Research Institute in Secure Hardware & Embedded Systems (RISE)

Máire O'Neill

QUEEN'S UNIVERSITY BELFAST
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES
in association with National Cyber Security Centre
EPSRC Engineering and Physical Sciences Research Council

UK Research Institutes in Cyber Security

RISE is 1 of 4 **multi-institutional Research Institutes in Cyber Security** funded by the National Cyber Security Centre (NCSC), UK Engineering and Physical Sciences Research Council (EPSRC) and the Centre for Protection of National Infrastructure (CPNI) with the aim of developing the UK's cyber security capability.

The other Institutes are:

- **RISCS: Research Institute in Science of Cyber Security**
  Director: Angela Sasse, University College London
- **RITICS: Research Institute in Trustworthy Industrial Control Systems**
  Director: Chris Hankin, Imperial College London
- **RIVeTSS: Research Institute in Verified Trustworthy Software Systems**
  Director: Philippa Gardner, Imperial College London

Need for Hardware Security

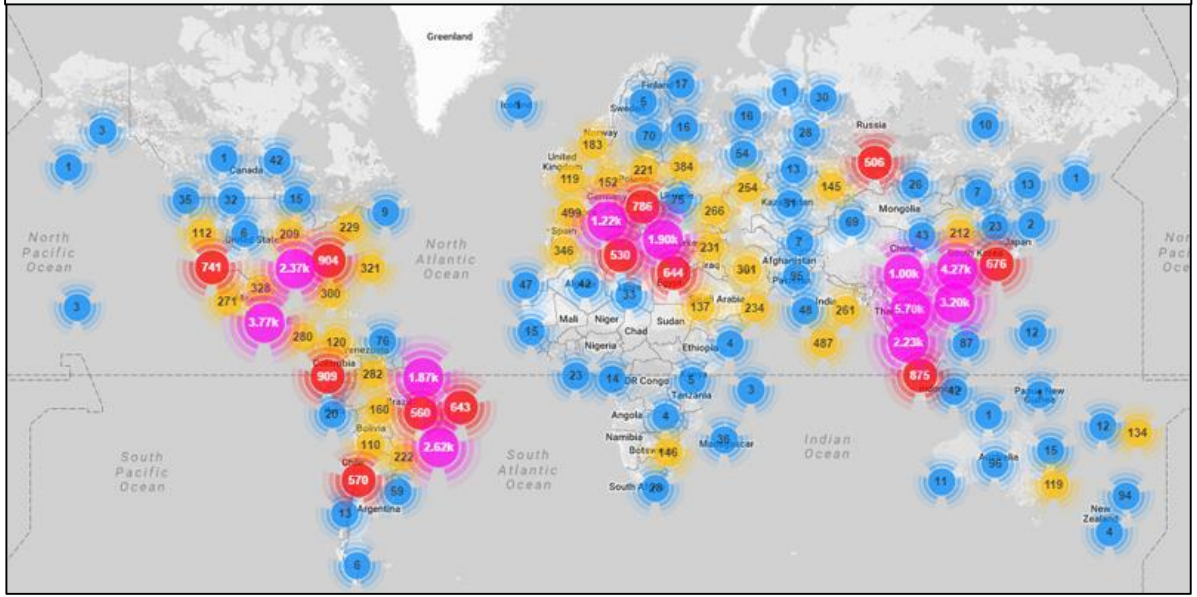
- Demand for Hardware Security research & innovation *increasing* with growing security needs in embedded & networking devices, and cloud services
- **A key driver is the Internet of Things (IoT)**
- Multi-layered approach to security needed - establishing a trusted computing baseline that anchors trust in tamper-proof hardware
- A strong **hardware security foundation** essential for realising secure systems

Need for Hardware Security

Practical attacks of IoT devices have already been demonstrated.

