Chapter 1

Implementation

1.1 Secure Boot

It was tried to setup a booting sequence in which the Secure World is booted first and boots the NW OS from this trusted base. This is the first step towards implementing a secure boot sequence to assure that the device starts from a known secure state.

OP-TEE is the TEE framework used in this thesis and is integrated with the linux distribution that is booted on the hardware.

1.2 Attestation TA

The attestation is mainly implemented in a Trusted Application. This is done to allow the Secure World to store measurements in the secure memory and have access to the Normal World memory. Ideally the TA doesn't need to rely on the NW OS (Linux) for the memory addresses but this is the starting point for the implementation.

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.