PhD Studentship

Identifying Trigger Conditions for Malicious Software Behaviours

University College London, Department of Computer Science

Supervisor: David Clark

Applications are invited for a PhD position at the Software Systems Engineering Group of the UCL Department of Computer Science, funded by the Government Communications Headquarters (GCHQ). The studentship is open only to UK nationals because of the funder's eligibility requirements. The successful candidate will be required to undertake an internship of approximately 2 - 4 weeks per year at GCHQ's headquarters in Cheltenham. To be considered for this studentship, candidates must therefore be prepared to undergo GCHQ's security clearance procedures.

The successful candidate will research methods of identifying trigger conditions for malware behaviours. Initial focus will be on the synthetic statistical search method called Importance Sampling. This uses a Performance Function that evaluates how close executions on sampled inputs are to the trigger event. The synthetic probability distribution is iteratively updated and resampled to move towards an ideal probability distribution in which the trigger event(s) have maximal probability and all other events have zero probability. The method has wide potential application to a number of problems in software engineering and computer science, including finding software vulnerabilities and improving automated analysis of code. In this PhD work, however, the goal will be application to the malware trigger problem. This will require the student to study reverse engineering of binaries and the use of virtual machines such as Qemu.

All research that is undertaken at UCL as part of the studentship will be unclassified and published in the open literature.

The studentship will be funded for a period of 3.5 years. GCHQ will cover the costs of UCL's fees (currently £4,640 per annum) and will provide a total tax-free stipend of £24,500 per annum. A generous travel budget is also provided to enable attendance at international conferences and workshops.

The start-date for the studentship will any time before October 2015.

We expect a candidate to have at least a strong 2:1 degree in Mathematics, Computer Science, Engineering, or a related MSc course, and good experience in programming. Some prior knowledge of assembly languages and empirical methods in data collection and analysis would be advantageous.

Applications should be submitted to University College London. Please follow the link here http://www.ucl.ac.uk/prospective-students/graduate/apply/research/how-to-apply/ to the online application.

You should specify on your application that you would like to be supervised by Dr David Clark and make it clear in your personal statement you are applying for the **‘Trigger Conditions for Malicious Software Behaviours’** studentship.

To apply for this post, please click on the Apply button below.

If you have any queries about submitting an application, please email Tania Green at tania.green@ucl.ac.uk

Your application must reach the Department by 30 March 2015.