Need for Hardware Security

Geo-locations of Mirai-infected IoT devices (Aug 2017)

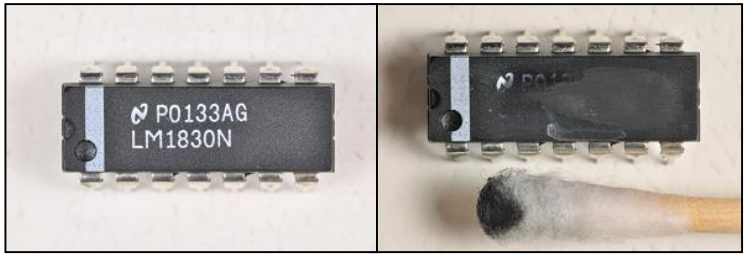


***Source**: Breaking down Mirai: An IoT DDoS Botnet Analysis, www.incapsula.com, Aug 2017*

Counterfeit Devices – The Internet of ‘Cloned’ Things

What about cloned devices and untrusted supply chains?

- Globalisation of supply chains - use of overseas foundries, third party IP, third party test facilities
- Supply chains susceptible to a range of hardware-based security threats
- Counterfeit devices could host malicious software, firmware or hardware

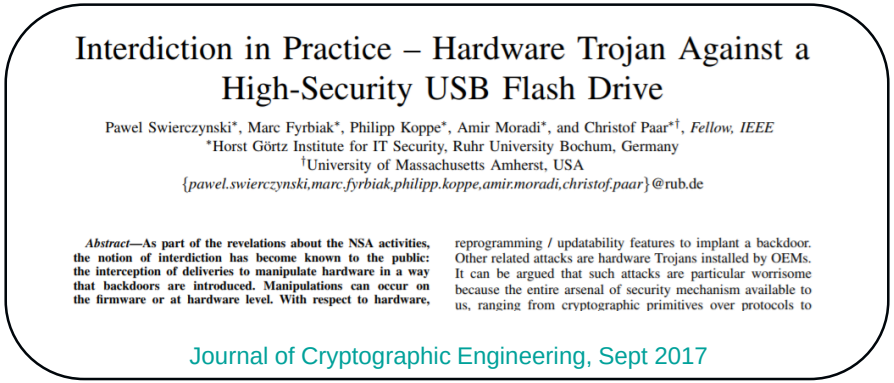


IEEE Spectrum, Oct 2013

“State-sponsored cloning is thought to be common”, IEEE Spectrum, April 2017

Threat of Hardware Trojans

First successful real-world FPGA hardware Trojan insertion into a commercial product



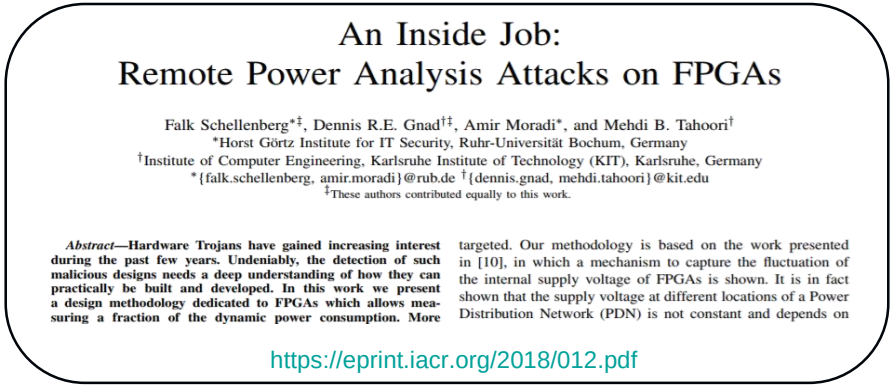
Interdiction in Practice – Hardware Trojan Against a High-Security USB Flash Drive

Pawel Swierczynski*, Marc Fyrbiak*, Philipp Koppe*, Amir Moradi*, and Christof Paar*†, *Fellow, IEEE*
*Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
†University of Massachusetts Amherst, USA
{*pawel.swierczynski,marc.fyrbiak,philipp.koppe,amir.moradi,christof.paar*}@rub.de

