barkhausen institut

Formal Verification of TPM-based Remote Attestation

Jannik Mähn

28.03.2024

About me

- PhD student
  - Trustworthy Data Processing - Group
- Barkhausen Institute
  - Trustworthiness for the IoT
- Topic:
  - Formal Verification of cryptographic protocols
  - Using SSProve library
  - Based on Coq theorem prover

The Project

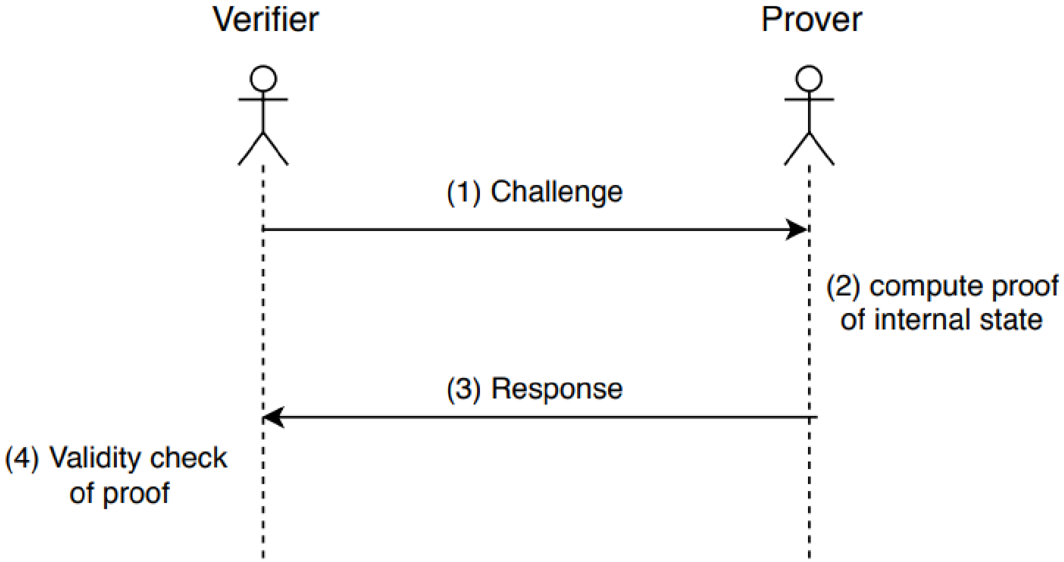
The Motivation of my research question

TPM-based Remote Attestation

- How to do Remote Attestation?

  → Trusted Platform Module (TPM)

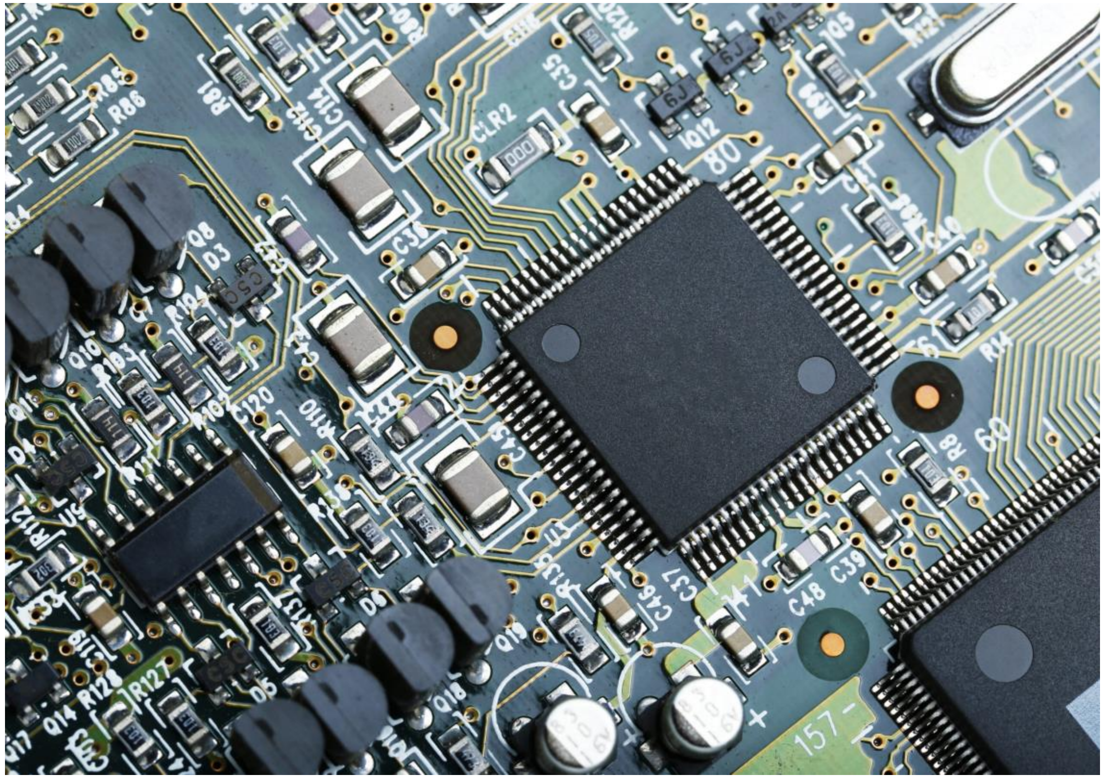
- Root of Trust
  - provides cryptographic functionalities



