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

Userspace Operating System measures **Boot loader** measures Hardware

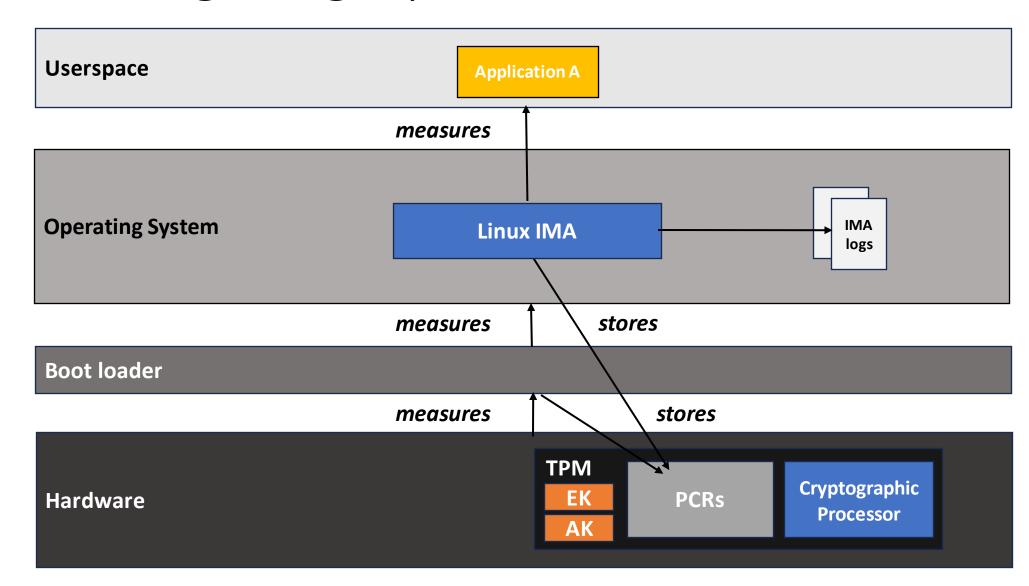
Defining Trust: Measurement

Userspace Operating System sha256:b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde measures **Boot loader** sha256:a97b84e295de545881d2915211fe240589b2475d90025e61acf7206a2c17a0 measures Hardware

