2022 REPORT ON FUTURE RESEARCH TRENDS IN SECURE HARDWARE AND EMBEDDED SYSTEMS

RISE Industry and Stakeholder
Advisory Board (ISAB)

SUMMARY

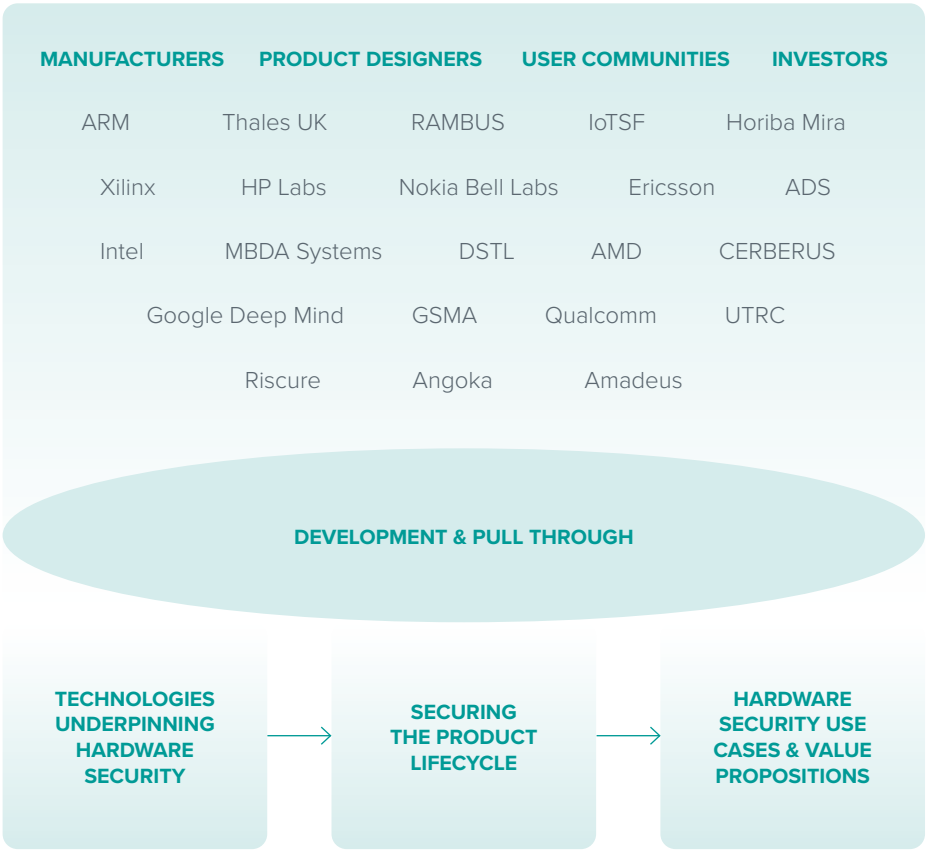
The purpose of this report is to provide a view of the future trends for RISE and to help predict the underlying hardware and embedded systems security research needed over the next five to ten years to meet industry requirements.

It has brought together non-academic experts from Industry to arrive at some conclusions to help predict where further research may be useful. As a caution, this is our current best efforts.

We identify the areas of importance as:

- Cryptography alternatives
- Improved security to meet legislation and physical security
- Supporting hardware security techniques
- Attacks mitigation
- Cloud secure hardware
- Supply chain security
- Energy efficiency
- Hardware management
- Testing stratagems
- Standards for interworking and protocols

RISE ECOSYSTEM



ROLE OF THE RISE INDUSTRY AND STAKEHOLDER ADVISORY BOARD (ISAB)

The key elements within RISE are the academic researchers, an Industry & Stakeholder Advisory Board (ISAB) and the Institute Management team. The RISE ISAB 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, with a focus on advancing the State-Of-The-Art (SOTA) and opportunities for transition for exploitation and 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,
- Growing the future UK STEM base in digital security and related areas.

CURRENT RISE 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

CURRENT RISE RESEARCH PROJECTS

The research challenges of RISE are being delivered through a series of projects funded by EPSRC and NCSC. 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 Belfast, the University of Cambridge, the University of Bristol and the University of Birmingham.

