Leveraging Tracing For Efficient Attestation

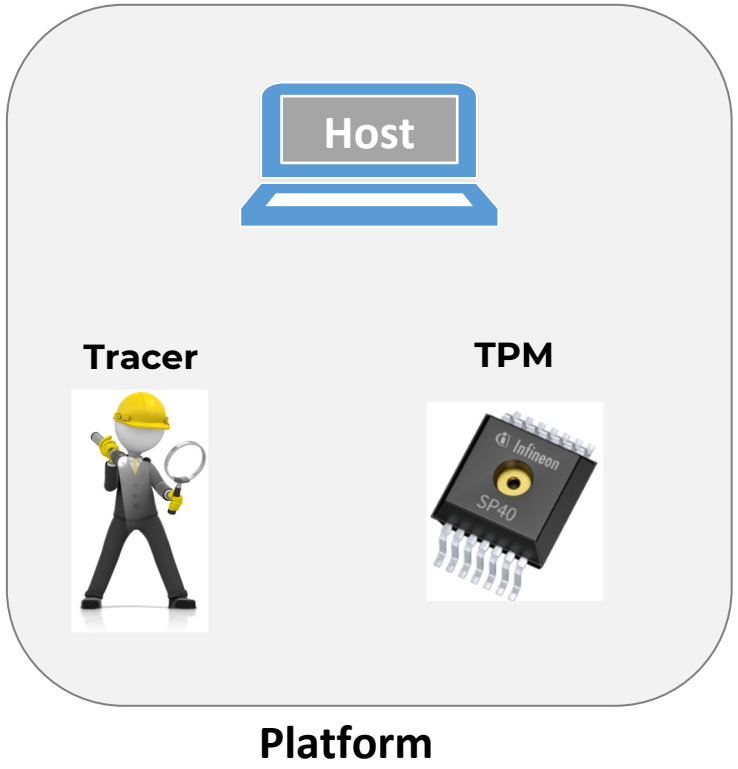
Stefanos Vasileiadis
Security Engineer, Security Group

UBITECH Ltd

ASSURED WEBINAR

Webinar | 20 June 2023

Trusted Computing Base



Challenges

- **Trusting the Tracer**
  - **OPTEE ARM Trustzone**
- **Semanting Trust between the Tracer and the TPM**
  - **ASSURED**

Integrity of Tracer / Authentication of Traces

- **The Tracer is responsible for continuously monitoring the processes executed in the device it belongs to, and collects information that is required in the context of the attestation schemes.**
- **This information can include control flow graphs used in Control-Flow Attestation (CFA), and hashes of configuration properties used in Configuration Integrity Verification (CIV).**
- **The Tracer is executed as a user space program and needs to be added to our Trusted Computing Base.**
  - *In order to prove the validity of the measurements that the TPM receives from the Tracer and uses in the context of the implemented attestation protocols, we employ a Pre-Installed Key*
  - *This key will be used to send signed traces to the Verifier, who is responsible for verifying their integrity.*
  - *Protocol securing the integrity of the reported traces. Protects against replay attacks and impersonation attacks, and ensures the integrity of the traces during correct protocol execution.*

