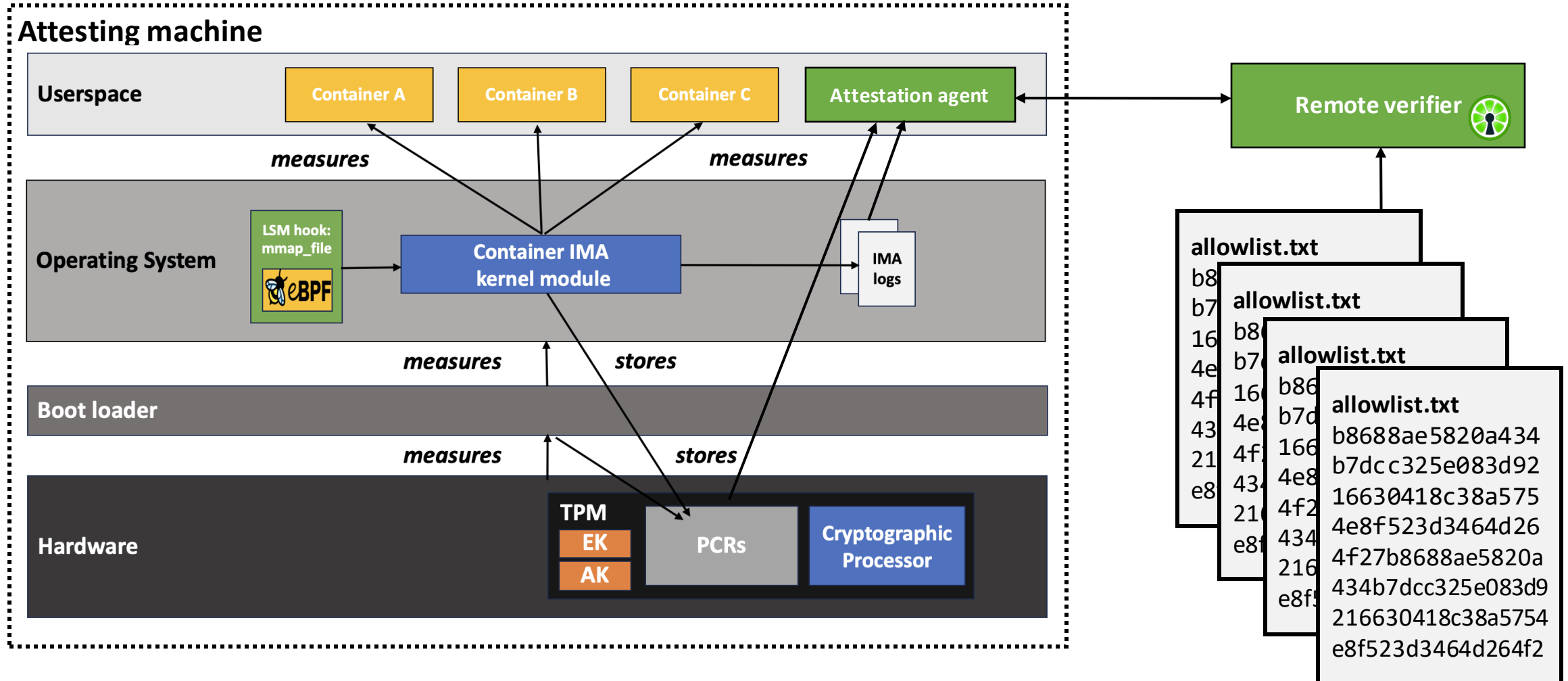


Enabling Container Attestation: A Preliminary Approach

