RISE
RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

INTRINSIC SECURITY

Funded by

in association with
National Cyber
Security Centre

EPSRC
Engineering and Physical Sciences
Research Council

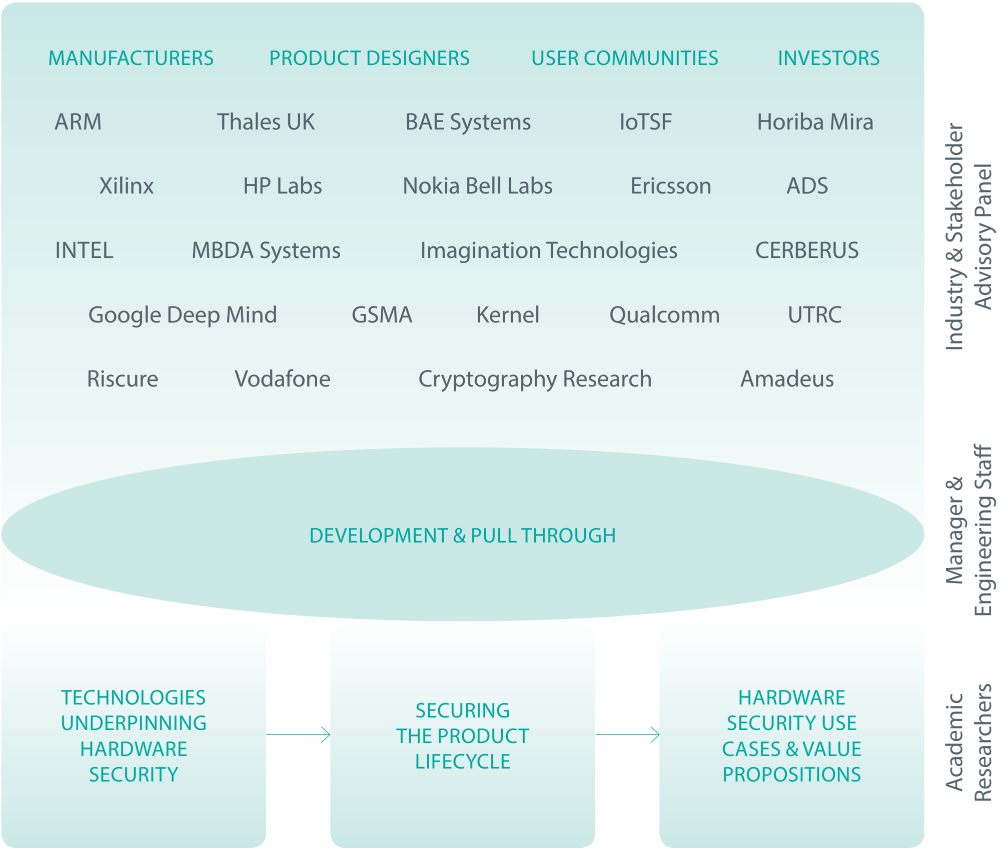
VISION

The £5M Research Institute for Secure Hardware and Embedded Systems (RISE) seeks to identify and address key issues that underpin our understanding of Hardware Security. RISE was launched in November 2017 under the directorship of Professor Máire O'Neill, Queen's University Belfast, with funding from the National Cyber Security Centre (NCSC) and the Engineering and Physical Sciences Research Council (EPSRC).

The vision for RISE over the next 5 years is to create a global centre for research and innovation in hardware security encouraging close engagement with leading UK-based industry partners and stakeholders.

A particular focus will be to accelerate the industrial uptake of the Institute's research output and its translation into new products, services and business opportunities for the wider benefit of the UK economy.

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

Industry & Stakeholder Advisory Panel

DEVELOPMENT & PULL THROUGH

Manager & Engineering Staff

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

Academic Researchers

HARDWARE SECURITY RESEARCH LANDSCAPE

The hardware encryption market is projected to reach 413.85 Billion USD by 2022[1]. 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.

