TRUDEVICE 2015 - 4TH WORKSHOP ON SECURE HARDWARE AND SECURITY EVALUATION
September 17th, 2015, Saint-Malo, France

The TRUDEVICE Workshop will provide an environment for researchers from academic and industrial domains who want to discuss recent findings, theories and ongoing work on secure hardware design and validation. The program consists of two keynotes from prominent experts from the secure hardware industry, contributed talks and poster presentations.

Registration: The registration link is available at https://www.cosic.esat.kuleuven.be/trudevice/registration_form.php

Final program:

8:50 - 9:00: Opening

9:00 - 10:00: 1st Keynote – **Physical(ly) unclonable functions: dreams and reality,** Ingrid Verbauwhede, KU Leuven, Belgium

10:00 - 10:30: Coffee break

10:30 - 12:10: 1st Session

Attacks, evaluation and testing strategies

- Mafalda Cortez, Said Hamdioui, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre and Ilia Polian. *Multi-segment Enhanced Scan-chains for Secure ICs*
- Benoit Gonzalvo, Eric Bourbao, Lilian Bossuet and Fabien Majéric. *JTAG Combined Attacks*
- Xuan Thuy Ngo, Zakaria Najm, Shivam Bhasin, Debapriya Basu Roy, Sylvain Guilley and Jean-Luc Danger. *Exploiting Custom Sensors to Leak Secret Keys*
- Bodo Selmke, Stefan Brummer, Johann Heyszl and Georg Sigl. *Precise Laser Fault injections into 90 nm and 45 nm SRAM-cells*

12:10 - 13:30: Lunch

13:30 - 14:30: 2nd Keynote - **Security trends in mobile solutions,** Marc Witteman CTO, Riscure

14:30 - 15:00: Coffee break

15:00 - 16:40: 2nd Session

Secure hardware design

- Pascal Sasdrich and Tim Güneysu. *Pushing the Limits: Ultra-Lightweight AES on Reconfigurable Hardware*
- Elena Ioana Vatajelu, Giorgio Di Natale and Paolo Prinetto. *Zero Bit-Error-Rate Weak PUF based on Spin-Transfer-Torque MRAM Memories*
- Apostolos Fournaris and Nicolas Sklavos. *Binary Edwards Curve Design Strategy for Efficient and Power Attack Resistant Architectures*
- Antonio Varriale, Elena Ioana Vatajelu, Giorgio Di Natale, Paolo Prinetto and Tiziana Margaria. *SEcubeTM: The most advanced, Open Source Security Platform in a Single Chip*

Posters: will be presented during coffee breaks

- Robert Hesselbarth, Salvador Manich and Georg Sigl. *Modeling and Analyzing Bistable Ring Based PUFs*
- Anton Biasizzo, Franc Novak and Gašper Kojek. *High Performance FPGA Fault Injection Platform*
- Yaara Neumeier and Osnat Keren. *Protecting Multilevel Memories from Fault Attacks Using Robust Codes*
- Kostas Papagiannopoulos. *Masked Implementations: The Last Mile*
- Stephan Kleber, Florian Unterstein, Matthias Matousek, Frank Kargl, Frank Slomka and Matthias Hiller. *Design of the Secure Execution PUF-based Processor (SEPP)*

Keynotes:

1st Keynote
Physical(ly) unclonable functions: dreams and reality, Ingrid Verbauwhede, KU Leuven, Belgium

Abstract:
Physically unclonable functions (PUFs) have been researched for a while. They are promised as a cheap, hardware-entangled, security anchor inside a silicon device, providing intrinsic security properties without extra processing steps. With the correct post-processing, they can be used for authentication as well as key generation.
In this presentation, we list the facts and the dreams regarding PUFs. We discuss essential properties of PUFs and PUF protocols. We list open problems and further research directions and try to figure out if we are reaching the dream?
At COSIC, research on PUFs has been performed in the context of the European projects UNIQUE, PUFFIN, HINT and currently HECTOR.

Bio:

Dr. Ingrid Verbauwhede is a Professor in the research group COSIC of the Electrical Engineering Department of the KU Leuven in Belgium. At COSIC, she leads the embedded systems and hardware group. She is also adjunct professor at the EE department at UCLA, Los Angeles, CA. She joined COSIC in 2003 and UCLA in 1998. Before joining UCLA she worked at UC Berkeley as a post-doctoral researcher and visiting lecturer, and later at TCSI and Atmel Lab in Berkeley, CA.
She is a Member of IACR and a fellow of IEEE. She was elected as member of the Royal Flemish Academy of Belgium for Science and the Arts in 2011.

She is a pioneer in the field of efficient and secure implementations of cryptographic algorithms in embedded context on ASIC, FPGA and embedded SW. It has been the main focus of her PhD and of her research at UCLA and KU Leuven. At COSIC she also supervises a hardware electronics lab to perform side-channel and fault-attacks.

She is the author and co-author of more than 300 publications at conferences, journals, book chapters and books. She graduated 27 PhD students between 2004 and 2015, which all have top positions in academia and in industry, all over the world.

Dr. Verbauwhede has been the general chair in 2012 and the program chair in 2007 of the IACR CHES (Cryptographic Hardware and Embedded Systems) workshop, which is the flagship venue for secure hardware design. She has been member of the program committee of a large number of conferences, including DAC, DATE, ISSCC, Usenix, SIPS, ISCAS, ISLPED, and more. Prof. Verbauwhede has participated in several EU funded hardware and embedded systems security projects. Currently her research group participates in the FP7 project HINT and the H2020 project HECTOR.
Her list of publications and patents is available at www.esat.kuleuven.be/cosic

2nd Keynote

Security trends in mobile solutions, Marc Witteman CTO, Riscure

Abstract:

Mobile products have a strong need for security for two main applications: mobile payment, and premium content. While smart phones and tablets are widespread, these products lack strong hardware security. As a result of that, new directions in software security are becoming popular.

This presentation explains the trends in protecting the security of mobile platforms and discusses the need for hardware security in the future.

Marc Witteman (MSc)
Chief Technology Officer

P +31 15 251 4090
M +31 62459 5408

witteman@riscure.com

Marc Witteman has a long track record in the security industry. He has been involved with a variety of security projects for over two decades and worked on applications in mobile communications, payment industry, identification, and pay television. Recent work includes secure programming and mobile payment security issues.

He has authored several articles on smart card and embedded device security issues. Further, he has extensive experience as a trainer, lecturing security topics for audiences ranging from novices to experts.

As a security analyst he developed several tools for testing software and hardware security. This includes Inspector, a platform for conducting side-channel analysis and JCworkBench, a logical test tool.

Marc Witteman has an MSc in Electrical Engineering from the Delft University of Technology in the Netherlands. From 1989 till 2001 he worked for several telecom operators, the ETSI standardization body and a security evaluation facility.

In 2001 he founded Riscure, a security lab based in the Netherlands. Riscure offers test tools and services to manufacturers and issuers of advanced security technology.

Between 2001 and 2009 he raised the company to a leading security test lab, and side channel test tool vendor. In 2010 Marc Witteman started Riscure Inc, the US branch of Riscure, based in San Francisco. At present he is the Chief Executive Officer of Riscure.