Remote Attestation with Constrained Disclosure

Michael Eckel
Fraunhofer SIT | ATHENE
Darmstadt, Germany

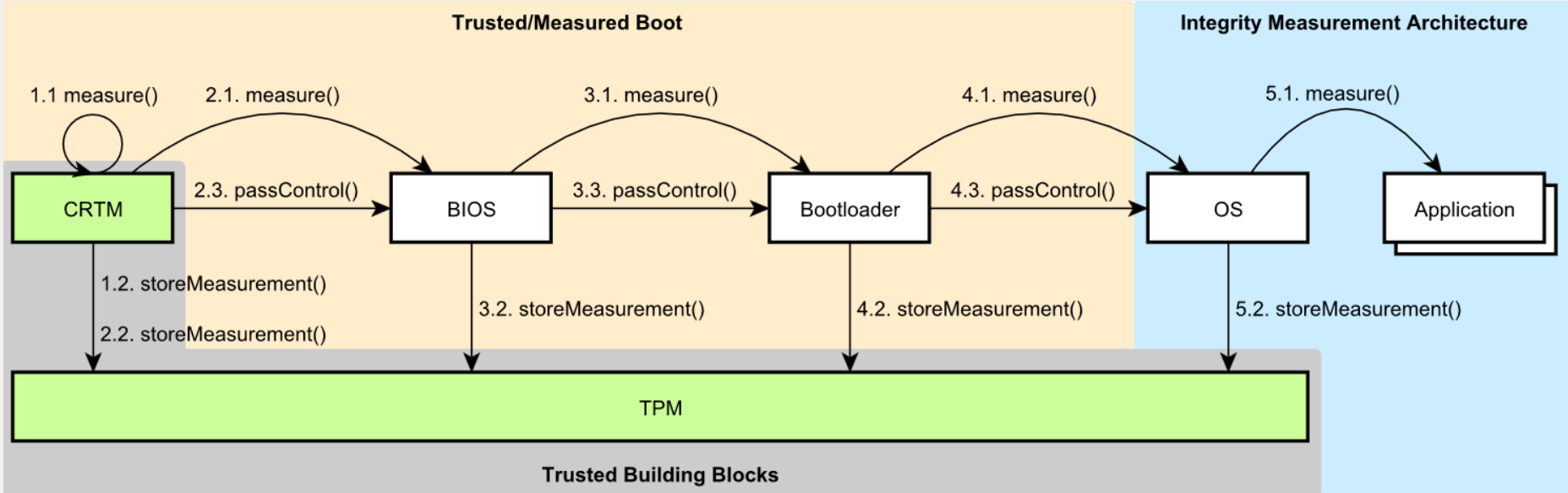
Dominik Roy George
Eindoven University of Technology
(TU/e), Netherlands

Böjrn Grohmann
gematik GmbH
Berlin, Germany

Christoph Krauß
Darmstadt University of Applied
Sciences, Germany

39th Annual Computer Security Applications Conference (ACSAC 2023) – 4-8 December 2023

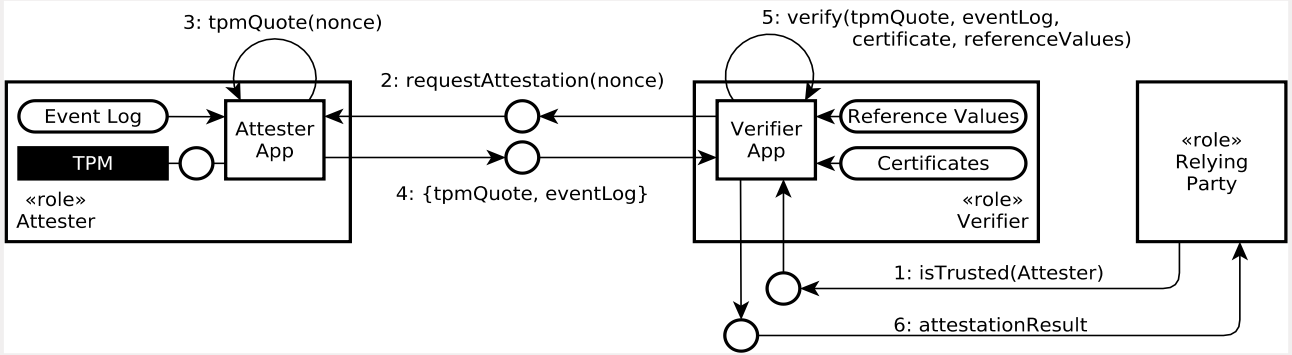
Measured Boot and Integrity Measurement Architecture



