Candidate Information

Position:	Research Fellow - Network Security for Critical Infrastructure
School/Department:	School Office (Elect, Elect Eng & Comp Sci)
Reference:	26/113749
Closing Date:	Monday 30 November 2026
Salary:	£42,972 - £48,339 per annum
Anticipated Interview Date:	Thursday 10 December 2026
Duration:	30 months or available until 30 June 2029, whichever is soonest

JOB PURPOSE:

This role addresses research into network security for critical infrastructure, such as gas, water, and electrical grids. This specifically concerns Cyber-Physical Systems (CPS) and the complex integration of IT-OT environments. The role requires a deep understanding of programmable networking, network traffic analysis and machine-learning for traffic profiling and monitoring and intrusion detection and prevention. A core activity will be the investigation of traffic profiling and monitoring and intrusion detection on encrypted traffic in a zero-trust, programmable network architecture. You will conduct research to collect network telemetry/observability data and design and implement in-network machine-learning-based intrusion detection mechanisms. The role involves close collaboration with networking researchers integrating the IDS with in-network access control and policy enforcement. The role also involves collaboration with AI researchers integrating the in-network IDS with endpoint AI detection and agentic response models

MAJOR DUTIES:

Research:

1. Undertake high-quality and novel research in the area of network security for critical infrastructure, in the context of threat detection in zero trust, programmable networks.
2. Design, develop, and refine experiments to evaluate in-network threat detection and response approaches, using testbeds that reflect real-world IT-OT critical infrastructure networks and devices.
3. Carry out analyses, critical evaluation, and interpretation using zero trust, programmable network methodologies and other techniques appropriate to IT-OT systems.
4. Coordinate research tasks, work packages, deliverables and publications with external academic research partners and industrial collaborators, including external visits where appropriate.
5. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
6. Prepare material, in consultation with the line manager, for publication in national and international journals and presentations at international conferences such as IEEE Security and Privacy and ACM Computer and Communications Security.
7. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
8. Undertake supplementary duties relevant to the success of the project including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Normally have or about to obtain* a PhD in computer science, engineering or physical sciences area. *Thesis must be submitted and examination process completed within 3 months of closing date of post.
2. Significant, relevant high quality research experience in cyber security and programmable networking, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Demonstrable competency in network programming (e.g., hands-on experience with P4, bmv2 and Mininet or OpenFlow SDN)
4. Demonstrable competency in network security systems design (e.g., software implementation of intrusion detection systems).
5. Software programming skills.
6. Excellent oral and written communication skills. Articulate, confident, and able to clearly communicate complex concepts.
7. Ability to work closely with other members of a large multidisciplinary team.
8. Prepared to work closely with industrial collaborators.

9. Ability to assess and organise resources and balance competing priorities.
10. Demonstrates a high degree of integrity, honesty and openness in professional conduct.
11. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
12. On-site presence required in accordance with QUB policy (currently for a minimum 3 days per week).

DESIRABLE CRITERIA:

1. Have or be about to obtain a PhD in an area related to programmable networking or cyber security.
2. Competency in applied machine learning (e.g., skills in designing and implementing ML models in Keras, PyTorch or Tensorflow for practical use cases).
3. Domain knowledge of critical infrastructure related technologies (IT-OT, CPS, ICS, etc.)
4. Proficient in Python or C
5. Experience related to intrusion detection methods.
6. Experience in network penetration testing.
7. Experience in initiating and developing research plans.
8. Experience in successful research with external partners (e.g. joint research publications or deliverables).