***Abstract*—As part of the revelations about the NSA activities, the notion of interdiction has become known to the public: the interception of deliveries to manipulate hardware in a way that backdoors are introduced. Manipulations can occur on the firmware or at hardware level. With respect to hardware, reprogramming / updatability features to implant a backdoor. Other related attacks are hardware Trojans installed by OEMs. It can be argued that such attacks are particular worrisome because the entire arsenal of security mechanism available to us, ranging from cryptographic primitives over protocols to**

Journal of Cryptographic Engineering, Sept 2017

A hardware Trojan that exploits the Power Distribution Network (PDN) in FPGAs



An Inside Job:
Remote Power Analysis Attacks on FPGAs

Falk Schellenberg*‡, Dennis R.E. Gnad†‡, Amir Moradi*, and Mehdi B. Tahoori†
*Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
†Institute of Computer Engineering, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
*{falk.schellenberg, amir.moradi}@rub.de †{dennis.gnad, mehdi.tahoori}@kit.edu
‡These authors contributed equally to this work.

***Abstract*—Hardware Trojans have gained increasing interest during the past few years. Undeniably, the detection of such malicious designs needs a deep understanding of how they can practically be built and developed. In this work we present a design methodology dedicated to FPGAs which allows measuring a fraction of the dynamic power consumption. More targeted. Our methodology is based on the work presented in [10], in which a mechanism to capture the fluctuation of the internal supply voltage of FPGAs is shown. It is in fact shown that the supply voltage at different locations of a Power Distribution Network (PDN) is not constant and depends on**

https://eprint.iacr.org/2018/012.pdf

Recent vulnerabilities affecting Hardware devices

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli
N. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas, ACM CCS, Nov 2017

Meltdown

Spectre

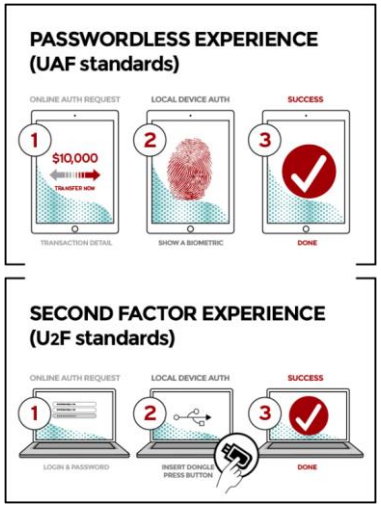
Major Research Challenges

- *How do we detect counterfeit devices?*
- *How do we detect manipulated devices?*
- *Is it possible to build attack-resilient hardware platforms?*
- *How do we deal with untrusted manufacturing processes & untrusted supply chains?*

Hardware Security Use-Cases

Combining hardware roots of trust (e.g. TPM, TEEs) with functional encryption/ signature approaches can allow sticky policies to be created for protected data, incorporating attributes, such as:

