RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

RISE ANNUAL REPORT

MARCH 2018 – MARCH 2019

Funded by

in association with
National Cyber
Security Centre

EPSRC
Pioneering research
and skills

CONTENTS

DIRECTOR'S MESSAGE

I write to you some 18 months after the launch of the UK Research Institute in Secure Hardware and Embedded Systems (RISE), pleased to report on the progress made on behalf of each of the academic institutions involved. We are also delighted to have commenced four new research projects with the Universities of Cambridge, Edinburgh, Manchester and Surrey, stemming from our call in summer 2018.

The hardware encryption market is projected to reach 413.85 Billion USD by 2021. One of the major drivers behind this growth is the rise of the Internet of Things (IoT), which offers enormous business opportunities for virtually every market. This is presenting exciting opportunities for research, and new business and economic impact in hardware security. This Research Institute in hardware security is, therefore, timely and is in a strong position to make further and significant contributions in all of these aspects and to help position the UK in terms of its international research reputation as well as enhance its economic and business competitiveness in this field.

The demand for hardware security research and innovation is increasing with growing security needs in embedded and networking devices and cloud services. It is important to address security throughout a device's lifecycle, from the initial design through to its operational environment. A multi-layered approach to security is needed, establishing a trusted computing baseline that anchors trust in tamper-proof hardware. It is evident that a strong hardware security foundation is essential in realising secure systems (such as the IoT) and hardware-based security services.

During the time RISE has been operational, we have seen further developments in the regulatory landscape of IoT. Whereas 4 years ago, the discussion within industry was very much around self-regulation for IoT, there has since been progress on standardisation activities and further publications on codes of practice.

In late 2018, the Department for Digital, Culture, Media and Sport (DCMS) published a Code of Practice for Consumer IoT Security. ETSI (The European Telecommunications Standardisation Institute) launched their technical specification (TS 103 645) for Cyber Security for Consumer Internet of Things in February 2019, welcome news for consumers. During our engagements with companies, we emphasise the importance of the principles of secure by design/default from product inception. This engagement with industry will obviously continue and the ETSI technical specification and DCMS Code of Practice provide excellent reference points.

Looking forward, the Industrial Strategy Challenge Fund (ISCF) Digital Security by Design challenge aims to radically update the foundation of the UK's insecure digital computing infrastructure. The programme is being funded by ISCF to a total of £70 million, with matched funding of up to £117 million from industry.

This continued development in standardisation, regulatory framework and the funding landscape are very positive in supporting our mission at RISE. Through our research and innovation activities, we will continue to endeavour to make the hardware and embedded ecosystem more secure.

Professor Máire O'Neill, RISE Director
Queen's University Belfast

THE RESEARCH INSTITUTE IN SECURE HARDWARE AND EMBEDDED SYSTEMS

The £5M Research Institute for Secure Hardware and Embedded Systems (RISE), which is hosted at the Centre for Secure Information Technologies (CSIT), Queen's University Belfast, seeks to identify and address key issues that underpin our understanding of Hardware Security. Funded by the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC), RISE is one of four cyber security institutes in the UK and aims to be a global hub for research and innovation in hardware security over the next five years.

RISE aims to address the following research challenges in Hardware Security:

1. Understanding the technologies that underpin hardware security, the vulnerabilities in these technologies and development of countermeasures.
    - State-of-the-art Hardware Security primitives: True Random Number Generators (TRNGs), Physical Unclonable Functions (PUFs).
    - Novel Hardware analysis toolsets and techniques.
    - Attack-resilient Hardware platforms, Hardware IP building blocks.
2. Maintain confidence in security throughout the development process and product lifecycle.
    - Confidence in Developing Secure Hardware devices.
    - Supply Chain Confidence.
    - Modelling of Hardware Security.
3. Hardware security use cases and consideration of value propositions.
    - Novel Authentication, e.g. alternatives to passwords.
    - Secure document viewers.
    - Securing BYOD – attestation, roots of trust.
4. Development and pull through.
    - Ease of Development and ease of leveraging best security options.
    - Understanding Barriers to Adoption.
    - Education of Potential User/Developer base.

RISE PROJECTS

The research challenges of RISE will be delivered through a series of projects. Four projects were funded during the original proposal phase, commencing Nov 2017, and are led by the forming RISE research partners from Queen's University, the University of Cambridge, University of Bristol and University of Birmingham.

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

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

User-Controlled Hardware Security Anchors: Evaluation and Designs.
University of Birmingham, Prof Mark Ryan, Dr Flavio Garcia and Dr David Oswald.

Deep Security: Investigating the Application of Deep Learning in SCA and HT Detection, with the ultimate goal of utilising deep learning.
Queen's University Belfast, Prof Máire O'Neill.

A subsequent call for projects ran during May–Jul 2018, leading to the award of a second tranche of four projects to be delivered by the Universities of Cambridge, Edinburgh, Surrey and Manchester. Work commenced on these projects in Nov 2018.

SafeBet: Memory capabilities to enable safe, aggressive speculation in processors. University of Cambridge, Prof Simon Moore.

GUPT: A Hardware-Assisted Secure and Private Data Analytics Service.
University of Edinburgh, Dr Pramod Bhatotia and Dr Markulf Kohlweiss.

TimeTrust: Robust Timing via Hardware Roots of Trust and Non-standard Hardware, with Application to EMV Contactless Payments.
University of Surrey, Dr Ioana Boreanu, Dr Tom Chothia, Prof Liqun Chen.

rFAS: Reconfigurable FPGA Accelerator Sandboxing.
University of Manchester, Dr Dirk Koch.

THE RISE INSTITUTE MODEL

Fulfilling the aims of a global centre for research and innovation in hardware security requires not only world-class research, but also close engagement with leading UK-based industry partners and stakeholders. This additional focus facilitates the accelerated translation of research output into new products, services and business opportunities for the wider benefit of the UK economy.

The key elements within RISE are the academic researchers, an Industry & Stakeholder Advisory Board (ISAB) and the Institute Management team.

The RISE ISAB is chaired by Charles Brookson OBE, and has been created to allow member companies and stakeholders to engage with the research community and to inform funding calls around their real world challenges.