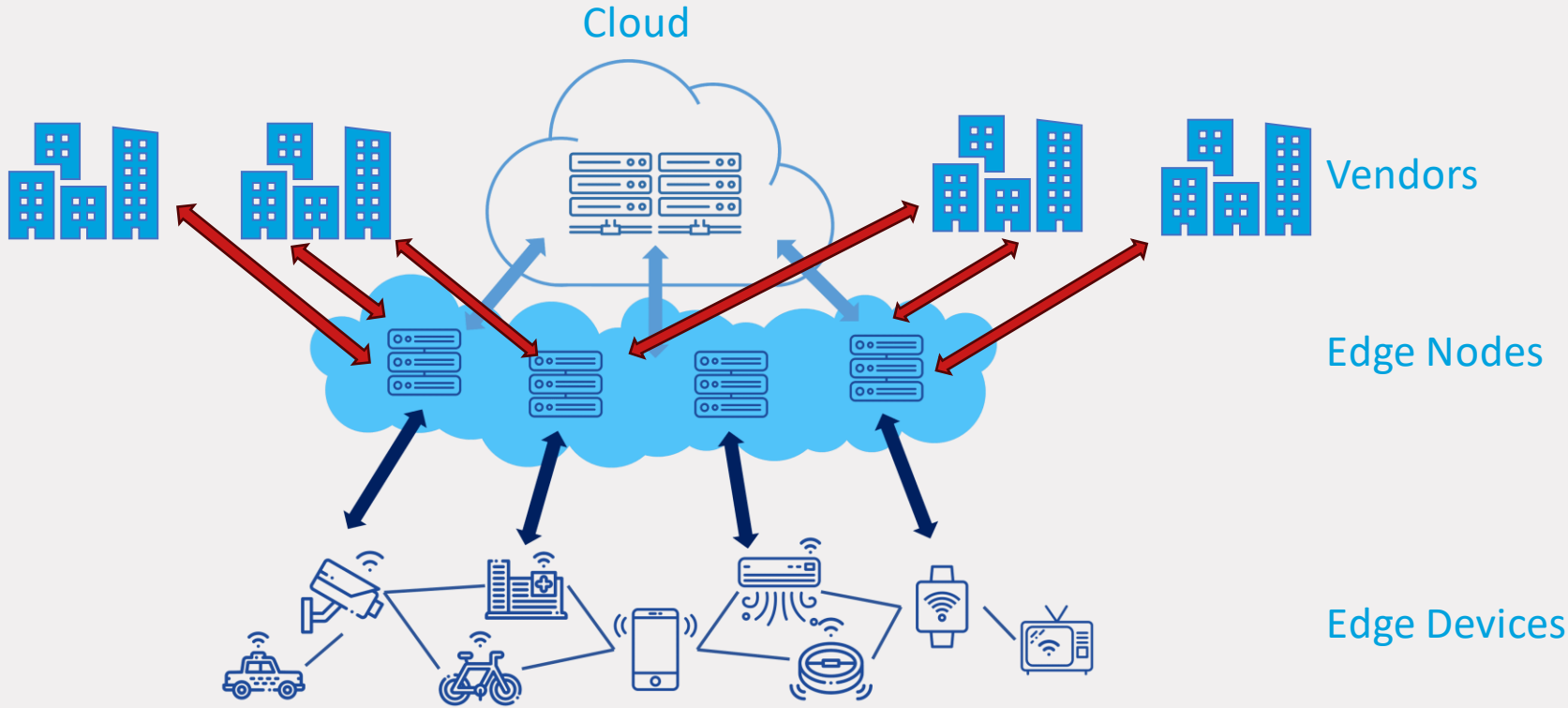
Remote Attestation

- **Involved Entities/Roles:**
  - **Attester**
    - Produces evidence to be appraised by the verifier
  - **Verifier**
    - Appraises the validity of evidence from the attester and produces attestation results
  - **Relying Party**
    - Consumes attestation results from the verifier

- **Involved Artifacts:**
  - **Evidence**
    - Digitally signed claims about the platform configuration, including measurements of software binaries and files
  - **Reference Values**
    - Verifier uses as a whitelist of known good measurements of software binaries and files to appraise evidence
  - **Attestation Result**
    - Produced by the verifier and that includes information about the trustworthiness of the attester