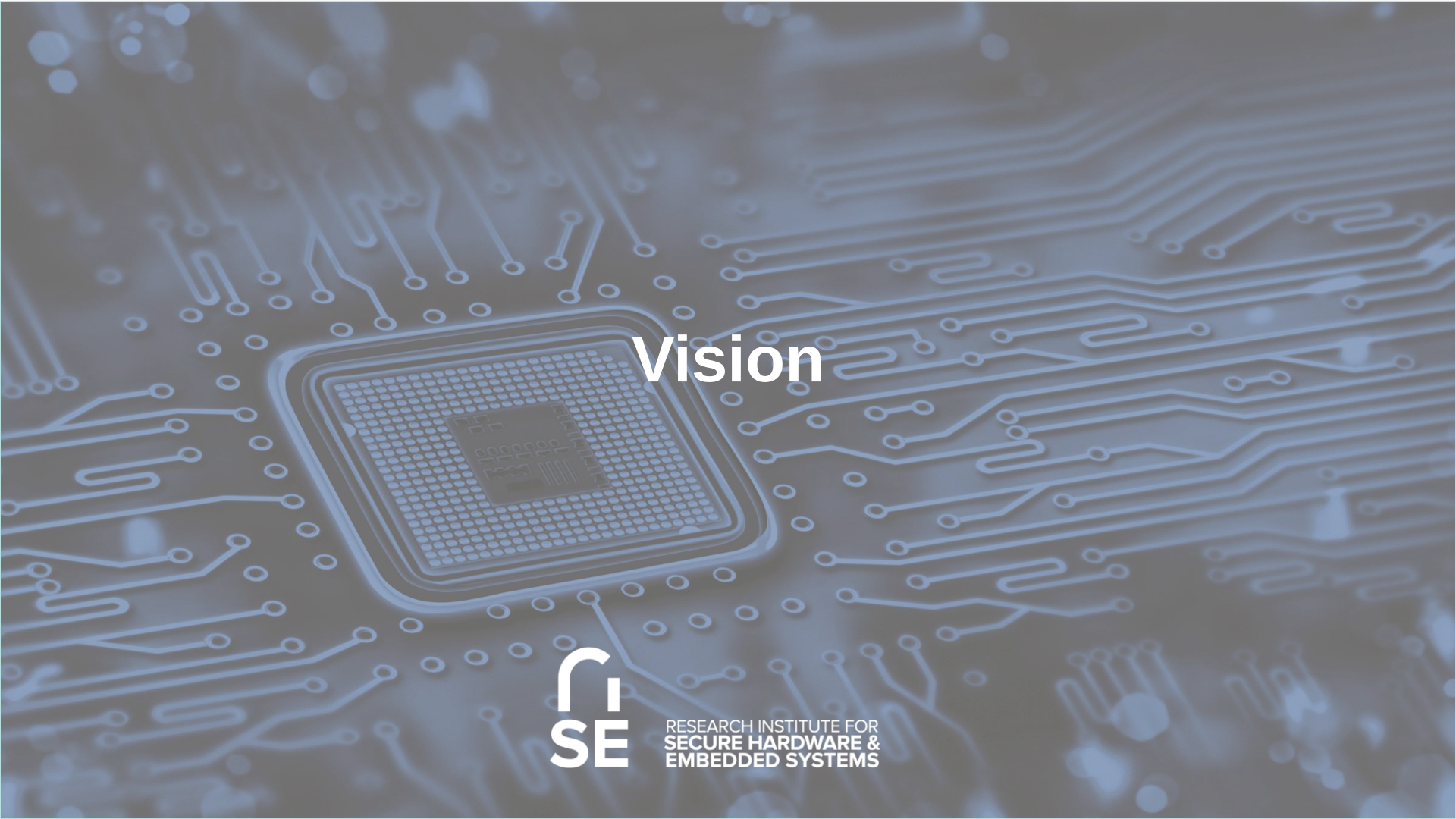
- ***Who*** (User ID): a trusted authenticator along with a TPM can use biometric or other info to attest a user ID but maintain user privacy
- ***What*** (Device ID): TPM can provide root of trust from system boot to identify a device's trust level.
- ***Where*** (Location): verify device location or user's presence
- ***When:*** time-limited attributes for automatic expiry
- ***How:*** read, write, print data access controls



© https://fidoalliance.org

Can we develop novel applications based on hardware roots of trust?

