Title: Towards Reproducible Intrusion Detection Research

Type of award PhD Research Studentship

Department Computer Science

Scholarship A minimum £14,777 p.a. for 2018/19 subject to contracts (please check below for further scholarship details)

Funding Duration 3.5 years

Eligibility Home/UK applicants only

Start date 1 October 2019

PhD Topic Background/Description

Computer systems are vulnerable. Not a day goes by without news of another data leak or security breach. Computer systems are massive, complex, human-created systems — and they are inherently flawed — we don’t have the technology to build perfect systems. Therefore, we need to develop mechanisms to respond quickly and accurately to intrusions. Our recent research efforts have focused on the development of provenance-based intrusion detection systems (IDS). We are becoming acutely aware of the difficulty of making any meaningful cross-evaluation of such systems due to inadequate availability of datasets and poor reproducibility practices. This project aims at exploring reproducibility literature, practises and tools to develop solutions adapted to IDS.

One of the major hurdles when one works on developing an IDS as an academic is how to accurately and fairly evaluate the system. In other words, to measure “how well” a given system behaves and compare this system against previously proposed approaches. One of the cornerstones of proper scientific enquiry is to make such evaluation repeatable. However, such an objective is mired by many issues, among those:

1) datasets used in previous systems are either not available or not adapted to the evaluated system;

2) source-code of most systems is not accessible even through interactions with authors, or when it is, the version used in a paper is not identifiable (the fabled grad student version);

3) evaluation metrics are inconsistent across papers, and this makes meaningful comparisons without 1) and 2) barely possible.

We propose to investigate methods to generate shareable IDS evaluations. The idea is not to build an IDS benchmark (a task seemingly impossible as systems must evolve alongside threats), but rather to explore technical and non-technical means to share software artefacts allowing the reproduction of an evaluation. Such a framework should also identify a set of minimum required properties that an IDS should fulfil.
The successful candidate will work in the Computer Science Department at the University of Bristol and will be supervised by Dr Thomas Pasquier (http://tfjmp.org/) and co-supervised by Prof Awais Rashid (http://www.bristol.ac.uk/engineering/people/awais-a-rashid/index.html).

Further Particulars

Candidate Requirements
First class in Computer Science or a related subject.

Basic skills and knowledge in Systems and Security required.

Scholarship Details
Scholarship covers full UK PhD tuition fees and a tax-free stipend at the current RCUK rate (£14,777 in 2018/19).

Informal enquiries
For informal enquiries, please email Dr Thomas Pasquier, Thomas.pasquier@bristol.ac.uk

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

Application Details
Prior to application if you are interested, please email (thomas.pasquier@bristol.ac.uk) with your CV and academic transcripts. The formal application process can then be discussed.

To apply for this studentship, submit a PhD application using our online application system [www.bristol.ac.uk/pg-howtoapply]

Please select PhD Computer Science on the Programme Choice page and enter details of the studentship when prompted in the Funding and Research Details sections of the form with the name of the supervisor.

Closing date for applications 24 February 2019.

Apply now