Chapter 1

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.

1.1 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.

1.2 Limitations and Challenges

To be discovered.

1.3 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.