JOB DESCRIPTION

<table>
<thead>
<tr>
<th>Job Title:</th>
<th>Research Assistant for Trustworthy Computing and Virtual TPM Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department / Unit:</td>
<td>Information Security Group</td>
</tr>
<tr>
<td>Grade:</td>
<td>RHUL 6</td>
</tr>
<tr>
<td>Accountable to:</td>
<td>Dr Daniele Sgandurra (PI)</td>
</tr>
<tr>
<td>Accountable for:</td>
<td>Head of Department</td>
</tr>
</tbody>
</table>

Purpose of the Post

The Information Security Group at Royal Holloway, University of London, is seeking a part-time highly motivated research assistant for the EU Horizon2020-funded FutureTPM project. The successful candidate will join the Systems and Software Security Lab (S3Lab), working on the development and integration of quantum-resistant cryptography into the Trusted Platform Module (TPM), on the development of a virtual quantum-resistant TPM for KVM, and on research activities of the project.

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.

Key Tasks

The main responsibilities of the post are:
- Integration/porting of QR algorithms SPHINCS and BIKE in the software QR-TPM
- Implementation of a virtual QR-TPM running on KVM that implements the QR functionalities available on a software TPM:
  - 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
  - others if needed (e.g., migration)
- Integration and test of the vTPM with a FutureTPM use case (device management)
  - make available a set of predefined TPM commands to the use case described in existing FutureTPM deliverables
- Attending FutureTPM conference calls in all relevant Work Packages
- Collaborating with the FutureTPM project partners towards common goals
  Collaborating on research papers describing the results of the developed work

## 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.