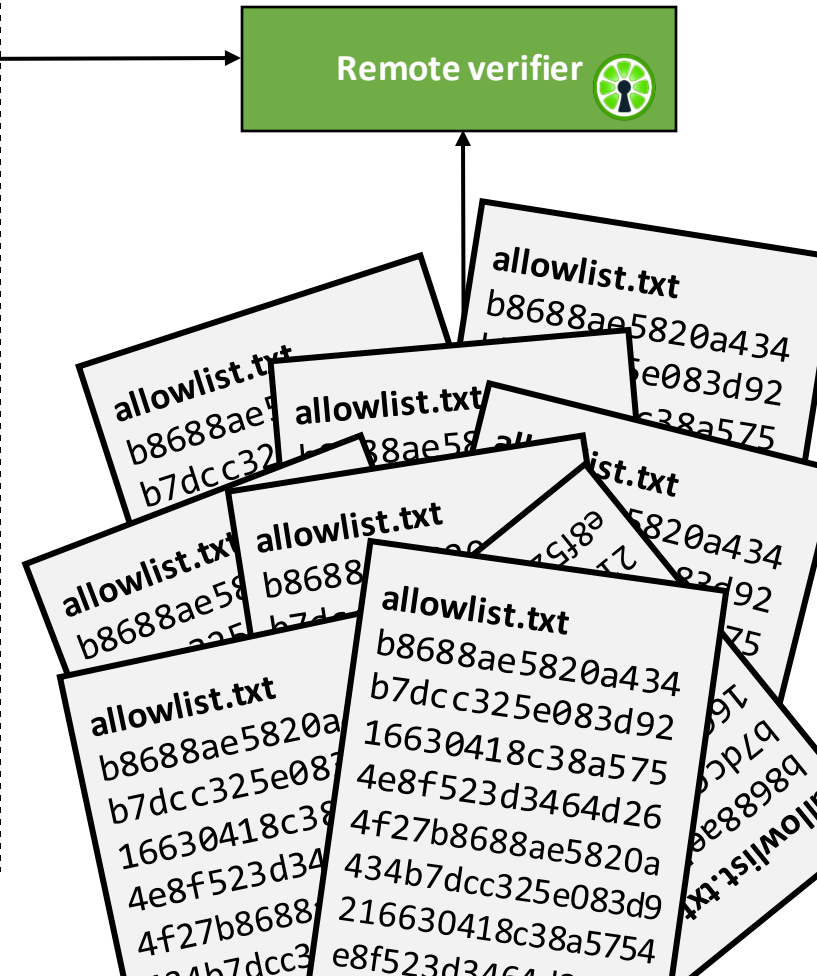
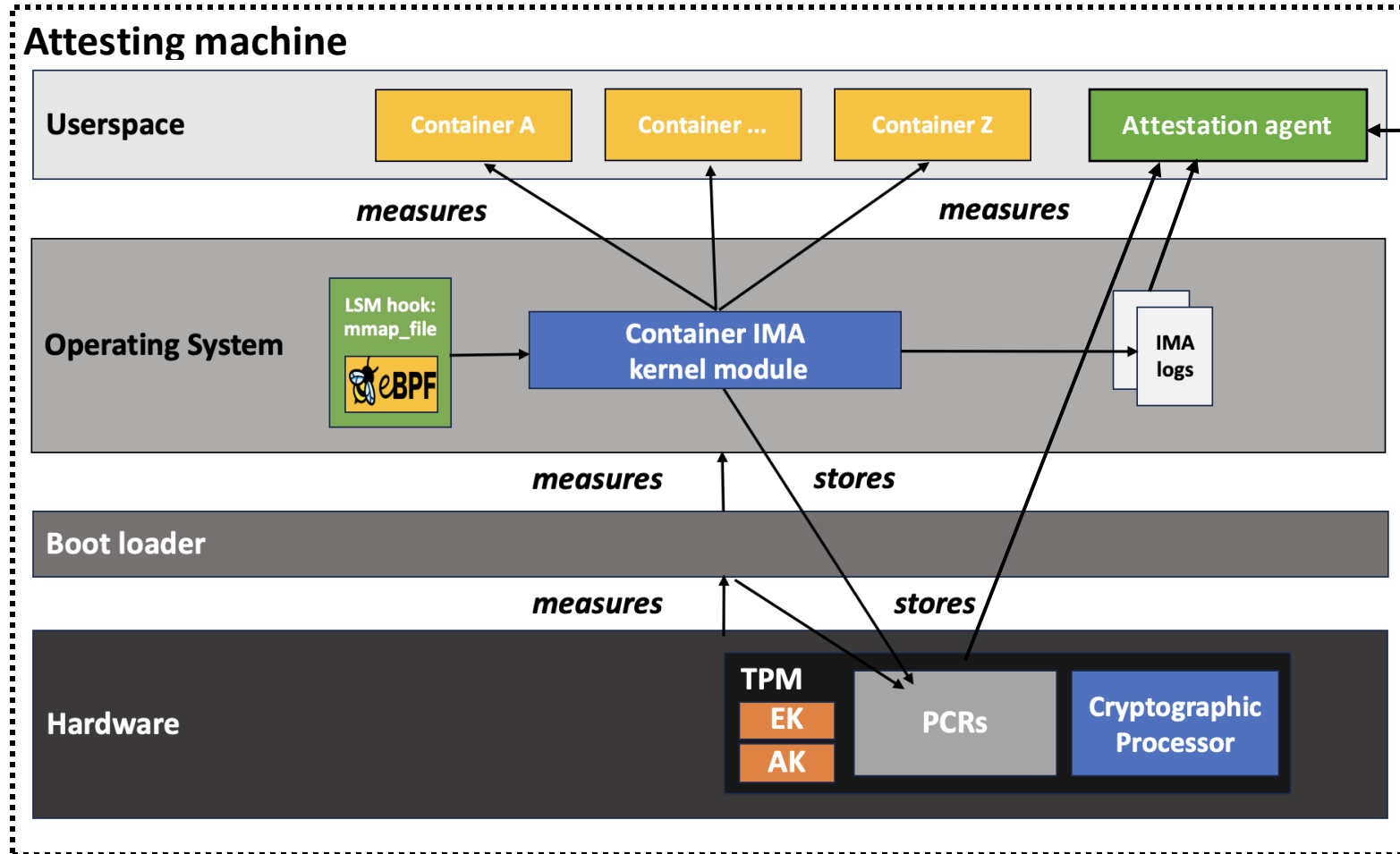
Extending IMA to Containers using eBPF



