How can a trusted verifier learn about run-time attacks and the dynamic behavior of an embedded device?

We present C-FLAT, a novel attestation scheme for run-time behavior.

Platform Requirements

A small trust anchor, such as TrustZone-M or TrustLite for isolating Measurement Engine

Proof-of-Concept on ARM TrustZone-A

Bare-metal prototype on Raspberry Pi 2
Single-purpose program instrumented using binary-rewriting
Runtime Monitor written in ARM assembler
Measurement Engine isolated in TrustZone-A Secure World