Publishable Summary

Project number:	317930
Project acronym:	HINT
Project title:	Holistic Approaches for Integrity of ICT-Systems
Start date of the project:	01.10.2012
Duration:	36 months
Programme:	FP7/2007-2013

Date of the reference Annex I:	20.12.2012
Periodic report:	Publishable Summary (as part of D6.5 “First annual report according to EC regulations of the model contract”)
Period covered:	01.10.2012 – 30.09.2013
Work packages contributing:	All
Due date:	September 2013 – M12
Actual submission date:	11.12.2013 – V1.0

Project Coordinator:	Dr. Klaus-Michael Koch Technikon Forschungs- und Planungsgesellschaft mbH (TEC)
Tel:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-Mail:	coordination@hint-project.eu
Project website:	www.hint-project.eu

Chapter 1 Publishable Summary

Project name: **HINT**
Grant Agreement: **317930**
Project website: http://www.hint-project.eu
Contact: coordination@hint-project.eu

Start date: 1st October 2012
Duration: 36 months

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.*

The HINT Project:

The main project results targeted by the HINT project are as follows:

- HINT develops innovative physical integrity checking technologies for hardware components based on Side Channel Analysis.
- HINT technology builds on physical authenticity checking based on the use of 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 defined to fit into Common Criteria as well as other standardisation tracks.

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 (passport and 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 and that 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.

Objectives & Technical Approach:

Secure architectures and platforms, 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 by developing technologies enabling to:

- perform “on board” checking of the global integrity of a system.
- 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.

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

WP1 User Requirements and System Architecture
The requirement phase (WP1) addressed specifications and use cases. They were refined based on market requirements and application areas provided by industrial partners. A system architecture based on the two core technologies of PUF based hardware integrity anchors and SCA based integrity checks was defined. Two application prototypes were defined. Future Common Criteria like evaluations were prepared through an analysis of required adaptions of specific Protection Profiles or Security Targets.

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 are studied:

- PUF technology for hardware integrity & authenticity 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 and authenticity checking of embedded systems. The objective is to demonstrate the capabilities of the developed technologies on real-life application use cases as provided by the end-users.

WP4 Integration, Prototyping, Validation
In work package 4, demonstrators will be built and evaluated in terms of functionality, performance and fulfilment of the requirements.

WP5 Security Evaluation
In work package 5, specific attention will be paid to the development of attacks and testing methodologies for the new security features.

WP6 Project Management
Finally, the work package 6 covers 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. Standardisation & IP-related issues are also covered there.

Description of the work performed and results in the first project period

During the first project phase, corresponding to the first project year, the focus was placed on the analysis of requirements and specification of the system architecture. All work packages, expect WP4 and WP5 that has not started yet, initiated work and produced altogether 5 deliverables (including this first Periodic Report).

At the beginning, major effort was put into the successful launch of the project. The main goal was to establish a sound basis for a good and fruitful cooperation among the project partners towards the research objectives. This has been achieved by strong leadership and by optimizing the organisation and infrastructures. We managed to provide all the relevant management components like contractual, financial, legal, technical, administrative and ethical issues as well as catching upcoming obstacles well ahead of time. Furthermore, a public project website and the internal IT communication infrastructure were established.

The progress achieved by all work packages within the first project year is in line with the initial plan and can be summarized as follows.

WP1 (User Requirements and System Architecture) was completed on time within this first reporting period. The first major achievement of WP1 was to describe and analyze the two targeted applications of HINT in order to derive use case requirements: one on Unclonable ID cards and one on Professional Mobile Radio (PMR). For each of these applications, WP1 partners analyzed and specified security and trust requirements following the methodology established for Common Criteria like evaluations. Secondly, the global architecture for holistic integrity checking of ICT-Systems has been defined, based on the two core technologies of PUF based hardware authenitcity anchors and SCA based integrity checks. This architecture forms the basis for the research and development work on the two core approaches done in WP2 and WP3 respectively. Another achievement is the description of the application prototypes for demonstration and evaluation of the HINT solutions for WP4. We specified an Unclonable ID-card application that will show the whole lifetime management of a PUF-based ID-card. The other prototype on PMR evinces the *modus vivendi* of HT detection on an actual product. Finally, an initial security analysis was conducted, which prepares the work to be done in WP5. All results generated in WP1 were documented in the two deliverables of the work package: D1.1 on use case and architecture requirements and D1.2 on specifications and overall architecture.

