PUFFIN

Physically unclonable functions found in standard PC components

Project number: 284833
FP7-ICT-2011-C

D4.2

Project Dissemination Plan

Due date of deliverable: 31. July 2012
Actual submission date: continous updates
current version 1. October 2013

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)	

Project Dissemination Plan

Tanja Lange (TUE)

continous updates
current version 1. October 2013
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. 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 document gives a detailed plan describig the dissemination activities plan of the consortium; it is updated on a regular basis throught the project.

Keywords: WP4, dissemination plan

Contents

1 Dissemination plan 1

1.1 Introduction . . . 1

1.2 Logo and templates . . . 1

1.3 Public website and twitter . . . 1

1.4 Dissemination in the academic and industrial community . . . 2

2 Achievements to date 3

2.1 Templates . . . 3

2.2 Website and electronic communication . . . 3

2.3 Press releases . . . 3

2.4 Presentations at industry forums . . . 5

2.5 Scientific presentations . . . 5

2.6 Workshop . . . 7

2.7 Upcoming actions . . . 8

Chapter 1

Dissemination plan

1.1 Introduction

Dissemination of the research results it 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 first 18 months of the project. For the second reporting period further venues of dissemination will open since the results from the first reporting period draw attention to the PUFFIN project and lead to invited presentations.

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.

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.

Chapter 2

Achievements to date

This chapter is being continuously updated during the first reporting period to give an accurate image of the achieved level of dissemination.

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. 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.

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.

2.3 Press releases

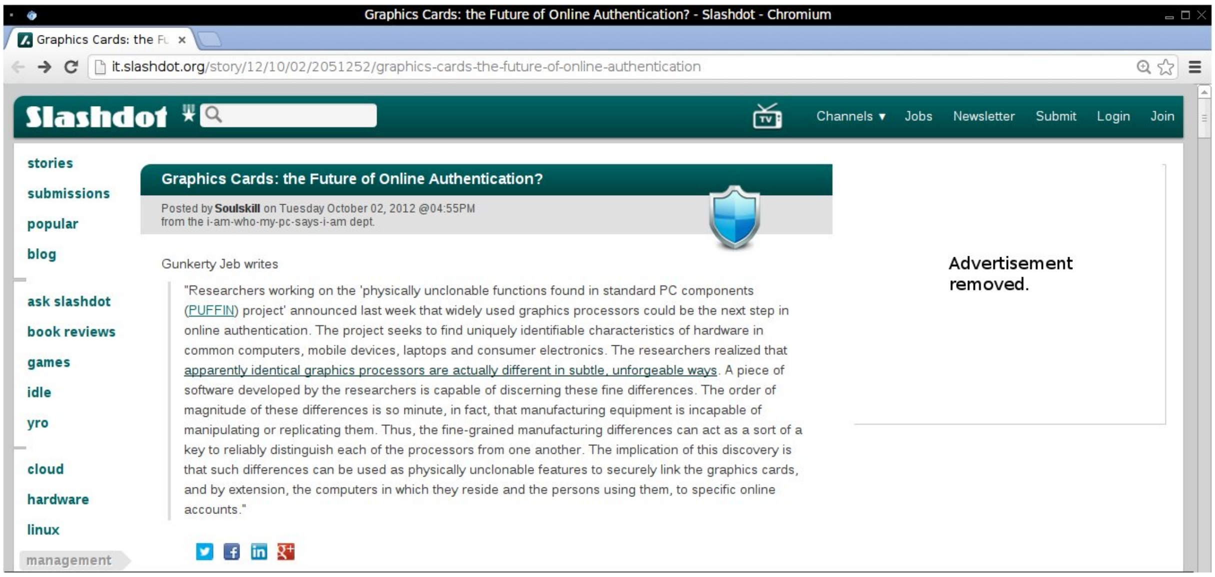
The first set of press release was posted M8 announcing the PUFFIN result that PUFs were identified in GPUs.

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.



Graphics Cards: the Future of Online Authentication?

Posted by **Soulskill** on Tuesday October 02, 2012 @04:55PM
from the i-am-who-my-pc-says-i-am dept.

Gunkerty Jeb writes

> "Researchers working on the 'physically unclonable functions found in standard PC components (PUFFIN) project' announced last week that widely used graphics processors could be the next step in online authentication. The project seeks to find uniquely identifiable characteristics of hardware in common computers, mobile devices, laptops and consumer electronics. The researchers realized that apparently identical graphics processors are actually different in subtle, unforgeable ways. A piece of software developed by the researchers is capable of discerning these fine differences. The order of magnitude of these differences is so minute, in fact, that manufacturing equipment is incapable of manipulating or replicating them. Thus, the fine-grained manufacturing differences can act as a sort of a key to reliably distinguish each of the processors from one another. The implication of this discovery is that such differences can be used as physically unclonable features to securely link the graphics cards, and by extension, the computers in which they reside and the persons using them, to specific online accounts."

Advertisement removed.

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.

We plan on having the next press release for early November, covering the PUFFIN workshop and the papers and poster presented at ACM-CCS and its side workshops.

