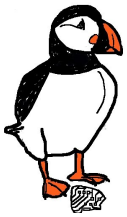


PUFFIN

Physically unclonable functions found in standard PC components

Project number: 284833
FP7-ICT-2011-C

D4.5

Final report for the use and dissemination of foreground

Due date of deliverable: 31. July 2014, postponed to 31. January 2015 to cover entire project
Actual submission date: Current version 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 1.2

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)	

Final report for the use and dissemination of foreground

Tanja Lange (TUE)

Current version 3. March 2015
Revision 1.2

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. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Abstract

This is the final version of the dissemination plan. Earlier versions were distributed as D.4.2.

Keywords: WP4, dissemination of project results.

Contents

Chapter 1

Dissemination

1.1 Introduction

Dissemination of the research results is essential in advertising the PUFFIN project and involving the larger scientific community in the research. This dissemination plan first lays out the strategy in this chapter and then, in the following chapter, reports on achievements during the project.

The following dissemination activities are foreseen:

- Create templates for dissemination activities such as presentations and publications.
- Create and maintain a public website that offers extensive information on the project, its results and news items.
- Issue press releases at strategic phases of the project.
- Distribute project results through scientific and industrial publications and through a workshop oriented towards a broader audience.
- Be available as expert for journalists and tech writers.

1.2 Logo and templates

It is important for the PUFFIN project to be easily recognized and to have the diverse results linked back to the project. Already before the official start of the project we designed the project logo — a PUFFIN with a digital footprint. This logo will be prominently displayed on the project website and on publications of the project, such as the project reports and slide shows. To create a uniform "project identity" we will design templates for these.

1.3 Public website and twitter

The public face of the project will be the project website. It will form the central source for all information for dissemination that includes newsletters, news items, press releases, project brochures and scientific articles.

To attract visitors to the site when new results are posted we will maintain a twitter account for the project. The tweets will be included in the webpage and serve as the "news" section of the page.

1.4 Dissemination in the academic and industrial community

The project plans to publish articles in both academic and industry journals, conferences and workshops. For cryptographic implementations the top conference is CHES (Cryptographic Hardware and Embedded Systems); for broader security and usability aspects ACM-CCS, eSMART, ISSE, TrustED are relevant. Journals are less important in this area but will be used to publish full versions of conference papers.

The academic partners will transfer knowledge to the broader scientific community by incorporating the scientific results of the projects in summer schools and training courses and by integrating part of the material in regular university courses.

1.5 Press interactions

At the beginning of the project it will be important to make news agencies and journalists aware of the project. The PUFFIN project will issue a press release and also employ twitter to reach out to technology writers. In later stages of the project we expect that PUFFIN has achieved enough visibility to be contacted by tech writers interested in the subject.

Chapter 2

Achievements of the PUFFIN project

This chapter reports on the achieved level of dissemination during the entire project.

2.1 Templates

Templates for presentations in latex were created in M3 and for reports in M5. A ppt version exists since M17.

2.2 Website and electronic communication

The PUFFIN website has been set up in M1 at http://puffin.eu.org. Along with the website PUFFIN project has set up email forwarding so that project members and management are reachable via puffin.eu.org-email addresses.

Additionally a PUFFIN twitter account https://twitter.com/puffin_project was created which is linked in to the PUFFIN website. Contents are updated by the work package leaders. The website is available at http://www.puffin.eu.org. The twitter feed has proven to be a very useful means of reaching people interested in technology; this was certainly aided by retweets from @FET_EU (thanks for that) but also by retweets from project members and interested individuals (most notably @ioerror with 86k followers).

2.3 Press releases

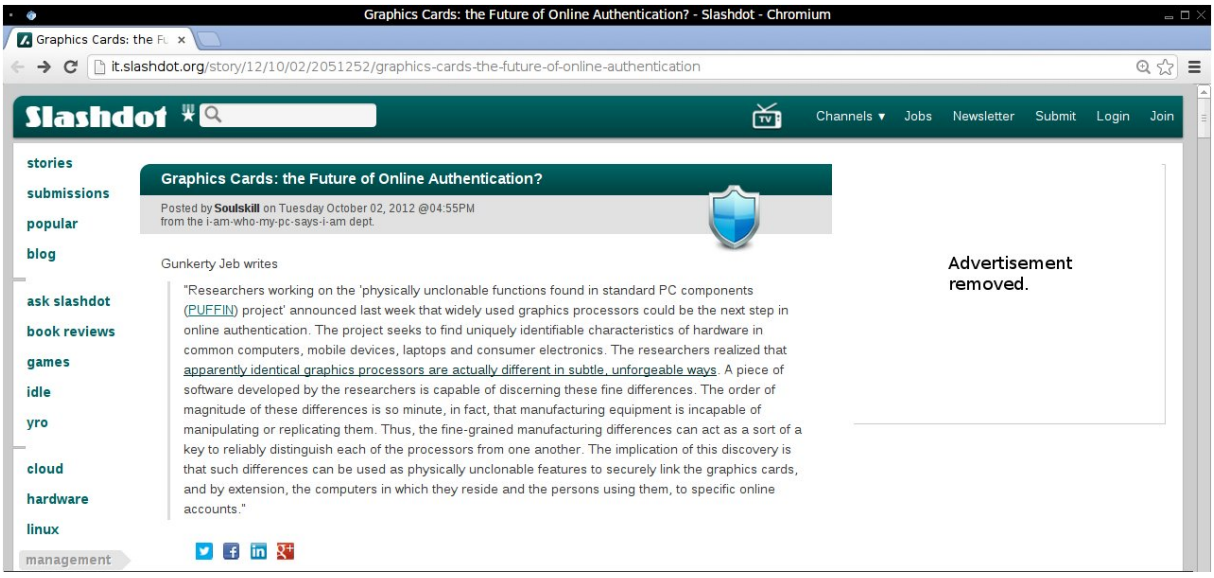
The first set of press release was posted M8 announcing the PUFFIN result that PUFs were identified in GPUs.