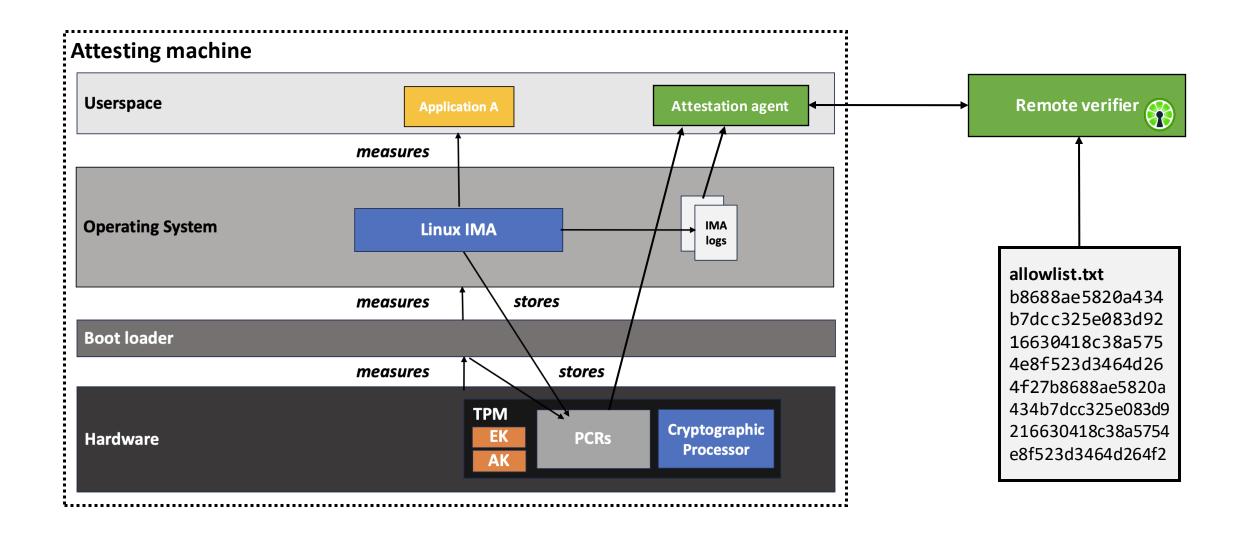
Building Trust from Hardware

Userspace Operating System stores measures **Boot loader** stores measures **TPM** Cryptographic Hardware EK **PCRs Processor**

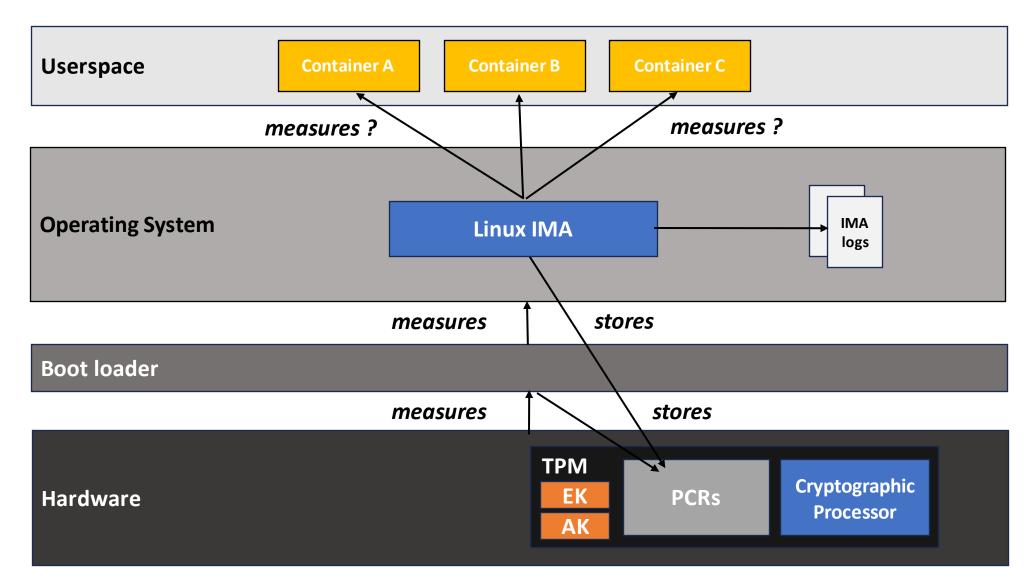
Extending Integrity Measurements in Runtime



