Thesis: Outline

Oberon Swings

February 19, 2022

Contents

Chapter 1

Introduction

Smartphones are everywhere, being used for more and more sensitive data. Hacking into these devices should be made as hard as hacking into someone's personal computer because for many those two have become interchangeable.

1.1 Problem statement

The hardware in smartphones is comparable to that of IoT devices, it is more powerfull in many occasions but the design principles are often the same. The problem with this is that IoT devices are not very secure, smartphones are in that sense lagging behind on security compared to how they are used (banking, health and identification applications).

1.2 Contributions

Major producers of smartphone chips are adding hardware support for security (Intel SGX, ARM TrustZone). The focus of this thesis lies in using ARM TrustZone to achieve a secure open platform from a smartphone equiped with ARM TrustZone.

1.3 Outline

In the next chapter more background information about among other things ARM TrustZone and Secure boot will be given. In the third chapter the methods of secure boot and secure applications will be explained. In the fourth chapter the goal and outcome of the experiments will be made clear. The final chapter will conclude this thesis informing the reader about limitations of this work and possible future directions of research.

Chapter 2

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.

2.1 PinePhone

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

2.2 Trusted Execution Environment

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

2.3 ARM TrustZone

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

2.4 Chain of Trust

To trust an application, the environment in which this application runs also needs to be trusted which often translates to the operating system, bootloader, hardware,...

2.5 Secure Boot

Secure boot is a booting process in which a Root of Trust is used to make sure that the code used for booting is not tampered with.

Chapter 3

Method

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

3.1 System Model

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

3.2 Attacker Model

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

3.3 Booting Process

The secure boot makes sure that the device starts in a secure, trusted and known state.

3.4 OP-TEE integration

OP-TEE is the TEE framework used in this thesis and is integrated with the linux distribution that is booted on the hardware.

3.5 Secure Applications

Secure applications make use of the TEE capabilities of ARM TrustZone with the help of OP-TEE. These secure applications make use of the secure world execution for sensitive tasks.

3.6 Security Properties

The secure boot process makes sure that TrustZone works as intended which should give confidence in the belief that secure execution of secure applications is guaranteed.

Chapter 4

Experiments

These experiments are based on proofs of concept.

4.1 Secure Boot

The secure boot is configured using OP-TEE and the interaction with OP-TEE will be tested.

4.2 Secure Application

The secure application will be a proof of concept of an application handling sensitive data.

Chapter 5

Conclusion

To achieve secure execution on the PinePhone some requirements need to be met. One of these requirements is that a chain of trust is achieved which is done using secure boot in this case.

5.1 Contributions

A detailed process of how to make secure boot happen on a PinePhone using OP-TEE. Besides integrating OP-TEE with the linux operating system of the PinePhone also showing how a secure application can be run from within this setup.

5.2 Limitations and Challenges

To be discovered.

5.3 Future Work

The secure application used in this thesis is only a proof of concept not really exploring very interesting features, a more realistic or challenging example can be created to discover weak points or further improvements in the system. With secure boot dealt with and ARM improving hardware support for virtualization it could be interesting to research virtualization on open platforms like the PinePhone.