TPMs and Keylime

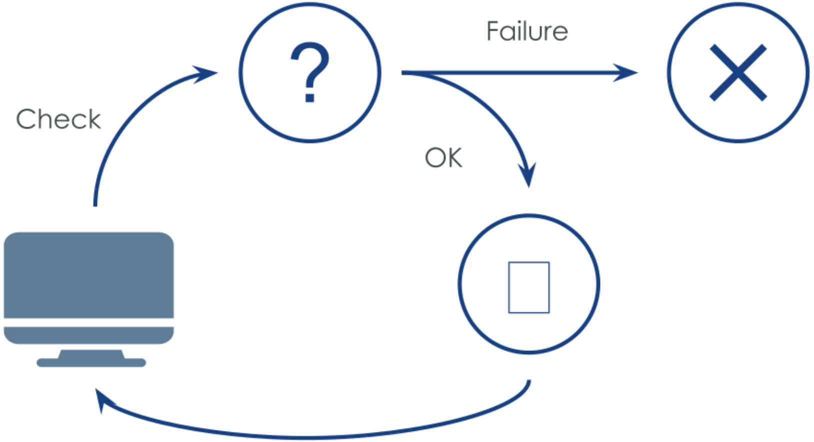
Thore Sommer (Keylime Maintainer)

CCC TAC 18.05.2023

The Problem

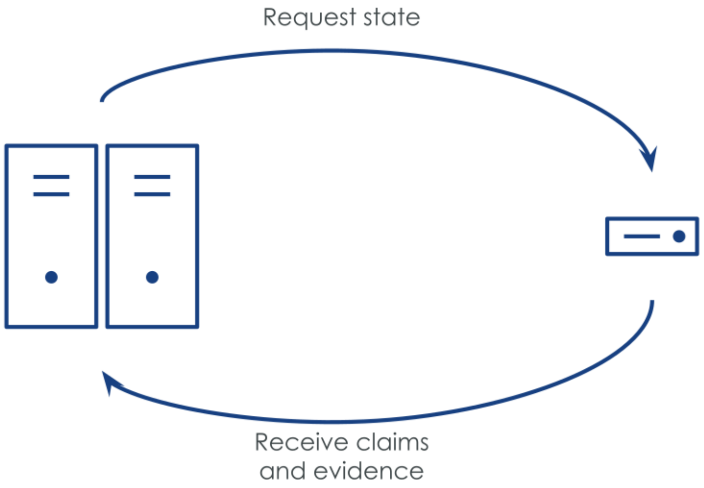
The Problem

- How to guarantee remote system integrity?



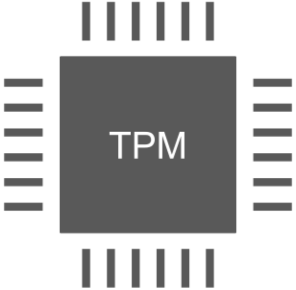
Remote Attestation

- A trusted entity requests the state of the monitored system
- A trusted agent running on the monitored system provides information about the current state of the system (claims and evidence)
- The trusted entity verifies the legitimacy of the quote and that the state is valid

