Firmware Binary Code Analysis for Vulnerability Detection Towards Cyber Security of IoT

**Type of award**  PhD Research Studentship

**Department**  Computer Science, Cyber Security Research Group

**Scholarship Details**  Minimum £18,500 p.a. subject to eligibility status.

**Duration**  4 years

**Eligibility**  Home (UK) and EU citizens who have confirmation of UK settlement or pre-settlement status under the EU Settlement Scheme.

**Deadline**  1 October 2021

**PhD Topic Background/Description**

Internet of Things (IoT) constitutes a variety of devices, ranging from tiny sensors and actuators to programmable controllers that drive critical infrastructure such as water, power, through to general purpose mobile devices in the home, work, or city environment. Irrespective of the type of a device, software code, the so-called firmware, remains a common component across all of them and it is (anecdotally) believed that such code is not updated frequently, thereby leaving bugs in code forever. A side effect of having such a heterogeneous computing environment is the variety of "compiled" code running on such a diverse set of devices. This poses a challenge for developing automatic program analysis techniques to cope with the syntactically different looking code. Past research has shown that vulnerability extrapolation is a possibility, for example, through approaches to systematically compare binary code to find patterns leading to vulnerable code.

In this project, we aim to investigate techniques that are tailored towards analysing binary code by stripping off syntactical differences. The project is open in the sense that one can investigate static as well as dynamic program analysis techniques, for example abstract interpretation, fuzzing etc. There is a particular focus on investigating the application of machine learning (ML) based approaches, e.g., natural language processing (NLP), to find similar code patterns. NLP-based techniques are known to work with languages with very different syntactical structure. One particular aspect is to map assembly code-based representation of compiled code in a form suitable for applying NLP. In short, the project will allow one to explore techniques to analyse binary code - your own creativity is the limit!

You will have either a strong background and interest in software program analysis with a keen desire, ability, and willingness to learn ML-based approaches. Alternatively, you will have a strong
background and interest in ML and AI with a keen desire, ability, and willingness to learn about software program analysis.

You will be part of the Bristol Cyber Security Group located within the Department of Computer Science. The group focuses on a wide spectrum of security topics, including software/system security, usable security, cyber-physical interface security. As a part of its EPSRC CDT in cyber security, a unique interdisciplinary PhD programme, you will have the opportunity to be part of an immersive training experience, in a cohort of the cyber security leaders of the future. The group maintains a good collaboration with industry that allows us to work on cutting-edge practical problems that matter! This PhD studentship will be conducted in partnership with Toshiba Research Europe Limited.

URL for further information: http://www.bristol.ac.uk/ctd/cyber-security/

**Further Particulars**

**Candidate Requirements**

Applicants must meet the entry requirements for the PhD Research programme they wish to apply to. Requirements can be found at http://www.bristol.ac.uk/study/postgraduate/2020/eng/phd-computer-science/ including English Language.

Basic skills and knowledge required:

- **Essential:** Excellent analytical skills and experimental acumen
- **Desirable:** Either a strong background and interest in software program analysis with a keen desire, ability, and willingness to learn ML-based approaches. Alternatively, a strong background and interest in ML and AI with a keen desire, ability, and willingness to learn about software program analysis.

**Scholarship Details**

This is a fully funded 4-year studentships covering:

- Minimum £18,000 tax-free stipend per year for living expenses
- tuition fees at UK/EU student rates
- equipment and travel allowance to support research related activities.

For EPSRC funding, students must meet the EPSRC residency requirements.

**Informal enquiries**

Please email Prof Awais Rashid (awais.rashid@bristol.ac.uk)

For general enquiries, please email sceem-pgr-admissions@bristol.ac.uk

**Application Details**

Prior to any application, please contact Prof Awais Rashid to discuss your research proposal to see if it aligns with his current research. No indication of an offer can be made until a completed application has been received.

To apply for this studentship submit a PhD application using our online application system [www.bristol.ac.uk/pg-howtoapply]
Please ensure that in the Funding section you tick “I would like to be considered for a funding award from the Computer Science Department” and specify the title of the scholarship in the “other” box below along with the name of the supervisor. Interested candidates should apply as soon as possible.

Deadline for applications: 31 July 2021.

Apply now