All four partners used their local channels to issue press releases and in addition to the English version featured also on the PUFFIN webpage, a Dutch (http://www.esat.kuleuven.be/news/COSIC_grafische_kaarten) and a German (https://www.tu-darmstadt.de/vorbeischauen/aktuell/einzelansicht_56960.de.jsp) press release were posted.

The press release was taken up very well by the general press in Belgium, Germany, and the Netherlands and the technical press internationally. The following list covers some of the stories that are still reachable to this date.

http://threatpost.com/authentication-implications-uniquely-identifiable-graphics-cards-100212/77066
http://www.newelectronics.co.uk/electronics-news/puffin-aims-to-protect-against-identity-theft/45139/
http://news.discovery.com/tech/graphics-cards-may-id-your-machine-121008.html
http://phys.org/news/2012-10-puffin-graphics-card-breakthrough-break-in.html
http://www.besttechguidance.info/puffin-offers-graphics-card-breakthrough-versus-break-in/
http://interesting.rk.net.nz/?p=114992
http://fooyoh.com/geekapolis_gadgets_wishlist/8032517
http://it.slashdot.org/story/12/10/02/2051252/graphics-cards-the-future-of-online-authentication
http://www.computable.nl/artikel/nieuws/infrastructuur/4567505/2379248/tue-ontdekt-onkloonbare-grafische-kaart.html
http://www.technischweekblad.nl/identificatie-door-onkloonbare-hardware.289557.lynkx
http://www.darmstadtnews.de/2012/10/04/massenware-unverwechselbar-und-individuell-wissenschaftler-entdecken-faelschungssichere-identitaeten-von-grafikkarten/
http://www.innovations-report.de/html/berichte/informationstechnologie/wissenschaftler_entdecken_faelschungssichere_203307.html
http://www.echo-online.de/region/darmstadt/studienortdarmstadt/technischeuniversitaet/Massenware-individuell-und-unverwechselbar;art477,3287144
http://www.buergerstimmen.de/wissenschaft/science_539.htm
http://www.silicon.de/41573393/forscher-entdecken-fingerabdruck-von-grafikkarten/
http://winfuture.de/news,72318.html

It even hit the front page of Slashdot after a report on Threatpost.



The twitter account gained several followers from the press releases and retweets by Tanja Lange (`@hyperelliptic`) and Daniel J. Bernstein (`@hashbreaker`) and one interview was arranged via twitter.

In summer 2014 the PUFFIN project was contacted by BBC about an article on password storage. Pim Tuyls gave an interview and the PUFFIN results were presented as one of the solutions to abolishing passwords in http://www.bbc.com/news/technology-28891938 *Has the flawed password system finally had its day?*. Here is the part reporting on the PUFFIN project:

> Researchers in Germany and the Netherlands have been exploring ways to identify devices accurately as part of a European project called Puffin - short for "Physically unclonable functions found in standard PC components".
>
> They have examined seemingly identical computer parts, such as memory chips, and found that tiny variations in conditions during the manufacturing process give each one has a unique digital fingerprint, or physically unclonable function (PUF).
>
> Software that can read these PUFs can be used to identify a computer or mobile device reliably, says Pim Tuyls, the chief executive of Intrinsic-ID, a commercial partner in the Puffin project.

Intrinsic-ID used their press channels to disseminate new results and to generally advertise PUF technology. Most recently they reported in https://www.intrinsic-id.com/intrinsic-id-wins-cybersecurity-procurement-from-the-netherlands-government-for-phone-as-a-security-token-technology that Intrinsic-ID won the Cybersecurity Procurement from the Netherlands Government for its "Phone as a Security Token" project. This project will bring to the market the WP3 demonstrator of secure phones and give PUFFIN a successful after live.

2.4 Presentations at industry forums

During the first reporting period André Schaller presented PUFFIN at http://trudevice.com/Workshop TRUDEVICE 2013 (joint short paper with Vincent van der Leest) *Physically Unclonable Functions found in Standard Components of Commercial Devices.*

Pim Tuyls has presented PUFs and the results of PUFFIN at industry fora to advertise the PUFFIN/IID result of securing phones using keys derived from SRAM PUFs found in the ARM processors. He gave a presentation on *Hardware Intrinsic Security to Protect Value in the Mobile Market* at ISSE 2014 http://www.revolution1.plus.com/isse/index.htm.

