Title: Trusted Mobile Platforms

Authors: B. Smeets, T. Johansson, N. Shahmehri, and A. Hunstad

Affiliations:
- Ericsson Research, Lund, Sweden, contact: ben.smeets@ericsson.com
- Dept. of Electrical and Information Technology, Lund University, Lund, Sweden
- Department of Comp and Info Sci, Linköping University, Linköping, Sweden

Abstract:

The MTM is the core for implementing the TCG Mobile Phone Working Group equivalent of the TPM. Ericsson participates in this working group. Within the framework we conducted a Master Thesis studies where we created a reference implementation of the MTM. Part of the results of this study were taken back to standardization and influenced Ericsson planning of potential MTM introduction.

Introduction

Technical solutions and devices that will operate in the internet will use rather standardized hardware, and a dominant portion of their cost will be related to software development and software licenses. Attacks on standard hardware is rather easy. Therefore companies must improve the protection of their software investments against unauthorized use or reverse engineering of their products. One important ingredient in the effort to achieve security is the need for trusted platforms. (Platform=s but also gadgets, and sensors)

Project Focus and Goals

1. Expand understanding of how to build hardware and software for trusted mobile devices as consumer products.
2. For software: determine industry needs with respect to security and tool capabilities with respect to needs
3. Influence affecting standards

Participation in standardization work

Implementation studies

Scientific studies and publications

Project Organisation and Partners

Five partners and two work packages. Ericsson is coordinator:

- Partners Workpackages
  - Ericsson WP1: Interplay of hardware and software for security functions that protect the platform. Implementation study of TCG MTM security functions and the use of ARM TrustZone
  - Lund University WP2: There is a need to enhance and assess the quality of software from a security perspective. Today there are a number of commercial tools that can be used to catch implementation errors; these are assumed to lead to improved software
  - Sony Ericsson
  - Linköping University FOI
  - Linköping University

Outcome of WP1

The work in WP1 has resulted in the following:

- Architecture studies how to realize authenticated boot solutions for trusted platforms. Summarized in a study report;
- MTM reference implementation study Master Thesis study;
- Study on MTM realization and ARM TrustZone: Ericsson study;
- The research was used contribute to guide the Ericsson standardization work in the Mobile Phone Working group the Trusted Computing Group organization and partly the work of OMTP on trusted execution environments.

Architecture studies

There are several ways to implement authenticated boot but all require the use of ROM or Firmware that can be verified at boot. The study shows that for high volume production current front-line ASIC technology gives a cost advantage to ROM code realizations at the risk of cost ROM code error fixes. Furthermore, ASIC technology used for high volume mobile devices, while focusing on lower-power realizations has poor capabilities for reprogrammable non-volatile storage. This complicates realization of, for example, MTMs for mobile devices.

MTM Implementation work

The MTM is the core for implementing the TCG Mobile Phone Working Group equivalent of the TPM. Ericsson participates in this working group. Within the framework we conducted a Master Thesis studies where we created a reference implementation of the MTM. Part of the results of this study were taken back to standardization and influenced Ericsson planning of potential MTM introduction.

TCG Standardization

Ericsson participates in the TCG Mobile Phone Working group and the creation of the MTM specification. In addition Ericsson was responsible for the use-case analysis document for MTM. Our own work has been very useful for generating insight in the potentials (and problems) of MTM.

Outcome of WP2:

2. Selected Mobile Phone Use Case Analysis v1.0, TCG, Mobile Phone Work Group, to appear.

Publications

Figure 2: Components and actors in the SHIELDS approach.