Newsletter

January 2014

HINT

In this issue:

Holistic Approaches for Integrity of ICT-Systems

Mission of HINT is to study a set of solutions to implement a framework for a system's authenticity and integrity checking. 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 project period of the HINT project has already passed. Four deliverables have been submitted and several milestones have been reached. The first HINT Review Meeting took place on the 13th of November 2013 in Leuven, Belgium. Now we take all the feedback of this quite successful meeting and use the strong basis built in the first year, to continue with the second HINT phase. Hardware integrity anchor, Hardware Trojan detection, security evaluation, unclonable ID-Card and PMR use case are only a few key words that will accompany us during the second project year.

We are looking forward to a successful next HINT project period and would like to take the opportunity to thank all partners for the great collaboration and their valuable work performed so far.

Results of the first project period - Public Deliverables

D1.1 - Report on use case and architecture requirements

D1.2 - Report on specifications and overall architecture

D6.1 - Project website and internal IT communication infrastructure

D6.2 - Initial Report of project dissemination, exploitation and standardisation

You are interested in the content of these public deliverables?
Have a look at the HINT project homepage: http://hint-project.eu/index.php/publications

Results of the first project period - Milestones

The following main milestones for the first HINT project year were pursued and successfully reached:

- Project start and kick-off, fulfilment of all legal requirements
- Availability of dissemination environment and communication infrastructure
- End of the Global Specification Phase from both, the development point of view and the security evaluation point of view.

Key Data:

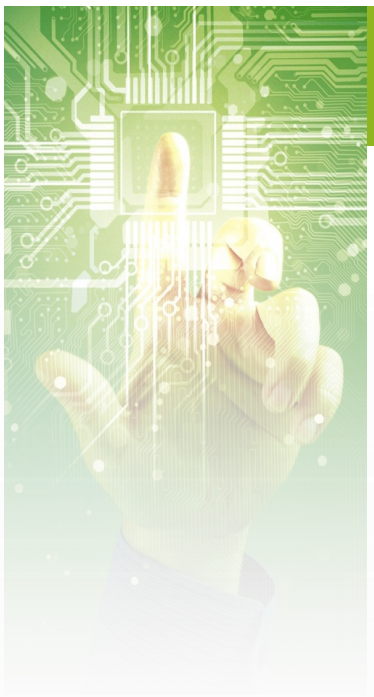
Start Date:	1 October 2012	*Consortium:*	7 partners (4 countries)
End Date:	30 September 2015	*Project Coordinator:*	Dr. Klaus-Michael Koch
Duration:	36 months		coordination@hint-project.eu
Project Reference:	317930	*Technical Leader:*	Dr. Jacques Fournier
Project Costs:	€ 5.103.893		jacques.fournier@cea.fr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

January 2014

Scientific Publications in Project Period 1

Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation. J. Delvaux, I. Verbauwhede, in *CT-RSA*, Springer, 2014

Key-recovery Attacks on Various RO PUF Constructions via Helper Data Manipulation. J. Delvaux, I. Verbauwhede, in *DATE*, 2014

Fault Injection Modeling Attacks on 65nm Arbiter and RO Sum PUFs via Environmental Changes. J. Delvaux, I. Verbauwhede, in *IEEE Transactions on circuits and systems*, 2014

Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise. J. Delvaux, I. Verbauwhede, In *6th IEEE International Symposium on Hardware-Oriented Security and Trust - HOST 2013*, IEEE, 2013

Participation in Conferences and Workshops

The HINT project management team has kicked off the second period with the presence at the **ICT 2013 - Create, Connect, Grow**, in Vilnius/LITHUANIA.

A complete list of all events, where the HINT project has been present until now can be found on our HINT project homepage: http://hint-project.eu/index.php/news

Outlook for the second HINT Project Year

We have made good progress during our first year of the HINT project, resulting in the achievement of all planned objectives. This provides a strong basis for the second period in order to accomplish all set goals and objectives.
The second year will focus on the implementation of cell arrays and optimized post processing of novel hardware integrity anchors. In parallel further novel attacks, but also countermeasures to protect against such attacks will be investigated. In addition, we will continue working on the detection of Hardware Trojans. Measurements will be used for refining template-based analysis of information extraction and integrity verification schemes. These will be complemented with the definition and implementation of robust, secure protocols to prevent impersonation attacks. The described development will then be integrated in the respective use cases namely PMR and Unclonable ID-card. In a further step we will pay special attention to the evaluation of the proposed security primitives and technologies.

The second Periodic Report will contain a description of our work during the second Project Period which will result in the following deliverables:

D2.1 - Report on novel cell and architecture concepts based on technology dependent research
D2.2 - FPGA-prototype including advanced post-processing methods and techniques
D3.1 - Report on Protocol choice and implementation
D3.2 - Report on detection methodology and performances
D3.3 - Prototype of the hardware integrity checking primitives
D4.1 - Report on the integration of a hardware security anchor
D6.3 - Report on dissemination, exploitation and standardization

Upcoming Events

CT-RSA 2014
24.-28. February, 2014, San Francisco/California
(Presentation of the publication "*Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation.*")

DATE 2014
24.-28. March, 2014, Dresden/Germany
(Presentation of the publication "*Key-recovery Attacks on Various RO PUF Constructions via Helper Data Manipulation.*")

Since we have a Technical Meeting in Dresden in the beginning of this week, **all HINT partners will be present at DATE!**

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