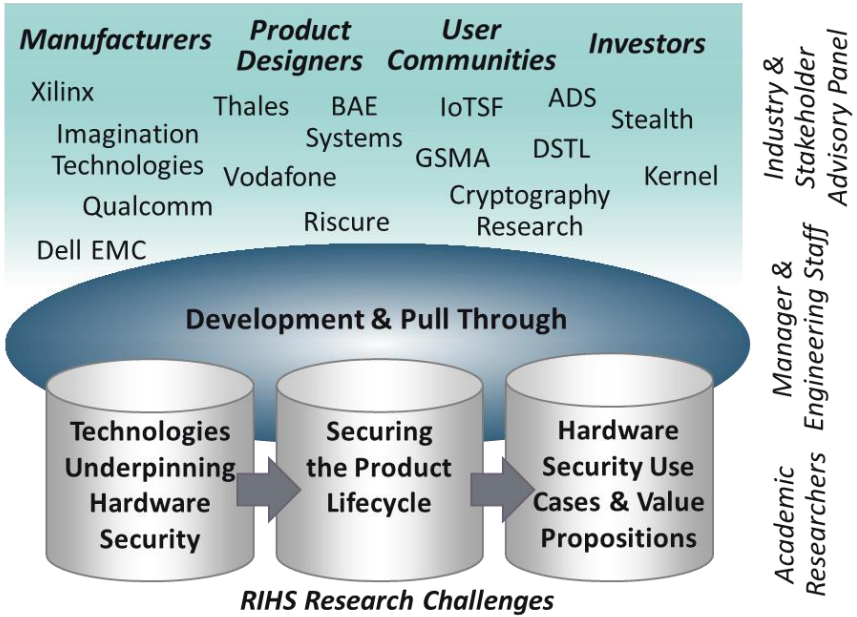
Vision



RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

RISE: Global centre for research & innovation in hardware security

- Close engagement with leading industry partners and stakeholders.
- ***Go-to* place for high quality hardware security research**
- Translation of research into new products, services and business opportunities for the benefit of the UK economy.
- A strong network of national & international collaborators & research project partnerships



RISE Research Challenges

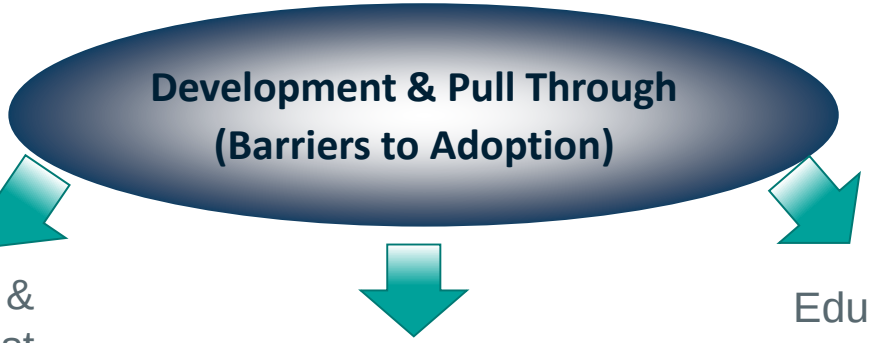
- State-of-the-art HW security primitives: TRNGs, PUFs
- Novel HW analysis toolsets & techniques
- Attack-resilient HW platforms, HW IP building blocks

- Confidence in Developing Secure HW Devices
- Supply Chain Confidence
- Modelling of HW Security

RISE Research Challenges

Hardware-based Security Services

- Novel Authentication, e.g. alternatives to passwords
- Secure document viewers
- Securing BYOD – attestation, roots of trust