[1] Hardware Encryption Market by Algorithm and Standard (AES and RSA), Architecture (FPGA and ASIC), Product (Internal and External Hard Disk Drive, Solid-State Drive, USB, and Inline Encryptor), Application, Vertical, and Geography - Global Forecast to 2022 - Source MarketsandMarkets 2017.

RESEARCH CHALLENGES

RISE was established to address a number of research challenges in hardware security and develop cutting edge solutions to these challenges.

Understanding the technologies that underpin hardware security, the vulnerabilities in these technologies and development of countermeasures.

This includes:

- 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

Maintaining confidence in security throughout the development process and the product lifecycle.

This includes:

- Confidence in Developing Secure Hardware Devices
- Supply Chain Confidence
- Modelling of Hardware Security
- Hardware enforcement of software-defined security policies

Hardware security use cases and consideration of value propositions.

A significant goal of this research is to introduce the research community to new hardware features, and encourage experimentation of novel applications.

This includes:

- Novel Authentication, e.g., alternatives to passwords
- Secure document viewers
- Securing 'Bring your own device' (attestation, roots of trust, device management)

Development and pull-through

- Ease of Development and ease of leveraging the best security option
- Understanding Barriers to Adoption
- Education of the Potential User/Developer base
- Secure device lifecycle management

RISE is one of four multi-institution Research Institutes in Cyber Security funded by NCSC and EPSRC with the aim of developing the UK's cyber security capability in this strategically important area. The other institutes are:

Research Institute in Science of Cyber Security (RISCS: https://www.riscs.org.uk)
Research Institute in Trustworthy Industrial Control Systems (RITICS: https://ritics.org)
Research Institute on Verified Trustworthy Software Systems (VeTSS: https://vetss.org.uk)

Core research projects initially funded under RISE in 2017 include:

SCARV: A SIDE-CHANNEL HARDENED RISC-V PLATFORM

Dr Daniel Page
University of Bristol

The research goals capitalise on investigating a RISC-V Instruction Set Architecture (ISA) design in a way designed to address advanced, persistent threats to our digital security, and, by extension, society. 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).

IOSEC: PROTECTION AND MEMORY SAFETY FOR INPUT/OUTPUT SECURITY

Dr Robert Watson, Prof Simon Moore, Dr Athanasios Markettos,
University of Cambridge

This project aims 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 this project aims to address.

USER-CONTROLLED HARDWARE SECURITY ANCHORS: EVALUATION AND DESIGNS

Prof Mark Ryan, Dr Flavio Garcia, Dr David Oswald
University of Birmingham

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

DEEP SECURITY: APPLYING DEEP LEARNING TO HARDWARE SECURITY

Prof Máire O'Neill
Queen's University Belfast

This project seeks to investigate the application of deep learning in Side Channel Analysis and Hardware Trojan 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.

Future specific research themes to be addressed include: Micro-architectural and Analogue Security Evaluation, Automated security verification in EDA tools and software tool chains, Supply chain security, and Hardware-based security services.

RISE INDUSTRY AND STAKEHOLDER ADVISORY BOARD

Independent Chair: Charles Brookson, OBE

Thales UK, Research & Technology, BAE Systems, Qualcomm, United Technologies Research Center, Vodafone, IOT Security Foundation, GSMA, Riscure, Rambus Cryptography Research, DSTL, Xilinx, Dell EMC, MBDA Systems, Imagination Technologies, ADS Group - Aerospace, Defence, Security & Space, Amadeus Capital Partners, Stealth, Kernel Capital, Thales E-Security, HP Labs, Nokia Bell Labs, Ericsson, Intel, ARM, Google Deep Mind, CERBERUS, Horiba Mira.

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

CONTACT DETAILS
W: www.ukrise.org
E: e.montgomery@qub.ac.uk
T: +44 (0) 28 9097 1771