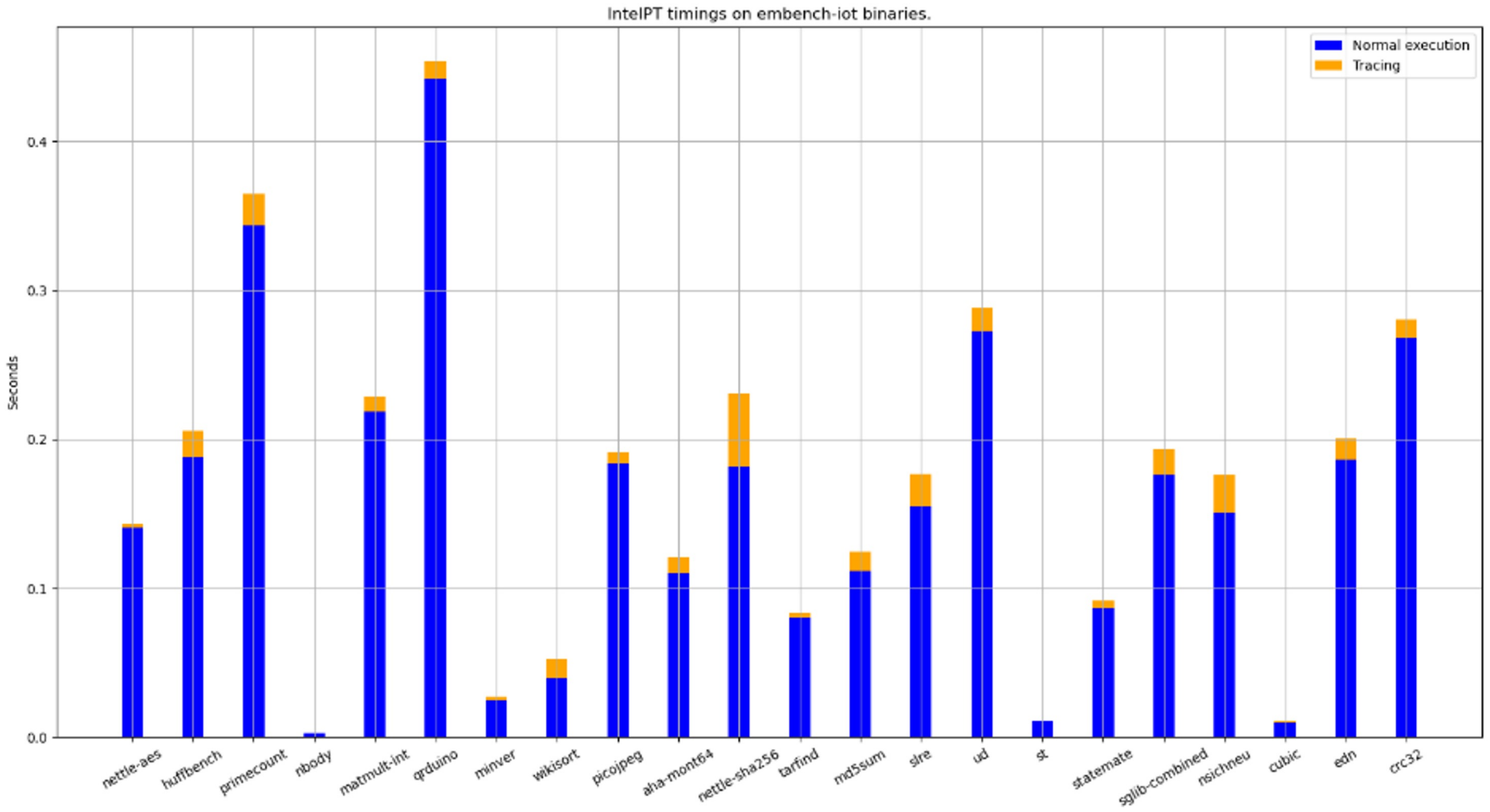
Traces Integrity && Authentication

- The TPM shares with the Tracer the Attestation Key's name.
- For every invocation of the Tracer the TPM creates a fresh policy session and shares the session nonce.
- The Tracer then calculates an authorization digest which includes the session nonce, the Attestation Key's name and the hashed traces.
- Tracer Signs the authorization digest with its private key.
- The TPM loads the Tracer's Public Key and executes TPM2_policySigned with the policy session that was created specifically for this challenge.

