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.

An open source implementation of attestation on the PinePhone which allows the Secure World to attest the Normal World and increase the security guarantees thereof.

1.2 Future Improvements

To allow the user to attest their device it is important that Trusted I/O is used to inform the user about the outcome of the attestation process.

The attestation application can be seen as one module that can be accompanied with a variety of different modules to increase the amount of checks that can be executed to check more possible attacks/ vulnerabilities.