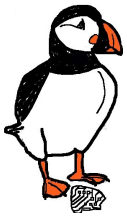

PUFFIN

Physically unclonable functions found in standard PC components

Project number: 284833
FP7-ICT-2011-C

D4.4

Periodic Report M19-36

Due date of deliverable: 31. January 2015
Actual submission date: 3. March 2015

WP contributing to the deliverable: WP4

Start date of project: 1. February 2012 Duration: 3 years

Coordinator:
Technische Universiteit Eindhoven
Email: coordinator@puffin.eu.org
www.puffin.eu.org

Revision 1.0

Project co-funded by the European Commission within the 7th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Periodic Report M19-36

All partners

3. March 2015
Revision 1.0

The work described in this report has in part been supported by the Commission of the European Communities through the FP7 program under project number 284833.

Abstract

This document is the second periodic report, covering activity in PUFFIN for M19 – 36.

Keywords: WP4, second overall report

Contents

Chapter 1

Publishable summary

"Physically unclonable functions found in standard PC components" (PUFFIN) was a 3-year STREP in ICT-2011.9.2 "High-Tech Research Intensive SMEs in FET research". PUFFIN started on 1 February 2012. Its objective was to identify, qualify and use "Physically Unclonable Functions" (PUFs) in standard PC components.

PUFs are used to uniquely identify electronic components and to protect valuable objects against counterfeiting. They allow creating a root of trust in a hardware system through generating device-unique "fingerprints" and deriving secret keys from the underlying physical properties of the silicon. Before the start of PUFFIN they were typically found in specially designed hardware components and result from the silicon properties of individual transistors. They exist in many forms, among which are the so-called SRAM PUFs.

The goal of the PUFFIN project was to study and show the existence of SRAM PUFs and other types of PUFs in standard PCs, laptops, mobile phones and consumer electronics. This was never attempted before. The mere existence of physical properties that depend on a component and are reproducible is only the first step to guarantee appropriate robustness, reliability and randomness properties for use as secret keys or trust anchors in mass-market applications. By uncovering the security properties of PUFs in standard components such as CPUs and GPUs, this project provided the first intrinsic and long-wanted basis for security in everyone's most common computing platforms: standard PCs and similar hardware. This new root of trust in turn adds security for mass-market applications, replacing or complementing the role of a trusted platform module and enabling security for applications such as broadcast applications, content protection for the gaming industry and secure day-to-day transactions for everyone. The results of the project were envisioned to allow for the first time an a-priori open platform, the most difficult element to secure in an information-technology system today, to inherit security properties from its own identity and its intrinsic physical properties.

The activities in the PUFFIN project were organized in three technical work packages:

- WP1: Exploration
- WP2: Analysis and qualification
- WP3: Use cases

The following sections summarize the goals and results from these work packages.

1.1 WP1: Exploration

The Exploration work package searched for new ways to physically identify PCs and other commodity hardware. It focused on standard PCs and handheld devices as they actually exist today and in the foreseeable future. The goal was not to modify components to make them easy to identify; the goal was to find identifiers that are already intrinsic in PCs and mobile devices. WP1

- attempted to read out the uninitialized memory of various GPU types;
- attempted to read out the uninitialized memory of various CPU types;
- attempted to find identifying properties of mobile devices such as smart phones that are hard to clone; and
- made a preliminary assessment of the quality of the so obtained data.

During the second period WP1 extended the range of hardware platforms and software tools for measuring undocumented behavior of several different types of chips. Most importantly it improved the discovery process for PUFs, bringing even hard-to-detect PUFs within reach. An intensive exploration of large CPUs gained access to the SRAM state at earlier and earlier times in the boot process until eventually reading out the state directly after powering on the chip. The measurements confirmed that the chip manufacturer was initializing the state before giving access to it (even under lab conditions using a development board) so that no useful PUF data could be gained but clearly demonstrating that the BIOS offers enough control to access the data, if only the chip manufacturers do not overwrite it. WP1 successfully measured *uninitialized* power-on SRAM states from several more chips and initiated a crowdsourcing project, continuing past the end of PUFFIN, to get access to more development boards. For each data set from the measurements WP1 carried out a preliminary assessment indicating that most of this data was of reasonable quality, justifying forwarding the data to WP2 for further analysis.

1.2 WP2: Analysis and qualification

WP2 was the natural follow-up to WP1 in this project:

- WP2 started with the development of statistical analysis tools and of mathematical and probabilistic models for the qualification of potential PUF data found and extracted in WP1.
- WP2 then proceeded to run the tools, perform such analysis and qualification on the different potential PUF instances identified in WP1, starting with GPU SRAM PUFs and continuing as new PUF instances were discovered throughout WP1.
- Finally, the analysis carried out led to useful insights and recommendations for the choice of security parameters required for protocols and security architectures built upon these PUFs in WP3.