Tracing Techniques

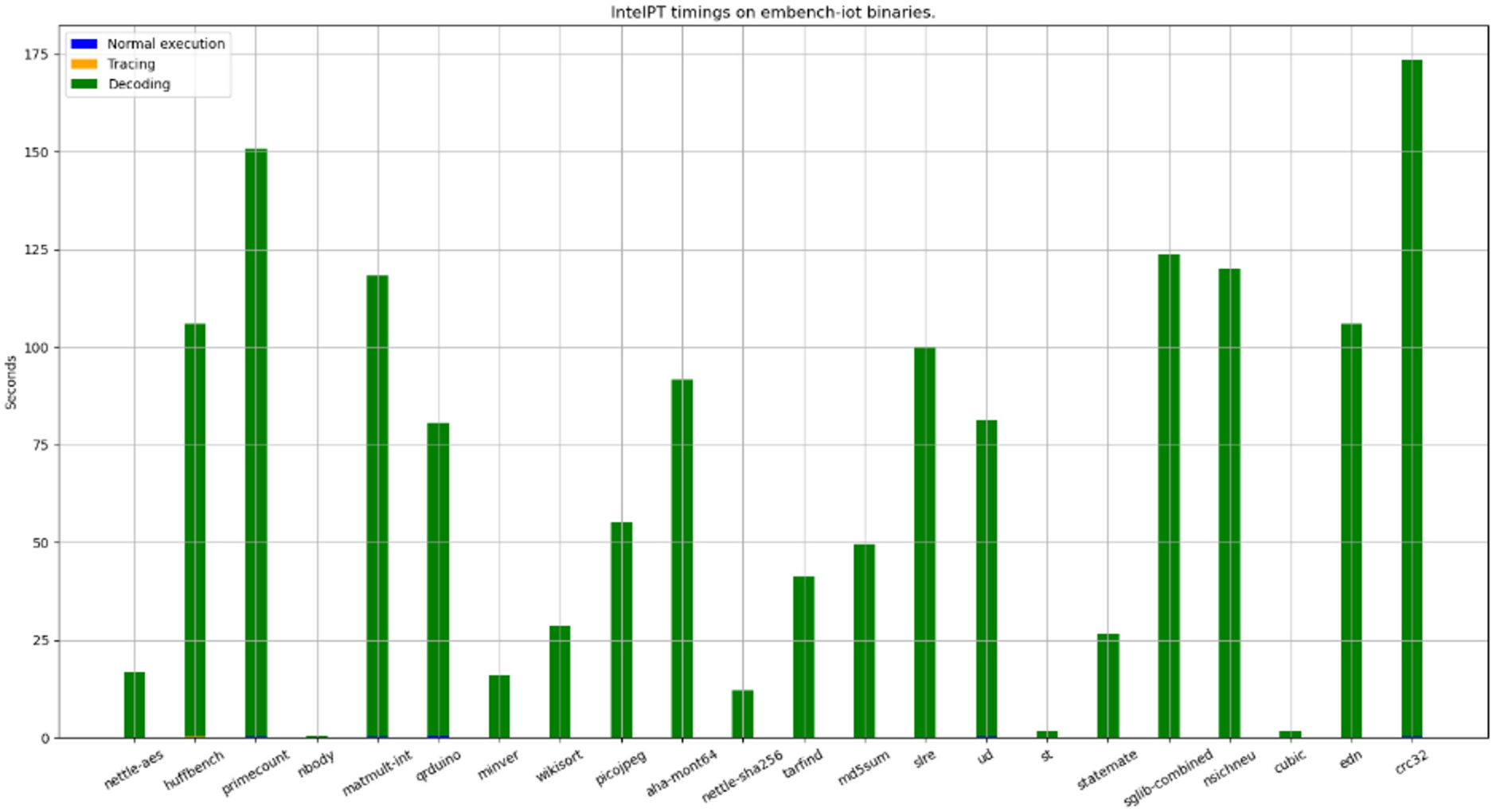
- **eBPF**
  - Fully software based solution, leveraging kernel hooks.
- **ASSURED Tracer**
  - Fully software based solution.
- **Intel PT**
  - Pseudo hardware based solution, requires support from an intel CPU.
- **Coresight Tracing**
  - Full hardware based solution.

