Chapter 1

Introduction

Smartphones

Everyone is assumed to have a smartphone of their own because it has become an essential gadget for our day to day lives.

Everywhere these smartphones can be spotted, people use them at home, on the bus or even at work.

Personal Computers seem less and less important to some people because all their needs can be fullfilled with a smartphone.

Sensitive data

Making connections that is what these smartphone devices are good at but it is important to keep in mind that there are certain security implications with every connection that is made.

Personal data is what drives the interactions with the smartphone. People use them to do online banking, send mails or even consult health related reports.

Related to IoT

Hardware similarities between smartphones and IoT devices are more prominent than one might expect. This is due to the fact that smartphones actually stem from IoT devices and not from personal computers.

Security features for IoT devices is a hot research topic, this is because not many solutions or standards that are present today are found to be adequate in terms of protection against the existing threats.

1.1 Problem statement

IoT security

Performance is the main focus when IoT devices are designed, they only have a small number of tasks but these need to be executed as fast or as energy efficient as possible.

Dynamic and distributed groups of devices form an IoT network, this implies that the security of this network is as strong as the weakest link in the chain (which can be very weak in the IoT environment).

Progressive functionality

Banking, e-Health and mails are applications most people trust their smartphone with, even though personal computers weren't even trusted with these kinds of functionality a few decades ago.

Missmatch

Progressive functionality is what smartphones have been bringing for their users and is what makes that the industry keeps growing every year.

Lagging or lacking security is the downside of this push for better functionality because it is very hard to make certain functionality secure but companies want to be the first to bring their products to the market.

1.2 Contributions

Reproduction of existing work is the first goal of this thesis, the solution of the paper is replicated as closely as possible (no source code available). The experiments in the paper are redone to be able to make a comparison between the original and the implementation discussed here.

Open source code is very important in the field of computer science because it allows other researchers to reproduce the experiments and review the work that has been done in a detailed manner.

Extra experiment measurements are executed to expand on their work and give a more complete picture of the solution.

Comparison with similar solutions is of course also important to evaluate whether this way of trying to solve the problem is in the right direction or whether different solutions have achieved more promising results.

1.3 Outline

In the next chapter more background information about among other things Remote Attestation and ARM TrustZone will be given. In the third chapter the methods to solve the problem will be explained. In chapter four the implementation of the attestation program are elaborated upon. In the fifth chapter the goal and outcome of the experiments will be made clear. The sixth chapter will conclude this thesis informing the reader about related work and future improvements. The final chapter will discuss the completed work.