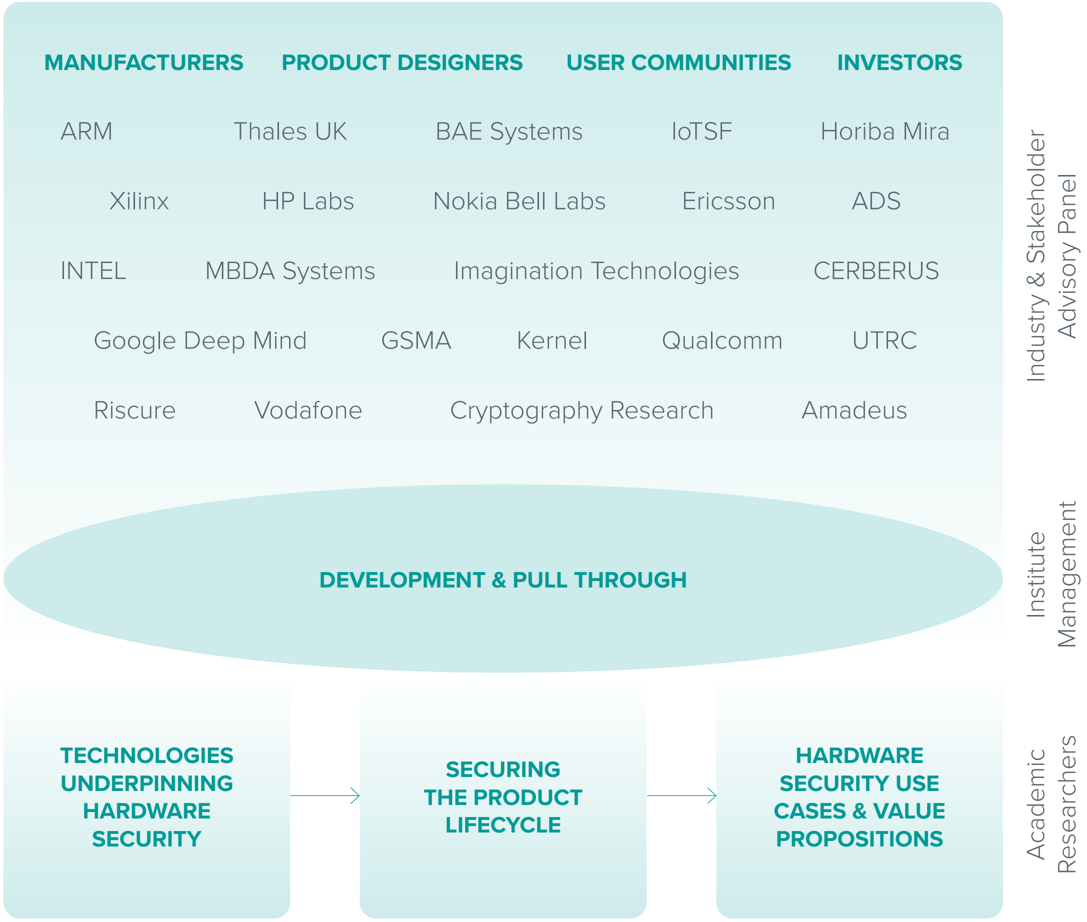
Other functions include:

- Receiving briefings on significant research outputs.
- Identification of research results, which are particularly appropriate for rapid commercialisation.
- Offer pathways to impact, e.g. licensing, spin-out support
- Highlighting shifts in technology or market demand with significance for RISE.
- Informing future RISE research proposal calls
- Helping to build a hardware security community in the UK

The Institute Management team, incorporating leadership and business development, functions to drive forward the development and promotion of the institute to industry and other stakeholders.

You can find out more about RISE and its activities by visiting www.ukrise.org

RISE ECOSYSTEM



MANUFACTURERS PRODUCT DESIGNERS USER COMMUNITIES INVESTORS

ARM Thales UK BAE Systems IoTSF Horiba Mira

Xilinx HP Labs Nokia Bell Labs Ericsson ADS

INTEL MBDA Systems Imagination Technologies CERBERUS

Google Deep Mind GSMA Kernel Qualcomm UTRC

Riscure Vodafone Cryptography Research Amadeus

DEVELOPMENT & PULL THROUGH

TECHNOLOGIES UNDERPINNING HARDWARE SECURITY → SECURING THE PRODUCT LIFECYCLE → HARDWARE SECURITY USE CASES & VALUE PROPOSITIONS

Industry & Stakeholder Advisory Panel

Institute Management

Academic Researchers

ACTIVITIES DURING THE PERIOD

From March 2018 – March 2019, RISE was represented at and present at a variety of events, including our own hosted events and shared learning initiatives. These included:

RISE SPRING SCHOOL 2018

This was our first hosted event and took place at the University of Cambridge, 28–29 March. It was a full program on both days, bringing together the hardware community, both academics and industry people.

RISE First Spring School Agenda Day One, 28 March

09.30 – 10.30	**Registration**
10:30 – 10:45	**Opening Remarks**
	Technologies Underpinning Hardware Security
10.45 – 11.25	Ahmad-Reza Sadegi, TU Darmstadt: Mind the Gap: Promises, Pitfalls and Opportunities of Hardware Assisted Security
11.25 – 12.05	Gang Qu, University of Maryland: Hardware based Lightweight Authentication for IoT Applications
12.05 – 12.45	Massimo Alioto, National University of Singapore: Perspectives on Hardware Security; embedding it everywhere, continuously and inexpensively
12.45 – 13.45	**Lunch**
13.45 – 14.25	Chongyan Gu, Queen's University Belfast: PUF: From Research to Practice
	Developing Secure Hardware Devices
14.25 – 15.05	Simon Moore, University of Cambridge: Winning the War on Memory
15.05 – 15.40	Break/Poster Sessions
15.40 – 16.20	Francesco Regazzoni, Universita della Svizzera Italiana (USI): Towards the Applications of Physical Attacks Countermeasures
16.20 – 16.35	Richard Grisenthwait, ARM: ARM's Perspective on the Importance of Hardware Security Research
19.00	**Dinner**

