Experimental Evaluation of Supply Chain Policies for Container Deployment

Stavros Kousidis

Bachelor thesis · Published: 2026-10-15

Research question

To what extent do signature- and provenance-based admission policies prevent unauthorized container deployments under defined attacker capabilities and operational failures?

Description

Container signatures and build attestations are useful only when a deployment system verifies them against meaningful expectations. A correctly signed image may still have been produced by an unauthorized workflow or under conditions that violate local security policy.

You will establish a small Kubernetes test environment and evaluate the Sigstore Policy Controller or an equivalent policy enforcement component. The thesis investigates the difference between cryptographic signature validity, identity authorization and verification of provenance claims.

Scope and evaluation

Define a concise attacker model and controlled scenarios, such as image substitution, acceptance of a valid but unauthorized signer, or inconsistent provenance information. Compare a baseline with progressively stricter admission policies. Evaluate detection and rejection outcomes, policy misconfiguration risks and the behavior of the system when evidence or verification services are unavailable. Identify whether a policy fails open or fails closed and assess the resulting availability costs.

Use synthetic container images and isolated infrastructure. Designing an entirely new policy language is not required.

Expected outcome

A reproducible testbed, a comparison of enforcement strategies and justified recommendations about the guarantees and operational limits of admission policies.

Starting points

- Sigstore: Kubernetes Policy Controller.
- SLSA v1.2: Verifying Build Artifacts.
- SLSA v1.2: Build Provenance.

Contact: stavros.kousidis@th-koeln.de
Code publication: open source by default; exceptions require prior agreement (policy).