During the second reporting period WP2 continued to play the important role of intermediary between WP1 and WP3, analyzing all raw PUF data found in WP1 and singling

out platforms for application development in WP3. The new devices analyzed are the BeagleBone development board, a Stellaris Launchpad board, and the Arduino Mega, along with many more GPU multiprocessors. However, the most exciting work in WP2 is new tests and methodologies for evaluating PUF behavior: specifically, in the second period, new research regarding the aging process in silicon and how to actively counteract this aging.

1.3 WP3: Use cases

WP3 was devoted to applications of and use cases for the PUFs investigated in WP1 and WP2. In particular, WP3 considered different ways for increasing the trust in computer systems through the use of PUFs found therein:

- WP3 developed hardware-entangled cryptographic primitives that draw their security directly on physical assumptions of the underlying PUF; an integral part of this task was to develop error correction schemes specifically tailored towards the error characteristics of the PUFs identified in WP1.
- WP3 investigated to which extent the PUFs developed in WP1 can be used to implement low-cost alternatives to Trusted Platform Modules for key storage and attestation.
- Finally, WP3 considered the use of PUFs in software security mechanisms that either guarantee the integrity of software or allow to securely bind software to a particular hardware platform; both problems naturally occur in solutions for anti-counterfeiting.

The security of the developed techniques was analyzed, culminating in proof-of-concept implementations.

WP3 developed several new use cases and security analyses during the second reporting period:

- Light-Weight Anti-Counterfeiting Solution for low-end commodity hardware using inherent PUFs.
- PUF-based code integrity protection on commodity hardware.
- Secure RSA key storage using PUFs on commodity hardware.
- Remote Wipe-Outs.
- Leakage in reverse Fuzzy Extractors.

The demonstrator showing how to bootstrap a secure boot application on cell phones from SRAM PUF in the CPU received a lot of attention and gained market relevance during the second reporting period. See Chapter 3 for the impact of PUFFIN on the involved SME.

1.4 Public web page

Up to date project information, the research deliverables, and publications resulting from the PUFFIN project can be found on the project web page at `http://puffin.eu.org/`.

Chapter 2

Project objectives, work progress and achievements

More and more information is stored on PCs and other consumer devices, and distributed with the intention to be accessible by a limited set of people. This information varies from confidential information on company intranets through personal information on social networks to sensitive information such as health-care or tax-related data in government databases. In addition, the increased availability of broadband connections for end users has triggered an invasion of commercial content such as ebooks, music, software, online gaming, and video on demand. Furthermore, embedded systems are increasingly used to perform security-critical tasks. For example, smartphones are used as payment systems, serve as (trusted) personal mobile access points, and consequently store a lot of privacy sensitive information.

Commercial incentives or legal requirements often demand that protection mechanisms are in place to prevent files from being accessed by unauthorized people or copied and further distributed. Traditional techniques include simple access control or encryption. The problem with these solutions is that they depend on the secrecy of a single piece of information such as a decryption key. Stressing a real-world analogy, anyone who possesses a door key, or a photograph of the key from a proper angle, can easily build a clone of that key, and later use the clone to open the door. Similarly, anyone who sees a cryptographic key can immediately copy it, and later use a copy of the key to decrypt data protected by the key and to forge data encrypted by the key. Security requires keeping door keys and cryptographic keys hidden from attackers. These keys have to be stored somewhere on the PC or communication device; as soon as this location is discovered and the key can be extracted, the protection mechanism is broken.

In an arms race with hackers and pirates, refuge has been sought in hardware-based solutions for key management. *It is now common wisdom in the IT security domain that a hardware-based foundation is necessary for secure and trustworthy systems.* For instance, smart cards are used to store cryptographic keys in set-top boxes (STBs) for television, and Trusted Platform Modules (TPMs) were introduced on personal computers (especially laptops) in order to provide a root of trust; TPMs have also been specified for mobile phones. Unfortunately, the introduction of hardware components induces extra cost and complexity. At this moment there is still a large number of PCs that do not have a TPM and it is likely that this will not change in the near future. It is therefore pressing to search for other roots of trust. *PUFFIN has shown that unique physical features that are intrinsically available in*

current consumer devices can be used as an alternative foundation of trust.

To increase the security of hardware components and embedded systems, some research projects have explored the use of unique physical hardware properties through Physically Unclonable Functions (PUFs). A PUF is a physical characteristic that acts as a noisy function: it receives an input (called a challenge) and responds with a noisy physical output (called a response); the PUF produces slightly different outputs for the same input. In order to obtain a noiseless output, error correction (in the form of fuzzy extractors) can be utilized.

