Chapter 1

Method

1.1 Detailed Problem

Context

Sensitive data is often stored on smartphone devices or being used and transmitted.

Mobile computing is the main usage scenario when talking about smartphones but this means that the signals it sends can be picked up by lots of people that are nearby.

Performance driven , that is still the slogan lots of designers or implementers for smartphones have in mind.

Security is needed in regards of the functionality these devices provide, yet it's nowhere near what personal computers can provide.

Solution

Hardware security features could be the solutions or at least part of the solution, these features make sure that the attack surface of the smartphone becomes very narrow and well defined.

Correct implementation is of course still necessary, this is why research in this area is of utmost importance and experience needs to be shared to educate engineers in how to use these frameworks.

1.2 System Model

Open platform

Multiple software providers with no mutual trust will want to be certain about their software running without it being interfered with by software of other providers.

The platform owner is the user themselves, with phones from large companies the company is still the actual owner because only software with a correct signature can be installed on the device.

Secure software execution

Software isolation should be used to ensure the software providers integrity of execution.

Secure data storage is necessary to make sure that data from one application cannot be read or modified by another one.

1.3 Attacker Model

Physical access brings along lots of risk because the adversary has a variety of possible attacks they could launch from this position.

OS/Firmware attacks have the risk of compromising all user level applications because the OS is the 'trusted' layer on which these user level applications rely.

Software attacks try to tamper with the control flow of certain program executions or get hold of sensitive data through malicious code.

1.4 Solution

Secure boot ensures that the device starts in a known secure state, to achieve this a Root of Trust is needed from which a Chain of Trust is constructed.

User attestation can be used to check the integrity of control flow, data structures etc. it should also be able to check authenticity of the code that is running.

Trusted Execution Environment will provide the desired characteristics of isolation,

- Secure boot
  - Root of Trust
  - Chain of Trust
  - Secure starting point
- User attestation
  - Integrity (control flow, data structures, ...)
  - Authenticity (code, ...)
- Trust
  - Execution
  - Data protection