Ease of Development & ease of leveraging best security option

Understanding Barriers to Adoption

Education of Potential User/Developer base

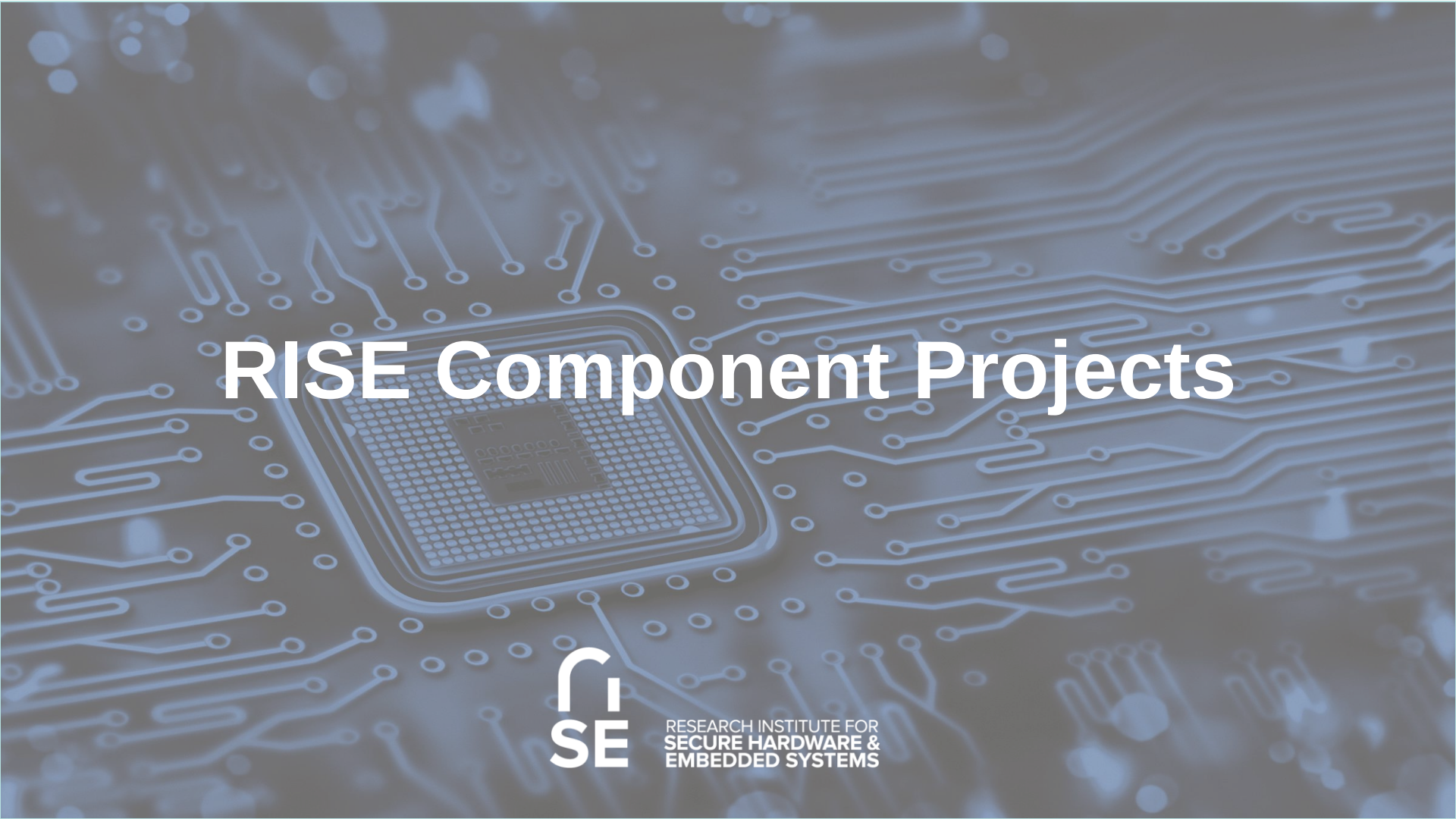
Component Research Projects

- Dr Daniel Page, University of Bristol
  SCARV: A Side-Channel Hardened RISC-V Platform

- Dr Robert Watson, Prof Simon Moore, Dr Athanasios Markettos, University of Cambridge
  IOSEC: Protection and Memory Safety for Input/Output Security

- Prof Mark Ryan, Dr Flavio Garcia, Dr David Oswald, University of Birmingham
  User-controlled hardware security anchors: evaluation and designs

- Prof Máire O'Neill, Queen's University Belfast
  DeepSecurity: Applying Deep Learning to Hardware Security


RISE Component Projects
RISE
RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

User-controlled hardware security anchors: evaluation and designs

Prof Mark Ryan, Dr Flavio Garcia, Dr David Oswald

UNIVERSITY OF BIRMINGHAM | Security and Privacy

Objectives:

1. To perform thorough security evaluations on a variety of hardware security anchors or enclaves being developed and marketed for user devices such as laptops and smartphones.
   Examples: Intel SGX, ARM TrustZone, platform security processors

2. To enhance those security mechanisms for user-centric applications. In particular, we address the challenges of user authentication in an device-rich IoT world.