Trusted Platform Module

- But: Heavily underspecified:
  - Pseudocode written in C
  - Missing Statements:
    - Correctness
    - Security

- Apply formal verification



SSProve

A tool to formally verify cryptographic protocols

State-Separation Proofs

Game-based: Indistinguishability

Real $\approx$ ***Random***

Reduction-based:

- Protocol → Mathematical Assumption

- SSProve brings SSPs to Coq

SSProve

SSProve – The basics

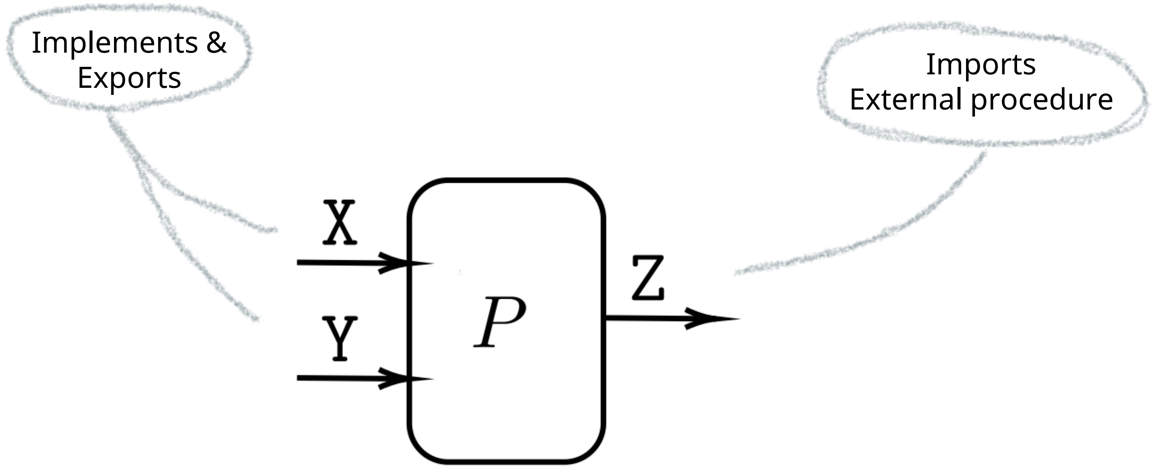


Figure 1. Package P.

```
package: P
mem: n : nat

X(b):                  Y():
  if b then              return 5
    return 1
  else
    return Z(n)
```

Figure 2. Possible pseudocode implementation for P.

A ***Distinguisher*** has the export: {run}.

A ***Game*** is a package with no import.

Definition 1 (Distinguisher advantage). *The advantage of a distinguisher $\mathcal{D}$ against a game pair $G = (G^0, G^1)$ is*

$$\alpha(G)(\mathcal{D}) = \left|\Pr\left[\mathsf{true} \leftarrow \mathcal{D} \circ G^0\right] - \Pr\left[\mathsf{true} \leftarrow \mathcal{D} \circ G^1\right]\right|$$

Research

Current state and future work

Current and future work

- Signature
  - Primitives
  - Protocol
- Remote Attestation
  - Primitives
  - Protocol
- **Future work:**
  - Signature Schemes
    - RSA Signatures
    - ECDSA

```
Theorem RA_unforg LA A :
    ValidPackage LA Att_int A_export A →
    fdisjoint LA (Sig_ideal_real).(locs) →
    fdisjoint LA (Sig_ideal).(locs) →
    fdisjoint LA (Sig_real).(locs) →
    fdisjoint LA (Sig_ideal).(locs) →
    (AdvantageE Att_ideal Att_real_ A
      <=
      AdvantageE Sig_ideal Sig_real A
    )%R.
```

```
Lemma ext_unforge:
  Sig_real ≈₀ Sig_ideal.
```

Formal Verification of TPM-based Remote Attestation

By Jannik Mähn

SSProve