ELASTIC Project

Secure Systems Group, Aalto University

Parsa Sadri Sinaki (Aalto), Zainab Ahmad (Ericsson, Aalto), Wentao Xie (Ericsson, Aalto), Merlijn Sebrechts (Ghent, imec), Jimmy Kjällman (Ericsson), and Lachlan J. Gunn (Aalto)

TrustMee: Self-Verifying Remote Attestation Evidence

- **Remote Attestation:** Establishing **trust** in **platform** integrity and confidentiality
- **Challenge:** TEEs use **different evidence formats** and verification logic
- **Solution: Bundle evidence** with its sandboxed **verification logic** whose identity is checked by policy

Introduction

- Remote **attestation** allows a Relying Party to assess whether a remote **platform** is **trustworthy.**
- A trusted Verifier (1) parses the evidence, (2) validates its signatures and certificates, and (3) checks the platform measurements, expressed as claims, against reference values.

Problem

- **Each TEE** platform requires **platform-specific parsing and validation logic**.
- Adding support for a **new TEE** or evidence format requires **adding** new code to the Verifier **TCB**.
- **Parsing and validation** code are **complex** and **vulnerability-prone**.

TrustMee

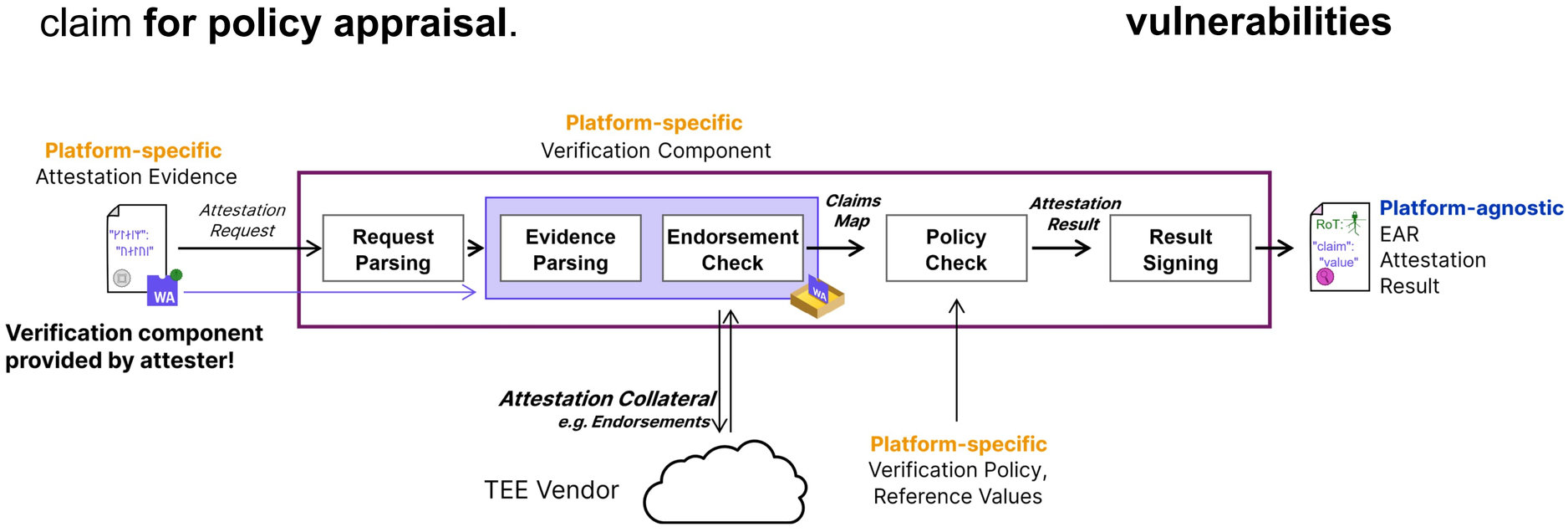
- The attester provides a **portable WebAssembly verification component** together **with** the **evidence**.
- The Verifier executes the component in a sandbox, limits its computation and network access, and **emits** the **component identity** as a claim **for policy appraisal**.

Sample Output

```
"ear.status": "affirming",                          // status of verification
    "annotated_evidence": {
        "tee_type": "tdx",                          // wasm verifier claim
        "verifier_component": "5a36...df5f",        // wasm verifier hash
        "claims": {                                 // platform-specific claims
            "rtmr_0": "5b5e...c913",
            "rtmr_1": "86d9...0394",
            ...
        }
    }
```

Contributions

- TrustMee extends verifier capabilities while keeping the verification latency within the state-of-the-art native verifier's range.
- TrustMee enables:
  - **Platform-agnostic** attestation verification
  - **Support** for **new TEEs without** Verifier code change or **redeployment**
  - **Reduces** the Verifier **TCB** and stops it from growing when supporting new TEEs
  - **Layered** and composite **attestation** verification
  - **Custom** evidence-**format verification**
  - **Sandboxed** execution of **complex** parsing and validation **logic**
  - **Prevents** cross-TEE verification **vulnerabilities**



arXiv:2602.13148

Aalto University

Co-funded by the European Union

The ELASTIC project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe programme, Grant Agreement No. 101139067. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.