Remote Attestation of AMD SEV-SNP Confidential VMs

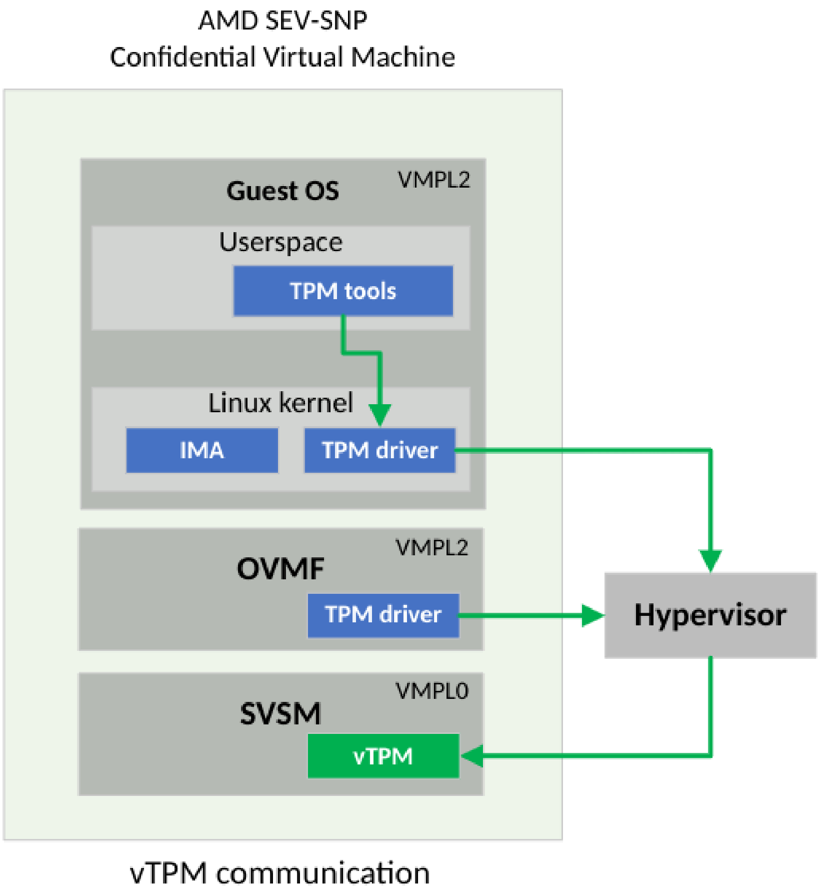
Claudio Carvalho

cclaudio@ibm.com

Linux Plumbers Conference, CoCo Microconference

November 14th, 2023

Virtual TPM for Confidential VMs



vTPM communication

- Why?
  - Standard vTPMs cannot be safely used in Confidential VMs since their state would be accessible by the hypervisor
- Privileged module in the SVSM
  - vTPM state is not accessible outside of the SVSM (e.g. hypervisor and guest OS)
- TPM drivers are enlightened to communicate with the SVSM-vTPM
  - TPM communication goes through the hypervisor, encrypted
- Existing TPM tools can be reused
  - IMA, tpm2-tools, etc.
- github.com/coconut-svsm/svsm.git
  - vTPM PR#135

Securing the vTPM state

- What is included in the vTPM state?
    - vTPM seeds, key hierarchies, objects stored in the vTPM NV, etc

- How much of the (post-)manufactured vTPM state need to be persisted across boots?
    - It really depends on the use case!

- Persistent vTPM state, generally speaking:
    - vTPM is manufactured once and securely persisted to a location outside of the CVM
    - Encrypted vTPM state is injected on every boot, e.g.:
        - Injected in the VM launch at a known memory region
        - Injected in the VM early boot (e.g. network or host proxy)
    - vTPM state should be loaded at early boot and only if the guest is in the expected initial state (early pre-attestation)
    - vTPM state changes should be securely persisted to a location outside of the CVM