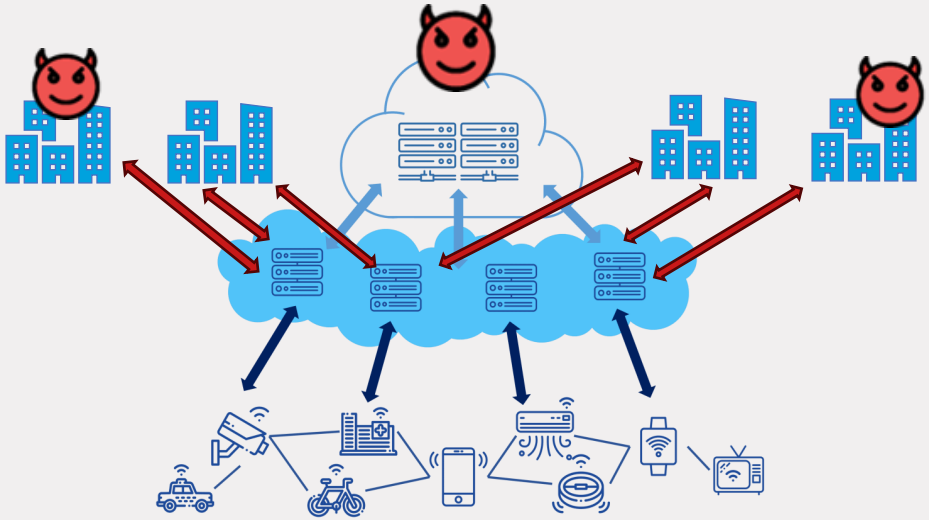
Use Case: Containerized Edge Node



Source : https://www.alibabacloud.com/knowledge/what-is-edge-computing

Adversary Model

- Honest-but-Curious Adversary
  - Following the exact steps of the protocol
- Dishonest Partial Verifier
  - Passively listening

