Newsletter

September 2013

HINT

Holistic Approaches for Integrity of ICT-Systems

The project aims to develop a solution to implement a common framework for a system's integrity checking based on Trusted Computing technologies. Further, the capabilities of the developed technologies will be demonstrated on real-life applications. It is planned to prepare the adoption of the proposed technologies by future Common Criteria evaluation schemes.

Main Project Information

Message from the Coordinator

The first year of the HINT project has almost passed. The global specification phase has been successfully completed. Due to the tight schedule the next months will be busy ones. Several deliverables and major milestones will arise until the second year of the HINT project, which is characterised by the phase of development for hardware integrity checking (Trojan, functional clone, counterfeiting detection). The preparations for the first HINT review meeting have already started. The HINT coordination team will be happy to support partners in the various endeavours in order to ensure clear communication, cooperation and the smooth running of the project.

Through this newsletter, it is our intention to start an information channel in order to provide news and discuss ongoing topics relevant to HINT for internal and external project partners.

Therefore we are proud to present within this first issue the successful completion of WP1 displaying first project results as well as to announce the presentation of HINT at two important events.

Upcoming Events:

Chip-to-Cloud Security Forum 2013
25th - 27th September 2013, Nice/France

ICT 2013 Create, Connect, Grow
November 2013, Vilnius/Lithuania

HINT Deliverables submitted

D6.1 - Project website and internal IT communication infrastructure

This deliverable describes the HINT website (www.hint-project.eu) and its functionality and the tools provided to facilitate cooperation and coordination.

D1.1 - Report on use case and architecture requirements

This document introduces the two application scenarios planned for the HINT project (Unclonable ID-cards and Professional Mobile Radio) and analyses use case requirements for these scenarios, with the focus on security analysis. Moreover, the main building technologies for the R&D work in HINT are described.

D1.2 - Report on specifications and overall architecture

Two architectures that shall constitute the backbone of the HINT technology are presented: one based on PUFs and the second one based on side-channel analysis. Further, a first idea of how it is intended to demonstrate those architectures through dedicated prototypes are provided.

Key Data:

Start Date:	1 October 2012
End Date:	30 September 2015
Duration:	36 months
Project Reference:	317930
Project Costs:	€ 5.103.893
Project Funding:	€ 3.350.000

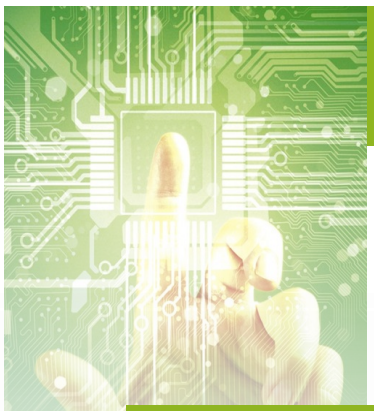
Consortium:	7 partners (4 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@hint-project.eu
Technical Leader:	Dr. Jacques Fournier jacques.fournier@cea.fr
Project Website:	www.hint-project.eu

The HINT project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-317930.

LinkedIn

FOLLOW US ON twitter

www.twitter.com/hint_project



Newsletter

September 2013

HINT

WP1 Objectives and Goals

The main objective of WP1 was to set up the basis for the development of PUF-based integrity and side-channel-based integrity components in the other RTD-work packages by defining targeted applications and requirements with respect to security and trust needs.

WP1: User Requirements and System Architecture - Results

Definition of targeted applications based on use case analysis

Two applications were identified to be targeted in HINT, one on Unclonable ID cards and one on Professional Mobile Radio (PMR). These applications were first outlined by the responsible industrial partners and consequently analyzed and defined in more detail.

Analysis of security and trust requirements for targeted applications

Security architectures linked to the two identified applications were reviewed, which lead to the identification of needed technological solutions (hardware integrity verification through 'hardware Trojan detection' and chip authentication through the use of PUFs) for enhancing trust.
The specific security requirements for Unclonable ID cards and PMR were analyzed following the methodology established for Common Criteria evaluations. For PMR, elements for defining a Protection Profile were specified. For Unclonable ID cards, the partners outlined adoptions to existing profiles for ID cards that would be necessary for cards deploying HW-based integrity anchors.

Definition of the global architecture of the HINT solution

The HINT global architecture was specified based on the two building blocks: PUF anchors for integrity checks of an embedded device (with the application example of an ID-card) and Side Channel Analysis (SCA) for detection of Hardware Trojans in embedded devices (with the application example PMR). An architecture integrating PUFs into ID cards as well as an architecture for SCA-based Hardware Trojan inclusion and detection on an FPGA board were specified.

Definition of the requirements for the technology (developed in WP2 and WP3)

From the analysis of the architecture of HW-based integrity anchors it was possible to derive the basic hardware architecture for a secure device including such an anchor and the requirements on software components for the post-processing of the response data. These initial specifications will be refined in WP2.
Regarding the SCA-based Hardware Trojan inclusion and detection, the HINT partners first outlined the basic structure of an SCA-based integrity/authenticity check mechanism and considered different possible variants for realizing the main components, e.g. a passive and an active approach for realizing an SCA-based detection component. The HINT partners outlined possible measurement equipment and a hardware platform for realizing the concept and derived architecture requirements. These results will be refined and realized in WP3.

Definition of the demonstrators (for WP4)

Based on the HINT global architecture definition, the overall architecture for the two HINT application prototypes was specified. The Unclonable ID-card application will show the whole lifetime management of a PUF-based ID-card. The PMR prototype evinces the modus vivendi of HT detection on an actual product.

Definition of the security targets based on the required security level to be achieved by HINT technologies (for WP5)

For the integration of HW-based integrity anchors into ID-cards, the required adaptation of existing Protection Profiles was discussed. For the application of the SCA-based approach to the PMR scenario, the main relevant parts of a Protection Profile were specified. The security analysis in WP5 will be based on these achievements.

HINT Project Coordination Team
Dr. Klaus-Michael Koch
Technikon Forschungs– und Planungsgesellschaft mbH
Burgplatz 3a, A-9500 Villach
Tel.: +43 4242 23355—71
Fax.: +43 4242 23355—77
E-Mail: coordination@hint-project.eu
Website: www.hint-project.eu

TECHNIKON

SEVENTH FRAMEWORK PROGRAMME