Attesting Container File Integrity



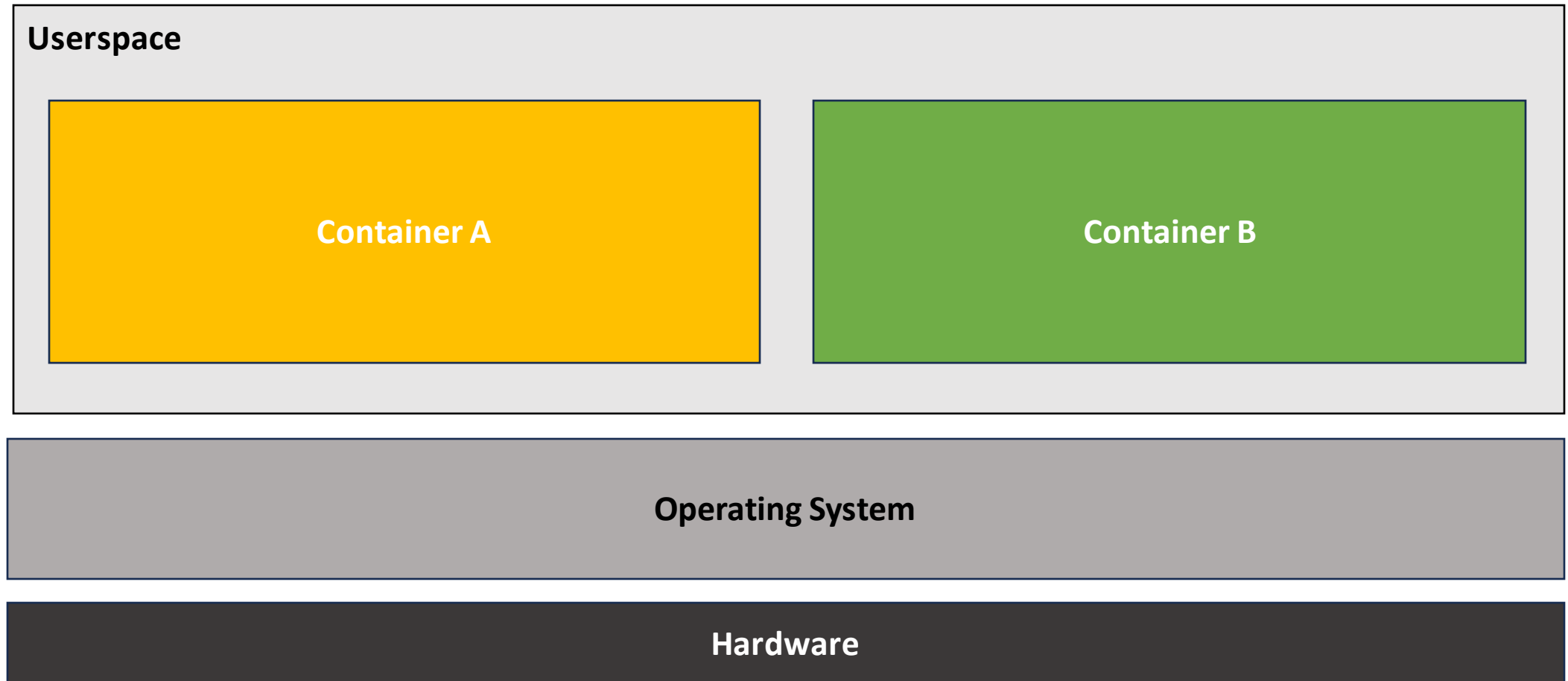
Attestation vs. Containers



Measuring Container Image