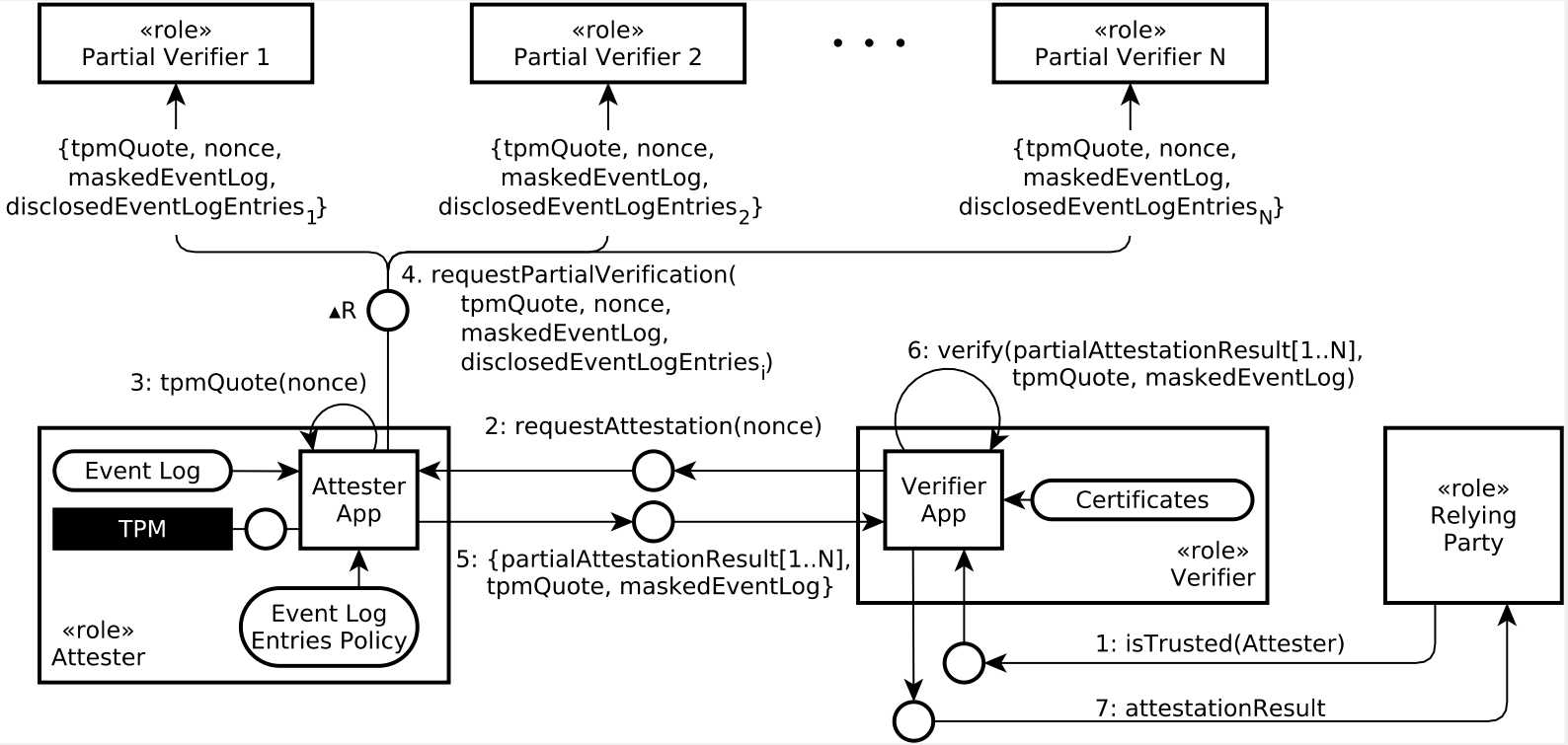


- Objective:
  - Obtain information about the software (versions) running on the attester's system
  - Query CVE database to identify and exploit vulnerable software

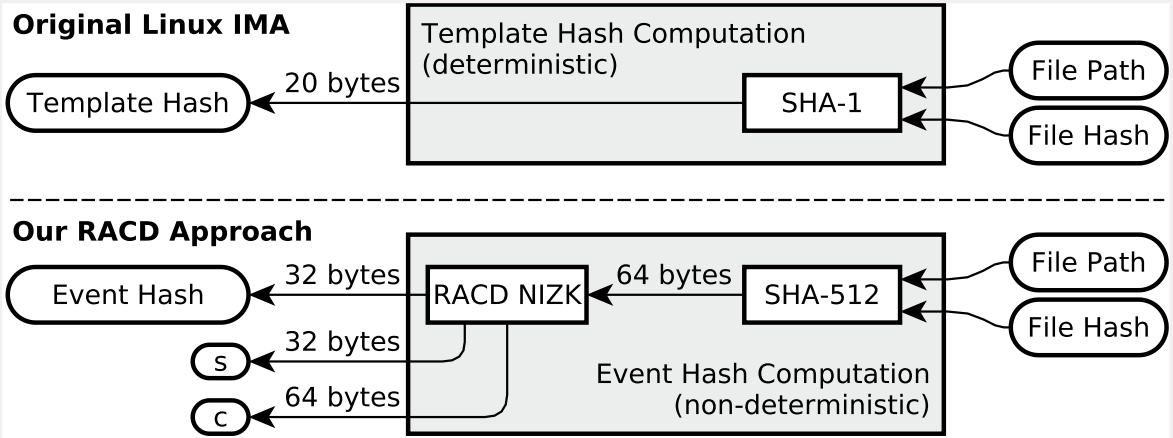
Requirements

- **Integrity and authenticity (R1)**
  - The TPM-anchored event log (with all loaded software) must be maintained
- **Secure communication (R2)**
  - Confidential communication must be established between attester and (partial) verifier
- **Mutual authentication (R3)**
- **Suitable elliptic curve (R4)**
- **Securely disclose any subset of event log entries (R5)**
- **Partial verifiers must not collude with each other (R6)**

