Chapter 1

Experiments

These experiments are based on a proof of concept of the attestation application.

1.1 Performance

The TA responsible for the attestation of the NW will be executed in a variety of circumstances and the execution time for measuring and attesting will be taken into account.

1.2 Performance Evaluation

The performance should give an insight on how often these measurements can be executed to avoid too much overhead but still be able to have good security measures.

1.3 Security Properties

The secure boot process makes sure that TrustZone works as intended which should give confidence in the belief that secure execution of trusted applications is guaranteed.

With secure execution of TAs guaranteed the Secure World can give similar guarantees as a remote attestation server would give. This implies that the attestation can happen on the device itself while still having strong confidence about the validity.

1.4 Security Evaluation