Integrity in the Kernel

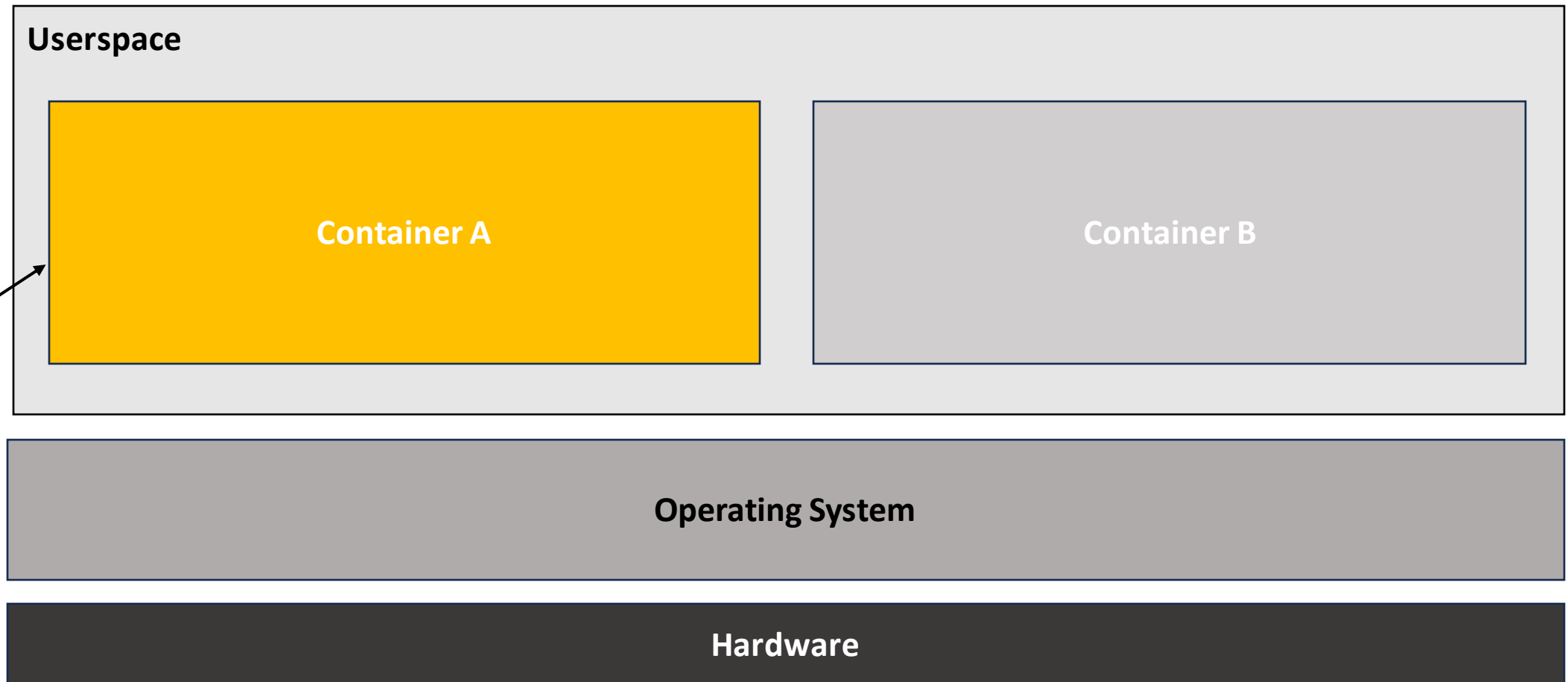
Container Image Integrity

- Goal: allow of attestation of ***container images***

