Publishable Summary

Project number:	238811
Project acronym:	**UNIQUE**
Project title:	Foundations for Forgery-Resistant Security Hardware
Start date of the project:	01.09.2009
Funding scheme:	33 months

Date of the reference Annex I:	September 23, 2011
Deliverable reference number: D6.1	**Publishable Summary** (as part of the 2nd Periodic report according to EC regulation of the model contract)
Period covered:	01.09.2010 – 31.05.2012 (M13-M33)
WPs contributing to the deliverable:	All
Due date:	31.05.2012 (M33)
Actual submission date:	2012-10-01 – Version 1.1

Responsible organisation:	Project Coordinator: Technikon Forschungs- und Planungsgesellschaft mbH (TEC)
Tel.:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-mail:	coordination@unique-security.eu
Project website:	www.unique-security.eu

2. Publishable summary

2.1 General Overview

Project Name: **UNIQUE** Start date: **Sept., 1st 2009**
Grant Agreement: **23881** Duration: **33 month**
Project Website: http://www.unique-security.eu

Contact: coordination@unique-project.eu

Mission of UNIQUE

“To enforce the security and assurance of hardware components against malicious attacks of unauthorized parties.”

The goal of the UNIQUE project was to tackle the problem of counterfeiting of and tampering with Integrated Circuits (ICs). Since ICs are at the core of modern and often critical electronics products and IT systems it is very important that their integrity can be guaranteed. Therefore an integrated approach to protect hardware systems against counterfeiting, cloning, reverse engineering, tampering, and insertion of malicious components were developed in UNIQUE. The technical focus with UNIQUE was on the development of new hardware based security functionality for hardware systems and components in general but in particular for those ICs and hardware components that provide cryptographic and security services (e.g. cryptographic co-processors, smartcards) within modern IT and communication systems. These new components can be used as security anchors in the devices they are embedded in. ICs equipped with these security anchors are referred to as “security hardware”. In order to address the IC counterfeiting and tampering problem comprehensively, the project succeed in investigating and developing a complete solution by covering all aspects starting from hardware-based crypto, security building block, security architectures, protocols and algorithms to system design and evaluation principles required to detect counterfeiting of or malicious components embedded in hardware.

To show the feasibility of the developed concepts a prototype was developed as an overall outcome.

2.2 Work performed and the final results

The UNIQUE project has ran for 33 month. During the first project phase corresponding to the first project year the main research issues were the identification of requirements and working on threat models and building blocks. In the second period the novel methodologies listed, described and designed and the approved structures were enhanced. Furthermore the test framework design, implementation, integration of the prototype and evaluation were achieved.

Accordingly to the time schedule of UNIQUE different deliverables were provided and milestones were reached. The development of UNIQUE was partitioned in six work packages, four technical (WP1 “Requirements, design and evaluation”, WP2 “Building blocks”, WP3 “Evaluation and validation”, WP4 “Prototype”) and two managerial (WP5 “Dissemination”, WP6 “Project management”). The work performed in the different work packages can briefly be summarized as follows:

The work plan of UNIQUE was structured according to the logical dependencies of the major tasks that have been defined for reaching the project’s goals. The project started with the examination of the main application scenarios relevant for achieving protection against counterfeiting and malicious tampering with hardware. This stage concluded with the definition of requirements to built tamper-proof and counterfeiting resistant hardware. Furthermore, the high-level security design, analysis and evaluation methodologies for the solutions developed within UNIQUE. Guided by the requirements of the application scenarios, security architecture was developed, defining abstract interfaces between hardware and software components of the system, which were developed in subsequent work packages. Therefore UNIQUE was partitioned in six work packages, four technical (WP1 “Requirements, design and evaluation”, WP2 “Building blocks”, WP3 “Evaluation and validation”, WP4 “Prototype) and two managerial (WP5 “Dissemination”, WP6 “Project management).

The Work Packages and their objectives are described shortly in the following:

WP1 Requirements, Design and Evaluation: developed solutions that combine hardware-based security features with modern provably secure protocols. Furthermore existing building blocks that can be used to achieve this goal were surveyed and analysed with respect to their strengths and deficits. The results were summarised in a deliverable that provides input for subsequent development activities. WP1 also defined a threat model, which was utilised during the evaluation phase.