2.4 Presentations at industry forums

Unfortunately, the scientific coordinator, Pim Tuyls, was not able to attend the FET events in the reporting period due to other obligations.

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.*

2.5 Scientific presentations

The first results of the PUFFIN project are now getting published at scientific events. The first was 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* which was published at HOST 2013.

This was soon followed by a paper at CHES 2013, the prime confernce on cryptographic hardware, by Roel Maes: *An Accurate Probabilistic Reliability Model for Silicon PUFs.*

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 will be 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) will be a major event to report on the scientific achievements of the PUFFIN project.

Two further papers are currently under review and several are in preparation, including one on PUFs from GPUs.

In addition, several partners participated in conferences and workshops and informally disseminated research results. This list includes travel not covered by the PUFFIN budget.

Full name of conference	**Date**	**Location**	**Partners**	**Relevance to PUFFIN**
DATE 2012 http://www.date-conference.com/date12/	2012.03.12–16	Dresden, De	IID	All WPs; one of the main hardware design conferences
Eurocrypt 2012 http://www.cs.bris.ac.uk/eurocrypt2012/	2012.04.15–19	Cambridge, UK	TUE, KUL	WP1, WP3; one of the 3 main conferences in cryptography
HOST 2012 http://www.engr.uconn.edu/HOST/HOST-2012.pdf	2012.06.03–04	San Francisco, US	IID	All WPs; workshop on hardware security, with dedicated session for PUFs
Crypto 2012 http://www.iacr.org/conferences/crypto2012	2012.08.19–23	Santa Barbara, US	TUE, KUL	WP1, WP3; one of the 3 main conferences in cryptography
CMS 2012 http://sec.cs.kent.ac.uk/cms2012/	2012.09.03–05	Canterbury, United Kingdom	TUD	General dissemination.
ACM MMSEC 2012 http://www.mmsec12.com/	2012.09.06–07	Coventry, United Kingdom	TUD	General dissemination.
CHES 2012 http://www.chesworkshop.org/ches2012/index.php	2012.09.09–12	Leuven, BE	TUE, IID, KUL, TUD	All WPs; main workshop on cryptographic hardware, several talks on PUFs
Crypto 2020 https://www.cosic.esat.kuleuven.be/ecrypt/cryptofor2020/	2013.01.22–24	Tenerife, ES	KUL	WP1, several presentations on cryptographic hardware
DATE 2013 http://www.date-conference.com/date13/	2013.03.18–22	Grenoble, Fr	IID	All WPs; one of the main hardware design conferences
Eurocrypt 2013 http://www.iacr.org/conferences/eurocrypt2013	2013.05.26–31	Athens, GR	TUE, KUL	WP1, WP3; one of the 3 main conferences in cryptography
WIC SITB 2013 http://www2.imec.be/be_en//education/conferences/wic-symposium.html	2013.05.30–31	Leuven, Belgium	TUE	General dissemination. Yearly Benelux symposium on information theory.

Full name of conference	Date	Location	Partners	Relevance to PUFFIN
TRUDEVICE 2013 http://trudevice.com/Workshop/	2013.05.30–31	Avignon, France	TUD	Presentation of PUFFIN project.
HOST 2013 http://www.engr.uconn.edu/HOST/HOST2013-Program-v4.pdf	2013.06.02–03	Austin, US	IID	All WPs; workshop on hardware security, with dedicated session for PUFs
CryptArchi 2013 http://labh-curien.univ-st-etienne.fr/cryptarchi/	2013.06.23–26	Frejus, Fr	IID	WP3; International Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices
International State of the Art in Cryptography - Security http://crypto.di.uoa.gr/CRYPTO.SEC/International-Crypto-Security.html	2013.05.31 – 06.01	Athens, GR	TUE, KUL	General dissemination; event involving academia and industry
Crypto 2013 http://www.iacr.org/conferences/crypto2013	2013.08.18–22	Santa Barbara, US	TUE, KUL	WP1, WP3; one of the 3 main conferences in cryptography
CHES 2013 http://www.chesworkshop.org/ches2013/start.php	2013.08.20–23	Santa Barbara, US	TUE, IID	All WPs; main workshop on cryptographic hardware, several talks on PUFs; presentation of PUFFIN results by Roel Maas
COSIC Crypto course 2013 https://www.cosic.esat.kuleuven.be/course/	2013.06.03–06	Heverlee, BE	KUL, IID	All WPs; course on basic building blocks of cryptography; presentation on PUFs and informal discussion on PUFFIN research

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 will combine presentations by external researches and presentations of PUFFIN results. The workshop webpage http://puffin.eu.org/workshop.html is online and registration will open very soon. In order not to overlap with the main conference and the side workshops at which PUFFIN results will be presented the PUFFIN workshop will take place on Sunday, November 3. We anticipate that the international attendees of CCS will arrive in Berlin on Saturday or Sunday morning, so that the Sunday afternoon time slot comes in handy. The workshop was announced during the Crypto 2013 rump session. Program and speakers will be announced shortly.

2.7 Upcoming actions

After the review meeting – once the deliverables are accepted – they will be made available on the PUFFIN webpage.

During or shortly after the PUFFIN workshop we will post the project presentations.