Title: Towards Interpretable and Provenance-based Intrusion Reports

Type of award PhD Research Studentship
Department Computer Science
Scholarship A minimum £22,000 p.a. subject to contracts (please check below for further scholarship details)
Funding Duration 3.5 years
Eligibility Home/UK applicants only
Start date January 2020

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 a mechanism to respond quickly and accurately to intrusions. Currently, there is much research focused on detecting intrusions, which is a good start, but once we detect an intrusion, the immediate question is, “What is the root cause of the intrusion? What kinds of information are involved in it? How do we fix it?” This is the problem we aim to address, through sophisticated visualisation of the system execution. Our goal is to transform intrusion detection systems and data into a visualisation that makes apparent the right action to take.

Information is only meaningful if it can be communicated effectively. While there is a growing security community exploring provenance-based intrusion detection. However, the impact on the industry has been minimal. On the one hand there is mounting pieces of evidence that the capture of causality relationships in provenance graphs improves greatly over standard audit log format; on the other hand, the average human is not efficient in interpreting large and complex graphs. The student work will be vital in moving this body of work outside of the research community, by providing means to communicate the results effectively. We identify Three main objectives:

1. To study graph summarisation techniques to extract human-relevant information.
2. To design effective communication vehicles targeted at well-defined audiences through graphical or textual means.
3. To study ML techniques used in automated provenance-based forensic and intrusion detection with the goal to identify methods to build more interpretable models.

The group:

The successful candidate will join the University of Bristol Cyber Security Group (UBCSG). UBCSG is recognised jointly by the National Cyber Security Centre (NCSC) and the Engineering and Physical Sciences Research Council (EPSRC) as an Academic Centre of Excellence in Cyber Security Research and hosts a
Centres for Doctoral Training in Cybersecurity. The successful candidate will join a dynamic and growing research and student community. He/She will have opportunities to work and collaborate with international partners in academia and industry.

Further Particulars

Candidate Requirements
First class in Computer Science or a related subject and experience in at least one of the following: Systems Security, Machine Learning, Human Factor of Security.

Basic skills and knowledge required in at least one of the following: Systems, Security, Graph Analysis, HCI, ML

Scholarship Details
Scholarship covers full UK PhD tuition fees and a tax-free stipend at the current NCSC rate (£22,000 in 2018/19).

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

For general enquiries, please email sceem-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 31 October 2019.

Apply now