WP2 Building Blocks: defined evaluation approaches for the developed building blocks and high-level protocols. Furthermore the core hardware building blocks considered in UNIQUE, Physical Unclonable Functions, were developed in WP2 Based on the results of WP1, WP2 started by developing a security model and design rules for PUFs. Subsequently, new PUFs were developed, designed and implemented, with the focus on the construction of reconfigurable PUFs, whose response behaviour can be changed on request in a low-cost manner into a PUF with completely different challenge-response characteristic. Furthermore, WP2 selected, optimised and implemented the required cryptographic building blocks that were used in applications in conjunction with PUFs. Another goal of WP2 was the development of hardware-entangled cryptographic primitives, i.e. cryptographic primitives (like block ciphers) that can be realised based on PUFs. The most important achievement of the work from WP2 is the successful creation of an ASIC, which contains six different PUF implementations. This ASIC is the core building block for the work performed in WP3 and WP4.

WP3 Evaluation and Validation: built on the achievements of WPs 1-2, focused on the evaluation of the building blocks developed in WP2 with respect to the requirements and design/evaluation approaches defined in WP1. In particular, WP3 had the goal of refining the evaluation methodology for PUFs and hardware Trojans and develop new evaluation mechanisms in case the existing ones are not suited for the purpose. Subsequently, WP3 tested the prototype PUF implementation developed within WP3 according to the selected methodology.

WP4 Prototype: was dedicated to the development of a research prototype, which shall illustrate the use of the technologies developed within UNIQUE in a realistic application scenario. In particular, both the developed PUFs and novel cryptographic primitives and architectures were combined in one demonstrator.

WP5 Dissemination: disseminated the project achievements and results. The creation of a project website, a leaflet, a logo a dissemination plan, and an internal communication infrastructure was also part of this work package.

WP6 Project Management: was responsible for the effective organisation of the project and covers the relevant management components.

Summarizing, within the work packages UNIQUE could achieve the following most important results:

- UNIQUE ASIC was successfully prototyped (containing six different PUF implementations)
- Two new PUF types have been introduced by the UNIQUE project to both the scientific as well as the industrial community: the Buskeeper PUF and the Logically Reconfigurable PUF (LR-PUF)
- Two use cases were defined (recyclable tokens, HW/SW-binding) for which threat models, security architectures and protocols have been created
- Using the building blocks implemented in the project, two demonstrators have been created successfully that show our solutions for the defined use cases
- Reliability and security evaluations of the PUF on the UNIQUE ASIC were performed
- New cryptographic primitives, specifically for use with (LR-)PUFs, have been created
- A large number of active participations at conferences (papers, workshops, etc.)
- Several UNIQUE publications in major journals

Overall UNIQUE has been the first project, which could integrate six different PUFs into one ASIC and has been the first, who could use this ASIC for an objective comparison of different PUF types in a given technology (in this case: 65nm).

2.2.1 The impact and use of results

Strategic and economical impact

While the approaches to defining and evaluating security in software and operating systems are maturing, detection and remediation of security flaws and breaches as well as assurance in hardware or mixed hardware/software environments are, in many respects, still an uncharted territory.

Surveys consistently demonstrate that it is the opportunity for economic gain that is driving most attackers or producers of malicious or unauthorized components. With the production of hardware devices becoming increasingly global and moving to geographies outside of Europe and North America, security assurance and innovative security architectures for hardware components, systems, and devices assume crucial importance. In the past, network, software and services were the focus of security analyses. It is necessary now to establish methodologies and processes to extend these methodologies to hardware and create new security techniques to ensure trustworthiness of hardware components. Definition of new robust and pragmatic methods that can establish trustworthiness, validity, and genuine nature of hardware components is of vital importance to ensure a safe computing environment for all levels of operations.

2.3 UNIQUE Project Consortium and website

The final goal of the UNIQUE project has been achieved through collaborations within a very strong consortium based on a team with outstanding scientific, engineering and manufacturing qualifications. The consortium consists of European organizations:[1] Technikon Forschungs- und Planungsgesellschaft mbH (TEC), Katholieke Universiteit Leuven (KULEUVEN), Technische Universitaet Darmstadt (TUD), Thales Communications & Security SA (TCS), Sirrix Aktiengesellschaft (SIRRIX), Intrinsic ID B.V. (IID) and Intel Performance Learning Solutions Limited (INTEL). UNIQUE brings together five academic and research institutions (including three leading universities and two research SMEs) and three large electronics companies from six European countries (Austria, Belgium, France, Germany, Ireland and the Netherlands). After the first reporting period the representative of partner Ruhr-University-Bochum (RUB), Prof. Ahmad Sadeghi moved to Technische Universitaet Darmstadt and the responsibilities of RUB were transferred accordingly.

The official UNIQUE project website is available at the following link: http://www.unique-security.eu

[1] Ruhr-University-Bochum (RUB) terminated in M16.