Tanja Lange and Daniel J. Bernstein gave a general *Physically unclonable functions found in standard PC components (PUFFIN)* presentation at the Intel International State of the Art in Cryptography workshop in December 2014.

2.5 Scientific presentations

A complete list of publications including preprints and links to electronic versions is available at http://puffin.eu.org/papers.html.

The first results of the PUFFIN project got published at scientific events as early as 2012. The first was *Tiny application-specific programmable processor for BCH decoding* by Anthony Van Herrewege and Ingrid Verbauwhede at ISSoC 2012.

This was soon followed by Mafalda Cortez, Said Hamdioui, Vincent van der Leest, Roel Maes, Geert-Jan Schrijen: *Adapting Voltage Ramp-up Time for Temperature Noise Reduction on Memory-based PUFs* at HOST 2013.

An early highlight was a paper at CHES 2013, the prime conference on cryptographic hardware, by Roel Maes: *An Accurate Probabilistic Reliability Model for Silicon PUFs.*

With all scientific personnel hired and trained the second reporting period brought even more publications and some preprints.

The following two papers got accepted for publication at TrustED, a pre-conference workshop of ACM-CCS:

- Anthony Van Herrewege, Vincent van der Leest, André Schaller, Stefan Katzenbeisser and Ingrid Verbauwhede: *Secure PRNG Seeding on Commercial Of-the-Shelf Microcontrollers.*
- Robbert van den Berg, Boris Skoric and Vincent van der Leest: *Bias-based modeling and entropy analysis of PUFs.*

At the main ACM-CCS conference PUFFIN was present with a demo

- Anthony Van Herrewege, André Schaller, Ingrid Verbauwhede, Stefan Katzenbeisser: *Inherent PUFs and Secure PRNGs on Commercial Off-the-Shelf Microcontrollers.*

The PUFFIN workshop (see below) was a major event to report on the scientific achievements of the PUFFIN project.

The spammed code offset method by Boris Skoric and Niels de Vreede appeared in IEEE Transactions on Information Forensics and Security, vol. 9, p 875 – 884.

PUFFIN was present again at HOST 2014 with Roel Maes and Vincent van der Leest's paper *Countering the Effects of Silicon Aging on SRAM PUFs* and at TRUST 2014 with *Lightweight Anti-Counterfeiting Solution for Low-End Commodity Hardware Using Inherent PUFs* by Andre Schaller, Tolga Arul, Vincent van der Leest, and Stefan Katzenbeisser.

Software Only, Extremely Compact, Keccak-based Secure PRNG on ARM Cortex-M by Anthony Van Herrewege and Ingrid Verbauwhede appeared at the 51st Design Automation Conference (DAC 2014).

The scope of PUFFIN had already extended to random number generation and hash function; the papers *On the Practical Exploitability of Dual EC in TLS Implementations* by Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham (USENIX Security Symposium 2014) and *SPHINCS: practical stateless hash-based signatures* by Daniel J. Bernstein, Daira Hopwood, Andreas Hlsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn, which will appear at Eurocrypt 2015, went further in these direction.

In addition, several partners participated in conferences and workshops and informally disseminated research results. The D4.2 deliverable contains a list of conferences and workshops attended by PUFFIN members during the first reporting period. If necessary a similar list can be provided for the second reporting period.

2.6 Workshop

A workshop was planned for M20 (September 2013). We postponed the workshop till M22 to host it in conjunction with ACM-CCS (Berlin, November 4-8) in order to attract more participants. The workshop combined presentations by external researches and presentations of PUFFIN results. In order not to overlap with the main conference and the side workshops at which PUFFIN results are be presented the PUFFIN workshop took place on Sunday, November 3. We anticipated that the international attendees of CCS would arrive in Berlin on Saturday or Sunday morning, so that the Sunday afternoon time slot came in handy. The workshop was announced during the Crypto 2013 rump session and via mailing lists. Unfortunately ACM was not willing to announce it on the ACM-CCS page unless PUFFIN would become a sponsor (at a fee of about the entire workshop budget).

Despite the weekend slot the workshop attracted close to 30 participants. Most importantly, the atmosphere was constructive, leading to interesting discussions between the participants. The external invited speakers were Claude Barral from Bactech and Kenneth Mai from Carnegie Mellon University.

Here is the list of scientific presentations (in order of the schedule):

- Claude Barral "PUF-based Security for Smart Objects"
- Daniel J. Bernstein "Computers as undocumented physical objects"
- Vincent van der Leest "How to recognize a bad PUF"
- Boris Skoric "The Spammed Code Offset Method"
- Anthony Van Herrewege "PRNGs on embedded devices"
- André Schaller "Bootloader Protection Using Inherent PUFs"
- Kenneth Mai, "Efficient Reliable Silicon PUF Design"

The workshop webpage http://puffin.eu.org/workshop.html now contains archived information about the workshop including slides from the presentations of all speakers.