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

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

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

Deep Security: Investigating the Application of Deep Learning in SCA and Hardware Trojan Detection.
Prof Máire O'Neill
Queen's University Belfast

A subsequent tranche of 4 projects was initiated in Nov 2018, delivered by the University of Cambridge, the University of Edinburgh, the University of Surrey, and the University of Manchester.

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

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

TimeTrust: Robust Timing via Hardware Roots of Trust and Non-standard Hardware, with Application to EMV Contactless Payments.
Prof Ioana Boreanu[1], Dr Tom Chothia[2], Prof Liqun Chen[1].
[1]University of Surrey, [2]University of Birmingham

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

Project details can be found in the RISE Annual Report and project update presentations are available on the RISE website (www.ukrise.org).

FUTURE TRENDS

The UK government, in recognition of the strategic importance of the digital hyper-connected world, has published several strategic documents. The 2022 National Cyber Strategy outlines the need to *'ensure that wherever possible the next generation of connected technologies are designed, developed and deployed with security and resilience in mind and as part of a concerted effort to embrace a 'secure by design' approach', while 'Building a secure and resilient world'* was identified as of one of UKRIs five strategic themes (UKRI Strategy 2022-2027). The rapid growth of a pervasive and network-connected world has created major challenges in terms of the privacy and vulnerability of information in storage and transmission as well as the security of critical national infrastructure.

There have also been similar international initiatives. The US CHIPS and Science Act, signed into law in August 2022, seeks to strengthen the US semiconductor manufacturing ecosystem with significant investment in securing the supply chains for critical industries and ensuring the safety and cyber security of products produced within the US. The EC announced the development of a European Chips Act with the aim of addressing semiconductor sovereignty concerns in Europe. Similarly, the UK is currently undertaking a review of the semiconductor sector, which is considering the sovereignty and security of our semiconductor supply chain amidst the current geo-political landscape. Therefore, it is imperative that we grow research UK expertise in this field and increase the number of researchers trained in this area

Sectors

In considering the future trends for possible research in hardware and embedded systems security, the following sectors were identified:

- Space
- Automotive
- Semiconductors
- Unmanned systems, such as drones
- Telecommunications infrastructure
- Built environment (smart cities etc)
- Maritime (autonomous boats)
- Trucks and transport

From these the RISE ISAB members predicted the trends for security for the next five to ten years defining critical industries and the supporting critical hardware.

Context for hardware security

There are broader contexts and drivers for superior security.

Examples are increasing:

- Geo-political tensions,
- Global reach and democratisation of technologies,
- Complexity of underpinning socio-technical networks,
- Supply chain challenges,
- Climate change,
- and demands for energy efficiency.

Worldwide there is an increasing recognition of these trends and increasing investment in Research and Development (R&D), in policies and legislation for better positioning in security. The UK must be a dominant leader in these endeavours.

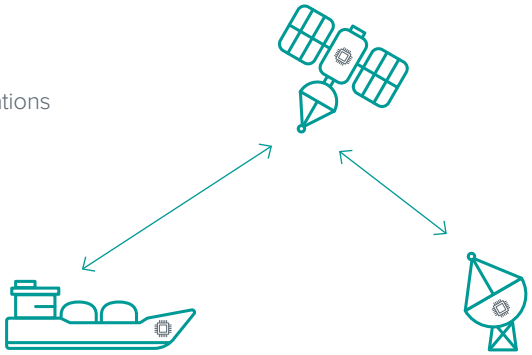
This report describes what we foresee are the areas of Critical Industries, and the demands for Critical Hardware.

Example scenarios for sectors

We identify two scenarios and examples within the sectors (and of course, others are possible).

