Chapter 1

Background

The smartphone that will be used is a PinePhone which is equiped with ARM TrustZone, it also comes with a component which can be used as Root of Trust to make secure boot possible.

1.1 Remote Attestation

- Goal
  - Verify integrity
- How it works
  - Verifier
  - Prover
  - Proof
- Assumptions
  - Trusted third party
  - Secure keys

Remote attestation allows a device to prove to an external verifier that the software running on it is not tampered with. This attestation can go a lot further than this by for instance also checking the data structures on the device to make sure these are logical.

1.2 Trusted Execution Environment

- Execution
  - Isolation

  - Authentic code
  - Runtime integrity
  - Strict interfaces
- Trust
  - Static
  - Dynamic
- Security
  - Data separation
  - Sanitization
  - Control of information flow
  - Fault isolation

A Trusted Execution Environment is a secure, integrity-protected processing environment, consisting of memory and storage capabilities.

1.3 ARM TrustZone

- Normal World
  - Rich OS
- Secure World
  - Trusted Kernel
  - NS-bit
  - Secure Configuration Register
- Peripherals
  - TZ Address Space Controller
  - TZ Protection Controller (interrupts)

ARM TrustZone is ARM's implementation of a TEE. This is achieved by having a secure and normal world in the System on Chip.

1.4 PinePhone

- Open source
  -
- Linux
  -
- ARM TrustZone
  -

The PinePhone is an open source smartphone which supports Linux as operating system which adds to it's openness.

1.5 Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes

- Solution
  - Overview
- Trusted Boot
  - Trusted load phase
  - Attestation during boot
- Remote attestation
  - Trusted execution time
  - Pagebased approach