Announcement Letter

Holistic Approaches for INtegrity of ICT-Systems

The security of modern ICT (Information and Communication Technologies) systems relies on the authenticity and integrity of the software and hardware components used to implement them. Such systems may be applied in homeland security markets (avionics, critical infrastructures, SCADA systems, cyber security, RFIDs…), embedded systems (health, transport, defence, consumer electronics, telecommunication…), smart cards (bank cards, ID cards, Pay TV cards, transportation, (U)SIM…) and personal identification technologies (passports or travel documents…).

While software integrity has been intensively researched over the past years, hardware integrity had been mainly taken for granted. However, attacks on such hardware components keep improving. Physical attacks, giving access to internal information, side channel attacks, using passive observations of execution time, power consumption or electro-magnetic (EM) radiations, or fault injection attacks using power glitches, light, laser and EM perturbations are 'proven' ways of retrieving secret data out of those devices. Today's security circuits offer protections against these attacks, but an absolute protection is not possible given that other means of attacks exist raising new security challenges:

- counterfeiting of hardware components (functional clones, over-production, repackaging…) is dramatically increasing, with approx. 5-20% of counterfeited components on the market. This not only represents a severe security risk for the systems embedding such counterfeited components but might have serious economic impacts with job losses and environmental concerns.
- the threat of "Trojans" or hidden functions in Integrated Circuits (IC) is moving from theoretical to real thus bringing in alarming security concerns (de-activation of critical parts of the circuit, leaking sensitive information…) whenever embedding a given IC coming from a third party provider or even from one's own delocalised production facilities.

The HINT project addresses these new challenges by proposing the development of novel technologies to provide a means of approval that a system is genuine and unmodified. Those technologies shall help to ensure the authenticity and integrity of the hardware components used in a given system.

- The first aspect of authenticity shall be addressed by investigating about and proposing novel, secure and robust ways of extracting fingerprints-like characteristics (also referred to as PUFs for Physically Unclonable Functions)) of a dedicated IC. Unresolved issues like improving the error rate of PUFs, improving the post treatment done on such measurements, their resistance to ageing, their scalability with respect to the latest technology trends and their resistance to learning-based attacks shall be addressed.

- A second aspect of integrity shall be investigated by looking at "on-board" methods of checking the integrity of a given IC through its Electromagnetic (EM) emanations. These methods of 'Trojans' detection shall be based on active methods where characteristic signatures are extracted from given test patterns.

Secure protocols for verifying those integrity features shall be proposed as well as their integration into established schemes like Trusted Computing (TC). Methods for testing those authenticity and integrity verification technologies shall be investigated with the view of proposing corresponding security testing criteria for established and widely adopted schemes like Common Criteria. The latter aspect shall reinforce the practical and commercial viability of the solutions proposed by HINT. In order to demonstrate the relevance and efficiency of the proposed technologies, two near-real-life demonstrations shall be carried, one based on a Professional Mobile Radios (PMR) platform and a second one on electronic ID cards.

The HINT consortium is well-positioned to achieve its objectives by bringing together leading European industrial companies, leading European research companies, an European research oriented SME as well as a high esteemed university from Europe. These seven project partners from 4 different countries form 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 has started on 01 October 2012 and will last 36 months. It has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 317930.

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

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

Email coordination@hint-project.eu