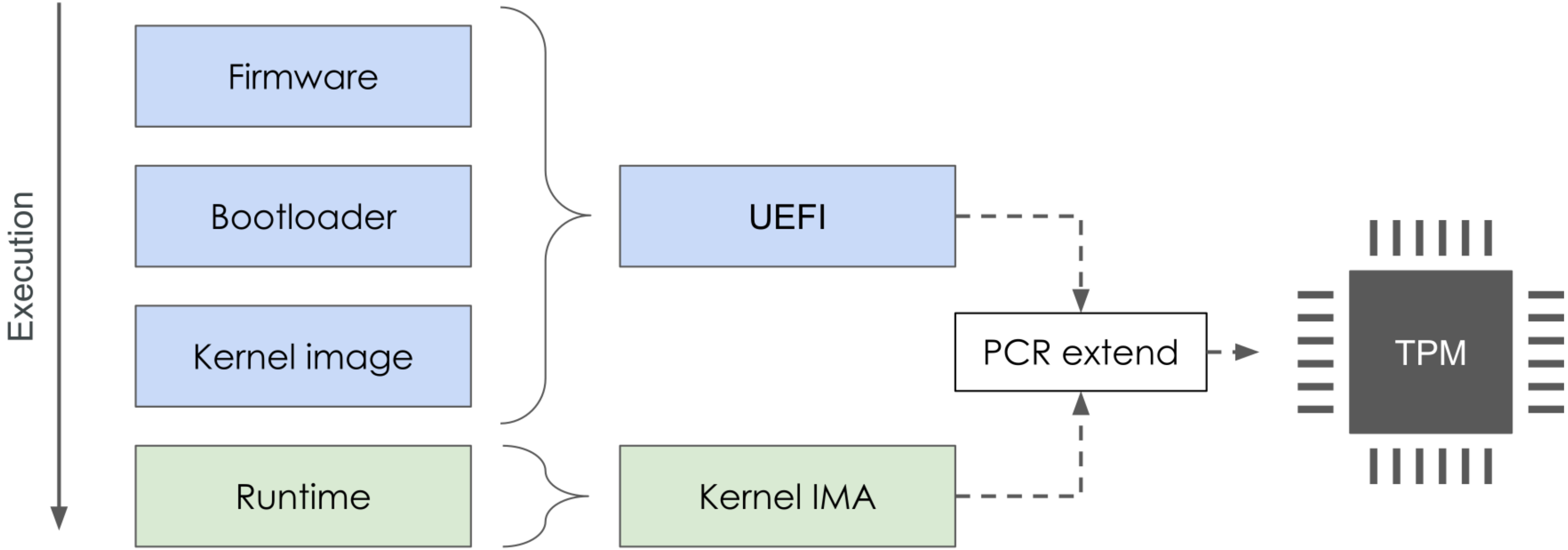


How to trust the remote agent?

- Trusted platform module (TPM)
  - Endorsement key (EK) certificate
  - Attestation key (AK)
  - Platform configuration registers (PCR)
  - Key storage
  - And other cryptographic operations

