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 Solution

Ideally the device is started with secure boot, this makes sure the SW is started from a known secure state.

During operation the user should be able to attest whether their device is still in a secure state.

This can be done using a TA that makes measurements on their device and reports back to them.

These measurements are checking the integrity of the code section of the running applications and OS.