KU LEUVEN

arm
TRUSTZONE

Thesis

Building A Secure and Open
IoT Platform with ARM TrustZone

Oberon Swings

KU Leuven

December 7, 2021

ref image: https://developer.arm.com/ip-products/security-ip/trustzone

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Goals

Goals of an open platform

Problems

Security is hard to guarantee in this setting

Security

Security goals of an open platform

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Trusted Execution Environment

What is a Trusted Execution Environment, difference between SEE and TEE

Secure and normal world

How the hardware enforces security

Root of Trust

Root of trust is needed to achieve these goals

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Hardware

Available hardware and support

Application

Open platform for mobile computing

OP-TEE

Open Portable Trusted Execution Environment on PinePhone

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Research Question(s)

Can the PinePhone be turned into a secure open IoT platform?

- What ARM TrustZone features does OP-TEE make availablee when being ported onto a PinePhone?
- Is it feasible to secure boot the PinePhone and in this way achieve a root of trust?
- Can the I/O of the PinePhone be secured using OP-TEE and ARM TrustZone?

Hypothesis

OP-TEE can be ported onto a PinePhone and will atleast enable secure boot and secure I/O. Booting process will be slowed down but not to an unpleasant extent. I/O will be slower due to switching between worlds, but I/O always suffers from OS overhead so the added overhead should be minimal.

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Past

Qemu emulator on laptop to play around with OP-TEE and secure applications.

Present

Booting the PinePhone with OP-TEE

Future

Tweaking the booting process to use secure boot Writing secure application to make use of secure I/O,...