Building Trust in Remote Environments

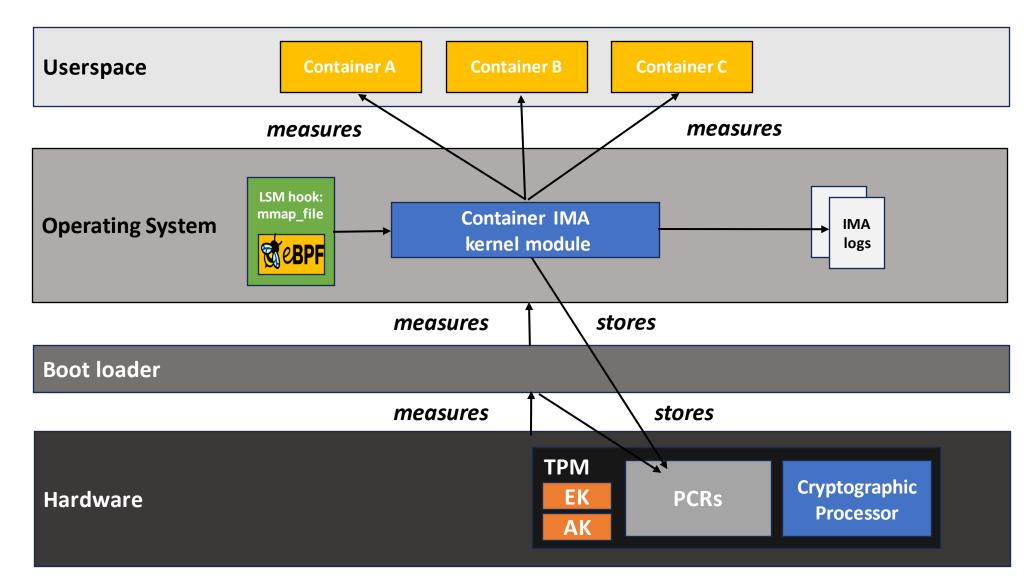


Container Present a Gap in Trust and Integrity

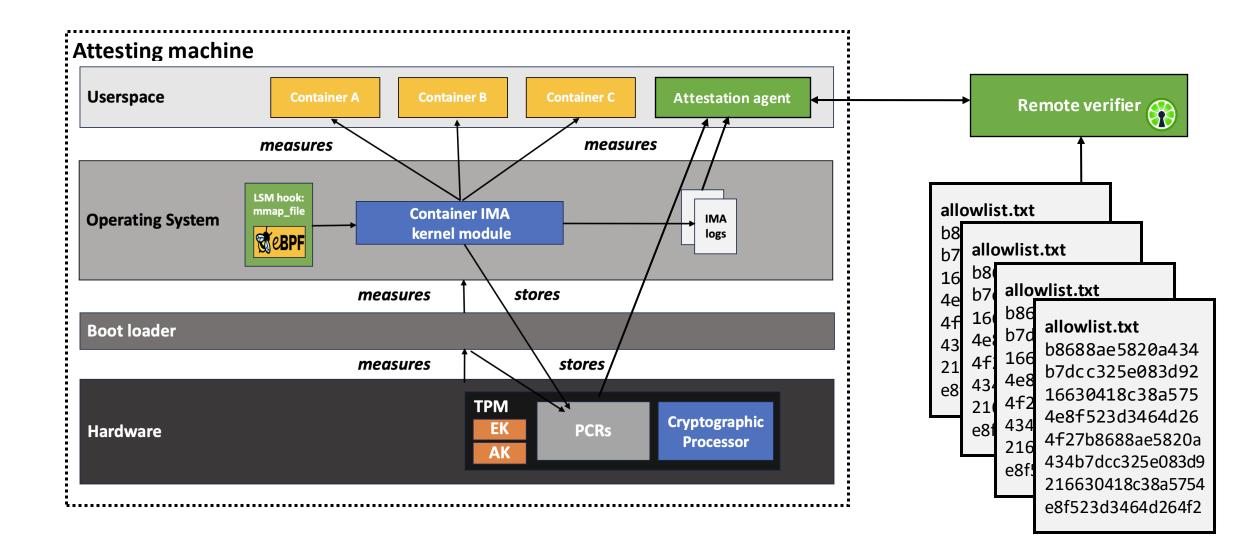


