RESEARCH INSTITUTE FOR SECURE HARDWARE & EMBEDDED SYSTEMS

in association with National Cyber Security Centre

Call for Small Equipment Bids: Secure Hardware & Embedded Systems

Closing date: 31st July 2018

Key Dates:

Activity	Date
Call Opens	14th May 2018
Call Closes	31st July 2018
Panel Review and Prioritisation	August-September 2018
Latest Purchase Date of Equipment	15 February 2019

Additional information: The Research Institute in Secure Hardware and Embedded Systems (RISE) is also currently running a related "Call for Research Projects", which may be of interest to applicants.

1. Overview

The Research Institute in Secure Hardware and Embedded Systems (RISE: www.ukrise.org) is inviting proposals for research equipment to support UK academic research projects in the field of hardware security, funded by the National Cyber Security Centre (NCSC).

2. Background

RISE is jointly funded by the Engineering and Physical Sciences Research Council (EPSRC) and NCSC, and seeks to identify and address key issues that underpin our understanding of Hardware Security.

The vision for RISE, which was launched in November 2017 under the directorship of Professor Máire O'Neill, Queen's University Belfast, is to create a global centre for research and innovation in hardware security with close engagement with leading industry partners and stakeholders. The aim is to bring together the hardware security community in the UK and build a strong network of national and international research partnerships. A key focus is 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 is hosted by the Centre for Secure Information Technologies (CSIT: www.csit.qub.ac.uk), Queen's University Belfast.

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)

3. RISE Research Challenges

The overall research challenges in hardware security being addressed by RISE include:

a. 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: TRNGs, PUFs
   - Novel Hardware analysis toolsets & techniques
   - Attack-resilient Hardware platforms, Hardware IP building blocks

b. 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

c. Hardware security use cases and consideration of value propositions. A significant goal of this research should be 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)

d. Development and pull-through
   - Ease of Development & ease of leveraging best security option
   - Understanding Barriers to Adoption
   - Education of Potential User/Developer base

4. Specific research themes to be addressed in concurrent Call for Research Projects

The specific research themes to be addressed in the concurrent Call for Research Projects are listed below. Further information on this parallel call can be found at: www.ukrise.org/CallforResearchProjects.

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 & 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 lifecycle
- 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

5. Funding

Funding of up to £140,000 is available through this call and is exclusively for the procurement of equipment. Costs for operating and maintaining equipment are not eligible and should be borne by the applicant institution. Further details of the requirements of this call are listed below.

- Costs will be awarded at up to 100% (including VAT).
- Equipment must clearly support research projects that address one or more of the RISE research challenges or specific research themes outlined above.
- If successful, equipment must be purchased by the 15 February 2019.
- It is envisaged that the equipment bids will typically be in the range of £20k to £50k, with appropriate justification provided. Higher valued bids will require a strong justification.

There is a requirement for successful applicants to provide a final report of key findings of the research completed arising from the equipment purchased. Applicants may also be required to present the related research outcomes at RISE events.

Please note that NCSC will be the contracting authority and contracts formed will use the NCSC's standard terms and conditions plus any special requirements as agreed by the NCSC.

6. Eligibility

All UK Higher Education Institutions that receive grant funding from one of the UK higher education funding bodies are eligible to apply to this call. Principal investigators must be academic employees and hold a permanent post at an eligible organisation.

7. Small Equipment Bid Proposal Format

Proposals should be written in single-spaced typescript in Arial 11 or other sans serif typeface of equivalent size, with margins of at least 2cm, and should include the following sections:

a. **Case for Support** (up to two A4 sides describing how the proposed item of equipment will support your planned research and research methodology in addressing one or more of the RISE research challenges or specific research themes outlined above. Please provide a short statement on the anticipated impact the equipment being purchased will have).
b. **Quotes for Equipment** (no page limit. Quotes for the proposed equipment should be included in the application).

Please note that applicants submitting to the concurrent 'Call for Research Projects' are encouraged to also submit to this Call for Small Equipment Bids, and the same planned research can be submitted for both calls; however, these will be need to be submitted as separate applications, and will be reviewed and processed individually.

8. Proposal Submission Process

Applicants should submit proposals to: ResearchCalls@GCHQ.GSI.GOV.UK **by Tuesday 31st July 2018**. Proposals will be evaluated by a panel of stakeholders during August/September 2018. If successful, equipment must be purchased by the 15 February 2019.

9. Assessment Criteria

Proposals will be assessed by a prioritisation panel resulting in a rank ordered list. Research proposals will be evaluated based on the following criteria:

a. **Appropriateness:** Appropriateness of the proposed equipment purchase in supporting the planned research in helping to address one or more of the RISE research challenges or specific research themes. Value for money.
b. **Impact**: Impact equipment will have on research and attaining research outputs.

Contacts:
Queries on this Call for Small Equipment Bids should be directed to:
ResearchCalls@GCHQ.GSI.GOV.UK .

For further information on RISE, please contact:

Mr Stephen Sloan, RISE Business Development Manager
E-mail: Stephen.Sloan@qub.ac.uk
Tel: 02890 971771