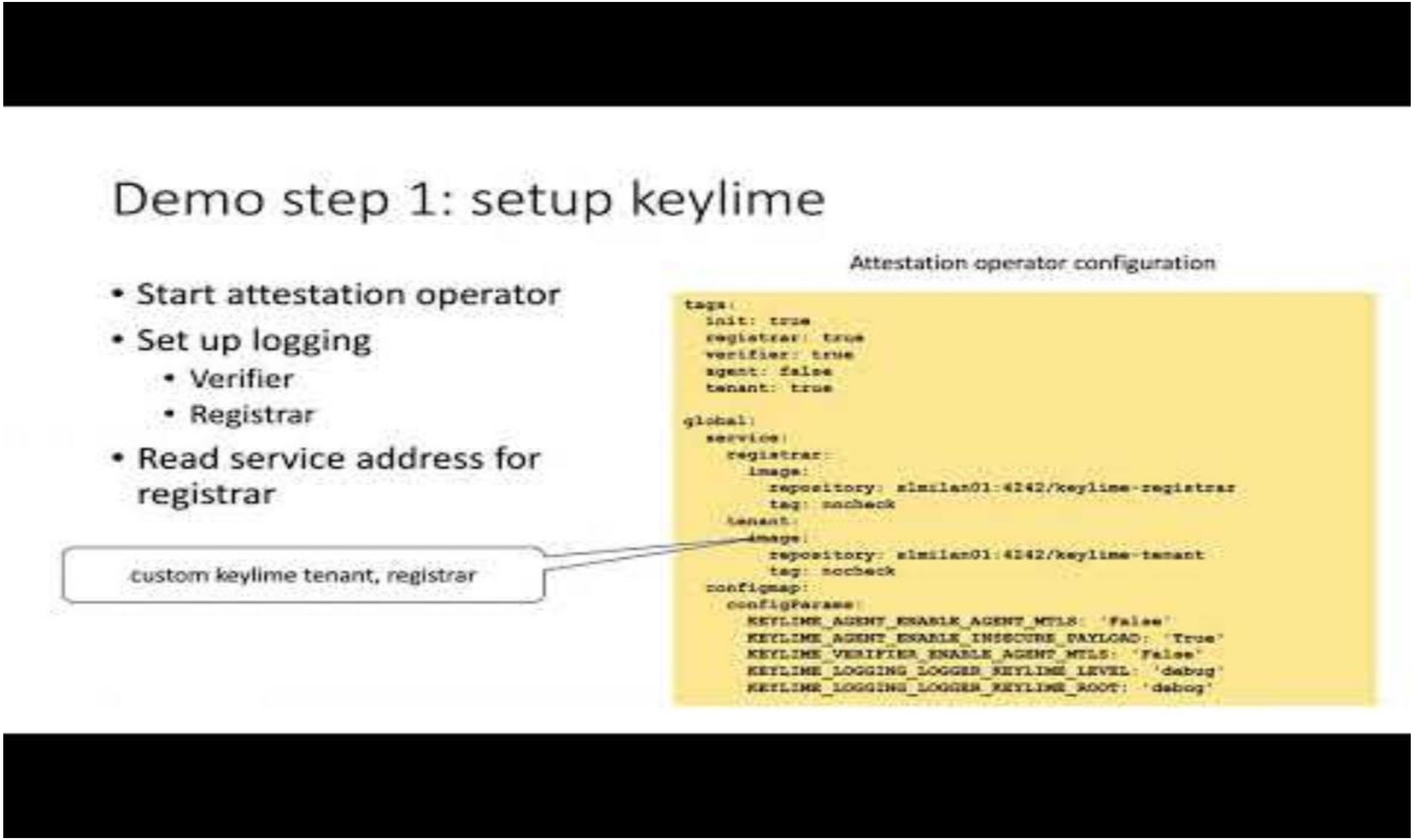
- What if the vTPM state is ephemeral?
    - vTPM is manufactured on every boot
    - vTPM state doesn't leave the confidential VM enclave

Remote attestation using an ephemeral SVSM vTPM

- PoC using keylime
  - 1. Keylime setup
  - 2. Attestation client registers the CVM on every boot with the Registrar
  - 3. Verifier attest the CVM against the policy

- For the demo: TPM EK certificate is replaced by the VMPL0 attestation report
  - Include the CVM launch measurement
  - Include vTPM information - sha512(EK_pub)
  - Report is signed by the Secure Processor using AMD key

- github.com/coconut-svsm/svsm.git
  - Attestation report, PR#69
- Annual Computer Security Applications Conference (ACSAC 2023)
  - Remote Attestation of Confidential VMs Using Ephemeral vTPMs



Demo step 1: setup keylime

- Start attestation operator
- Set up logging
  - Verifier
  - Registrar
- Read service address for registrar

custom keylime tenant, registrar

Attestation operator configuration

```
tags:
  init: true
  registrar: true
  verifier: true
  agent: false
  tenant: true

global:
  service:
    registrar:
      image:
        repository: elmilan01:4242/keylime-registrar
        tag: nocheck
    tenant:
      image:
        repository: elmilan01:4242/keylime-tenant
        tag: nocheck
  configmap:
    configParams:
      KEYLIME_AGENT_ENABLE_AGENT_MTLS: 'False'
      KEYLIME_AGENT_ENABLE_INSECURE_PAYLOAD: 'True'
      KEYLIME_VERIFIER_ENABLE_AGENT_MTLS: 'False'
      KEYLIME_LOGGING_LOGGER_KEYLIME_LEVEL: 'debug'
      KEYLIME_LOGGING_LOGGER_KEYLIME_ROOT: 'debug'
```

Demo: https://youtu.be/Bv6aMoxo5B8