PUFs provide intrinsic security: A PUF is physically unclonable—even after thoroughly inspecting the PUF, an attacker cannot build another device that responds to inputs in the same way, because doing so is an infeasible (or too expensive) engineering challenge. PUFs therefore do not need to be kept hidden from attackers. A PUF can be temporarily loaned to someone, and then returned to the owner, who verifies that the PUF responds to various inputs in the same way as before; the owner is then sure that the PUF has not been replaced with another one, is sure that the borrower does not have a copy of the PUF, and is sure that the borrower no longer can produce PUF responses to yet unknown challenges. The latter is due to the PUF security property of unpredictability: without physical access to the PUF, an attacker cannot predict the PUF response to a previously unused challenge.

Over the past ten years PUFs have been built from a wide variety of technologies, including magnetic stripes, coatings added to chips, and glass bubbles that refract light. For example, dedicated hardware read-out circuits using intrinsic SRAM variations can generate reliable secret keys. SRAM in existing field-programmable gate arrays (FPGAs) can be used as PUFs, allowing copy protection for designs loaded into FPGAs. In each case the PUF output is dictated by uncontrollable random variations in the PUF manufacturing process. At the forefront of research and development in this area is a European SME: Intrinsic-ID; the same SME is, not by coincidence, the initiator and leader of this project.

Common applications of PUFs are in the domain of key storage, authentication and anti-counterfeiting. PUFs can provide security for key storage due to their unpredictability: cryptographic keys do not need to be stored directly in memory; rather, keys can be derived from PUF responses 'on the fly' whenever a cryptographic operation needs to be performed. This reduces the time period during which keys are stored in memory, thereby minimizing exposure to attackers. PUF unclonability can be used to authenticate devices in a secure fashion: only an authentic device can answer a random unused challenge with the correct response. The latter is a key ingredient to prevent counterfeiting of hardware components.

So far, in all application scenarios considered for PUFs, a dedicated PUF has to be built and added to the system. This results in a complex system design, longer time to market and increased cost of a product. However, since PUFs can, for instance, be built from memory modules, it may be possible to use the unique physical properties of components that *are already available* in PCs, smartphones, etc. as PUFs. At the start of the PUFFIN project this direction was completely unexplored, and it was open where the research would lead.

The PUFFIN project produced a breakthrough in PUF usability, demonstrating that standard consumer devices are already full of components that can be combined into a high-security PUF. Devices do not have to be modified; system integrators do not have to purchase add-on PUFs, which is particularly important for small mobile devices having high cost constraints; users do not have to carry around key rings full of dongles. This breakthrough will enable applications ranging from anti-counterfeiting and access control to content protection and high-security encryption. Our long-term vision is that users on the Internet will no longer have to worry about attackers stealing their credentials and privileges through software bugs

or Trojans; security will be guaranteed by intrinsic properties of the devices.

Even for PCs equipped with a TPM it may be advantageous to use existing PC components as a PUF, to add an extra layer of security. For example it can help to make sure that the TPM chip is indeed part of the specific PC, and not moved to another PC. Further, PUFs can enhance the security of TPM-based secure storage against physical attacks, which are not yet considered when designing TPM chips. In the future, PUFs may become the new root of trust in PCs. Set-top boxes, game consoles or other embedded systems need similar protection as PCs, as witnessed by recent attacks against game consoles and smart phones. At the same time, their architecture is—due to cost issues—increasingly composed of standard components that share many similarities with PC parts. Of course, PUFFIN was never limited to traditional PCs: it always included mobile computation platforms, such as smart phones.

> *PUFFIN has shown that security can be obtained from properties that are inherent to the components that constitute a modern computer or mobile computation platform.*

In order to realize this vision of intrinsic security, PUFFIN targeted three goals during the duration of the project:

- First, PUFFIN investigated the potential use of standard PC components and embedded devices as PUFs. The main research challenge addressed was to find ways to adequately access the PUFs. In particular, one of the big problems with memory PUFs is to get access to the raw memory, before it is overwritten or initialized.
- Second, PUFFIN analyzed the identified PUFs in terms of reliability, uniqueness, and unclonability. Theoretical models were developed to measure PUF robustness and randomness properties, and were used to identify the most reliable and secure PUFs for use in applications.
- Third, PUFFIN investigated ways to use PUFs as a "root of trust" for applications running on a PC platform or a smartphone. As a common basis for the applications, PUFFIN investigated how intrinsic PUFs can be used as core components in the construction of cryptographic primitives and protocols.

2.1 Project objectives

PUFFIN was divided into three work packages, matching the division into three goals listed above. The following subsections list the particular tasks targeted by these work packages.