Enabling Container Attestation: A Preliminary Approach

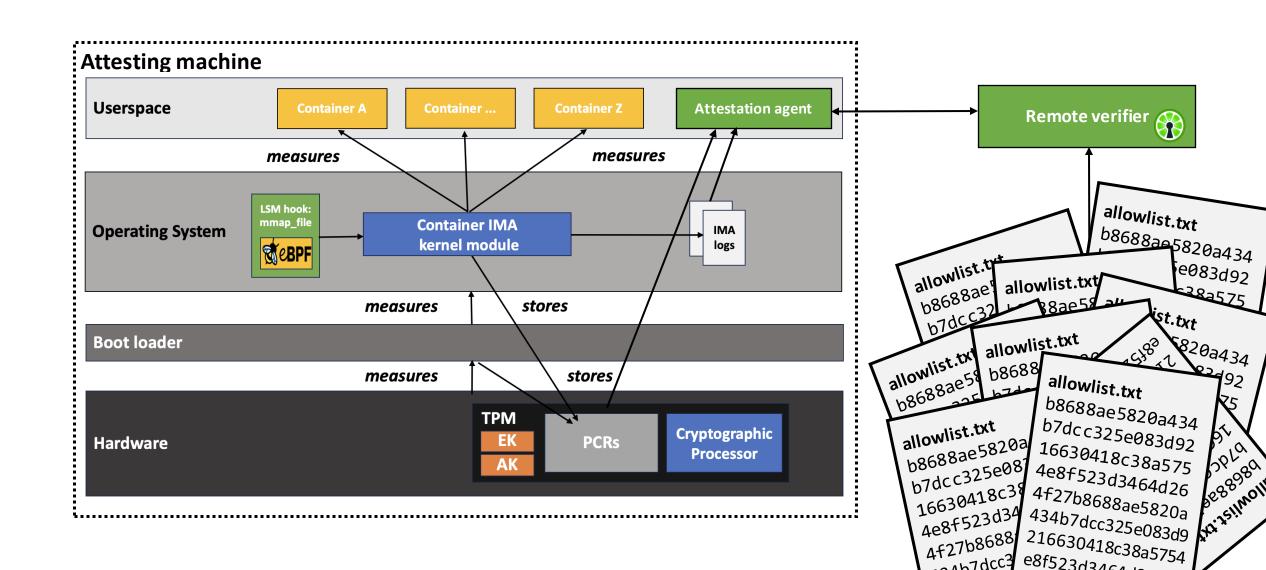
Extending IMA to Containers using eBPF



Attesting Container File Integrity

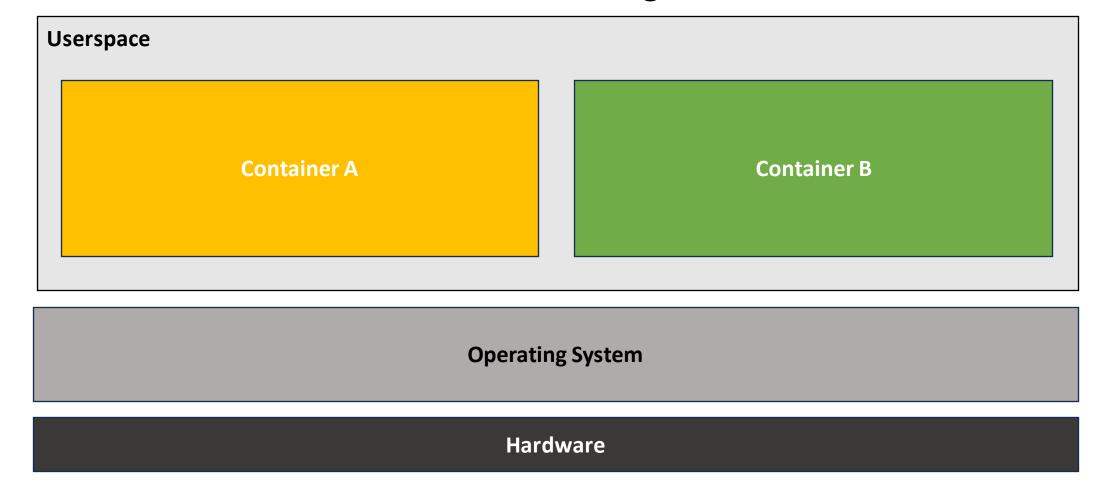