System Model - Remote Attestation with Constrained Disclosure



Software Measurement Process



Attester

$$h_{eventhash}(r_i, x_i) = g^{r_i \cdot \varphi(h_T(x_i))}$$

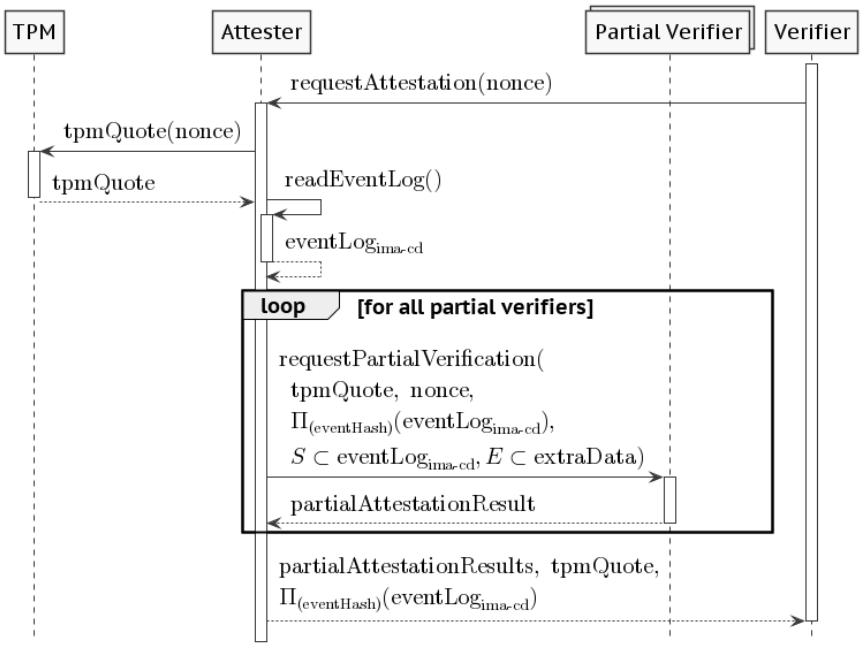
$$v_i \leftarrow\!\!\$\ \mathbb{Z}$$

$$t_i \leftarrow g_i^{v_i}$$

$$c_i \leftarrow H(g_i, t_i, h_{eventhash}(r_i, x_i))$$

$$s_i \leftarrow v_i - c_i \cdot r_i \mod |L|$$

Remote Attestation Process



Attester		Partial Verifier
$h_{eventhash}(r_i, x_i) = g^{r_i \cdot \varphi(h_T(x_i))}$		
$v_i \leftarrow\!\!\$\ \mathbb{Z}$		
$t_i \leftarrow g_i^{v_i}$		
$c_i \leftarrow H(g_i, t_i, h_{eventhash}(r_i, x_i))$		
$s_i \leftarrow v_i - c_i \cdot r_i \mod \lvert L \rvert$		
	$(c_i, s_i), h_{eventhash}(r_i, x_i) \longrightarrow$	
		$t_i' \leftarrow g_i^{s_i} \cdot h_{eventhash}(r_i, x_i)^{c_i}$
		$= g_i^{v_i - c_i \cdot r_i} \cdot h_{eventhash}(r_i, x_i)^{c_i}$
		$c_i' \leftarrow H(g_i, t_i', h_{eventhash}(r_i, x_i))$
		if $c_i = c_i'$ return *true*

Security Considerations

- RACD preserves integrity and authenticity of TPM Quote (digital signature over the TPM's internal state) and event log (R1).
- Encrypted communication (TLS) and mutual authentication (R2 and R3).
- Suitable elliptic curve identified and implemented (R4).
- Attester preserves unlinkability between disclosed (non-deterministic) event hashes and actual software binary (R5).
- Partial verifiers aren't allowed to communicate with each other (R6).

```
Weak secret x_i is true.
Query not attacker(x_i[]) is true.
Query not attacker(r_i[]) is true.
Query not attacker(v_i[]) is true.
Query event(trustable) ==> (event ↙
    (sendAttestationResult ↙
    (tpmQuote_signed,partialAttestationresults)) ↙
    ==> event(verifiedAttestationResult ↙
    (n,c_i',event_hash,result))) is true.
```