RISE First Spring School Agenda Day Two, 29 March

08.30 – 09.30	Registration
	Developing Secure Hardware Devices
09.30 – 10.10	Robert Watson, University of Cambridge: CHERI – Architectural Support for Memory Protection and Compartmentalisation
	Development and Pull Through
10.10 – 10.50	Andrea Höller, Infineon Technologies Austria: FIDO and the Future of Simpler and Stronger Authentication
10.50 – 11.40	Break
11:40 – 12:15	Louise Cushnahan, CSIT: Accelerating Innovation
12.15 – 12.50	Charles Brookson: Why, Who, How and Where of Standards
	Hardware Security Vulnerabilities
12.50 – 13.30	Marc Witteman, Riscure: How to use Deep Learning for Hardware Security Testing
13.30 – 14.30	Lunch
14.30 – 15.10	Dr Daniel Gruss, Graz University of Technology: Software-based Micro-architectural Attacks
15.10 – 16.00	Shivam Bhasin & David Berend, Nanyang Technical University of Singapore: Physical Attacks: Towards Combined Threat, Protection and Beyond
16.00	Closing Remarks

You can view the available videos at **www.ukrise.org/springschool/programme/**

CSIT SUMMIT 2018

Running on 9–10 May, Belfast 2018 was CSIT's 8th Annual World Cyber Security Summit. Part of the Summit's uniqueness is its bringing together the international research community alongside industry leaders, government policy makers and start-ups and SMEs from around the world. For researchers and technologists, the event focused on a future digital society and how to secure enabling systems and technologies. For the commercially minded, it represented an opportunity to learn from, and contribute to, the growth of new cyber security companies with global ambitions.

RISE Director Máire O'Neill gave a keynote at the CSIT Summit and acted as the academic lead on 2 panel discussions: "Device Authenication: An Industry perspective on the Importance of Hardware Security" and; "Device Authentication – Quantum-safe cryptography: a new era for information security".

CHES2018

RISE was a sponsor of the Conference on Cryptographic Hardware and Embedded Systems (CHES) which took place in Amsterdam, the Netherlands, over 4 days. Attended by around 600 delegates from across the world, CHES is a specialist conference and RISE received global profile with our collateral included in the delegate welcome packs. September 2018.

CHES 2018

RISE FIRST ANNUAL SUMMIT

This took place at Nova South in London in November 2018. The full day plenary program included two keynotes from distinguished industry speakers, Jo Van Bulck (KU Leuven) and Patrick Koeberl (Intel). Each of the 4 RISE projects gave updates to the audience of around 80 participants with a panel completing the line-up. Thank you to all speakers who took part and to all the Guests who attended.

RISE First Annual Summit Agenda

09:30 – 10:00	Registration
10:00 – 10:10	Welcome Prof. Máire O'Neill, Director, RISE, Queen's University Belfast
10:10 – 11:00	Keynote Jo Van Bulck, KU Leuven – "Leaky processors and the RISE of hardware-based trusted computing
11:00 – 11:45	RISE Core Project Updates
	Simon Moore, University of Cambridge – IOSEC: Protection and Memory Safety for Input/Output Security
	Dan Page, University of Bristol – SCARV: A Side-Channel Hardened RISC-V Platform
	David Oswald, University of Birmingham – User-Controlled Hardware Security Anchors: Evaluation and Designs
	Máire O'Neill, Queen's University Belfast – Deep Security: Applying Deep Learning to Hardware Security
11:45 – 12:05	Introduction to New Research Projects
	Dirk Koch, University of Manchester- rFAS – reconfigurable FPGA accelerator Sandboxing
	Simon Moore, University of Cambridge – Safebet | Memory capabilities to enable safe, aggressive speculation in processors
	Pramod Bhatotia, University of Edinburgh – GUPT: A Hardware-Assisted Secure and Private Data Analytics Service
12:05 – 12:50	Lightning Talks – Early Career Researchers
	Sujoy Sinha Roy, University of Birmingham – Hardware implementation of post-quantum PKC and homomorphic encryption
	Franck Courbon, University of Cambridge – Partial hardware reverse engineering for combined attacks and authenticity verification
	Vasileios Mavroudis, University College London – Cryptographic Hardware from Untrusted Components
	Jorden Whitefield, University of Surrey – Formal Analysis and Applications of Direct Autonomous Attestation
	Elif Kavun, University of Sheffield – Resource-efficient Cryptography against Physical Attacks
	Ayesha Khalid, Queen's University Belfast – Handling the side channel vulnerabilities for Lattice based cryptography
12:50 – 14:10	Lunch/Poster Session/Networking
14:10 – 15:00	Keynote Patrick Koeberl, Principal Engineer, Security and Privacy Research, Intel Labs – Vehicle to Cloud: Security Research Challenges for Intelligent Vehicles
15:00 – 15:45	Industry Panel Session Future Research & Innovation Challenges in Hardware Security Chair: Charles Brookson Panel: • Ilhan Gurel, Expert, HW & SW Security, Ericsson • Alex van Someren, Amadeus • Madeline Cheah, Cyber Security Innovation lead, Horiba-Mira • Bob Edge, Technical Director, Cyber 1st
15:45	Close

Please visit the RISE website where you can view the presentations where we have consent to share them online: **www.ukrise.org/rise-2018-annual-conference/**

RISE Summit 2018 opening keynote, Jo Van Bulck, KU Leuven

Industry Panel Session
Future Research & Innovation Challenges in Hardware Security
EPSRC

RISE Summit 2018 Industry Panel: (L-R) Charles Brookson, Ilhan Gurel (Ericsson), Madeline Cheah (Horiba-Mira), Alex Van Someren (Amadeus) & Bob Edge (Cyber 1st)

RISE Summit Keynote speaker, Patrick Koeberl, Intel Labs Europe discussing security research challenges for intelligent vehicles

NEW RESEARCH PROJECTS

The call for new Research Proposals was made in 2018 with the aim of expanding the RISE research community. Funding from NCSC was made available for proposals of up to £300k per project for 4 new research projects. The Universities of Surrey, Edinburgh, Manchester and Cambridge were all successful in securing the funding. Further details on these new projects can be found later in the report.