2.1.1 WP1: Exploration

WP1's first task, "Identification of potential PUFs in PCs", endeavored to find identifying digital fingerprints in as many of a PC's components as possible. Specific targets identified in the Description of Work included CPU caches and SRAM on GPUs. This task led to two milestones: MS11 (measurements from GPUs) and MS12 (measurements from CPUs).

WP1's second task, "Identification of potential PUFs in mobile devices", asked analogous questions regarding components of mobile devices such as smartphones and tablets. This task led to a third milestone: MS13 (measurements from mobile devices).

WP1 was prepared with a contingency plan in case it was unable to find suitable PUFs: namely, plugging add-on FPGA boards into PCs and measuring SRAM PUFs that were already known to be present in those boards. WP1's success at finding PUFs meant that this contingency plan was unnecessary, as discussed in the first review. WP1 also identified a task of "PUFs for the future" considering non-SRAM technologies such as phase-change memory and SSDs, but deferred this task to future work for several reasons: first, some of the most promising future technologies are not yet readily available; second, SRAM proved to be an excellent source of PUFs, warranting additional exploration.

2.1.2 WP2: Analysis and qualification

There were two main tasks for WP2 in the PUFFIN project. The first was creation of mathematical models and development of statistical analysis tools, which can be used to evaluate PUF measurements focusing on reliability and uniqueness. In this context reliability is the stability with which a PUF response can be reproduced under varying ambient conditions, over time, etc. Uniqueness indicates that the probability that two PUFs have closely resembling properties is exponentially small. In order for PUFs to be usable for security implementations they should both be reliable and unique.

The second task was evaluation of the PUF measurements from WP1 based on the two main properties of PUFs mentioned above, reliability and uniqueness. Based on this evaluation can be assessed which PUFs from WP1 are suitable for deployment in use case implementations of WP3.

These tasks led to three milestones: MS21 (mathematical models are created and statistical analysis tool is developed), MS22 (qualification of potential GPU PUFs discovered in WP1), and MS23 (qualification of potential CPU PUFs and mobile-device PUFs discovered in WP1).

2.1.3 WP3: Use cases

WP3 collected use cases for intrinsic PUFs, developed protocols and implementations based on the identified use cases, and evaluated the security of the proposed protocols and implementations.

Task 1 — Hardware-based trust establishment — aimed at the development of protocols and architectures, which exploit the hardware properties of the underlying PUF instances to be secure. In particular, this task considered cryptographic building blocks, such as random number generators, block and stream ciphers, authentication and key exchange protocols, which are based on intrinsic PUFs rather then on complexity-theoretic hardness assumptions. Additionally, new Helper Data schemes and Fuzzy Extractor approaches were investigated, which are specialized on the peculiarities of intrinsic PUFs. Finally, WP3 explored the possibilities to replace traditional Trusted Platform Modules (TPMs) by intrinsic PUFs, such that PUFs instances can be used for key storage or platform authentication.

Task 2 — PUF-based software security — aimed at the protection of software against modification or unauthorized duplication. Thus, WP3 explored approaches to intertwine PUF challenges and responses with a given binary. The main challenge was to prevent attackers to passively listen to PUF challenges and responses transmitted between the PUF instance and the software instance on a virtualization layer. The attacker would be able to emulate the PUF instance and break and thus break its security.

Finally, Task 3 — Security evaluation and implementation — aimed at evaluating the security properties of the results from task 2.

2.2 Work progress and achievements

PUFFIN's work was remarkably successful, achieving all of the core project goals and several unexpected results beyond those goals.

2.2.1 WP1: Exploration

WP1 introduced three important advances to the process of discovering new PUFs. First, WP1 extended its list of targets to include *microcontrollers*. Microcontrollers are low-cost low-power CPUs used in a wide range of embedded applications; they are of interest as stepping-stones towards more complex CPUs, and they are also of interest as security devices per se. Starting with microcontrollers meant that WP1 was able to leap into action, rapidly developing exploration tools and successfully obtaining uninitialized SRAM data from a range of different devices.

Second, to handle the challenges of more complex platforms with other software components that clear SRAM, WP1 developed tools to take control of each platform at the deepest possible level, extracting SRAM data as early as possible in the boot process. These tools allowed WP1 to distinguish "tough PUFs" cleared by software from non-PUFs cleared by hardware.

Third, to enable its techniques to be reused for as many devices as possible, WP1 heavily automated its measurement processes, developed open-source software, and initiated a crowdsourcing project.

These advances allowed WP1 to locate uninitialized SRAM on a surprisingly wide range of platforms, including several different microcontrollers, two development boards with the same types of processors used in many smartphones (Pandaboard using ARM Cortex-A9, and BeagleBone using ARM Cortex-A8), and an NVIDIA GeForce GTX 295 graphics card. For each device type, WP1 systematically collected measurements on many "identical" devices, including 510 separate multiprocessors on 17 "identical" GPUs.