- Verification results of ProVerif on the RACD protocol

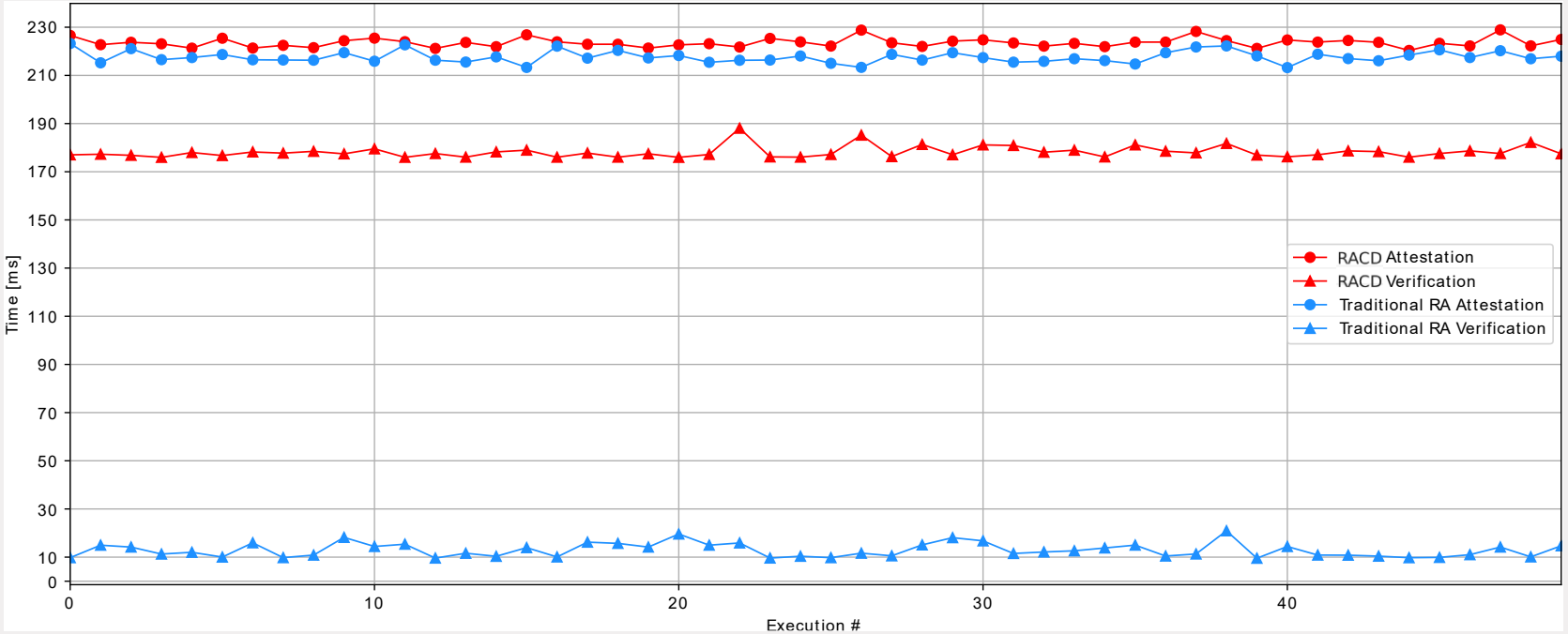
Evaluation

- Proof-of-Concept implementation on a Raspberry Pi 3 Model B V1.2 running Raspberry Pi OS lite "bullseye"

- LetsTrust TPM featuring an Infineon Optiga™ SLB 9670 TPM 2.0 attached to the GPIO ports

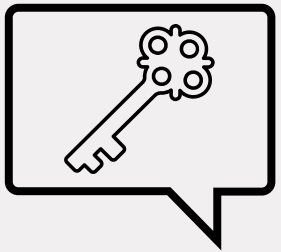
- Measurements taken from two Raspberry PIs: one attester system and one verifier

Performance Assessment



Remote Attestation between Attester and Partial Verifier

Conclusions and Future Work



- Extended existing remote attestation architecture to include constrained disclosure
- Leveraged non-interactive zero-knowledge proof (NIZK) for selective disclosure
- RACD verification took ~ 180 ms longer than traditional remote attestation

- Future Work
  - Deeply investigate RACD in the context of VMs and software containers
  - Investigate alternative selective disclosure techniques
  - Integrate RACD into Linux kernel

Fraunhofer SIT

ATHENE National Research Center for Applied Cybersecurity

h_da Hochschule Darmstadt University of Applied Sciences

TU/e Eindhoven University of Technology

Dominik Roy George

PhD Candidate
Security Group --- Faculty of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, The Netherlands
email: d.r.george@tue.nl

39th Annual Computer Security Applications Conference (ACSAC 2023) – 4-8 December 2023

Limitations

•Nonce (as a salt or freshness key) might seem simpler and more elegant compared to our NIZK method, it comes with limitations. For instance, all verifiers must be online during the (measured) boot process to supply the nonce.

•Our NIZK approach offers the advantage of transferability, eliminating the need for verifiers to be online during boot-up.

•NIZK also securely proves the validity of the data without disclosing the underlying secret and allows for the verification of the obfuscated hash.

• The computational burden associated with using NIZK for information security and limited disclosure is acknowledged. We also concur that increasing the volume of log entries would proportionally elevate the processing time.

DAA and EPID

- Our RACD approach targets the secrecy of binary measurements during remote attestation. There exists the Direct Anonymous Attestation (DAA) protocol to keep the identity of a TPM secret.
- However, DAA, Enhanced Privacy ID (EPID), etc., are orthogonal to our approach and can be used in conjunction with it.