SPRING SCHOOL 2019

A 2-day event hosted at ECIT in Belfast with the aim of bringing together the hardware security community, from academia to industry and the second time RISE had run this. Themes that were covered included Technologies Underpinning Hardware Security, Building Supply Chain confidence and Attack Resilient Hardware Platforms. February 2019.

Spring School 2019 Agenda Day One, 28 February

09:30 – 10:30	Registration
10:30 – 10:40	Opening Comments
	Session 1: Importance of Hardware Security
10:40 – 11:20	Martin Dixon, Intel: Opportunities in Hardware Security Research
11:20 – 12:00	Joe Fitzpatrick, SecuringHardware: Millions for Defence, not one cent for security
12:00 – 12:40	NCSC view of Hardware Security Research
12:40 – 13:50	Lunch
	Session 2: Developing Secure Hardware Devices
13:50 – 14:30	Ingrid Verbauwhede, KU Leuven: Design methods for hardware roots of trust
14:30 – 15:10	Samuel Pagliarini, Carnegie Mellon University: Can we build a trustworthy Billion Transistor chip?
12:05 – 12:50	Lightning Talks – Early Career Researchers
12:40 – 13:50	Break
	Session 3: Hardware Security Evaluation
15:40 – 16:20	Emanuel Prouff, ANSSI: Deep Learning for Embedded Security Evaluation
16:20 – 17:00	Sylvain Guilley, Secure-IC & Telecom-ParisTech: Direction of cache-timing attacks on cryptographic libraries, including post-quantum cryptography
19:00	Dinner at Titanic Hotel

Spring School 2019 Agenda Day Two, 1 March

08:30 – 10:00	Registration
09:00 – 10:00	Tutorial Ilhan Gurel, Expert Hardware and Software Security, Ericsson: End to End IoT Security
	Session 4: Development & Pull Through of HW Security Technologies
10:00 – 10:50	Shahram Mossayebi, Crypto Quantique Securing Connected Devices: Story of a deep-tech cybersecurity start-up in the UK
10:50 – 11:30	Jayne Brady, Kernal Capital: Challenges with Commercialisation of Early Stage Deep Tech
11:30 – 12:00	Break
12:00 – 12:40	Dimitrios Schionianakis, Nokia Bell Labs: Challenges of Homomorphic Encryption
12:40 – 13:20	Ayesha Khalid, Queen's University Belfast: Physical protection of Lattice-Based cryptography – Challenges and Solutions
13:20 – 14:30	Lunch
14:30 – 15:10	David Oswald, University of Birmingham: Trusted Execution in Practice – a gentle guide
15:10 – 15:50	Simon Moore, University of Cambridge: Thunderclap – Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals
15:50 – 16:30	Dirk Koch, University of Manchester: FPGA acceleration a boon or bane?
16.30	Closing Remarks

You can view the talks at **www.ukrise.org/springschool2019/programme/**

RISE HARDWARE SECURITY TRAINING

Courses for PHD Students, Post Docs and Early Career Researchers (ECRs) who were associated with RISE-funded research projects. RISE paid for training for 3 sets of 15 people over the week long course at three locations.

The courses took place in:

- Belfast at ECIT
- The University of Edinburgh and;
- The University of Surrey between February and March 2019.

The course was convened by Joe Fitzpatrick from securinghardware.com and covered these 2 main areas:

- Applied Physical Attacks on Embedded and IoT Systems and;
- Applied Physical Attacks and Hardware Pen-testing.

SECURINGHARDWARE.COM

CORE PROJECTS PROGRESS REPORTS

A set of four core projects commenced in November 2017, delivered by the forming partners of RISE. Below is a summary of the projects, including an overview of their aims and progress updates.

SCARV: A Side-Channel Hardened RISC-V Platform

Background to Research

RISC-V is an Instruction Set Architecture (ISA) design. An ISA is essentially a specification for the instructions any compatible processor implementation should be able to execute, and the resources those instructions can access; it acts as the interface between the processor implementation (hardware) and programs that execute on it (software). In sharp contrast with proprietary analogues such as the x86 ISA from Intel, RISC-V is an open source design. This means it can be used freely by anyone for any purpose, which, in part, has meant rapid development of a rich support infrastructure around the project: this includes a) vibrant developer and user communities, built around an associated non-profit foundation, b) numerous implementations of the ISA, both in HDL (i.e., a soft core for use on an FPGA platform) and silicon (i.e., physical ICs), and c) ports of programming tool-chains (e.g., GCC and LLVM) and operating systems (e.g., Linux).

Similar openness is a core principle in security-critical contexts, contrasting with the alternative often colloquially termed "security by obscurity". This is particularly true in the field of cryptography, a technology routinely tasked with ensuring secrecy, robustness and provenience of our data (communicated or stored), and the authenticity of parties we interact with: open development of cryptographic standards, designs, and implementations is the modern norm. As a result, RISC-V presents various opportunities when used to execute cryptographic software. The proposed research goals capitalise on these opportunities, in a way designed to address advanced, persistent threats to our digital security, and, by extension, society. Specifically:

1) Since RISC-V can be implemented by anyone, it is possible to develop a core hardened against specific types of attack; the focus will be on the threat of side-channel attacks (which is particularly relevant to embedded use-cases, e.g., IoT). As well as doing so, the proposed research will investigation how detailed information about the implementation can be harnessed to produce more effective security evaluations.

2) Since RISC-V can be adapted by anyone, it is possible to develop various cryptography-specific extensions or variants of the ISA that offer either, for example, higher efficiency. If cryptographic software is more efficient it can also be more secure, because, for example, larger keys or more robust attack countermeasures can be deployed without as significant an impact on latency.

3) Evaluation of side-channel security can be prohibitive in the sense it needs various specific items of equipment. Harnessing a platform based on RISC-V, the proposed research with address this problem by offering a "lab. free" (i.e., cloud-based) acquisition and analysis workflow available to anyone.

Proposed Research

WP-A: Produce hardened implementations of the RICS-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.

WP-B: Explore additions or alterations to the RISC-V design that will better equip it to support the current and next generations of crypto implementations.

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

Publications

- 11/18: Released XCrypto
- 03/19: B. Marshall
  On Hardware Verification in an Open Source Context.
  Workshop on Open Source Design Automation (OSDA), 2019.