The multi-pronged success in collecting SRAM data, from more devices than initially anticipated and with more phenomena worthy of study, warranted deferring investigation of other types of PUFs in favor of a continuing focus on SRAM. The same success also meant that WP2 and WP3 were provided with ample test and demonstration platforms throughout the project, without having to resort to add-on FPGAs.

Statement on the use of resources

Here is an overview stating the planned and actual person months spent on WP1. For further explanations of the deviations see section 2.2.4.

TUE		IID		KUL		TUD		total	
planned	actual	planned	actual	planned	actual	planned	actual	planned	actual
16 PM	18PM	5 PM	6.3 PM	5 PM	1 PM	1.5 PM	3 PM	27.5 PM	28.3 PM

2.2.2 WP2: Analysis and qualification

WP2 developed three new methodologies for evaluating PUF behavior. All of these were accepted for publication at security workshops during 2013 and 2014.

The first new methodology focuses on analyzing PUF *reliability*. This work introduces a new reliability model taking an observed heterogeneous nature of PUF cells into account. A substantial experimental validation has demonstrated that the new predicted distributions from this model describe the empirically observed data statistics almost perfectly, even considering sensitivity to operational temperature. This will allow to study PUF failure behavior in full detail, including the average and the worst case probabilities.

The second new methodology evaluates PUF *uniqueness*. The aim of this work was to develop and implement a new methodology for accurately estimating the entropy of PUFs. This novel method estimates the extractable entropy by calculating the mutual information between enrollment and reconstruction measurements.

The third new methodology evaluates PUF *aging*. This methodology shows how SRAM behaves over time, depending on different use-case scenarios. The results show that it is possible to influence the aging behavior of SRAM PUFs depending on how data is stored in these SRAMs while the device is powered. This way it is possible to make sure that SRAM PUFs will behave reliably over time, regardless of how long the lifetime of a device is.

Furthermore, WP2 successfully analyzed a torrent of measurements from WP1 (overall more than 6 gigabytes in compressed form). Deliverables D2.1 and D2.2 present an overview of the performance of all devices identified by WP1 in several different PUF sets. The most important conclusion that can be drawn from these results is that PUF behavior can be found in the SRAMs of many different commercially available platforms. Most of the SRAMs that have been measured show promising results and therefore are suitable for use in PUF implementations; however, the amount of pre-processing required on the data will vary between the platforms.

Statement on the use of resources

Here is an overview stating the planned and actual person months spent on WP2. For further explanations of the deviations see section 2.2.4.

TUE		IID		KUL		TUD		total	
planned	actual	planned	actual	planned	actual	planned	actual	planned	actual
1.5 PM	0.5 PM	6 PM	9.1 PM	9 PM	5 PM	1.5 PM	3 PM	18 PM	17.6 PM

2.2.3 WP3: Use cases

WP3 has produced several exciting papers on the security impact of the PUFs discovered within PUFFIN.

Starting from an intrinsic PUF on a modern ARM system-on-chip platform (as in a smartphone), WP3 extracted and reconstructed a cryptographic key unique to single instances of this platform. By modifying the platform's bootloader, WP3 successfully bound the bootloader to the extracted key and thus to the hardware itself, enabling a lightweight secure boot approach, which does not need additional hardware modifications (such as TPM chips). WP3 also designed and implemented techniques to use PUFs to protect the integrity of code, and

to extract RSA *public keys* from PUFs rather than just secret keys. WP3 also found a way to use PUFs to guarantee remote *erasure* of data.

Furthermore, WP3 was able to create a new Helper Data scheme, which takes into account the peculiarities of intrinsic PUF measurements. This way, a new variant of so-called Zero Secrecy Leakage of the Helper Data was achieved, even though – especially in the case of intrinsic PUFs – the PUF measurements are not uniformly distributed. WP3 also analyzed the influence of SRAM PUF aging upon the security of authentication protocols.

During the analysis of different microchips towards their PUF characteristics, WP3 realized that for some microchips it is possible to exploit the noise inherent to every PUF measurement to provide a secure pseudo-random number generator. Random numbers are essential for almost all cryptographic primitives (secret keys in block ciphers, secret keys in stream ciphers, secret keys in public-key signature systems, and so on), and the quality of this randomness is critical for security. However, in the case of lightweight embedded devices, sources of secure random numbers are rare. WP3 succeeded in exploiting the entropy from the noise of the PUF measurements to extract a high-quality seed for a pseudo-random number generator on such devices. Thus, WP3 was able to use the inherent noise in PUF measurements to strengthen an important cryptographic building block. PUFFIN also had a spinoff paper quantifying the weakness of a previous non-PUF-based random-number generator.