Attestation vs. Containers



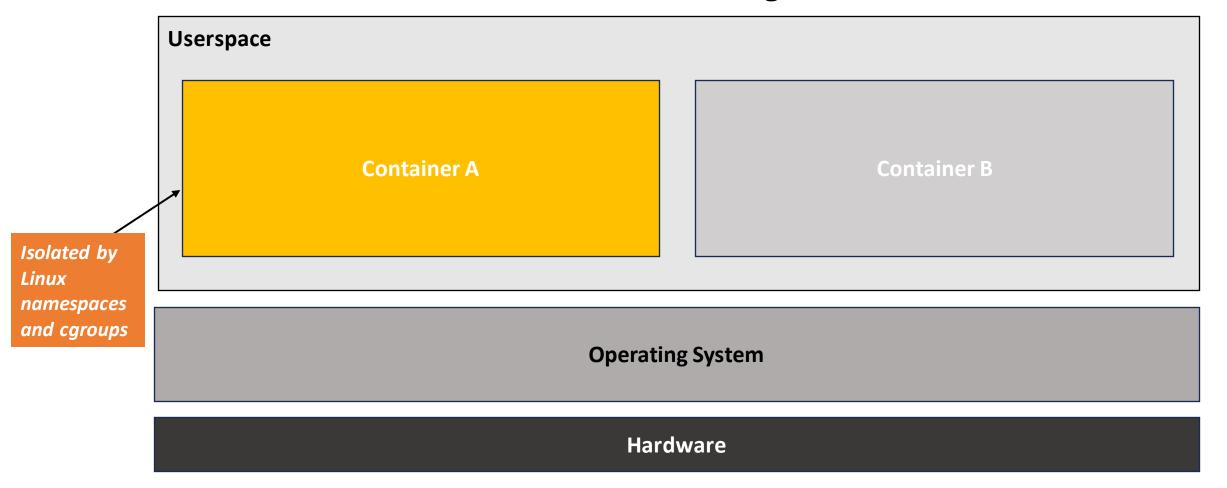
Container Image Integrity

• Goal: allow of attestation of *container images*

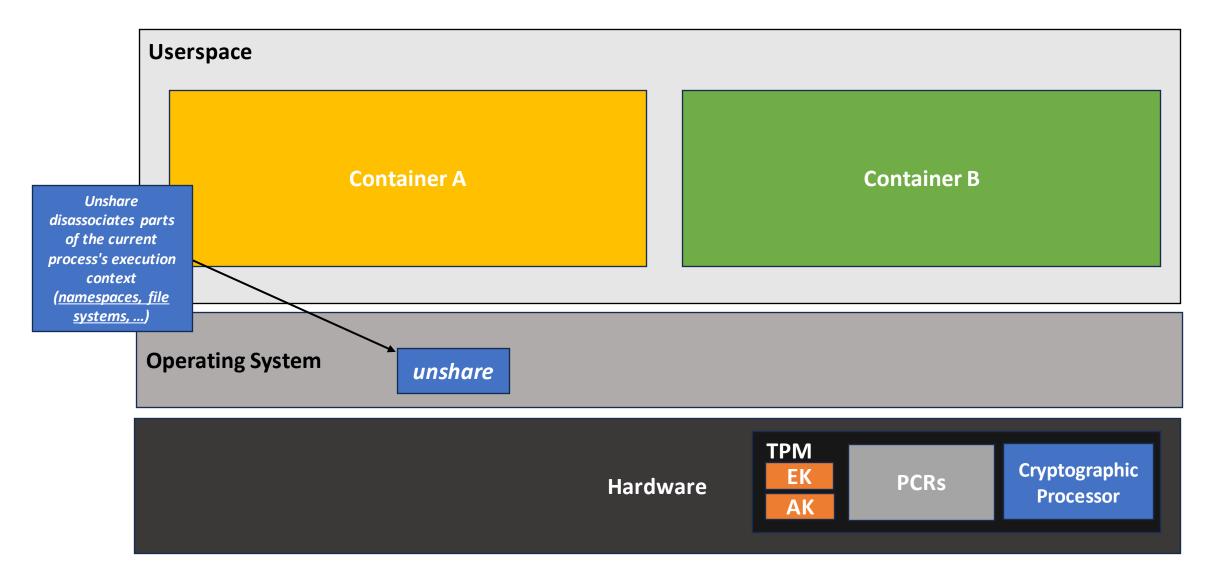


Container Image Integrity