Related Engagement Activities

- Attended Bristol RISC-V meet-up – October 2018
- RISE Annual Summit – 14 November 2018
- Presented at BSC event on open source security – February 2019
- RISE Spring School 28 February – 1 March 2019
- Attended RISE hardware security training event 28 February – 1 March 2019

Outputs and Activities

- Program (Co-)Chair for (T)CHES 2018 (Dan Page) – September 2018

University of BRISTOL

IOSEC: Protection and Memory Safety for Input/Output Security

Project Overview

We wish to re-architect current computer input/output (I/O) systems with security as a first-class design constraint. Existing I/O has evolved organically over the decades and now faces a 'perfect storm' of security vulnerabilities, which we aim to address.

Computers today are full of processors: advertised, hidden and even unintentional. Processors, in the form of embedded microcontrollers, are hidden in 'devices' that we name as 'wireless card' or 'system management controller', but fundamentally they form a heterogenous distributed system. The software these processors run is often poorly scrutinised and may be actively malicious. As this field becomes more visible, vulnerabilities are being discovered with increasing frequency.

Worse still, the trend is for 'pluggable' devices via interfaces such as USB Type-C and Thunderbolt 3: users are being trained to pick up processors, thinking they are innocuous because they are shaped like chargers or dongles. For instance, many buildings, aircraft, trains and buses now provide 'USB charging', but, without protection, the Type-C user may be exposing themselves to unexpected threats. Such threats are of substantial and increasing concern to businesses, government and consumers. By redesigning I/O with security at the core, we aim to considerably improve on today's weaknesses. We will investigate the weaknesses of current I/O and propose safer alternatives through three threads of research:

1. We will begin by performing a survey of the state-of-the-art of access-control protections in current hardware and software designs, to understand the limits of current pluggable-device security. We will focus in particular on current utilisation of Input/Output Memory Management Units (IOMMUs), which are the primary current defence that prevents devices from having unlimited Direct Memory Access (DMA) - the 'key to the kingdom' of system security that otherwise permits total compromise of firmware, OS, and applications from malicious devices. We will characterise current security-performance tradeoffs to establish a performance baseline. We will systemise new vulnerability classes and develop a corpus of vector-specific attack techniques which future defences must prevent or mitigate.

Our existing preliminary results investigating IOMMU use in modern operating systems, and a growing attack literature, suggest substantial security and performance shortcomings. We therefore propose two strands of research to develop and evaluate technical approaches to defend against I/O-based attackers:

2. Many I/O devices (e.g., USB and network cards) communicate with the host operating system through messages sent and received via DMA. We will develop new techniques to restructure CPU-to-I/O interconnects to provide a message-based abstraction for untrustworthy devices, rather than depending on DMA, as is current (and highly vulnerable) best practice.

3. To address devices for which a memory-oriented semantic is intrinsic (e.g., GPUs and Remote-DMA enabled network cards), we will explore new distributed-memory protection techniques that avoid the granularity and performance limitations of IOMMU-oriented approaches. This will enable greater control of device access to host memory while improving security-performance tradeoffs. For instance we might delegate specific memory access rights to devices, with policy and unforgeability enforced by the interconnect bridges.

All research will be performed via hardware-software co-design methodology and FPGA prototyping, with evaluation relative to performance, complexity, compatibility, and security metrics for both hardware and software. We will pursue these goals in close collaboration with ARM Ltd, who provide key insights into industry requirements and a transition path into commercial technologies.

Publications

- Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals. A. Theodore Markettos, Colin Rothwell, Brett F. Gutstein, Allison Pearce, Peter G. Neumann, Simon W. Moore, and Robert N. M. Watson. Proceedings of the Network and Distributed Systems Security Symposium (NDSS), 24–27 February 2019, San Diego, USA.

Related Engagement Activities

- RISE Annual Summit – 14 November 2018
- RISE Spring School 28 February – 1 March 2019

Outputs and Activities

The media pick-up on Thunderclap and IOMMU:

- UK tech website, The Register: https://www.theregister.co.uk/2019/02/26/thunderclap_hacking_devices/
- And Naked Scientist (which is carried in audio form by the BBC and others): https://www.thenakedscientists.com/articles/science-news/laptop-cables-grant-hackers-access

UNIVERSITY OF CAMBRIDGE

User-Controlled Hardware Security Anchors: Evaluation and Designs

Project Overview

Many modern processors are equipped with hardware extensions that enable some kind of Trusted Execution Environment (TEE). This allows programs to run securely - protected from other programs or operating system software running on the processor. By establishing a secure interface between the user and the hardware-anchor, we can make user platforms and devices more resilient to malware and other types of cyber attacks.

One of the main goals of this project is to promote and facilitate the adoption of TEE as the main trust anchor for our security architectures. As such, the security of the TEEs themselves is of paramount importance. We will perform a thorough evaluation of the security features of different TEE implementations to determine their suitability as trust anchors. This includes assessing cryptographic protocols, side-channel vulnerabilities, and implementation weaknesses.

Hardware supported TEEs aim to ensure that code can execute securely. However, user interface devices (for example, a keyboard, display or touch screen) are usually not connected directly to the secure hardware, which means that the user cannot interact securely with the TEE. We will address the limitations of users interacting directly with TEEs through analysing use cases and developing secure interfaces using auxiliary devices and dedicated features.

Authentication today is largely based on user-supplied information like passwords or biometrics. These approaches often use information that is easy to steal or brute force. The industry has been moving towards multi-factor authentication as a means of spreading risk, but these approaches impose usability challenges while still relying on weak factors. We will investigate opportunities to leverage strong hardware-based security mechanisms to improve both the strength and usability of authentication. We will also build an architecture for designing protocols and user experiences that leverage these hardware security primitives to enhance the security, manageability, and usability of user authentication over existing approaches.

The analysis and applications of our research findings will be demonstrated and implemented on suitable platforms including secure hardware, smart devices and integration with authentication tokens.

Overall Goals

- 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.
- To enhance those mechanisms for user-centric applications. In particular, we address the challenges in a device rich IoT world.

