Chapter 1

Experiments

1.1 Performance

Reproduction

Trusted boot is based on the attestation of the normal world before giving it control. In the paper they talk about 107 MB of filesystem image that is being measured so this could be a valuable starting point to compare their performance with the performance achieved in this thesis.

Overhead is measured in the paper by executing system services from the linux kernel and running this experiment with and without the attestation.

Additional

Attestation time should be measured for a program with a certain size to be able to evaluate how often this attestation should be executed to have a balance between performance overhead and security assurance.

1.2 Performance Evaluation

Comparison between the performance achieved in the paper and the performance measured in this thesis is important to be able to interpret the results correctly.

Balance between performance overhead and security assurance depends on the usecase but in the context of the smartphone some statements could be made.

1.3 Security Properties

Integrity of the measurement execution is of utmost importance when it comes to attestation, in remote attestation this is achieved because of a hardened server but here the trusted execution environment needs to take care of this.

Secure storage of results is also important, first of all to make sure the reference values are not tampered with and second of all to correctly react to results that indicate a violation.

1.4 Security Evaluation

Security guarantees that can be made are the integrity of the measurement execution and the security of the results that are being stored. These are achieved due to secure boot enabling the trusted execution environment but are key assumptions in the field of remote attestation.

Shortcomings in terms of security are the OS/firmware attacks because the solution still relies on the rich OS rather heavily.

Extensions in terms of additional aspects of the system that can be attested are necessary to protect against software attacks.