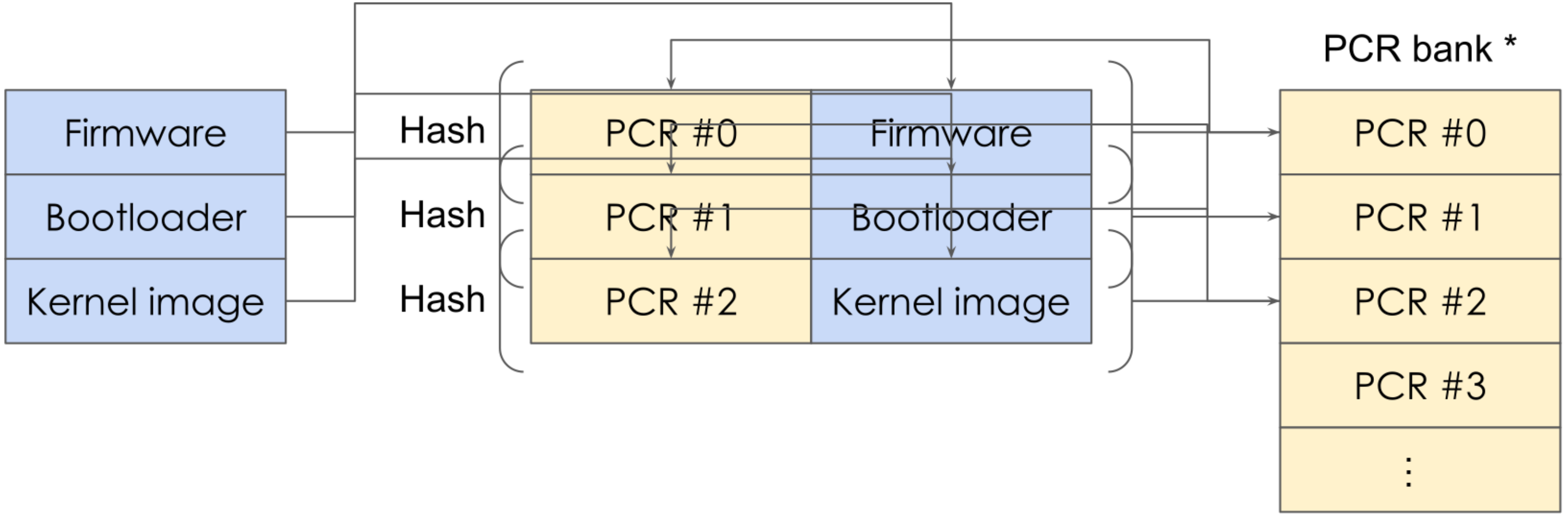


Measurement



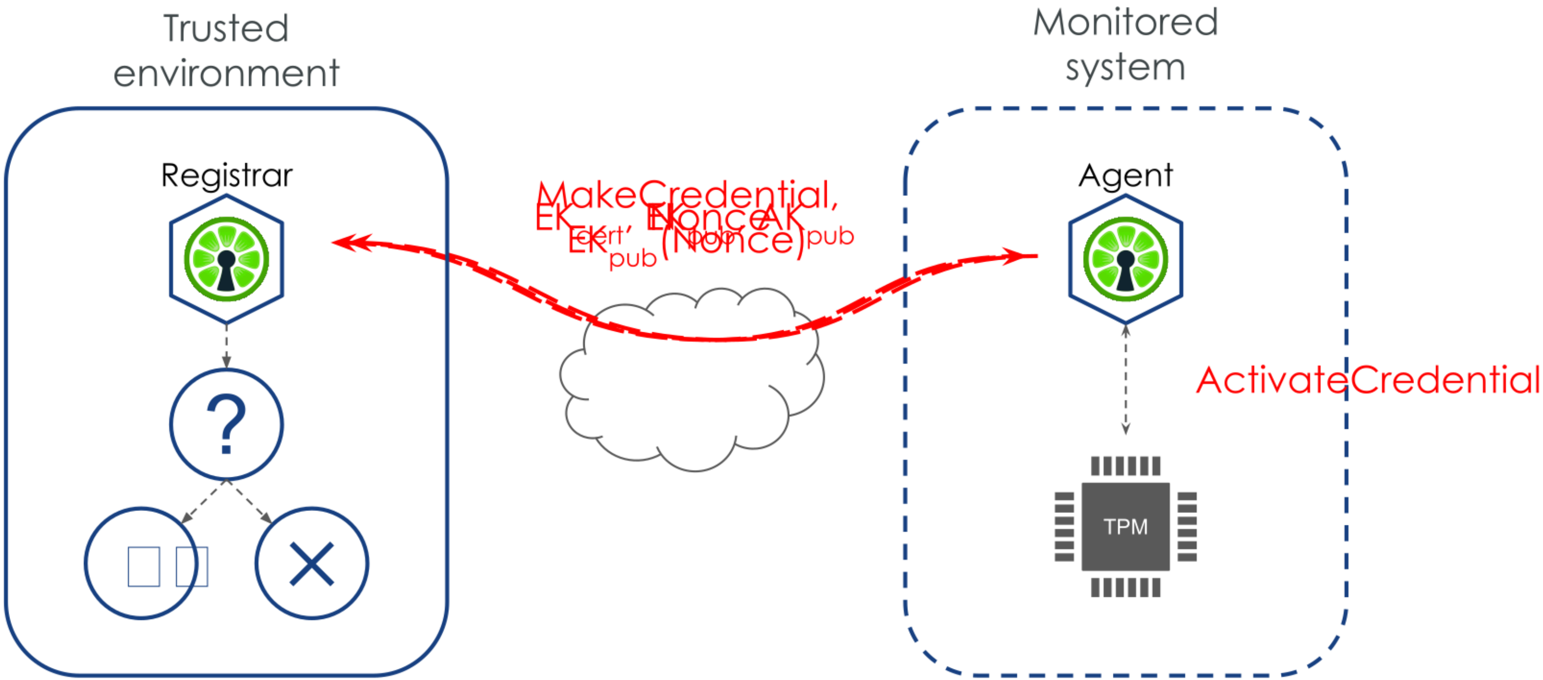
PCR extend algorithm

- The state depends on all previous states
  - Extend: PCR = Hash(PCR | Measurement)