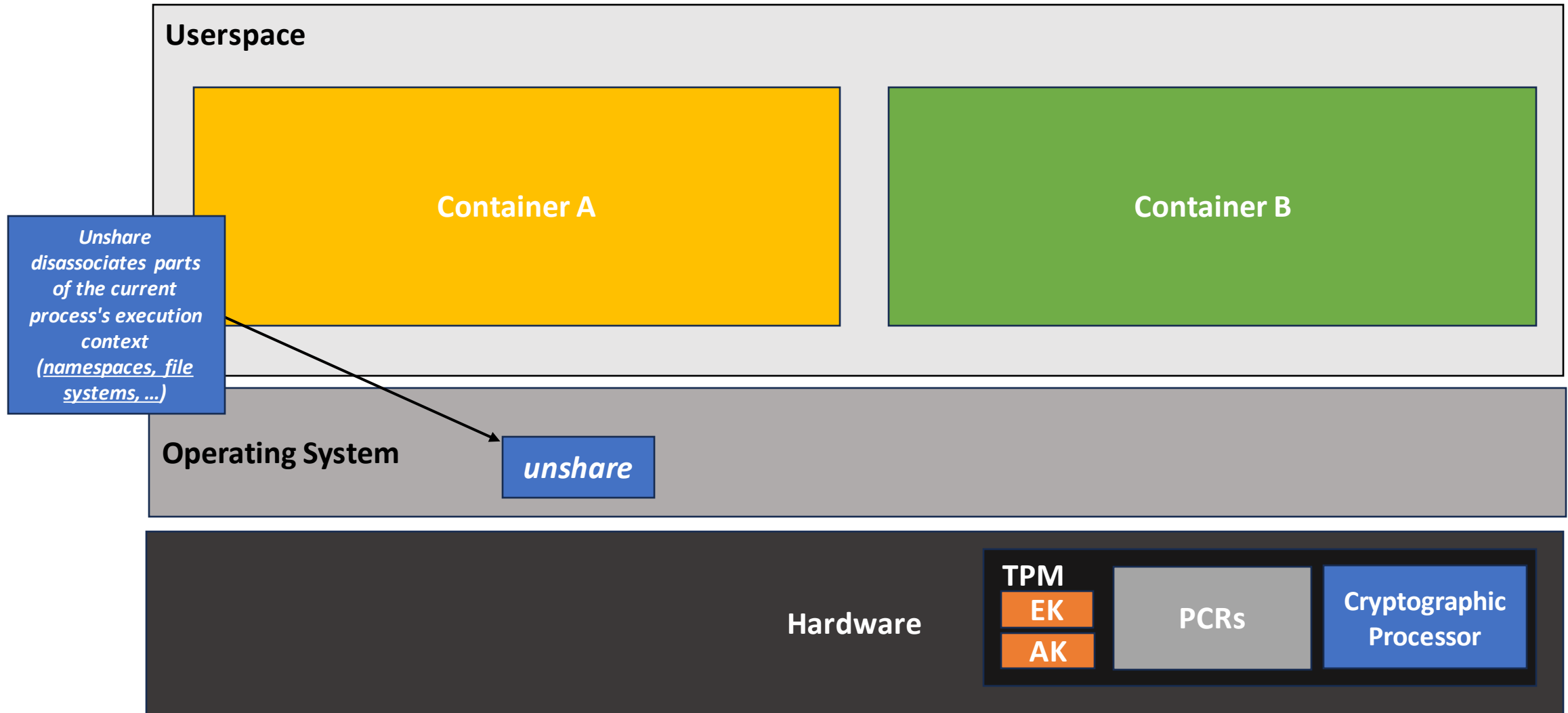


Container Image Integrity

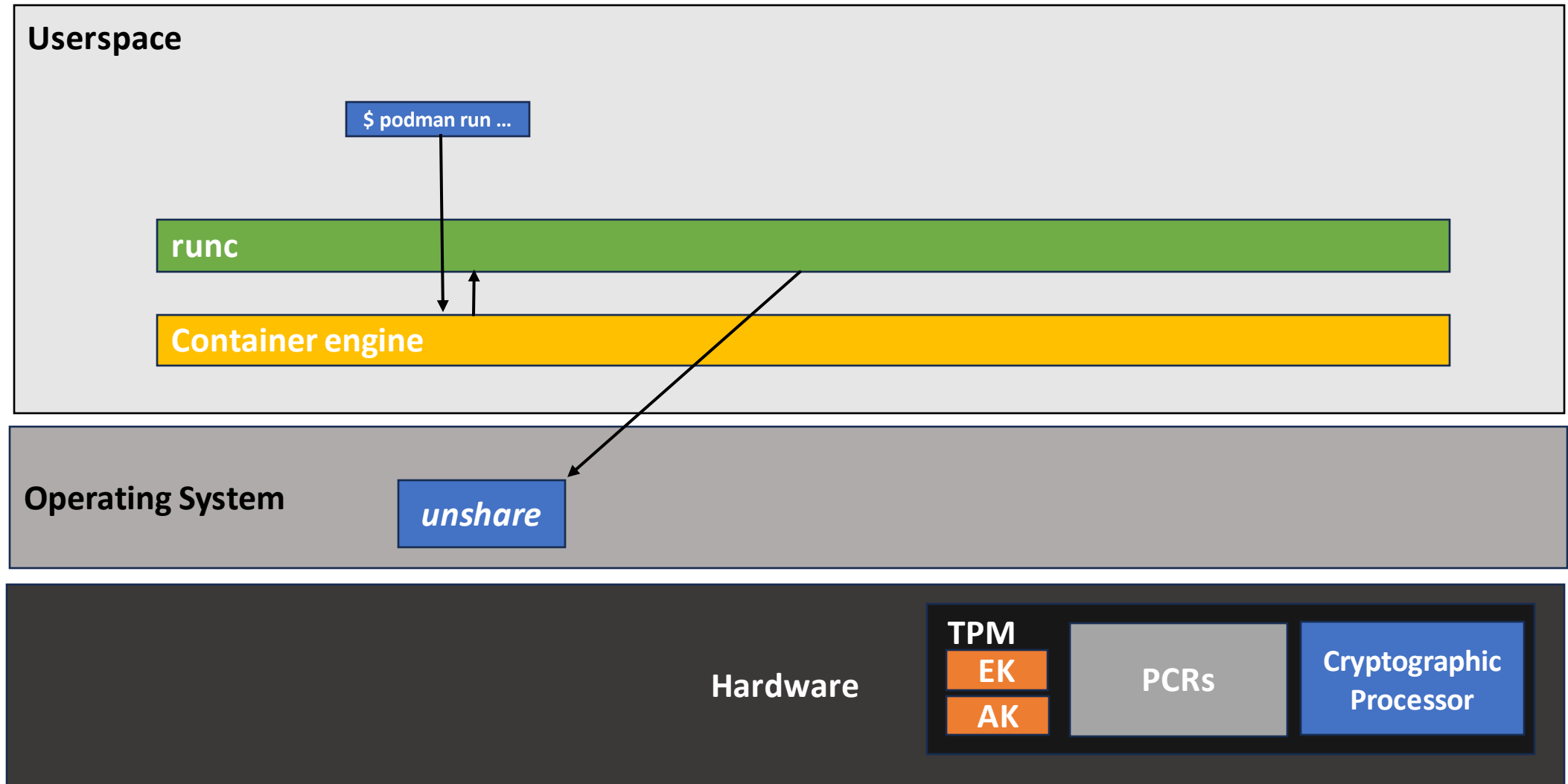