During the first project year, in **WP2 (Robust Energy-Optimized Nano Structures for Integrity-Anchors)**, work has been performed on novel concepts for hardware integrity & authenticity anchors, based on research on technology dependencies in deep sub-micron CMOS flash technologies, as they are used for state-or-the-art security controller ICs. A deep understanding of artefacts in an actual industrial 65 nm technology has be achieved and knowledge gained out of this research could already be exploited to propose novel cell and architecture concepts for hardware integrity anchors. A specification for FPGA-based emulation of such novel concepts has been developed and implementation of such FPGA-based emulation has started. In parallel, work on attack concepts on PUFs has been performed and published.

During this first period, **WP3 (Holistic Integrity Checking for Components in ICT-Systems)** has been mainly focusing on the specification of the building blocks of the SCA-based integrity checking mechanism, the implementation of a test environment to allow all partners to perform their research work using the same tools and the same devices under test and the first measurements. The building blocks of the SCA-based detection scheme were defined: the device under test, the measurement tool, the information extraction tools, the integrity verification mechanisms, the active checking mechanism(s) and the protocol level implementations. A first implementation of the test environment was done on the SASEBO GII board and is being translated to the SAKURA G bought by each partner to have a common test bench. A reference Trojan-free AES and infected AES circuits have been implemented. First technical works were done on the tailoring of the measurement test bench, the first tests on template-based analyses, active checking based on the ‘excitation’ of a circuit through the clock and power consumption modeling for Trojan detection.

WP6 (Project Management and Dissemination) was responsible for the effective organisation of the project and covered all relevant management components as well as for the dissemination of project results. Some of the main achievements so far have been: the organization of meetings (e.g. Kick-Off and GA Meeting), the implementation of monthly EB

Telcos, monitoring of the work plan (Quarterly Management Reporting) and supporting partners in everyday issues. A robust IT infrastructure (website, SVN repository including web access, mailing lists including mailing list archives) has been established and regularly updated. Several dissemination activities to raise the awareness (press release, newsletter, poster, project flyer, poster presentations, etc.) of the HINT project have been performed, several scientific articles have been submitted and a presentation at HOST 2013 took place. Upcoming dissemination activities are regularly announced on https://www.hint-project.eu/index.php/news.

Expected final results and their potential impact and use

The HINT project aims to contribute to an essential building block needed for trustworthy ICT by providing a holistic, multi-level approach towards device integrity & authenticity. ICT systems with means for integrity assurance for their hardware components as well as for multi-component sub-systems will – together with means of confidentiality, authenticity and non repudiation – allow for a new quality of trustworthiness in ICT. Even more the assurance of system integrity will help to make sure that all other means for trustworthiness are in the correct and desired state whenever they are applied for execution of security- or trust-critical protocols, even in a hostile environment and in the presence of attackers.

HINT is targeting the increase of Trust in ICT systems, thus strengthening the development of one of Europe's main contributors to future welfare. Trusted IT is both a business area in which Europe has been leading for decades – e.g. in the smart card and security ICs area and in the Trusted Platform business – as well as an enabling technology for future development. Many ICT applications relevant for the already seen upcoming societal challenges, like for example individualized medical information systems or smart grid roll outs are still under pressure of retarded development due to lack of integrity of the involved ICT systems.

HINT has a very wide application area: Any application requiring the use of electronic devices is potentially concerned by integrity checking and specifically hardware integrity checking. Secure devices (improving the resistance of systems towards attacks), safety oriented devices (counterfeiting detection) or any device handling personal or valuable information (Trojan detection). Four markets have been identified by the HINT partners as first targets: the homeland security market, the embedded security market, the smart card market and the personal identity market.

The HINT Consortium

The HINT project brings together leading European industrial companies, leading European research companies, a 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.

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.

HINT project public website

The official HINT project website is available at: http://www.hint-project.eu

HINT Disclaimer

All public information will be marked with the following HINT project disclaimer: *"The HINT project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT- 317930."*