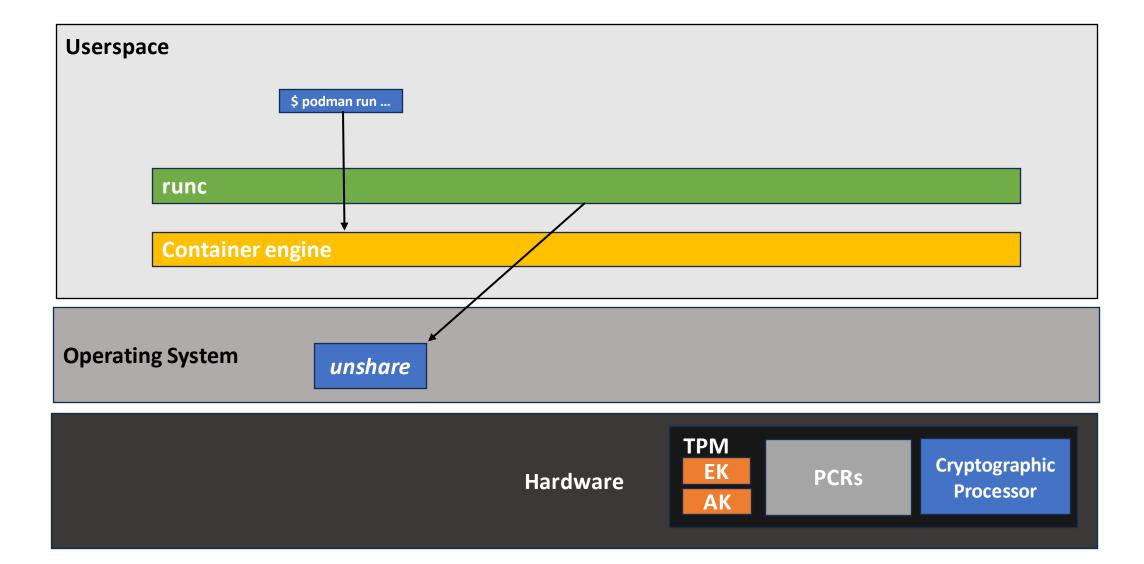
• Goal: allow of attestation of *container images*



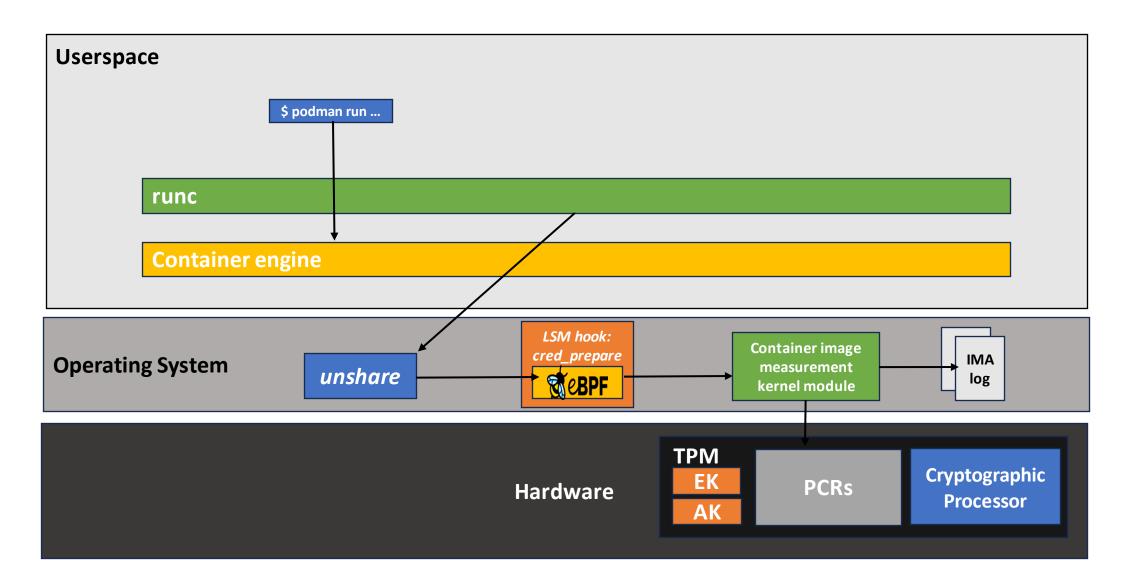
Visibility of Container Creation in the Kernel



