Holistic Approaches for Integrity of ICT-Systems.

HINT

Project number: **317930**
Project website: **www.hint-project.eu**
Project start: **October 1, 2012**
Project duration: **3 years**
Total costs: **EUR 5.103.893,-**
EC contribution: **EUR 3.350.000,-**

The project is co-financed by the European Commission (under the Seventh Framework Programme).

Contact

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55 – 0
Fax: +43 4242 233 55 – 77
E-mail: coordination@hint-project.eu
Web: www.hint-project.eu

Technical Leader
Dr. Jacques Fournier
Commissariat à l'Energie Atomique et aux Energies Alternatives
Rue Leblanc 25
75015 Paris 15
France
Tel.: +33 4 42 61 67 34
Fax: +33 4 42 61 65 92
E-mail: jacques.fournier@cea.fr

Consortium

The HINT project brings together leading European industrial companies, leading European research companies, an European research oriented SME as well as a high esteemed university from Europe. The seven project partners from 4 different countries (Austria, France, Belgium, Germany) form a complete chain stretching from basic research and service design, via applied research, up to end-user oriented service providers. In addition to these partners a third party linked to ARMINES, namely, Ecole Nationale Supérieure des Mines de St Etienne' supports the consortium.

We have a small but well balanced and very focused consortium, which is strongly oriented in obtaining the results expected from the project. Overall opinion is that this mixture of multinationals, SMEs and world-class research organisations constitutes the optimal consortium to achieve the given innovation objectives.

1 **Technikon Forschungs- und Planungsgesellschaft mbH (Austria, Villach)**

2 **Commissariat à l'Energie Atomique et aux Energies Alternatives (France, Paris)**

3 **Infineon Technology Austria AG (Austria, Villach)**

4 **Cassidian Cybersecurity SAS (France, Elancourt)**

5 **Association pour la Recherche et le Développement des Méthodes et Processus Industriels (France, Paris)**

6 **KU Leuven – University of Leuven (Belgium, Leuven)**

7 **Morpho Cards GmbH (Germany, Flintbek)**

Mission of HINT:

- Is to develop a solution to implement a common framework for a system's integrity checking based on Trusted Computing technologies.
- Is to demonstrate the capabilities of the developed technologies on real-life applications.
- Is to prepare the adoption of the proposed technologies by future Common Criteria evaluation schemes.

Motivation:

Modern ICT (Information and Communication Technologies) systems involve complex schemes like 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 identity technologies (passports or travel documents…). The security of such systems, which relies on the authenticity and integrity of the hardware components used to implement them, is continuously challenged by improving attacks. Hence new methods for testing the authenticity & integrity of those hardware devices must be sought.
Physical attacks, based on the passive or active spying of those devices, are 'proven' ways of retrieving secret data out of them. Today's security circuits offer protections against these attacks, but an absolute protection is not possible in practice and the need of extra barriers arises, especially with the growing concerns about the fact that:

- counterfeiting of hardware components is dramatically increasing, with approximately 5-20% of counterfeited components on the market.
- the threat of "Trojans" or hidden functions in Integrated Circuits (IC) is moving from theory to practice.

The HINT project addresses these new challenges by proposing the development of novel technologies to verify that a system is a genuine and non-modified one. Those technologies shall help to support assurance of authenticity and integrity of the hardware components used in a given system.

Objectives:

Secure architectures and platforms, where secure storage and computations are managed by hardware components, have shown their efficiency for many applications, from user's identification and authentication (e-id, banking cards), to ensuring the security of more complex systems (HSM, SAM, TPM, root of trust). However, even if the security of such tamper proof (or tamper resistant) integrated circuits is better than any other solution, some weaknesses still exist.

The HINT project addresses these problems and intends to develop technologies enabling to:

- perform "on board" integrated checking of the global integrity of a system (hardware and embedded software)
- check the "genuineness" of the secure integrated circuits (detection of functional clones or of counterfeited circuits), using PUF-based authentication schemes and
- detect the presence of Hardware Trojans.

To achieve those goals, the HINT project will focus on some specific technologies like:

- the PUF technology, enabling to authenticate a given hardware component using a physical, intrinsic and unique signature of the device.
- SCA (Side Channel Analysis) based analysis to monitor the behaviour of hardware components and to detect changes from their original specifications and implementations.

Technical Approach:

The work plan for the HINT project is structured into three phases and six work packages.

WP1 User Requiremens and System Architecture
The requirement phase (WP1) addresses specifications and use cases. They will be refined based on market requirements and application areas provided by end users and industrial partners. Metrics like the complexity, the cost and the security of the sought solutions shall be particularly addressed.
Future Common Criteria evaluations will be prepared through the definition of a specific Protection Profile or Security Target.

WP2 Robust Energy-Optimized Nano Structures for Integrity-Anchors
WP3 Holistic Integrity Checking for Components in ICT Systems
The research phase (WP2 & WP3) will cover the development of technologies for the objectives previously defined. In HINT, two technologies shall be studied in particular:

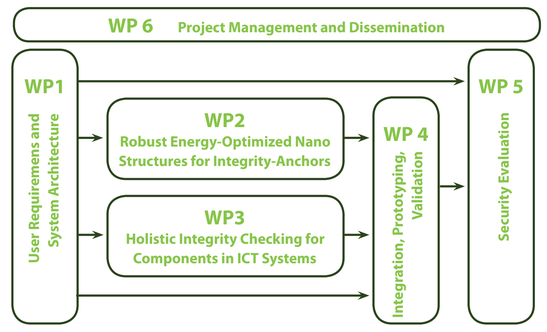
- PUF technology for hardware integrity assessment, and
- SCA for the detection of Hardware Trojans, functional clones and counterfeited parts.

The integration phase deals with the integration of the proposed technologies into a common framework covering all aspects of integrity checking of embedded systems (hardware and software). The objective is to demonstrate the capabilities of the developed technologies on real-life application use cases as provided by the end-users.

WP 4 Integration, Prototyping, Validation
In work package 4 demonstrators will be built and evaluated in terms of functionality, performance and fulfilment of the requirements.

WP 5 Security Evaluation
In work package 5, specific attention will be paid to the development of attacks and testing methodologies for the new security features.

WP 6 Project Management and Dissemination
Finally, the work package 6 will cover the management of the project, the interface with the European Commission and the dissemination of the results of the project towards both academia and industry.



Project Results:

- **HINT** develops novel physical integrity checking technologies for hardware components based on Side Channel Analysis.
- **HINT** technology builds on physical integrity checking based on PUFs (Physically Unclonable Functions).
- **HINT** novel integrity components integrate seamlessly with software components in complex systems-on-chip and systems-on-board.
- **HINT** derives novel integrity testing methodologies that will be part of Common Criteria as well as other standardisation tracks.