3. To directly contribute to the security of tomorrow's COTS devices.

4. To provide convincing demonstrators of our mechanisms and use cases.

Industry Partners: HP Inc, Yubico

IOSEC: Protection and Memory Safety for Input/Output Security

Dr Robert N. M. Watson, Prof. Simon W. Moore, Dr A. Theo Markettos
Department of Computer Science and Technology
University of Cambridge
<firstname.lastname@cl.cam.ac.uk>

IOSEC Research objectives

Overall aim: To re-architect current computer input/output (I/O) systems with security as a first-class design constraint.

1. Build an **open source FPGA platform** to enable security evaluation of input/output (I/O) devices including pluggable devices like Thunderbolt 3 and USB-C.

2. **Evaluate current access control mechanisms** for a range of commodity hardware and operating systems for Thunderbolt 3 and USB-C.

3. Explore **current use of input/output memory management units** (IOMMUs) and their ability (or otherwise) to prevent attacks and their impact on performance.

IOSEC Research objectives

4. Explore **new message-based IO architectures** that avoid exposing memory to peripheral devices, thereby mitigating current security vulnerabilities while improving performance.
5. Explore **distributed memory protection technologies** that avoid the centralised bottleneck of the IOMMU.

Industry Partner: ARM Ltd

University of BRISTOL

SCARV: A Side-Channel hardened RISC-V platform

Dr Daniel Page

Objective

Overarching objective is to harness RISC-V to explore and provide an open, secure, flexible drop-in hardware platform for high-assurance use-cases.

Such a platform could form part of a wider, layered solution where security-aware design of hardware, software, and algorithms all play a role.

Collaborators

- Cerberus Security Laboratories
- Thales

Work Packages

1) Produce hardened implementations of the RISC-V design that can be deployed as a drop-in solution where side-channel resilience is an important design metric (e.g., smart-card, IoT, or cyber-physical systems)

2) Explore additions or alterations to the RISC-V design that will better equip it to support the current and next generation of crypto implementations

3) Deliver a platform that democratises side-channel evaluation by facilitating a "lab. free" (i.e., cloud-based) acquisition and analysis workflow

DeepSecurity: Applying Deep Learning to Hardware Security

Professor Máire O'Neill

Deep Security

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Overall Goal

To investigate the use of Deep Learning for security verification in EDA tools, specifically in relation to Hardware Trojan detection and Side channel analysis to allow non-security experts to receive feedback on how to improve the security of their designs prior to fabrication.

Industry Partners: Rambus, Riscure, BAE Systems

Deep Security: Research Objectives

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- Examine and compare the application of DL techniques in SCAs against both protected & unprotected crypto implementations on different platforms.
- Investigate attack/defender strategies in side channel analysis to, initially, increase the attack efficiency of deep-learning models, and subsequently improve side-channel resistant designs.
- Conduct the first comprehensive evaluation of the application of supervised and unsupervised ML and DL techniques in Hardware Trojan detection
- Evaluate how the approaches proposed for side channel analysis and Hardware Trojan detection could be utilised in a security verification framework in EDA tools, providing feedback to a designer

Next Steps

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

RISE - Next Steps

- **Open call for participation in Advisory Board**
  - Independent Chair: Charles Brookson
  - Member companies & stakeholders will have an opportunity to:
    - Engage with the research projects and gain early sight of project outputs.
    - Provide feedback on exploitation potential & offer commercialization opportunities.
    - Inform future calls related to the Institute's research challenges.

RISE - Next Steps

- **Events to bring together the Hardware Security community in the UK**
  - Spring School – 28-29 March 2018, University of Cambridge
- **Develop International linkages & research partnerships**
- **Further targeted project calls throughout lifetime of project**
  - Next call for proposals ~ Summer 2018

ukrise.org | info@ukrise.org | @UK_RISE