How to Build a Confidential Attestation Client?

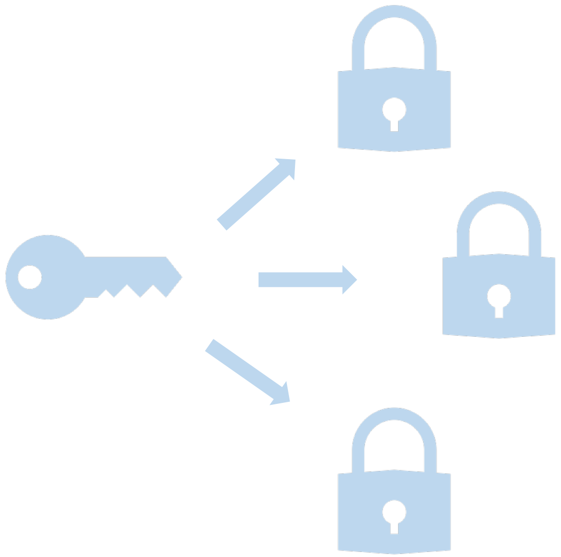
Tobin Feldman-Fitzthum

IBM Research

Linux Plumbers Conference 2023

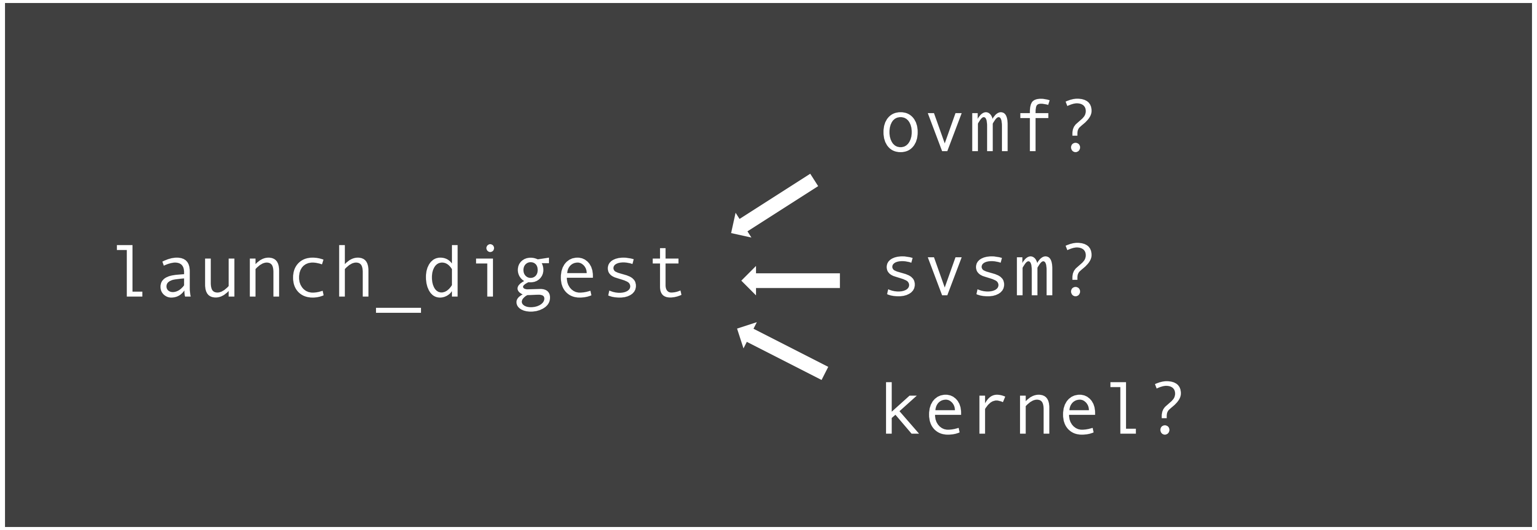
Evidence Factories

- What is the worst thing an attacker can do if they break into an enclave?
  - Is there something worse than stealing guest secrets?
  - Can an attacker impersonate a valid guest?
- Who can they attack with this evidence?
  - How generic is the evidence?
- Is there any way to prevent this?
  - Can the evidence be less generic?
  - Can access to the evidence be limited?



Metadata

- How does the verifier know what to expect?
  - How can it validate opaque measurement values?
  - Can the client provide some hints?
- Should guest information be maintained by the guest or by the host?
- How should a guest be identified?



launch_digest

ovmf?

svsm?

kernel?

Networking

- Does a client need access to a network stack?
  - Can we rely on the host to proxy requests to the KBS?

- Does the URI of the KBS need to be measured?
  - Can the KBS meaningfully validate its own URI?
  - Could another entity use the information later?