Publishable Summary of the UNIQUE Project

Project number:	238811
Project acronym:	**UNIQUE**
Project title:	Foundations for Forgery-Resistant Security Hardware
Start date of the project:	01.09.2009
Funding scheme:	30 months

Date of the reference Annex I:	June 10, 2009
Deliverable reference number: D6.1	**Publishable Summary of the first period of the UNIQUE Project** (as a part of the 1st Periodic reports according to EC regulation of the model contract)
Period covered:	01.09.2009 – 31.08.2010 (M01-M12)
WPs contributing to the deliverable:	All
Due date:	2010-08-31 (M12)
Actual submission date:	2010-12-01 – Version 1.2

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

1 Publishable summary

Mission of UNIQUE: To enforce the security and assurance of hardware components against malicious attacks of unauthorized parties.

1.1. Motivation

Counterfeiting of goods and Intellectual Property (IP) has reached a level that threatens industrial production, organisational function, health systems and even national security when malicious elements are deployed for critical infrastructures. Many industry sectors already employ or are considering hardware based security solutions. As an example, the pharmaceutical industry will incorporate integrated circuits (IC) into product packaging to prevent counterfeiting. However, such approaches are vulnerable to counterfeiting if the IC itself can be cloned. Unclonable security primitives such as Physically Unclonable Functions (PUFs) offer a route to creating ICs which are unclonable in any practical sense. The resultant higher level of security will significantly raise the effort level required for the counterfeiter. The adoption of such innovative approaches will enable enhanced counterfeit prevention and IP protection strategies. PUF-based security solutions are still in their infancy and Unique will focus on growing and developing the field.

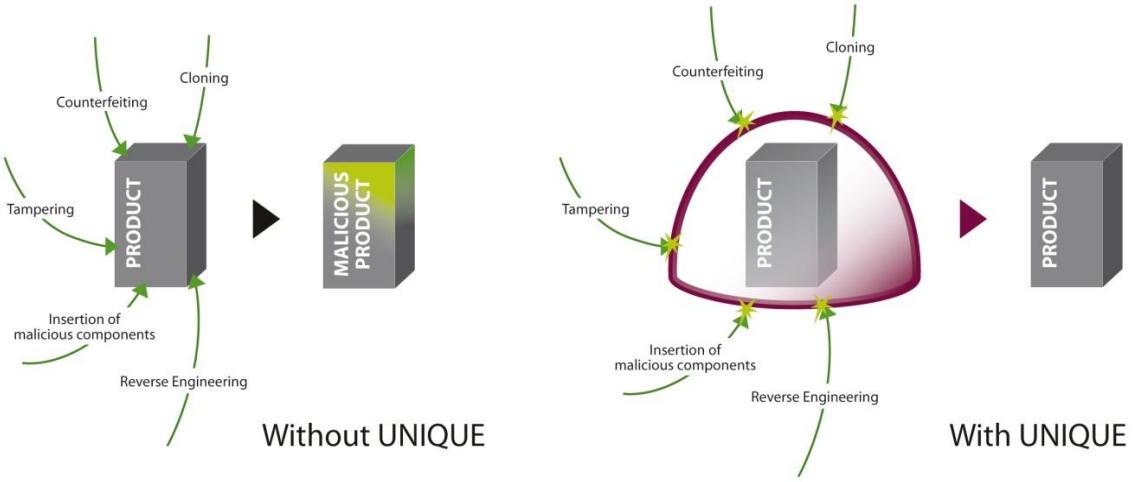

Figure 1: UNIQUE Concept

1.2. Objectives and overall Strategy

The UNIQUE project intends to increase the protection of hardware systems against the following security vulnerabilities: counterfeiting, cloning, tampering, reverse engineering and insertion of malicious components. In UNIQUE, hardware-based cryptography and security building blocks, security architectures, protocols, algorithms, design and evaluation principles will be combined to mainly enhance embedded hardware components with security functionalities.

The goal of the UNIQUE project is to develop solutions to the counterfeiting problem. These solutions need to be supported by strong, novel and consistent design and evaluation methods that have to ensure the security on three different levels: application and deployment level (counterfeiting, verifiability, auditability and detection of malicious hardware), design and implementation level (sub-micron physical security primitives – primarily Physically Unclonable Functions, PUFs – and entanglement of cryptography and physics) and evaluation level (cryptographic and security framework). The main research

issues during the first project year are: identification of requirements, threat models and building blocks. In the second period the novel methodologies will be listed, described and designed and the approved structures will be enhanced. For the last year the test framework design, implementation, integration of the prototype and evaluation are planned.

1.3. Description of Work done in the first year and results

The project started in September 2009, it is running for 30 months. The goal of the UNIQUE is to build foundations as well as practical tools and designs for forgery resistant security hardware. This implies that the project has two very important parts: i) the building of theoretical models and concepts and ii) the development of a practical demonstrator in which the properties of the theoretical models can be demonstrated. Since this implies a very interdisciplinary approach (combination of crypto knowledge, mathematics, physics and hardware building blocks and design), good teamwork between the various partners of the project is a necessary requirement to turn this project in a success.

