KU LEUVEN

Thesis

Building A Secure and Open IoT Platform with ARM TrustZone

Oberon Swings

KU Leuven

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

December 14, 2021

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Goals

- Middleware
- Connect, manage, support,...
- Openness
  - Open-source
  - Open standards
  - Open APIs
  - Open data
  - Open layer

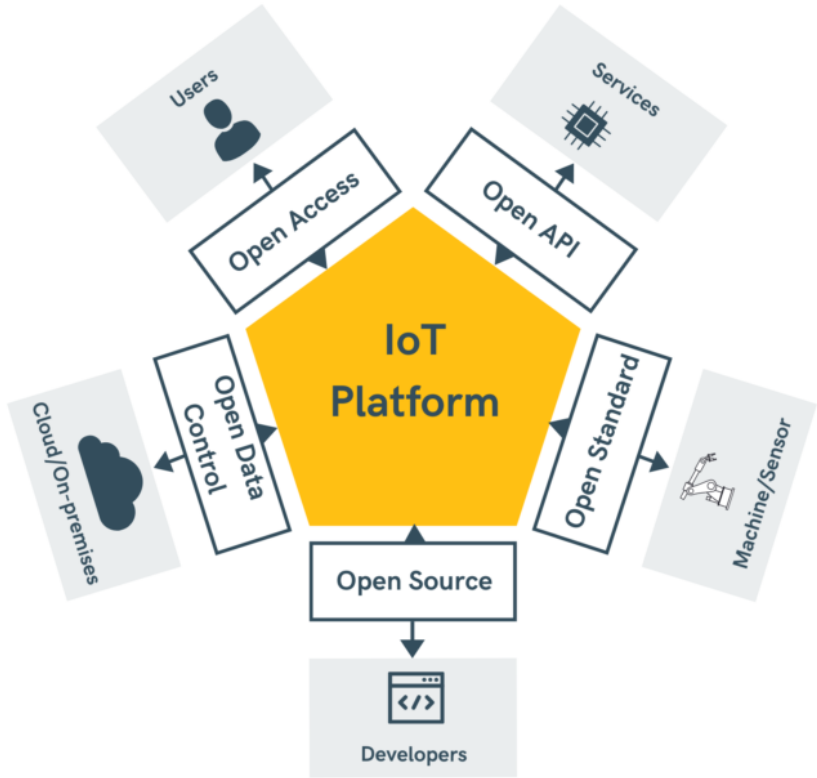


image: https://www.record-evolution.de/en/what-is-an-open-iot-platform-and-why-use-one/

Problems

- Shared resources
  - I/O
  - Memory
  - CPU
- Lack of trust
  - Software providers
  - Operating system

Security

- Software isolation
- Secure I/O
- Secure communication
- Remote attestation

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Trusted Execution Environment

- TEE (Trusted Execution Environment)
  - Authenticity (execution)
  - Confidentiality (states)
  - Integrity (code and data)
  - Minimize TCB

Implementation

- Processor level vs OS level (Intel SGX)
- Secure and normal world
- Hardware isolation
- TrustZone Address Space Controller

Root of Trust

- Chain of trust
  - Secure application
  - TEE framework
  - Booting process
  - Secure module
- Root of trust

