Chapter 1

Method

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

1.1 Detailed Problem

- Lots of functionality
  - Sensitive data
  - Mobile computing
- Performance driven
  - All resources to functionality
  - Little room for security
  - Extensive security measures needed
- Hardware security solution
  - Security embedded in hardware
  - Better for performance
  - Correct implementation required

1.2 System Model

- Open platform
  - Multiple software providers
  - Platform owned by user
- Secure software execution

  - Software isolation
  - Secure data storage

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

1.3 Attacker Model

- Physical access
  - Threats
  - Vulnerabilities
- OS/Firmware attacks
  - Threats
  - Vulnerabilities
- Software attacks
  - Threats
  - Vulnerabilities

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

1.4 Solution

- Secure boot
  - Root of Trust
  - Chain of Trust
  - Secure starting point
- User attestation
  - Integrity (control flow, data structures, ...)
  - Authenticity (code, ...)
- Trust
  - Execution
  - Data protection

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.