- Goal: allow of attestation of ***container images***



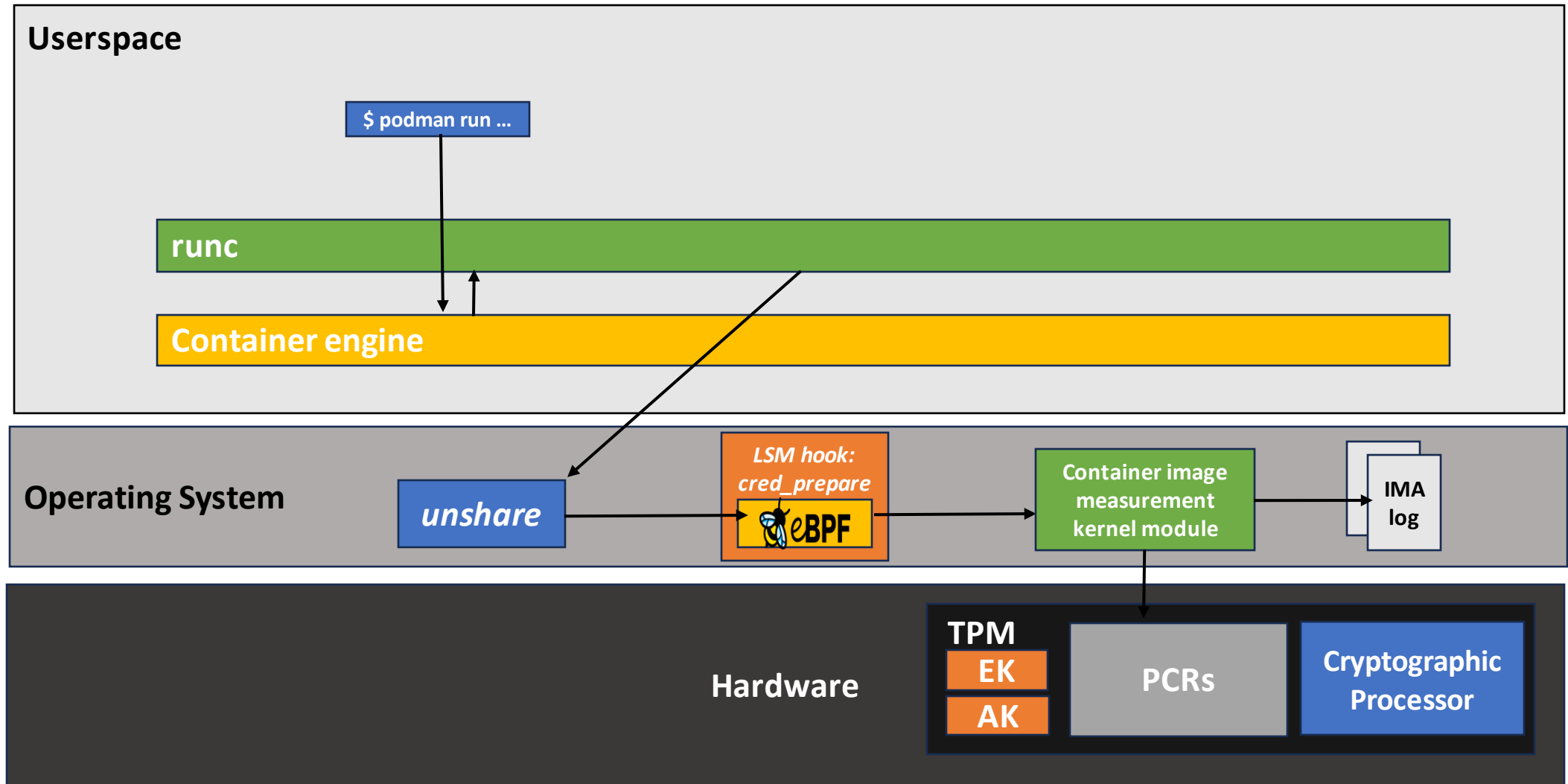
Visibility of Container Creation in the Kernel