In order to ensure this good team work and set the right goals for the project, we started with a kick-off meeting in Eindhoven where all partners were present. During this meeting the goals were clearly defined and some organizational agreements were made.

In order to get the right scientific and technological setting, the work started with WP1 where various use cases, requirements and threat models were defined (Deliverable 1.1).

The demonstrator of an anti-counterfeiting system will be one of the most important results of the project. A core component of the demonstrator is an ASIC in which a Physical Unclonable Function is implemented. Typically, the throughput time to build an ASIC, even for demonstration purposes is rather long (one year – one year and a half). Therefore the process of defining this ASIC and development of the components that have to be implemented in the ASIC were started in an early phase of the project. Basic architecture design of the ASIC started in M7. During the development of the ASIC many important decisions had to be taken by the consortium regarding budget, back-end design, technology node, selection of the PUFs to be implemented and how to implement potentially a reconfigurable PUF. In order to take these decisions in a proper way various meetings and teleconferences were organized in which all the involved project partners actively participated. The main decisions taken in this way were:

- Selection of the PUFs to be implemented: SRAM PUF, Latch PUF, Flip-Flop PUF, Arbiter PUF, Ring Oscillator PUF. The variety of PUFs available in the ASIC will allow to carry out a comparative study regarding implementation complexity and impact, reliability, security, area and power consumption, etc.
- Reconfigurable PUF: During the development process of the reconfigurable PUF a distinction between two concepts was made: i) the logical reconfigurable PUF and ii) the physical reconfigurable PUF. The concept of a logical reconfigurable PUF is being worked out into more detail and it is made sure that the ideas developed around both a logical as well as a physical reconfigurable PUF can be verified on the ASIC prototype.
- IC production: For back-end design, IMEC a Belgium design-house has been chosen, which will be responsible for the synthesis, back-end design and supervision of the production of the UNIQUE ASIC. IMEC's divisions InvoMEC (back-end) and Europractice programme (ASIC production) are involved. The technology node will be 65nm and TSMC our foundry. The reason for this choice stems from the fact it allows to show that the developed concepts work in a leading technology node of the biggest foundry of the world.

In order to evaluate the use of the prototype system for anti-counterfeiting purposes, a flexible PUF Evaluation Platform based on the PUF ASIC and an FPGA has been defined. On top of evaluation, this platform will enable the prototyping of the applications defined in the requirements using supporting cryptographic primitives, protocols and other functionality.

In addition to the ASIC development work and studies into reconfigurable PUFs, other research has been performed as well. First ideas have been developed to entangle crypto primitives with PUFs. Also new ideas for building a PUF based RFID tags are being investigated. Furthermore, work is being performed on a security model for PUFs, for which a preliminary draft has been set up. This draft will be the basis for further discussions and refinement.

To create awareness and to rise public interest about the project UNIQUE several dissemination activities have been performed e.g. UNIQUE project website is available and a public available UNIQUE leaflet has been produced. In addition the consortium members have supported scientific cooperation at the FET- Open level and extended public awareness of project achievements by participating in various workshops and conferences, as well as by elaborating publications regarding UNIQUE research. To ensure that the UNIQUE ideas reach broader audience the consortium agreed on the production of a project video that will be published in various internet sources; this is planned at the beginning of the second project year.

Finally, all the planned objectives for the first project year have been achieved; the project made very good progress and is consistent with the original planning. The work carried out so far provides a strong basis for the second UNIQUE period in order to accomplish all the goals and objectives as foreseen in Annex I. It is important to stress that this is the result from a very good and strong collaboration between the academic and industrial partners, who all contribute a lot of knowledge and expertise to turn this project into a success.

1.4. UNIQUE Project Consortium

The final goal of the UNIQUE project will be achieved through collaborations within a very strong consortium based on a team with outstanding scientific, engineering and manufacturing qualifications. The consortium consists of eight European organizations: Technikon Forschungs- und Planungsgesellschaft mbH (TEC), Ruhr-University-Bochum (RUB), Katholieke Universiteit Leuven (KULEUVEN), Technische Universitaet Darmstadt (TUD), Thales Comunications SA (TCF)[1], 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 involved organizations are forming a chain stretching from basic research and security design to applied research and end-user producers for consumers and industry.

The total volume of the project is estimated to be 4.215 million Euro, part of which will be contributed by the EC. For more information about the UNIQUE project please visit the project's website **www.unique-security.eu** or contact

Technikon Forschungs- und Planungsgesellschaft mbH

[1] and its sister company, Thales Security Solutions & Services (T3S) who has a third party status in this project.

Burgplatz 3a, 9500 Villach, Austria
Phone: +43 4242 233 55
Fax: +43 4242 233 55 77
E-mail: coordination@unique-security.eu
Web site: www.unique-security.eu

Figure 1: UNIQUE Consortium at Kick-off-Meeting in Eindhoven September 2009

Figure 2: UNIQUE Logo

Disclaimer:

All public information will be marked with the following UNIQUE project disclaimer:
The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.