Statement on the use of resources

Here is an overview stating the planned and actual person months spent on WP3. For further explanations of the deviations see section 2.2.4.

TUE		IID		KUL		TUD		total	
planned	actual	planned	actual	planned	actual	planned	actual	planned	actual
2 PM	3 PM	6 PM	8 PM	5 PM	3 PM	15 PM	17 PM	28 PM	31 PM

2.2.4 Statements on the use of the resources

While the planned research advanced according to plan, there are some differences between the planned hours and the hours actually worked on the PUFFIN project. The differences in paid PMs are reflected in the financial statements. The following paragraphs give justifications for the deviations and explains how the deviations from the plan were handled.

TUE

After spending less paid time in the first reporting period, TUE caught up. Ruben Niederhagen was hired in M20 (mostly for WP1) and Meilof Veeningen in M32 (mostly for WP3). Some efforts were shifted from WP2 to WP3. Bernstein led WP1 as a volunteer without financial support by PUFFIN.

IID

Intrinsic-ID has spent slightly more effort on the PUFFIN project than was estimated in the original budget. As WP-leader for WP2, a bit more effort was required for the three new analysis methodologies that have been developed in this WP.

During the second period, several other (FP7) research project at Intrinsic-ID ended, freeing more resources for PUFFIN. Additionally, management involvement for this project became larger due to IID's increased business interest in the mobile market.

KUL

KUL spent less time on PUFFIN due to personnel reasons. The work has been picked up by other partners.

TUD

The main effort of TUD is in WP3; the two 2 PMs from the first phase were delayed to the second phase of PUFFIN to built upon the results of WP1 to concentrate our work on WP3. The stated PMs include unpaid work by Stefan Katzenbeisser, die leader of WP3.

Chapter 3

Intrinsic-ID's follow up on PUFFIN

The PUFFIN project has shown the possibilities of having PUF technology in mobile devices. On the one hand because WP1 and WP2 have shown that it is possible to use SRAM on mobile devices for PUF purposes, like the PUFs found on the Texas Instruments OMAP4430/60 processors (which are common processors for tablets and smartphones). On the other hand because of the use cases from WP3, which have shown the added value of PUFs on mobile devices. In a follow up on these results from the PUFFIN project, Intrinsic-ID has achieved two major milestones at the end of the year 2014 in regard to their presence in the continuously growing mobile market. This chapter contains snippets from two recent press releases by Intrinsic-ID, which are based on development that has been inspired by the research from the PUFFIN project.

3.1 Intrinsic-ID Wins Cyber Security & Privacy Innovation Award

The full press release is available online.

Eindhoven, The Netherlands, November 4, 2014. Intrinsic-ID, a leading provider of device-unique security solutions, won an EU-backed Cyber Security & Privacy Innovator award from IPACSO. IPACSO is a pan-European consortium comprised of a diverse range of industry, academic, R&D and policy-making experts collaborating to spur innovation and market opportunities in the areas of privacy and cyber security.

Intrinsic-ID was awarded the Privacy or Cyber Security Innovator award for its groundbreaking work providing device-unique security solutions based on its patented Hardware Intrinsic Security™(HIS) technology. This technology is now available as the Saturnus® Security Framework, an Application Programming Interface (API) for developers of secure mobile applications.

> Intrinsic-ID stands out as a leader because of how it leverages the unique ID of a chip to provide secure and convenient protection of mobile and desktop applications. Authentication is a key infrastructure requirement for the future of the Internet, especially when it comes to the Internet of Things and Industrial Control Systems.

said Mr. Ulrich Seldeslachts, CEO of LSEC, one of the organisations behind IPACSO.

The jury praised Intrinsic-ID for its innovative approach in defining a unique ID to a device. The Saturnus Security Framework uses innate characteristics of the chip in a smartphone, by means of physical unclonable functions (PUF), to turn the mobile phone into a unique identifier. The phone then is able to authenticate to applications and services, prevent potential cyber threats, preserve the privacy of the user and enable secure transactions.

"This endorsement from the EU and IPACSO validates our strategy to bring high-end security technology to mobile devices," said Dr. Pim Tuyls, CEO of Intrinsic-ID. The independent awards review commission screened 100 entries to select winners in six categories.

3.2 Intrinsic-ID Wins Cybersecurity Procurement from the Netherlands Government for Phone as a Security Token Technology

The full press release is online.

Eindhoven, The Netherlands, January 29, 2015. Intrinsic-ID, a leading provider of device-unique security solutions, today announced the company has won a procurement from the Small Business Innovation Research (SBIR) program of the national government of the Netherlands for its phone as a security token project. The SBIR is a collaboration between the Netherlands' government and local entrepreneurs to bring to market innovative products and services that solve important social problems.