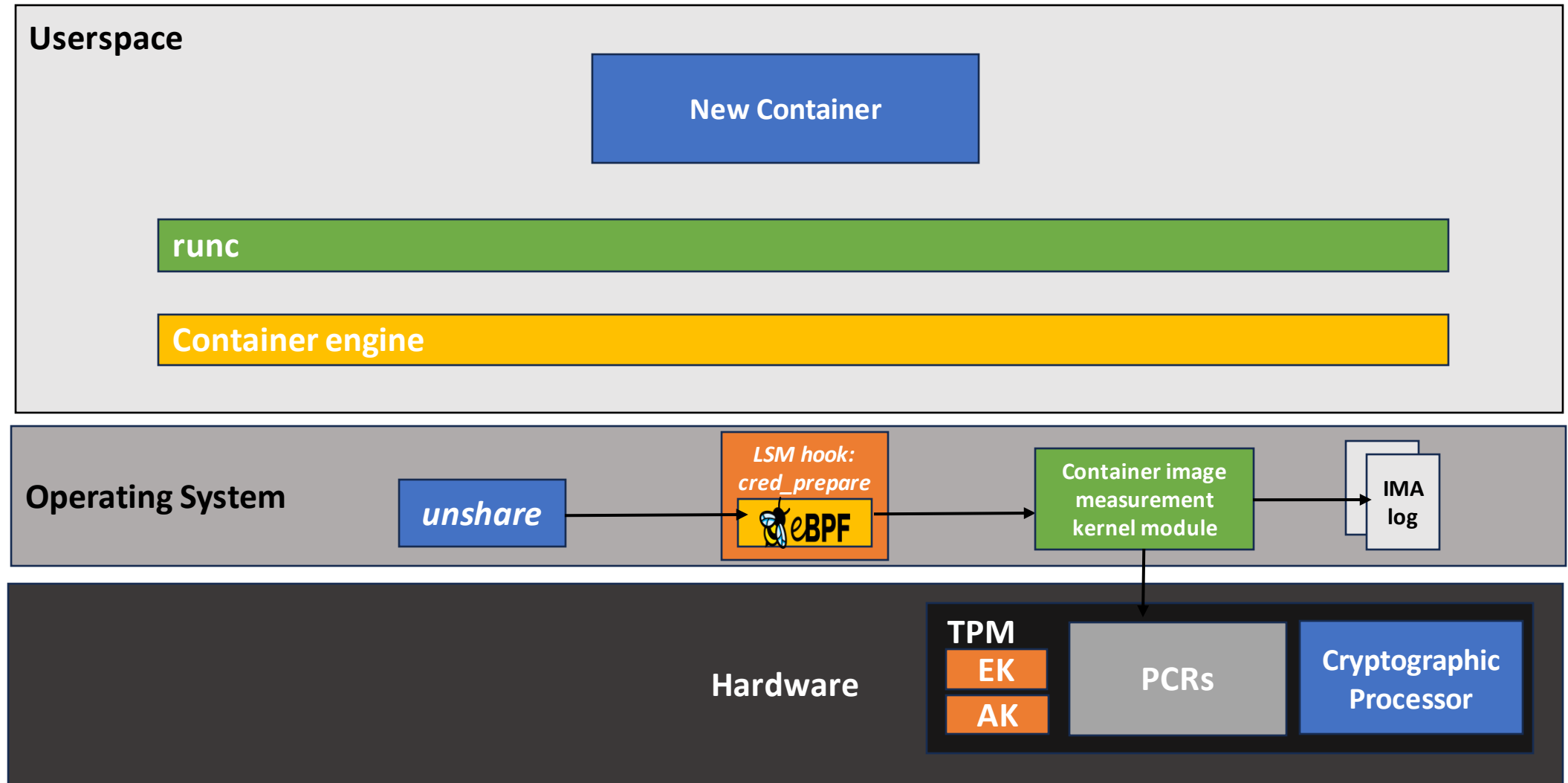
Visibility Through the Unshare System Call