Publications

- IFAL: Issue First Activate Later Certificates for V2X Eric Verheul (Radboud University); Christopher Hicks and Flavio D. Garcia. In proceedings of 4th IEEE European Symposium on Security and Privacy (Euro S&P). To appear.
- Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars Lennert Wouters (KU Leuven), Eduard Marin, Tomer Ashur (KU Leuven), Benedikt Gierlichs (KU Leuven) and Bart Preneel (KU Leuven). In proceedings of Transactions on Cryptographic Hardware and Embedded Systems (TCHES). To appear.

Related Engagement Activities

- RISE Annual Summit – 14 November 2018
- RISE Spring School 28 February – 1 March 2019
- Attended RISE hardware security training event 28 February – 1 March 2019
- Delegation met with Hewlett Packard March 2019 to discuss possible collaborations.

Outputs and Activities

- Our ongoing work has resulted in the identification of several memory corruption security vulnerabilities in various trusted execution environments (TEEs). Microsoft has acknowledged one of our security vulnerabilities and has assigned a CVE to it (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0876).
- Flavio D. Garcia. Invited talk 'Beneath the Bonnet: A Breakdown of Diagnostic Security' at CRYPTACUS'18 conference, Rennes, France (September 2018).
- Flavio D. Garcia. Invited talk 'Automotive Security, the Bad and the Ugly' at EU policy-makers awareness meeting, Brussels (November 2018).

UNIVERSITY OF BIRMINGHAM

Deep Security to investigate the application of deep learning in SCA and HT detection, with the ultimate goal of utilising deep learning.

Overall Goal
With the globalisation of supply chains the design and manufacture of today's electronic devices are now distributed worldwide, for example, through the use of overseas foundries, third party intellectual property (IP) and third party test facilities. Many different untrusted entities may be involved in the design and assembly phases and therefore, it is becoming increasingly difficult to ensure the integrity and authenticity of devices. The supply chain is now considered susceptible to a range of hardware-based threats, including hardware Trojans, IP piracy, integrated circuit (IC) overproduction or recycling, reverse engineering, IC cloning and side-channel attacks. These attacks are major security threats to military, medical, government, transportation, and other critical and embedded systems applications. The proposed project will use a common approach to investigate two of these threats, namely the use of deep-learning in the context of side-channel attacks and hardware Trojans.

Side-channel attacks (SCAs) exploit physical signal leakages, such as power consumption, electromagnetic emanations or timing characteristics, from cryptographic implementations, and have become a serious security concern with many practical real-world demonstrations, such as secret key recovery from the Mifare DESFire smart card used in public transport ticketing applications and from encrypted bitstreams on Xilinx Virtex-4/5 FPGAs. A hardware Trojan (HT) is a malicious modification of a circuit in order to control, modify, disable, monitor or affect the operation of the circuit. Although there have been no public reports of HTs detected in practice, in 2008 it was speculated that a critical failure in a Syrian radar may have been intentionally triggered via a hidden 'back door' inside a commercial off-the-shelf (COTS) microprocessor.

The proposed project seeks to investigate the application of deep learning in SCA and HT detection, with the ultimate goal of utilising deep learning based verification processes in Electronic Design Automation tools to provide feedback to designers on the security of their designs. In relation to the call, the project addresses the challenge of 'maintaining confidence in security through the development process', and more specifically 'building supply chain confidence' and 'novel hardware analysis toolsets and techniques'.

Publications
None.

Related Engagement Activities
- RISE Annual Summit – 14 November 2018
- Spring School 28 February – 1 March 2019
- Attended RISE hardware security training event 28 February – 1 March 2019

Outputs and Activities
- RISE PI, Prof Maire O'Neill was a prize-winner at the prestigious Blavatnik Awards, which honours outstanding young scientists. Prof O'Neill was awarded the funds due to her world-class reputation for research and invention in the field of hardware security, in particular for her work developing attack-resilient computer hardware platforms and chip designs. January 2019.
- The Irish Times also listed Prof O'Neill in their distinguished "50 people to watch in 2019: Ireland's hottest young talent".

QUEEN'S
UNIVERSITY
BELFAST

TRANCHE 2 RESEARCH PROJECTS

A call was made between May-Jul 2018 to fund a further set of projects, covering the following areas;

a. Micro-Architectural and Analogue Security Evaluation
The recent software-based analogue attacks on digital technologies (e.g., RowHammer) and micro-architectural attacks (e.g., Spectre and Meltdown), and their impact on the microelectronics industry has highlighted the need for further research on securing microprocessor architectures. Under this theme, the following topics may be considered:

- Investigating software-based analogue and micro-architectural vulnerabilities from multiple attack vectors.
- Evaluation of novel countermeasures against software-based analogue and micro-architectural attacks.
- Development of software- based attack-resilient hardware platforms.

b. Automated Security Verification in EDA tools and Software Tool Chains
Electronic Design Automation (EDA) tools and software tool chains mainly focus on evaluating and verifying functional correctness and performance. As implementation attacks are now a key concern, particularly for hardware and embedded systems designers, automated security verification approaches are needed. Under this theme research projects should consider:

- Automated physical attack vulnerability identification, e.g. side channel vulnerabilities.
- Integration of security assessment of designs and their implementations into tool flows.
- Automated validation of countermeasures and a cost benefit analysis of the security within the design and implementation.

c. Supply Chain Security
The supply chain is considered susceptible to a range of hardware-based threats, including hardware Trojans, IP piracy, IC overproduction, reverse engineering, IC cloning, etc, but also software-based threats like unreliable data, unauthorized manipulation of software products and unsolicited product descriptions. In addition, complex devices now contain a combination of both IP and software elements, with the possibility that sensitive information may be leaked between these different elements. This theme seeks:

- Novel approaches to providing supply chain confidence throughout the development process and product life-cycle
- Consideration of provisioning or generating cryptographic keys on devices during manufacturing
- Novel approaches that allow a complex device comprising different elements of software/IP to be confirmed as 'authentic'.
- Novel approaches that necessitate devices to be enabled in their final environment, such that they are unusable in the raw.

d. Hardware-Based Security Services
With the continual growth in the abundance of data available from IoT devices and cloud usage, the need for effective data-centric security approaches is becoming critical. Achieving data centric security requires a marriage of data and identity. Solutions that use advanced cryptographic techniques (for e.g. identity- or attribute- based encryption) combined with trusted hardware, such as a TPM/TEE or HSM, could allow sticky policies (e.g. related to security levels or location) to be created for protecting and managing data, offering hardware-based security services with data-centric security. Research challenges under this theme include:

- Novel approaches to using trusted hardware to provide data-centric security.
- Novel applications of hardware-based security services, e.g., the novel application of software-based HSMs (e.g. vTPM) to develop scalable and secure key management services.
- Easy-to-use attestation protocols and services, e.g., novel approaches that allow guests to attest their data in a cloud environment.
- Post-quantum secure hardware roots of trust and hardware cryptographic modules.