Intrinsic-ID was one of six companies awarded funds as part of Phase II of the SBIR Cybersecurity initiative and competed against 72 other proposals as part of Phase I. The Intrinsic-ID project, named: Bring Your Own Security (BYOS), aims to turn a standard smartphone into a universal, two-factor authentication device with the use of Intrinsic-ID's proprietary Physically Unclonable Function (PUF) technology, also known as Hardware Intrinsic Security^{TM}(HIS). This enables to use your standard cell phone for sensitive and private applications, without compromising other features or adding costs.

Intrinsic-ID's project to bring advanced PUF technology to standard cell phones was ranked first among all the participants in this round. The evaluation commission mentioned that it has "high expectations from the impact of the project as the innovation solves the authentication issue, one of the critical problems in cybersecurity." The evaluation commission included security experts of 4 Dutch ministries (Justice, Interior, Defence, Finance) as well as private sector experts. The Dutch Enterprise Agency (RVO) is responsible for the implementation of the SBIR Cybersecurity program.

The SBIR program is a government procurement program that focuses on solving concrete social challenges requiring technological innovation and entrepreneurship. The Intrinsic-ID project being funded essentially uses Intrinsic-ID's PUF-based HIS technology to make a standard cell phone act as a security token. The project involves cooperation with smartphone manufacturers for the integration of Intrinsic-ID's HIS technology in new smartphones. In addition, Intrinsic-ID will develop the Saturnus Security Framework software development kit (SDK), which will enable software developers to develop secure applications such as secure cloud access, secure enterprise network access, mobile payments, banking and authentication in general.

"Winning this procurement is a key milestone for us and our efforts to make Hardware Intrinsic Security more broadly available," said Dr. Pim Tuyls, CEO of Intrinsic-ID and the inventor of Hardware Intrinsic Security. "With the endorsement of the Dutch Enterprise

Agency as well as the opportunity to work with other partners in this program, we will be able to bring our concept to market much more rapidly and fully then if we did this on our own. We appreciate the efforts of the SBIR program in supporting entrepreneurs in all key phases of product innovation from research and development to commercialization."

Chapter 4

Project management

As this was a small-scale project with four partners that already had a long-standing collaboration (in part while some of the key researchers had other affiliations), the project used a lean governing culture. The Project Management Board (PMB) consisted of one senior representative per partner complemented with all the WP leaders. For the whole duration of the project these were the following:

- Project Manager: Tanja Lange, TUE.
- Scientific Manager: Pim Tuyls, IID.
- WP1 leader: Daniel J. Bernstein, TUE.
- WP2 leader: Vincent van der Leest, IID.
- WP3 leader: Stefan Katzenbeisser, TUD.
- WP1 co-leader: Frederik Vercauteren, KUL.

4.1 Scientific and Industrial Advisory Board (SIAB)

The SIAB is chaired by the Scientific Manager and consists of the Project Manager as well as a senior researcher from each of the four partners complemented by several senior researchers from European industry and academia. The following experts form the SIAB of PUFFIN:

- David Naccache, École normale supérieure, France.
- Christof Paar, Ruhr-Universität Bochum, Germany.
- Jean-Jacques Quisquater, Université catholique de Louvain, Belgium.
- Claire Vishik, Intel, UK.

In the second reporting period it was not possible to find a time when more than one SIAB member could make it to a meeting, so we decided to postpone the meeting to November (M33). We met on November 11, 2014, in Leuven – this day is a national holiday in Belgium and France and was the only day that we could find. Three of the four SIAB members were present and all of the workpackage leaders and several more PUFFIN members. The discussions were lively and constructive. The minutes of the meeting are available on the review page.

4.2 Communication and coordination activities

Coordination was mainly done by email via the general mailing list `all@puffin.eu.org` which reached everybody involved with PUFFIN. During the second reporting period we reduced the number of meetings because research groups had formed and were progressing steadily.

4.2.1 List of project meetings, dates and venues

For all the meetings mentioned below all partners were represented.

2013-11-03 PUFFIN workshop in Berlin. Several presentations by PUFFIN members and two external presentations. See workshop website http://puffin.eu.org/workshop.html and D4.5 for details.

2014-07-03 General research meeting in Leuven. We invited Pol van Aubel (Nijmegen) to talk about his work on finding PUFs in CPUs. This led to a collaboration between him and Ruben Niederhagen (TUE). Other topics were thoughts about the crowdsourcing project and in general measuring small boards. Ruben Niederhagen, André Schaller, and Anthony Van Herrewege coordinated.

2014-11-11 Second SIAB meeting. See minutes online.

4.3 Impact of possible deviations from the planned milestones and deliverables

The project progressed smoothly throughout its lifetime, following the plan in all essential respects; see Tables 4.6.1 and 4.6.2 for details.