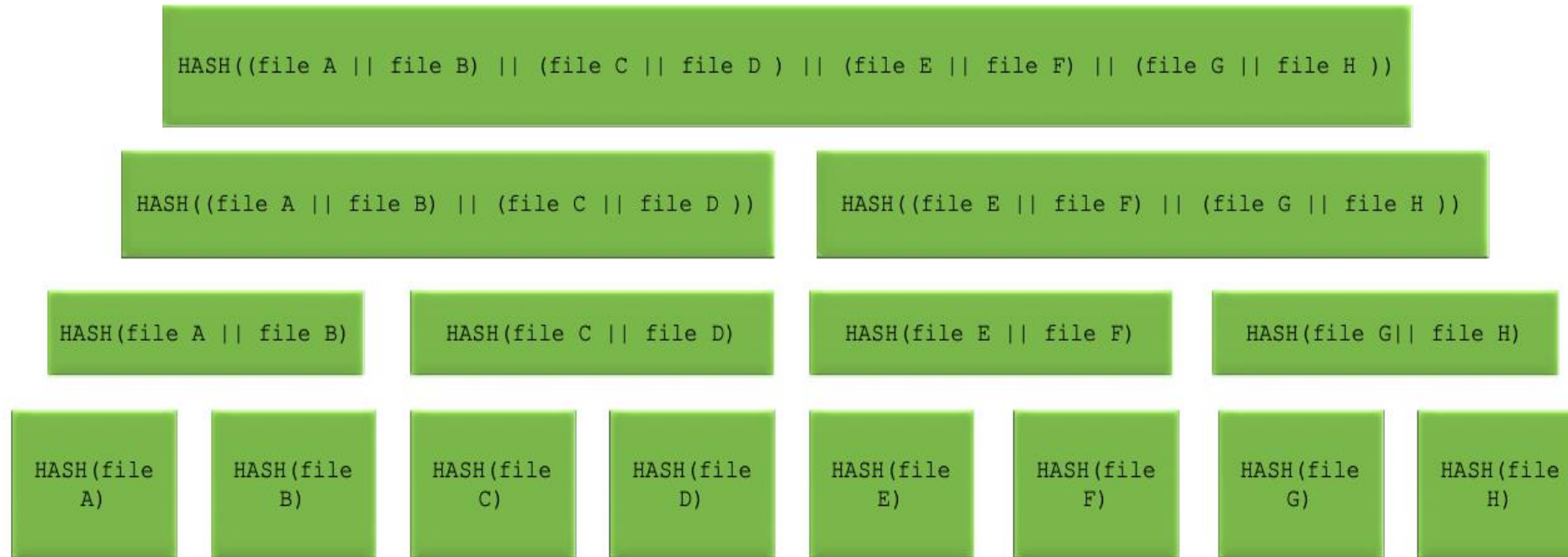
Visibility Through the Unshare System Call



Measuring Container Images From the Kernel



Kernel-Verifiable Image Digests



Extending the IMA log with Image Digests

- TODO

Evaluating Measurement Overhead

- EVALS TODO

Demo Environment

- TODO

Enabling Container Integrity Verification

- Current image digests are dependent on images layers, manifest files, image ids, ...
- Kernel-verifiable digests need to be provided to extend the chain of trust from hardware up to each container instance

Building trust in containers through image integrity measurements leveraging trusted hardware.

avery.blanchard@duke.edu

<https://github.com/avery-blanchard/container-ima>

<https://github.com/avery-blanchard/container-integrity-measurement>