European FP7 project HINT No. 317930: Final press release

Fighting for the integrity of electronic hardware – new measures against Hardware Trojans and counterfeiting

The security of modern ICT (Information and Communication Technologies) systems relies on the authenticity and integrity of their software and hardware components. New security challenges are emerging with recent trends of sophisticated attacks, like counterfeiting of hardware components and the threat of Hardware Trojans (HT) or hidden functions in Integrated Circuits (IC).

The HINT project, led by Dr. Klaus-Michael Koch from Technikon in Austria, adopted and implemented for practical industrial issues three Hardware Trojan detection methods (side channel based, timing based and on-chip sensor based). It also developed new PUF (Physically Unclonable Function) structures and new post processing schemes for PUFs for IC authenticity and security. These new technologies highly support the assurance of genuineness and integrity of future electronic devices. The consortium has also actively helped in launching a new ISO standard on "PUF Security Assessment" (ISO SC 27) as a vital first step for the uptake of the PUF technologies by the industry.

The project technical leader, Dr. Jacques Fournier from CEA in France, points out the progress made with two industry-oriented prototypes: an ID-card with inherent hardware cloning protection and a Hardware Trojans resistant professional mobile radio (PMR) demonstrator. In order to detect malicious structural modifications in an IC (which correspond to HTs) or counterfeits, concepts have been patented and developed using either off-chip (external electromagnetic) sensors or on-chip (using Ring Oscillators) sensors. Secure protocols, using the PUF technology in-turn, have been specified and demonstrated to carry out HT detection in the field. Those concepts have been successfully tested on Field Programmable Gate Arrays (which allowed rapid prototyping of hardware designs) laying solid grounds for further validation on Application Specific Integrated Circuits in sequel projects. Such concepts shall also fabless design houses to test the integrity of their ICs when the latter are fabricated by third party fabs.

The HINT technologies shall primarily benefit the European IC industry in a B2B2C context. For example, the IC manufacturers integrating the new PUF technologies developed and demonstrated in the project shall offer enhanced security and anti-cloning features to the solutions' providers integrating those chips: for the final customer this means reduced fraud and counterfeiting. A second example, relative to HT detection, is the ability for European security solution providers to test the integrity of the ICs they embed into their products, providing the end customer not only with enhanced security but also higher reliability and trust.

The HINT consortium brought together seven project partners from 4 different countries. They formed a complete chain stretching from basic research and service design, via applied research, up to end-user oriented service providers. The HINT-partners are:

- TECHNIKON Forschungsgesellschaft mbH, Austria
- Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA-LETI), France
- Infineon Technologies Austria AG, Austria
- Cassidian Cybersecurity SAS, France
- Association pour la Recherche et le Développement des Méthodes et Processus Industriels (ARMINES), France
- Katholieke Universiteit Leuven, Belgium
- Morpho Cards GmbH, Germany

The HINT project was successfully completed with the final review meeting on 29th of October 2015 in Gardanne/France.

For more information visit http://www.hint-project.eu

Contact information:

Project Coordinator
Dr.-Ing. Klaus-Michael Koch
TECHNIKON Forschungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Email: coordination@hint-project.eu

Technical Lead
Dr. Jacques Fournier
Commissariat à l'Energie Atomique et
aux Energies Alternatives (CEA-LETI)
17 Rue des Martyrs
38054 Grenoble Cedex 9
France

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 317930.

March 2016