Newsletter

November 2014

HINT

In this issue:

Message from the Coordinator

The **HINT** project started in October 2012 and is set to run for 36 months. During the second project year, the focus was placed on the development of HW integrity checking and the development of demonstrators. Altogether 7 deliverables throughout the second project year have been produced and submitted. The progress achieved by all work packages within the second project year is essentially in line with the initial plan.

The 2nd HINT Project Period

During the second project year, all work packages except WP1 (already terminated in M08) successfully started and continued work. **WP2 Robust Energy-Optimized Nano Structures for Integrity-Anchors** is fully on track with respect to the description of work. Both deliverables scheduled for year two (D2.1 Report on novel cell and architecture concepts based on technology dependent research as well as D2.2 FPGA – prototype including advanced post-processing methods and techniques) have been submitted in time. The intensification of work towards the FPGA platform being used not only for post-processing, but also as an emulation of the error behaviour of the cell array is a dedicated added value beyond the original plan as described in the Description of Work. Both FPGA-parts together will allow for highly efficient evaluation of helper data algorithms and support research towards application development especially in the eID use case in WP4. In **WP3 Holistic Integrity Checking for Components in ICT-Systems**, the milestone MS3 (*hardware integrity checking scheme is built and functional*) has been reached. All partners have been working hand in hand (setting up common evaluation benches and test circuits, sharing measurements and analysis tools) to provide a scheme that successfully identifies the presence of Hardware Trojans in FPGA-based hardware cryptographic circuits using power & electro-magnetic measurements. Passive, active and on-chip approaches have been studied. The proposed scheme has been analyzed on the protocol level in order to make sure to have a secure system. All three deliverables have been delivered in time. In **WP4 Integration, Proto-typing, Validation,** we first theoretically study how HINT technologies can be used to enhance the chain of trust of TPMs. Three demonstrators have been defined and will be shown at the end of the project: one showing a 'holistic approach' for hardware integrity & authenticity checks; one showing integrity checking in PMRs; and one showing hardware authentication for the ID card use case. Those analyses and specifications are reported in the current draft version of D4.1. The goal of **WP5 Security Evaluation** is to evaluate the security technologies proposed and developed in the HINT project. Most of this work will be performed during the third project year. Partners have prepared work schedules by discussing and specifying the testing task that will be performed. **WP6 Project Management and** Dissemination was responsible for the effective organization of the project and covered the relevant management components. In addition, dissemination and exploitation activities have been undertaken. All foreseen objectives have been achieved and all foreseen deliverables as well as the Periodic Report have been submitted according to the planned schedule.

Key Data:

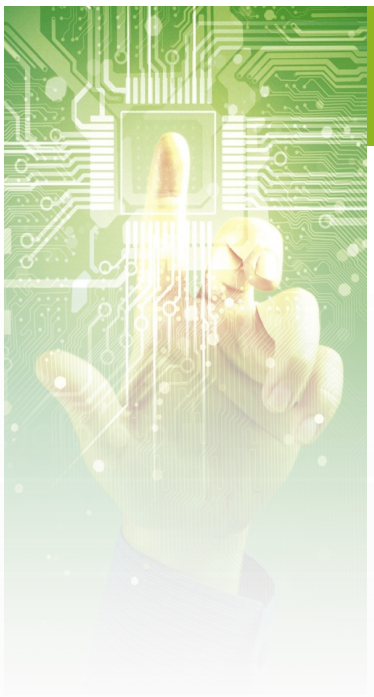
Start Date:	1 October 2012	*Consortium:*	7 partners (4 countries)
End Date:	30 September 2015	*Project Coordinator:*	Dr. Klaus-Michael Koch
Duration:	36 months		coordination@hint-project.eu
Project Reference:	317930	*Technical Leader:*	Dr. Jacques Fournier
Project Costs:	€ 5.103.893		jacques.fournier@cea.fr
Project Funding:	€ 3.350.000	*Project Website:*	http://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

November 2014

HINT

Participation in Conferences, Workshops and Events

- TRUEDEVICE Training School on Trustworthy Manufacturing and Utilization of Secure Devices, July 2014, Lisbon/PORTUGAL
- CHINACRYPT 2014, August 2014, Zhengzhou/CHINA - *Best Paper Award*
- Chip-to-Cloud Security Forum, September 2014, Marseille/FRANCE
- CHES 2014, September 2014, Busan/KOREA

Technical & General Assembly Meeting in Paderborn

From 9th - 10th September 2014 HINT partners met for a technical and General Assembly Meeting in Paderborn, hosted by partner Morpho. Main topics of this face-2-face meeting were the discussion of the technical status of each WP, preparation work for the second review meeting as well as management related issues.

Thomas Hübner (MOR), Julien Francq (CCS), Sandra Lattacher (TEC), Martin Deutschmann (TEC), Jacques Fournier (CEA), Barbara Nussbaumer (TEC), Holger Bock (IFAT), Carsten Rust (MOR), Benedikt Gierlichs (KUL)

Outlook for the final stage of the HINT project

Following the excellent progress obtained in the second year, the HINT project has all the premises for a successful third and last period by delivering on all goals and objectives as foreseen in the work plan. Further research will be done on post-processing of PUF-based data. Using the FPGA platform will allow for efficient testing of the Helper Data Algorithms (HDAs) as well as for preparative work towards the demonstrator planned in WP4. Based on the outputs of WP2 & WP3, the focus within WP4 will be placed on the 'holistic' demonstrator, the PMR demonstrator and the ID-card demonstrator. Based on the preparation work during the second project year, the third year will be affected by testing, checking and evaluating. The integrity checking schemes proposed in WP3 shall be stress-tested, in particular in terms of robustness with respect to changing environmental conditions & technology variations. Relevant tests to Common Critera-like approaches will be carried out. The feedback from these evaluations will be used to update the corresponding technology, where relevant and necessary. Good cooperation between consortium members and the EC will continue to be fostered. As the last period approaches the consortium will also put more emphasis on the proper exploitation and standardization activities. Additional efforts will be put on the dissemination of the technical results obtained during the second period as well as those that will be obtained during the third period.

Upcoming Public Deliverables & Milestones

D4.1 - Report on the integration of a hardware security anchor (M28)
D6.4 - Final dissemination, exploitation and standardisation report (M36)
D6.7 - Third annual report according to EC regulations of the model contract + final project report (M36)

MS4 - Delivery of reports of the prototype (M30)
MS5 - End of Security Evaluation Tasks (M35)
MS6 - Project Completion (M36)

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