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 Related work

- Secure boot, Trusted boot and remote attestation for ARM TrustZone-based IoT Nodes
- DAA-TZ: An Efficient DAA Scheme for Mobile Devices Using ARM TrustZone
- SecTEE: A Software-based Approach to Secure Enclave Architecture Using TEE
- TZ-MRAS: A Remote Attestation Scheme for the Mobile Terminal Based on ARM TrustZone
- TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone

1.2 Comparison of Approaches

- Effectiveness
  - Reached goal
  - Defends most variety of attacks
  - Stronges security guarantees
- Assumptions
  - Least assumptions
  - Most realistic

1.3 Future Improvements

- Best approach
  - Overview
  - Reasoning
- Weaknesses
- Possible improvements
  - inspiration from Lightweight and Flexible Trust Assessment Modules for the Internet of Things
- Different solutions

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.