RISE
RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

in association with
National Cyber
Security Centre

Call for Research Projects: Secure Hardware & Embedded Systems

Closing date: 31st July 2018

Assessment Process: This is a single stage process via a full proposal. Full proposals will be assessed by a prioritisation panel resulting in a rank ordered list.

Key Dates:

Activity	**Date**
Call Opens	14th May 2018
Call Closes	31st July 2018
Panel Review and Prioritisation	August-September 2018
Expected Start Date of Research Projects	November 2018
Latest Completion Date of Research Projects	31st March 2022

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

1. Overview

The Research Institute in Secure Hardware and Embedded Systems (RISE: www.ukrise.org) is seeking to expand its research community and is inviting 3-year research proposals for academic research projects, funded by the National Cyber Security Centre (NCSC), to form part of the institute.

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 understanding the technologies that underpin hardware security, the vulnerabilities in these technologies and development of countermeasures; maintaining confidence in security throughout the development process and the product lifecycle; hardware security use cases and consideration of value propositions; and development and pull-through of hardware security solutions. Further information on these general research challenges can be found at the RISE website: www.ukrise.org.

4. Research Themes to be addressed in this Call

Prior to the launch of this grant call, a consultation exercise was held with the RISE Industry and Stakeholder Advisory Board (ISAB) to help inform the research themes to be addressed in the call. Their input was sought to help identify four main research themes and we are grateful to them for providing feedback based on their extensive expertise in the sector.

Based on the above consultation exercise, this call is seeking research projects related to the following specific research themes:

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 is available to the UK academic community for 3-year research projects up to a maximum value of £300k over their lifetime. We expect to fund 3-5 research grants under this call, and if possible, projects should start as soon as possible in FY 2018/19 (the expected start date is 1 November 2018 and the latest start date is 1 April 2019) with a final completion date of 31 March 2022 at the latest. Funding of up to £250k is available in 2018/19 and approximately £400k is available in subsequent years to support the call. PhD students (including international students) can be funded under this call if the above project timelines are observed. Collaborative research projects with other UK academics and/or joint projects with industry that leverage funding from the industry partner are encouraged.

There is a requirement for successful applicants to provide interim and final reports of key findings at appropriate points during the research project and to report on progress. Applicants will also be required to present their research outcomes at RISE events throughout the project lifetime.

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. Equipment

We do not expect proposals to request significant items of equipment under this call. Where possible, researchers are asked to make use of existing facilities and equipment, including those hosted at other universities or at industry partners. If new equipment is needed to support the research project, applicants are encouraged to apply to the associated call, 'Call for Small Equipment Bids'. Further information on this parallel call can be found at: www.ukrise.org/CallforSmallEquipmentBids.

Please note that the submission of a proposal to this call should not be dependent on achieving success in the associated call mentioned above.

7. 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.

8. Research Proposal Format

Research proposals should adhere to the page limits outlined below and be written in single-spaced typescript in Arial 11 or other sans serif typeface of equivalent size, with margins of at least 2cm.

Proposals should include the following sections:

a. **Case for Support** (six A4 sides describing the proposed research, its context, how it addresses one or more of the specific research themes detailed above, measurable objectives, and the work programme and research methodology to be followed. References and illustrations should be included within the page limit)
b. **Impact** (two A4 sides describing potential beneficiaries, how the research may impact them and how the proposed work will facilitate this)
c. **CVs** (two page CVs of the individuals who will be involved in the research work should be provided and should include any relevant background knowledge and expertise related to the proposed project)
d. **Justification of resources** (two A4 sides justifying the resources requested. If a recruitment exercise is needed for staff, this needs to be made clear, along with the likely timing and impact of this on the project)
e. **Workplan** (one A4 side - illustrated using a diagram (e.g. Gantt chart or similar). This should include a timeframe for delivery of interim and final outcomes, including quarterly progress reports)
f. **Funding Requirement** (two A4 sides outlining the funding requested for the research project. The proposed amount of grant funding required for each year of the programme (£s) should be provided. The proposed grant funding costs should include a breakdown on the daily pay rates, grade and number of days allocated to each member of the project team as well as stating the total costs per year. If VAT is chargeable, it should be quoted

separately. Expenses for non-staff costs must also be detailed separately, as should an estimate of travel expenses that are likely to be incurred. The research will be funded at Full Economic Cost.

g. **Industry Partner Letters of Support** (as appropriate)

9. 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. Negotiation with successful applicants to agree the final scope of the research project may also occur.

Projects should aim to start as soon as possible during FY 2018/19 once project proposals have been agreed, and where possible the expected start date is November 2018. Projects must complete in full at any time prior to 31 March 2022.

10. Assessment Criteria

This call involves a single stage application process via a full proposal. Full 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. **Novelty**: Novelty and ambition of the proposed research related to the research themes of the call.
b. **Quality**: Appropriateness of proposed methodology. Feasibility – will it deliver as planned.
c. **Impact**: Relevance and appropriateness of any beneficiaries or collaborators as part of the research project. Plans for dissemination, knowledge exchange and/or commercialisation opportunities.
d. **Applicant Ability**: Leadership quality and experience of the Principal Investigator and track record and balance of skills of the project team.

Contacts:
Queries on this Call for Research Projects 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