Newsletter

August 2015

HINT

Message from the Coordinator

The **HINT** project started in October 2012 and is set to run for 36 months. During the third project year, the focus was placed on the finalization of Graphical User Interface, HW Anchor integration, and the implementation of the non-clonable ID-card prototype. The third period is rich in publications, participation in conferences, workshops and other events. The project is in the final stage, all work is provided and submitted according to the plan. Moreover, HINT has been identified as a success story in ICT Security and Trust by the FP7 project "SecCOrd".

List of Publications

- **Electromagnetic Circuit Fingerprints for Hardware Trojan Detection**
  J.Balasch, B.Gierlichs, I.Verbauwhede, 2015, IEEE.
- **A Survey on Lightweight Entity Authentication with Strong PUFs**
  J. Delvaux, R. Peeters, D. Gu, I. Verbauwhede , 2015, ACM.
- **Resilient Hardware Trojans Detection based on Path Delay Measurements**
  Ingrid Exurville, Zussa Loïc, Jean-Baptiste Rigaud and Bruno Robisson , 2015, IEEE.

The 3rd HINT Project Period

During the third project year, all work packages except WP1 (already terminated in M08) and WP3 (terminated in M24) successfully continued work. **WP2 Robust Energy-Optimized Nano Structures for Integrity-Anchors** is in the final stage with respect to the description of work. On the system level there were some implementations on the soft- and hardware: CRC-16 has been implemented and the Graphical User Interface (GUI) has been finalized. Long-term evaluation of the GRACE code has started. From the testing and validation task lots of research activities were undertaken, which lead to the implementation of a Helper Data manipulation detection tool. In **WP4 Integration, Proto-typing, Validation,** partners were closely working on D4.1 "Report on the integration of a hardware security anchor" and submitted the final version in M28. The FPGA board for embedding the PUF model was ordered and the set-up was fine-tuned. In the frame of the PMR use case, two HTs have been validated and the use case is ready for demonstration. Also, 7 more HTs have been implemented to assess the efficiency of our HT detection methods on a broader spectrum of HTs. Final implementation of non-clonable ID-card prototype and it evaluation is expected. The goal of **WP5 Security Evaluation** is to evaluate the security technologies proposed and developed in the HINT project. During the third period partners have contributed to the robustness analysis of active HT detection, and future work analysis based on the results. Within the last period technologies were designed and implemented in order to ensure a stable scheme analysis and a new FPGA chip. A couple of papers have been submitted for the follow conferences: HOST conference, DSD conference; CARDIS; and EMC 2015. **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
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:	http://www.hint-project.eu/

Linked in

FOLLOW US ON twitter
www.twitter.com/hint_project

Newsletter

August 2015

Participation in Conferences, Workshops and Events

- Success Stories of FP7 ICT Trust & Security Projects - HINT identified as "Success Story"
- International Solid-State Circuits Conference (ISSCC), February 2015, San Francisco\CALIFORNIA
- ENISA Workshop: Threat Analysis in Research, February 2015, Brussels\BELGUM
- TRUDEVICE Workshop , March 2015, Grenoble\FRANCE
- DATE 2015 Conference, March 2015, Grenoble\FRANCE
- CSP Innovation Forum, April 2015, Brussels\BELGUM
- PHISIC 2015, May 2015, Gardanne\FRANCE
- Summer School on real-world crypto and privacy, June/July 2015, Sibenik\CROATIA
- CryptArchi 2015 Conference, June/July, Leuven\BELGUM
- International Course on Cyber Security and Cryptography, July 2015, Leuven\BELGUM
- CECC 2015 - Central European Conference on Cryptology, July 2015, Klagenfurt\AUSTRIA

Technical & Liaison Meetings

VIENNA

From 23rd - 24th February 2015 HINT partners met for a technical face-to-face meeting in Vienna/AUSTRIA. During the meeting the technical status of active WPs as well as upcoming deliverables were discussed. Also, all project objectives (HW Trojan detection, functional clone detection, counterfeiting detection, electromagnetic analysis, PUF, post-processing techniques, trusted computing approach) were reviewed and current and future standardization activities were discussed and planned.

GRAZ

From 22nd - 23rh April 2015 partner IFAT hosted both the liaison meeting with the MATTHEW FP7 project and the technical HINT meeting. The main objective of the liaison meeting was to introduce the projects to each other and to exchange information and results. A common publication was been planned and is currently being worked on. The liaison meeting was followed by a technical meeting where the technical status of WP2, WP4 and WP5 were presented and discussed. The main focus was put on the results of new test chip, the PMR and ID card demo, and HT detection techniques. Moreover, upcoming deliverables were addressed and work towards their finalization was planned. Also standardization activities as well as future dissemination activities, upcoming meetings and the review meeting were discussed. Particular attention was paid to the ISO standardization on PUFs.

VILLACH

From 23rd - 24th July 2015 HINT partners met for a technical face-to-face meeting in Villach\AUSTRIA. This meeting was focused on the achievements and final tasks in active WPs, such as evaluation results of new PUF data, attacks on post processing, and security evaluation. Progress in the holistic PMR and ID Card demo was also part of the discussions. Furthermore, upcoming deliverables have been planned and news on standardization activities have been reported. Finally, the meeting was a good platform to discuss organizational issues with regards to the final review meeting.

Upcoming final review meeting

The final review meeting is planned to take place on the 29th of October 2015 hosted by partner CEA-LETI in Gardanne/FRANCE. This meeting will include a technical and scientific overview of the past project period and summarize the work and results of the HINT FP7 project. Furthermore, a report on the use of resources will be presented.

Milestone achieved

MS4 End of security evaluation task was accomplished in M32.

Upcoming Public Deliverables & Milestones

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)

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