After the slightly slower start at the beginning of the first reporting period all partners caught up on hiring and significantly increased the manpower of PUFFIN. The second reporting period saw a significant takeup in the workforce and the output.

4.4 Development of the project website

The project website was established in M1 and continuously updated since. WP leaders have direct access to the sections on their WP. Interaction with the internal (SIAB) and external reviewers is handled via password protected websites.

All scientific papers resulting from the PUFFIN project so far have been made available at least in author-copy versions and this part will be updated with future papers. Also the deliverables of the first reporting period have been made available and (once accepted) those of the second one will follow.

4.5 Statement on the use of resources

Here is an overview stating the planned and actual person months spent on management.

TUE		IID		KUL		TUD		total	
planned	actual	planned	actual	planned	actual	planned	actual	planned	actual
0.8 PM	1.5PM	1 PM	3.7 PM	0 PM	0 PM	0 PM	0 PM	1.8 PM	5.2PM

TUE

TUE spent a bit more effort on management to deal with the larger number of people in the second reporting period.

IID

IID has used more resources for project management than was listed in the original budget. This was to make sure that the research in this project was in close alignment with new business opportunities for the SME of this project.

4.6 Deliverables and milestones tables

Table 4.6.1: Deliverables

Deliverable number	Deliverable name	Version	WP number	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I	Actual/forecast delivery date	Status	Comments
D1.1	Scientific contribution of WP1, part 1	1.0	1	1	R	PU	M18	M20	✓	
D1.2	Scientific contribution of WP1, part 2		1	1	R	PU	M36	M36	✓	
D2.1	Scientific contribution of WP2, part 1	1.0	2	2	R	PU	M18	M20	✓	
D2.2	Scientific contribution of WP2, part 2		2	2	R	PU	M36	M36	✓	
D3.1	Scientific contribution of WP3, part 1	1.0	3	4	R	PU	M18	M20	✓	
D3.2	Scientific contribution of WP3, part 2		3	4	R	PU	M36	M36	✓	
D4.1	Project website and internal ICT communication infrastructure	*	4	1	O	PU	M3	M1	✓	
D4.2	Project dissemination plan	*	4	1	R	PU	M6	M8	✓	
D4.3	First report according to the Grant Agreement	1.0	4	1	R	PU	M18	M21	✓	
D4.4	Second report according to the Grant Agreement		4	1	R	PU	M36	M36	✓	
D4.5	Final report for the use and dissemination of foreground	*	4	1	R	PU	M30	M36	✓	
D4.6	Report on IPR		4	1	R	PU	M36	M36	✓	

Standard codes for the nature of the deliverable: R = Report O = Other
Standard codes for dissemination level: PU = Public

*: Web site updated continuously, D4.2 updated till first review; after that updated D4.5.

Table 4.6.2: Milestones

Milestone number	Milestone name	WP number	Lead beneficiary	Delivery date from Annex I	Achieved	Actual/forecast delivery date	Comments
MS11	Measurements from GPUs	1	1	M4	✓	M1	*
MS12	Measurements from CPUs	1	1	M10	✓	M10	
MS13	Measurements from mobile devices	1	3	M10	✓	M15	
MS14	Integration of FPGA SRAM PUFs	1	1	M27		M27	**
MS21	Mathematical models are created and statistical analysis tool is developed	2	2	M10	✓	M8	
MS22	Potential GPU PUFs discovered in WP1 are either qualified or disqualified	2	2	M10	✓	M1	*
MS23	Potential CPU PUFs and mobile-device PUFs discovered in WP1 are either qualified or disqualified	2	2	M16	✓	M13	
MS31	Preliminary analysis of high-level requirements for PUFs	3	4	M10	✓	M5	
MS32	Initial evaluation of PC PUF suitability	3	4	M18	✓	M16	
MS33	Decision on protocols and security architectures to be implemented as proof of concept	3	4	M20	✓	M20	
MS41	Elements of ICT infrastructure usable	4	1	M1	✓	M1	
MS42	Kick-off meeting	4	1	M2	✓	M3	
MS43	Website up and running	4	1	M3	✓	M1	
MS44	Initial project dissemination plan completed	4	1	M4	✓	M6	
MS45	SIAB established	4	1	M6	✓	M8	
MS46	First meeting of the SIAB	4	1	M18	✓	M18	
MS47	Second meeting of the SIAB	4	1	M30	✓	M34	
MS48	Workshop	4	1	M20	✓	M22	

Milestones are managed internally to keep the project on track.

* Multiple rounds of GPU measurements and analyses, most recently in M34.
** PUFFIN found many suitable PUFs in commodity hardware so that (as discussed in the first review) it was not necessary to resort to FPGAs as external trust anchors. This milestone was included as risk mitigation and luckily was not necessary.