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.