As a result of the evaluation process, a further four projects were awarded to the University of Cambridge, University of Edinburgh, University of Surrey and the University of Manchester, as follows;

SafeBet: Memory Capabilities to enable Safe, Aggressive Speculation in Processors

Overall Goal

We wish to explore the promising approach of capability-based protection on the micro-architectural speculation of complex out-of-order cores to mitigate new speculative side-channel attacks similar to Spectre. To evaluate the work, we will establish a specification framework to describe safe speculation in a microarchitecture, and a verification framework to explore the speculative abilities of processor cores.

The Spectre family of vulnerabilities has recently exposed micro-architectural speculation as a rich source of information about protected state in the computer system. Early pipelined processors needed to begin execution of instructions before the correct path of execution was known, and thus designers introduced the ability to speculatively execute potentially illegal code paths, backtracking to the correct path if a mistake was discovered. Today's complex processors can speculatively travel hundreds of instructions through multiple branch points before realising that a wrong turn was made and dropping all results from the incorrect paths. While the actual values produced in these paths are carefully discarded to preserve the illusion of only following the correct path, it is possible for a program to observe shadows of these alternate paths through the timing of execution, especially cache response times. The vast majority of information exposed in these alternate paths are otherwise available to the observing program, but clever attackers can influence speculation to expose information forbidden by the security model of the system.

We have previously developed CHERI capabilities [12, 10] which tie bounds atomically to every pointer, and these bounds are asserted on each memory access. Capabilities point to data and code, allowing efficient compartmentalisation (sandboxing) of code and providing control-flow robustness. Our initial analysis (see technical report [11]) indicates that CHERI capabilities may be able to help mitigate Spectre-like attacks by preventing misspeculation of bounds checks. As capabilities are tagged and are easily identified by the microarchitecture, CHERI capabilities can also enable safe data value prediction while preventing potentially unsafe speculation of capability pointer values, including unsafe arithmetic on speculative data values with capabilities. Moreover, given the fine-grained compartmentalisation model, it may be feasible for a CHERI core supporting aggressive speculation to guarantee that the microarchitecture will never initiate a memory access that is outside of the set of segments legally delegated to the running process, preserving compartmentalisation guarantees even in speculation. Thus, with suitable extensions, a refined CHERI microarchitecture may allow safe speculation while preventing unsafe speculation. This may both save power by eliminating incorrect speculation, and also make the microarchitecture safe from classes of Spectre attacks. While we have begun to consider these directions, this proposed project would allow us to validate these hypotheses on a superscalar processor design, providing to the community the detailed insights that accompany implementation and careful evaluation.

In order to progress with a clear methodology to validate this intuition, we propose developing a simple specification for safe speculation in a processor core. The specification may be composed of rules in the following form:

- No speculative memory access causes a cache miss if its address is illegal in the current context.
- Branch predictions must only be based on state derived from that instruction.
- Dereference of speculated capability pointers is not allowed.

We propose to implement a trace-based verification tool for this speculation specification which observes the execution of an out-of-order core to assert that its speculative paths fit a legal speculative execution and did not, for example, load data unavailable to the current context or jump to an address not previously observed as a target of the predicted branch. Our tool could both observe execution when running a large code base, and could also generate tortuous sequences known to cause misspeculation in out-of-order cores.

We plan to apply this speculation verification tool to recently-available open-source out-of-order RISC-V cores to both expose each known variant of Spectre, and to guide our exploration of micro-architectural mitigations. We expect CHERI extensions to these cores will provide very strong and fine-grained protections without limiting aggressive speculation in the common case, but we would also implement best-effort mitigations without CHERI to identify the complexity and performance cost of techniques applied to legacy instruction sets.

UNIVERSITY OF CAMBRIDGE

GUPT: A Hardware-Assisted Secure and Private Data Analytics Service

Overall Goal

In the digital age, we increasingly rely on cyber-physical systems and online services based on "data-driven intelligence". Such applications require four important design properties: reliability, real-time performance, scalability, and security & privacy. The state-of-the-art for designing, developing, and deploying such applications follow ad hoc practices, where application programmers explicitly manage computational resources and application state on a per application basis. However, such adhoc practices easily become unmanageable because the underlying computing infrastructure composed of cloud, edge, and IoT computing resources is heterogeneous, and comes with varying degree of performance, cost, reliability, and security & privacy guarantees. Our proposal aims to build an end-to-end system supporting the design, development and deployment of a wide range of data-driven intelligent applications. The application developers, including machine learning experts, data scientists and privacy and ethics experts, focus on their core business logic/algorithms/expertise, and our system transparently provides the aforementioned four design properties.

Research Proposal Overview

The rise of data-driven intelligent applications. Our research proposal is motivated by three important trends from the last decade:

- The deluge of big data, where we are seeing increasingly large amounts of data is being collected and processed in computing;
- The advancements in hardware across all layers of the system stack, including computing, networking, and storage; and lastly;
- The advancement in research for machine learning, computing vision and artificial intelligence. Together these three trends are enabling a wide-range of intelligent applications that are based on data-driven learning [26]. These intelligent applications are increasingly becoming the cornerstone of cyber-physical systems [9,14,23]; prominent examples include robotics based workflows, automotive industry, UAV drones, virtual reality, healthcare, consumer devices, but also surveillance and advertisement.