Intel PT Evaluation



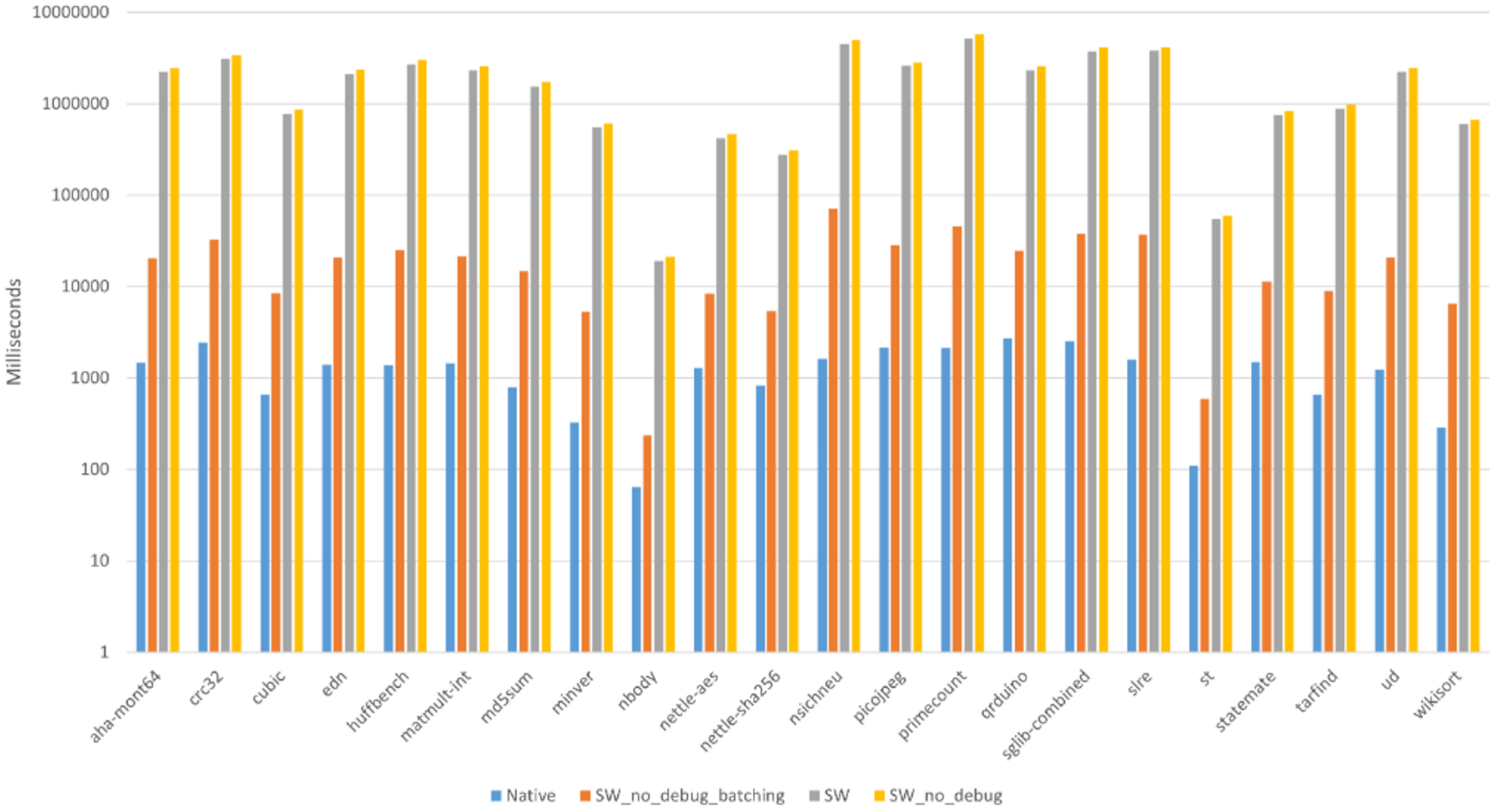
- **Evaluated against a laptop that has an intel CPU and support pt tracing.**
- **Results Extracted for embench IOT applications.**

Intel PT Evaluation



- **Even though the pseudo hardware based solution adds just a small overhead on the execution of the application, it's really heavy to decode the traces.**

ASSURED Tracer Evaluation



- **When we are not batching or decoding the debug symbols we get really good results.**
- **There is no comparison between the coresight Tracer.**
- **Almost the same or even better in some cases with the pseudo hardware based solution (Inte PT).**

THANKS

PROJECT-ASSURED.EU

@Project_Assured

ASSURED project is funded by the EU's Horizon2020 programme under Grant Agreement number 952697