Chapter 1

Method

The main goal of this work is to achieve a secure open platform on the hardware.

1.1 System Model

The system model describes an open platform with no or minimal trust among stakeholders.

1.2 Attacker Model

The attacker has physical access, can launch OS/firmware and software attacks. The Trusted Platform Module is assumed to be tamper resistent.

1.3 Booting Process

The secure boot makes sure that the device starts in a secure, trusted and known state.

1.4 OP-TEE integration

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

1.5 Secure Applications

Secure applications make use of the TEE capabilities of ARM TrustZone with the help of OP-TEE. These secure applications make use of the secure world execution for sensitive tasks.

1.6 Security Properties

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