As these applications become an integral part of our daily lives, we have to ask the uncomfortable question: Are these intelligent applications really trustworthy? It turns out that building intelligent applications on which we can rely on is very challenging! When building such applications an application programmer such as a machine learning expert or a data scientist, not only has to get the core of the application logic correct, but also needs to ensure that the system as a whole meets the following four key design properties to make the application trustworthy in practical settings:

- Scalability: These applications should be able to support millions of active (mobile/stationary) users.
- Reliability: Cyber-physical systems, in general, require a very high degree of reliability guarantees because failures/ unavailability can have dire consequences.
- Security & Privacy: Since these applications process (often private) data in the cyber-physical ecosystem, they require strong confidentiality and integrity guarantees for the execution.
- Performance: Lastly, these applications need to be high performant since they operate in low-latency environments requiring predictable performance.

Research Objectives

In this work, we strive to answer the following question:
How to write scalable, fault-tolerant, secure & private data-driven intelligent applications for real-time analytics in a heterogeneous parallel and distributed infrastructure?

Design Overview

Our work aims to build a general distributed computing platform to design, develop and deploy a wide range of data-driven intelligent applications. The overarching goal is to enable application developers (such as a data scientist or a machine learning expert, etc.) to solely focus on their application logic without requiring to manage the underlying computing infrastructure and other key design properties. The developer builds her application using our programming framework. In addition, the developer would provide a set of design requirements. These design requirements consist of the reliability, performance (latency/throughput), scalability and security & privacy guarantees required by the application. Thereafter, our system transparently enforces these design requirements!

THE UNIVERSITY of EDINBURGH

TimeTrust: Robust Timing via Hardware Roots of Trust and Non-standard Hardware – with Application to EMV Contactless Payments

Overall Goal

TimeTrust will deliver a step-change in the provision the security, accountability and trust in wireless and especially contactless systems. Such applications are clearly ubiquitous: we use contactless bankcards to make electronic payments every day, whilst passive-keyless-entry fobs open and even start our modern cars as we approach them, without our inputs. However, all these wireless or contactless applications are particularly vulnerable to man-in-the-middle attacks stemming from relaying. In a relay-attack, one piece of fraudulent equipment is placed near the victim (and their authentication device) and it relays signals from the victim's device to a second piece of rogue equipment found near the contactless payment-terminal, the car, or the door-lock, etc. This has already become a common technique for car-theft.

Impact & Timeliness of TimeTrust. The academic team has compound expertise, of world-class level, in all TimeTrust's ingredients: proximity-based primitives, HW-RoT, security analysis and EMV. Our outputs will be wide-reaching, from proximity-based services in 5G (5th Generation Mobile Networks) to ubiquitous contactless payments by EMV, and beyond.

Project Updates

- We had a paper accepted at Financial Crypto 2019 on one of the main topics of TimeTrust. The proceedings will be out soon.

  The paper addresses the issue of rogue contactless EMV (Europay Mastercard Visa) payment-terminals taking part in relay attacks when in fact they should detect and stop these. We call this type of vulnerability "collusive relaying". We show three novel proximity-checking protocols that protect contactless EMV payments against collusive relaying. They are hierarchical with respect to the protection level, but also w.r.t. the level of change required for them to be adopted on top of the ubiquitous EMV infrastructure for e-payments.

- With Consult Hyperion (partner in TimeTrust), we are building a proof-of-concept implementation of the EMV designs in this paper. This should be ready by the end of July.

- We had our first meeting with the Strategic Advisory Board (Visa, Mastercard, ConsultHyperion, HP) in May 2019, and the Financial Crypto 2019 designs that suggest modifications to the current Mastercard version of EMV with relay protection was reasonably received by Mastercard.

rFAS: Reconfigurable FPGA Accelerator Sandboxing

Overall Goal

In the rFAS - reconfigurable FPGA Accelerator Sandboxing project we will develop and test methods to run partially reconfigurable modules, which could be considered as dynamic hardware plugins, in a secure and encapsulated environment such that they cannot leak information from other parts of a system or compromise the integrity of the system. This will be achieved through traditional techniques such as; memory protection mechanisms on the address spaces used by the accelerator modules; as well as through a new configuration management unit that ensures encapsulation of partial modules into allocated resources and a bitstream analysis tool (similar to a virus scanner known from software systems). This detects malicious sections in FPGA configuration binaries to prevent short circuit configurations that may damage an FPGA, hinder modules accessing wires from other parts of the system, and detect other critical section in the configuration bitstream. With this, rFAS will, for the first time, add an infrastructure to the FPGA ecosystem, which guarantees trustworthy integration and execution of reconfigurable hardware modules on FPGAs, which are one of the most favourable technologies to fulfil the requirements of future high performance embedded systems.

Project Updates

We are working on a larger survey on FPGA hardware security to provide a holistic overview on security aspects (including attack and attack mitigation strategies). A very encouraging outcome of that work is that only very little research is focussing on attack mitigation strategies, which is the core area of research in rFAS. We also work on a new design for carrying out DPA attacks on FPGAs.

While DPA attacks are considered to be a major issue in FPGA-based systems (as they can be carried out remotely without the need to physically access the FPGA), this thread is still rather theoretic as so far attacks could only be successfully carried out for relatively slow running cryptographic cores (e.g., AES, DES).

We are therefore researching more sensitive FPGA soft-logic oscilloscopes. We have a first setup working successfully but research will have to continue.

SMALL EQUIPMENT BIDS

Funding was made available through a parallel call to the tranche 2 project call of May-Jul 2018. This funding was open to all UK institutes, for the purpose of procurement of equipment. The call was publicised on the RISE website with funds to be spent by Feb 2019.

The four winning bids were:

BIRMINGHAM CITY
University

- Birmingham City University: “Dynamic Hardware – Rooted Trust Architecture for Large-Scale IoT Systems”, Prof Paul Kearney

UNIVERSITY OF
CAMBRIDGE

- University of Cambridge: “SafeBetFPGA – FPGA Platform to explore safe, aggressive speculation in processors”, Prof Simon Moore

University of
Kent

- University of Kent, “UK Quantum Randomness Beacon”, Prof Julio Hernandez-Castro

UNIVERSITY OF
OXFORD

- University of Oxford, “Machine Learning for Systems Security”, Prof Tom Melham & Prof Daniel Kroening

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

CONTACT DETAILS
W: www.ukrise.org
E: info@ukrise.org.uk
T: +44 (0) 28 9097 1771
@UK_RISE