Chapter 1

Conclusion

1.1 Related work

Secure boot, Trusted boot and remote attestation for ARM TrustZone-based IoT Nodes is the paper on which the implementation and experiments are based.

DAA-TZ: An Efficient DAA Scheme for Mobile Devices Using ARM TrustZone implements Direct Anonymous Attestation on a mobile ARM TrustZone device.

SecTEE: A Software-based Approach to Secure Enclave Architecture Using TEE implements enclaves on a CPU with ARM TrustZone technology.

TZ-MRAS: A Remote Attestation Scheme for the Mobile Terminal Based on ARM TrustZone uses ARM TrustZone to protect the attestation service on the mobile device from being tampered with.

TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone utilizes the functionality of the secure world to shield applications from untrusted OSes.

1.2 Comparison of Approaches

Effectiveness

The goal of these papers are all a little different but it is important to evaluate which ones actually realized their goal and how this compares to the goal set out by this thesis.

Most variety of attacks that the solution defends against is a clear measure on how effective the solution is in the field.

The strongest security guarantees that were made and achieved also indicate how well the solution works.

Assumptions

The least assumptions that were made by the authors of the paper the more widely applicable the solution is because there is enormous hetergeneity among devices and assumptions put restrictions on the devices for which the paper is usefull.

The most realistic assumptions are of course also important to look at, if the assumptions are not realistic they are not practical to adhere to and the solution will be worthless if it can't be applied to the real world.

1.3 Future Improvements

Weaknesses

Rich OS dependency is very undesirable, it is thus important to look at different solutions that achieve similar outcomes to avoid this aspect of the current solution.

Uncomplete attestation introduces a fake sense of security because not all possible attacks are checked, for instance modified data structures that influence the control flow of a program. (inspiration from Lightweight and Flexible Trust Assessment Modules for the Internet of Things)

Additional features

- Based on the related work papers some additional features could be stated or solutions could be combined to achieve protection against a wider variety of attacks.