# Trusted Mobile Platforms

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

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
Totalförsvarets forskningsinstitut, Linköping, Sweden

## 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= servers 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

### HOW

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<br>Lund University<br>SonyEricsson | 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 |
| Linköping University<br>FOI<br>SonyEricsson | 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 |

## 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 code 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 focussing on lower-power realizations has poor capabilities for reprogrammable non-volatile storage. This complicates realization of, for example, MTMs for mobile devices.

Figure 1: Trusted Mobile Platform study has impacts on coming products.

### 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:

In this WP work was concentrated around two aspects: a) to be able to design viable security metrics and assessment methods, it is vital to identify the needs for security levels, b) to be able to choose appropriate tools to improve security, there is a distinct need to define and design what the appropriate security levels are. Furthermore, defining such levels and identifying requirements on software tools also requires appropriate security needs to be defined
The work in WP2 has resulted in the following:

- a structure of needs for security levels associated to the security status of systems;
- a preliminary set of security metrics focusing on the aspects of security levels, or scales, based on an interpretation of the structure of identified needs;
- identification of critical issues in current security tools that prevent them from meeting the needs of users; and
- a design of an architecture for a new generation of security tools that will mitigate the most critical issues in todays tools.
- an EU FP7 project SHIELDS

### The SHIELDS approach

We have proposed an alternate approach to security tools that could mitigate the issues we identified by developing formalisms for modeling security knowledge, and storing models in a shared repository, where they can be accessed by tools. This approach was developed into an EU FP7 project named SHIELDS. A simplified overview of the main SHIELDS components and actors is shown below.

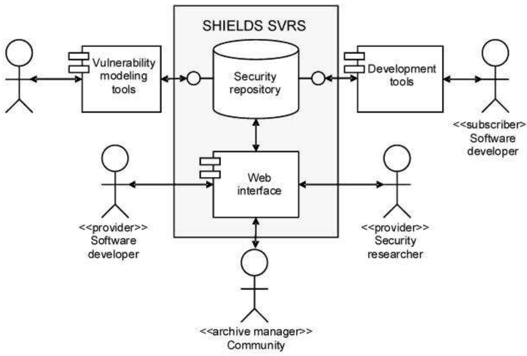
SHIELDS SVRS
Vulnerability modeling tools
Security repository
Development tools
Web interface
<<subscriber>> Software developer
<<provider>> Software developer
<<provider>> Security researcher
<<archive manager>> Community

Figure 2: Components and actors in the SHIELDS approach.

## Publications

1. Tools and metrics for assessing trusted mobile platforms: an evaluation of needs, N. Shahmehri, et. al., Linkping University, 2008.
2. Selected Mobile Phone Use Case Analysis v1.0, TCG, Mobile Phone Work Group, to appear.
3. Architecture Study for Trusted Platforms, B. Smeets, T. Johansson, M. Hell, Lund University, 2008.
4. Emanuelsson P., Nilsson U., 'A Comparative Study of Industrial Static Analysis Tools', Electronic notes in theoretical computer science, Vol 217(2008): s. 5 - 21 2008, also as extended Tech report