

JOB DESCRIPTION

Job Title:	Two Research Assistants for Trustworthy Computing and Malware Analysis
Department / Unit:	Information Security Group
Grade:	RHUL 6
Accountable to:	Dr Daniele Sgandurra (PI)
Accountable for:	Head of Department
Purpose of the Post	
<p>The Information Security Group at Royal Holloway, University of London, is seeking <u>two</u> highly motivated research assistant researchers for the EU Horizon2020-funded FutureTPM project. The successful candidates will join the Systems and Software Security Lab (S3Lab), working on the development of a virtual quantum-resistant trusted platform module (TPM) for KVM, as well as supporting S3Lab research activities (e.g., malware analysis) and actively participating to various project and S3Lab events. The positions are fixed term full-time for a period of 15 months.</p> <p>The goal of FutureTPM is to create a Quantum-Resistant (QR) Trusted Platform Module (TPM) by designing and developing QR algorithms suitable for inclusion in a TPM. The algorithm design will be accompanied by implementation and performance evaluation, as well as formal security analyses in the full range of TPM environments: i.e. hardware, software and virtualization environments. Use cases in online banking, activity tracking and device management will provide environments and applications to validate the FutureTPM framework.</p>	
Key Tasks	
<p>The main responsibilities of the posts are:</p> <ul style="list-style-type: none"> • Implementation of a virtual QR-TPM running on KVM that implements the QR functionalities available on a software TPM: <ul style="list-style-type: none"> ○ sharing of software TPM across virtual machines ○ preserving state of the TPM and key association ○ create and store certificates in NV with the primary key generated by one of the existing QR algorithms ○ integration and test of the vTPM with a FutureTPM use case ○ describing the results in project deliverables ○ others if needed (e.g., VM migration) • Attending FutureTPM conference calls in all relevant Work Packages • Supporting S3Lab development and research activities, e.g. related to S3Lab research areas (in particular, malware analysis, evasion and machine learning), research papers, and various events 	
Other Duties	

The duties listed are not exhaustive and may be varied from time to time as dictated by the changing needs of the College. The post holder will be expected to undertake other duties as appropriate and as requested by his/her manager.

The post holder may be required to work at any of the locations at which the business of Royal Holloway is conducted.