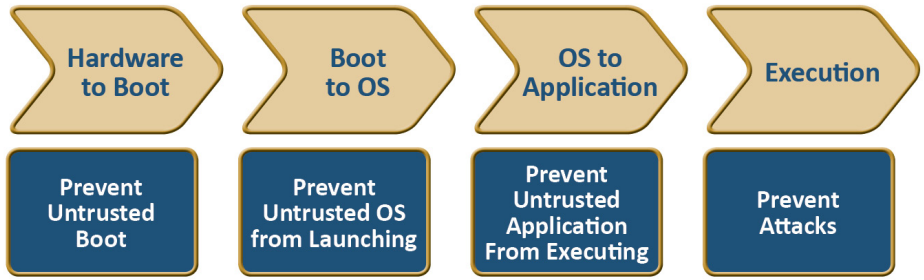


image: https://www.phaedsys.com/principals/iconlabs/Iconfloodgatesecureboot.html

Outline

Secure Open Platform

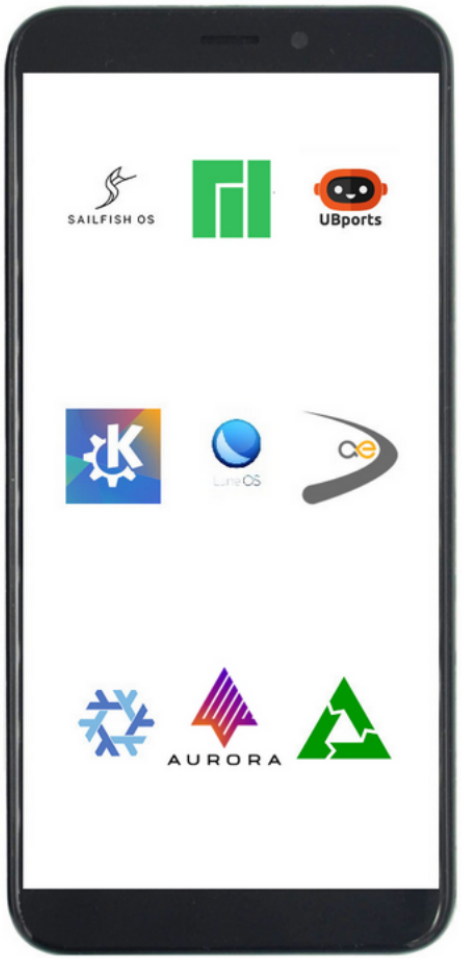
ARM TrustZone

PinePhone

Research

Progress

Hardware



PinePhone

- Quad-Core Allwinner A64 @ 1.152 GHz
- Up to 3GB LPDDR3 RAM
- Quectel EG25-G with worldwide bands
- Bootable microSD and 16GB/32GB eMMC
- Kill switches for LTE, Cameras, Wifi/BT, and Microphones
- Six pogo pins allowing for custom hardware extensions

Go to Store

image: https://www.pine64.org/pinephone/

Application

- Open-source smartphone
  - Open standards
  - Open data
- Linux
  - Open source
  - Open APIs
- Open platform for mobile computing

OP-TEE

- Open Portable Trusted Execution Environment
- Relies on ARM TrustZone
- Client and OS
- Interacts with Linux

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Research Questions

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

- What security features from OP-TEE are necessary to achieve a secure open platform on the 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 ARM TrustZone and secure boot.
- The secure boot will ensure that OP-TEE is started from a secure and trusted space ensuring it will work correctly.
- Secure applications will be able to make use of ARM TrustZone through OP-TEE and in this way achieve secure I/O on the device.

Outline

Secure Open Platform

ARM TrustZone

PinePhone

Research

Progress

Past

- Literature study
- Qemu emulator
- Secure applications
- AuthenticExecution framework

Present

- Booting PinePhone with OP-TEE

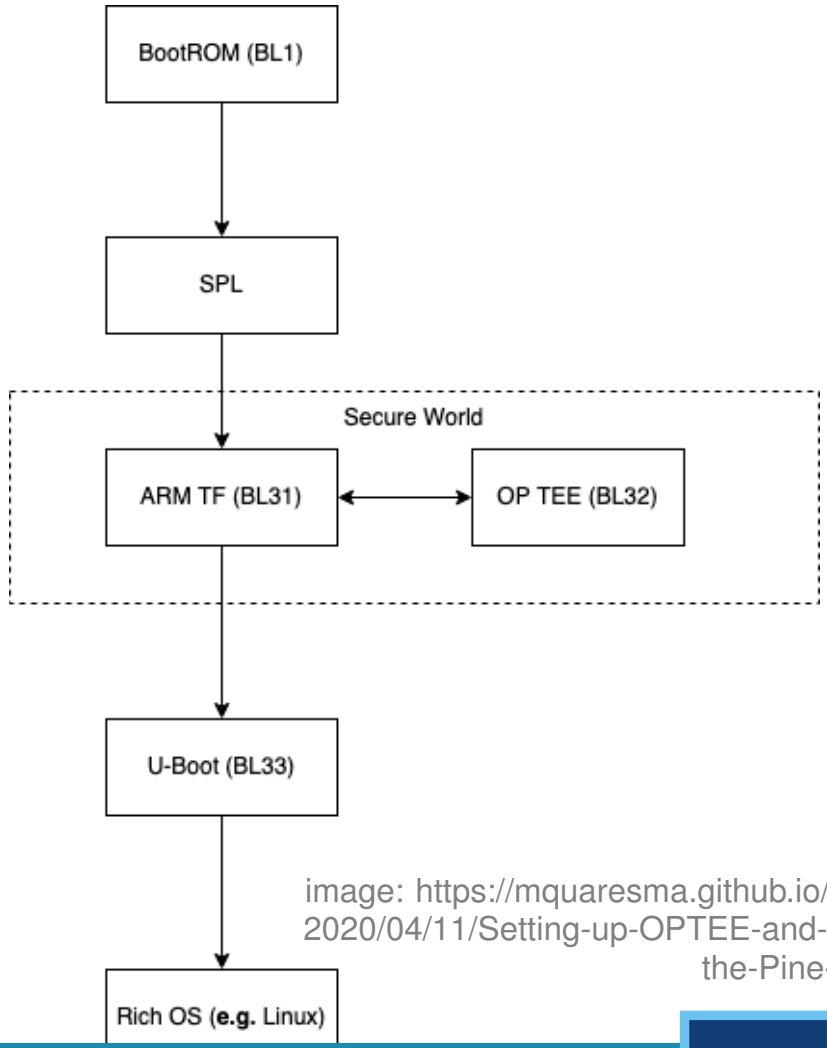


image: https://mquaresma.github.io/pine/a64/2020/04/11/Setting-up-OPTEE-and-Linux-for-the-Pine-A64.html

Future

- Tweak booting for secure boot
- Proof of concept for secure I/O
- Write thesis

Questions?

image: https://www.toonpool.com/cartoons/Question_376876