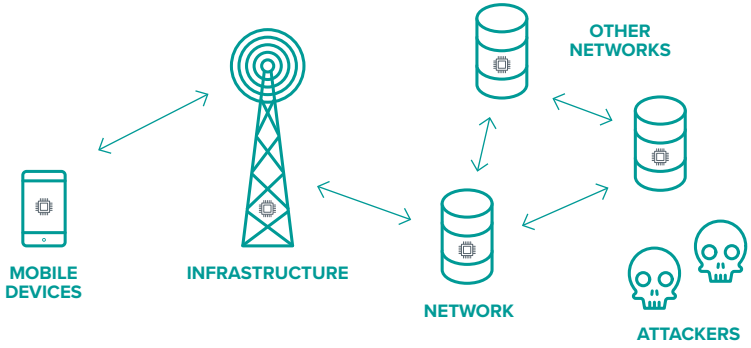
Maritime

Secure standards
Security testing
Secure hardware
Secure communications
Crypto



Telecommunications infrastructure

Effiency
Secure hardware
Secure cloud
Testing
Standards



Critical industries

There are a range of critical industries that we see important for research to support with underlying hardware security and dependability:

- Critical infrastructures,
- Cryptography,
- Communications,
- Internet of Things
- Data science and analytics,
- Assured Artificial Intelligence (AI)/Machine Learning (ML),
- Resilient systems,
- Model based Systems Engineering,
- High Performance Computing and ICT,
- Increasing virtualisation,
- Supply chains,
- Human Machine Teaming,
- Education,
- Healthcare,
- Manufacturing (private networks and robotics, industry 4.0).

Different industries will have different risks, maturity and appetite. There will be an impact for the desire for more secure hardware and secure by design, driven by the demands of industry, consumers and legislation.

Critical hardware

We have also identified critical hardware areas:

Cryptography alternatives: Alternatives such as quantum (and others such as wave or biological) will impact conventional cryptography

Improved security to meet legislation and physical security: There is an increasing trend for security legislation worldwide that will impact the demand for better security. This may be for better physical protection, ensuring lifetime security, and providing core security services for future products and services

Supporting hardware security techniques: There will be a requirement for better hardware techniques to ensure protection, correct operation, identification (of devices, processes and roles and responsibilities).

Attacks mitigation: There will be increasing attacks from both nation states, terrorism and ransomware. This will result in increasing defence mechanisms and methods to ensure correct operation. Side channel attacks will become increasingly sophisticated.

Cloud secure hardware: Demand for outsourcing and remote servers for services such as connectivity and IoT will require secure hardware for operation.

Supply chain security: There will be an increasing risk of supply chain issues due to global trade, and the effects of climate change. There will also be a need to ensure that components are genuine.

Energy Efficiency: Energy efficiency will become more important. This will place increased demands on energy consumption, heat dissipation - hardware will need to reflect this.

Hardware management: There will be an increasing requirement to manage underlying hardware securely, and to ensure its correct operation.

Testing stratagems: There will be a demand for improvement in the detection and management of hardware security, and the consequential minimisation of security threats.

Standards for interworking and protocols: Secure interworking will produce a demand for better secure operation in devices, and the supporting protocols.

RISE INDUSTRY AND STAKEHOLDER ADVISORY BOARD (ISAB) MEMBERS

Independent Chair: Charles Brookson, OBE

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

BIBLIOGRAPHY

1. RISE Annual report,
   https://www.ukrise.org/wp-content/uploads/2022/01/RISE_Annual_Report_2021.pdf

2. Telecommunications (Security) Act 2021,
   https://www.legislation.gov.uk/ukpga/2021/31/enacted

3. Product Security and Telecommunications Infrastructure Bill,
   https://www.gov.uk/government/publications/product-security-and-telecommunications-infrastructure-bill-documents

4. ENISA 5G Cybersecurity Standards,
   https://www.enisa.europa.eu/publications/5g-cybersecurity-standards

5. NCSC Annual Review 2021,
   https://www.ncsc.gov.uk/collection/annual-review-2022

6. USA CSIS Strategic Technologies Program,
   https://www.csis.org/programs/strategic-technologies-program

7. UK National Cyber Strategy 2022,
   https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

8. US CHIPS and Science Act,
   https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

9. European Chips Act,
   https://digital-strategy.ec.europa.eu/en/library/european-chips-act-communication-regulation-joint-undertaking-and-recommendation

Acknowledgements

Acknowledgement is made to the individual RISE ISAB Board members who helped provide input into this report.

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

CONTACT DETAILS
W: www.ukrise.org
E: info@ukrise.org
T: +44 (0) 28 9097 1700
@UK_RISE