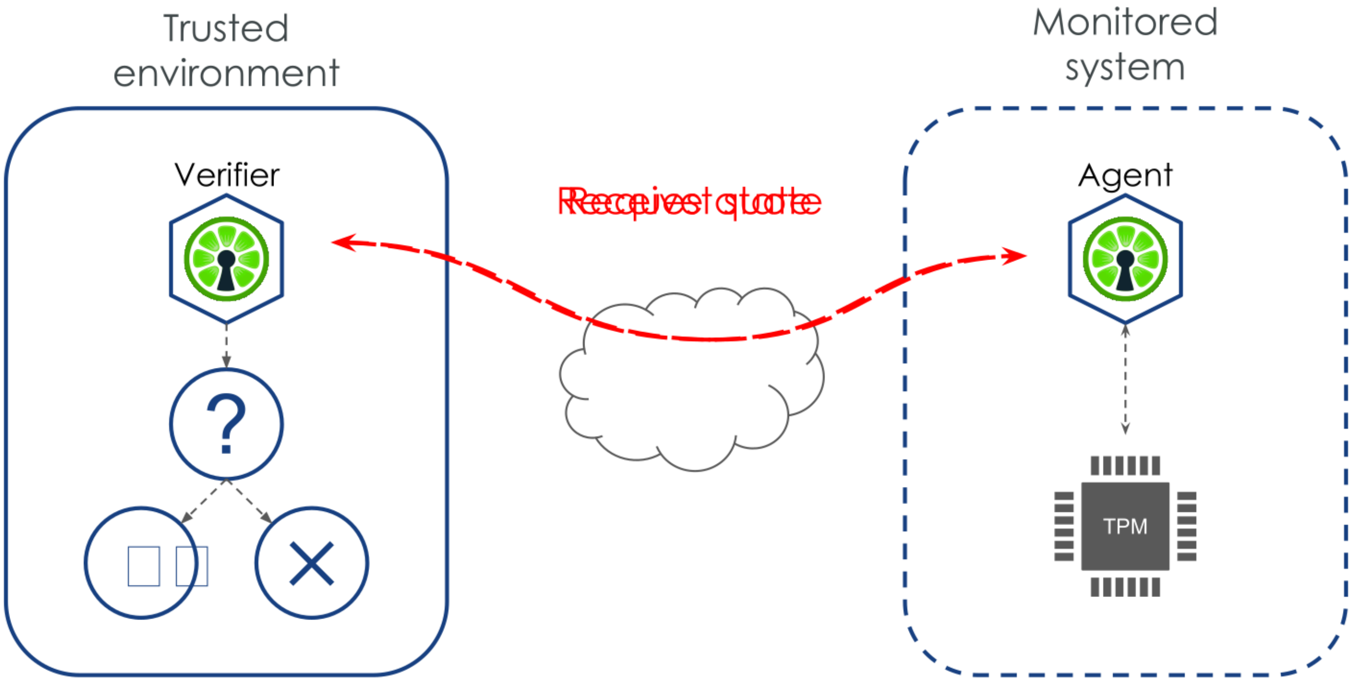


* This is just illustrative, the actual registers used for each part are defined here

How Keylime works – Registration



How Keylime works – Runtime



Keylime Overview

- Parsers and validators for IMA and Measured Boot
- Server in Python, Agent in Rust
- Started at MIT lincoln Lab, now CNCF project
- Contributors from IBM, Red Hat, SUSE, FHNW and more
- Users
  - IBM: Measured Boot
  - CAMPLA (FHNW): Measured Boot and IMA

Confidential Computing

- Attestation of TEEs is new for us
- SEV-SNP proof-of-concept was implemented
  - Provides a vTPM and attestation report instead of EK Certificate
- Provide library for attesting TEEs (starting with SEV-SNP)
  - Hosting this code under the CCC
  - Module/Plugin for Keylime
- Working on standards for Attesting TEEs
  - Share knowledge and code between projects
  - Common terminology (CCC attestation SIG, RATS, DICE etc.)

Future Work and Plans

- UEFI log parser in pure Python (mostly complete)
- Evaluation of policy engines (e.g. Regor)
- General attestation Infrastructure
  - Plugins/Modules
  - Integration of SEV-SNP attestation
  - Extending the agent (e.g. also IDevID)
  - Different agent bootstrap methods
- Separation of
  - Collection of claims and evidence
  - Validation of evidence
  - Evaluation of evidence and policies
- Agent push model
- Durable attestation (e.g. for forensics)
- Keylime and CCC

Questions?

keylime.dev

#keylime on CNCF Slack