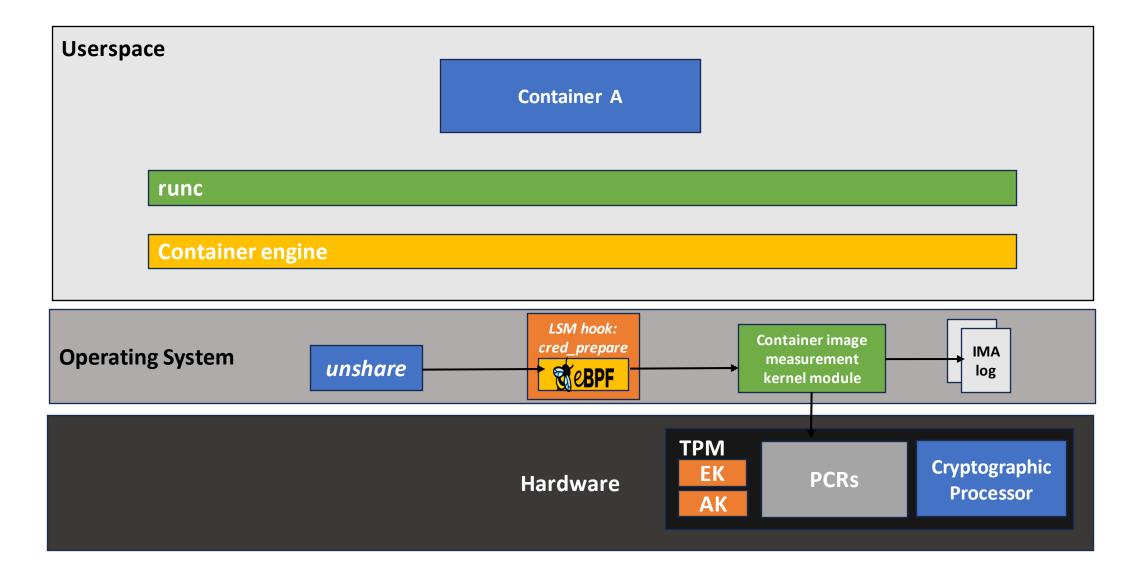
Visibility Through the Unshare System Call



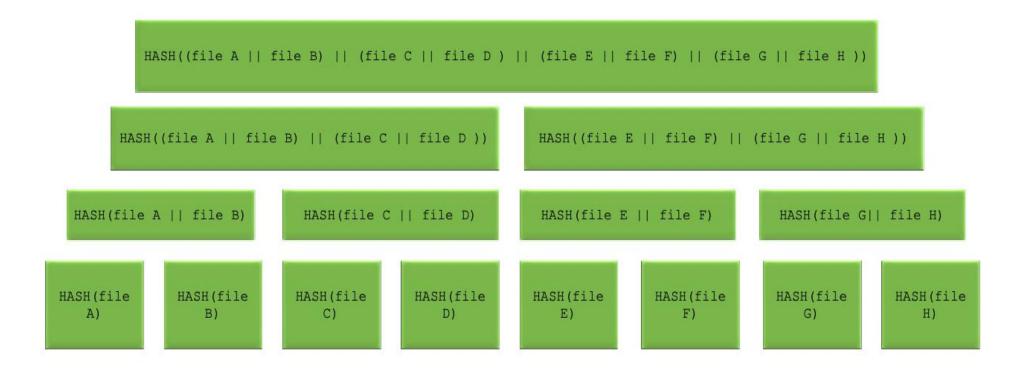
Visibility Through the Unshare System Call



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