

Candidate Information

Position: Research Fellow in Cyber Security and Digital Twins
School/Department: Centre for Secure Information Technologies
Reference: 23/110926
Closing Date: Monday 5 June 2023
Salary: £36,333 per annum
Anticipated Interview Date: Wednesday 21 June 2023
Duration: Fixed Term for 36 months, or available until 31/05/2026, whichever is sooner.

JOB PURPOSE:

To investigate new research opportunities in, 1) the security of Digital Twins, and 2) the use of Digital Twins to support cyber security monitoring and attack responses for Cyber-Physical Systems (CPS).

To research novel methods in digital twins for cyber security and resilience, CPS modelling and control approaches, and applying machine learning/AI approaches for security.

To develop CPS use-cases, integrate testbeds, and perform experiments to prove novel security techniques.

MAJOR DUTIES:

1. Investigate security challenges and threats introduced by the integration of Digital Twin technologies into emerging applications (such as electrical smart grids, smart manufacturing facilities, robots, avionics systems, and emerging autonomous systems), and to propose novel solutions to mitigate these threats.
2. Investigate Digital Twin models and technologies, and their potential application to improve cyber security and resilience in cyber physical systems (CPS).
3. Design, develop and refine methods for formally analysing cyber physical systems, taking account of system architectures, sub-systems, components, control loops, embedded computing platforms, cyber trust boundaries, communication networks, threat models, etc. This may involve the adaption or extension of established methods and frameworks, such as Data-Flow-Diagrams, OCTAVE, PASTA, STRIDE, etc.
4. Develop CPS use-cases and testbeds to analyse and critically evaluate proposed solutions.
5. Produce high quality research outputs consistent with project aims and commensurate with career stage and experience. This will include collaborating and co-authoring with PI and project team (as appropriate) on outputs.
6. In consultation with the project team, present research milestones and outputs at national and international conferences, and journals (commensurate with career stage and experience).
7. Assist grant holder in the preparation of funding proposals and applications to external bodies.
8. Carry out occasional educational supervision, demonstrating or lecturing duties within the post holder's area of expertise and under the direct guidance of a member of academic staff.
9. Undertake supplementary duties relevant to the success of the project including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Have (or about to obtain) a PhD in Computer Science, Electrical and Electronic Engineering, or a related discipline.
2. At least 3 years of research/work experience (including PhD research) in an area related to cyber-security, or an area related to cyber physical systems (such as systems engineering, control systems, or formal modelling) with experience related to IT systems.
3. Strong publication record, commensurate with stage of career.
4. Proven ability to contribute to broader management and administrative processes.
5. Contribute to the School's outreach programme by links with industry, community groups etc.

6. Sufficient breadth and depth of specialist knowledge in the discipline and of research methods and techniques to work within established research programmes.
7. Practical problem-solving skills, independence of thought and initiative.
8. Proven ability to communicate complex information effectively in oral and written format.
9. Demonstrable ability to assess and organise resources.
10. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.

DESIRABLE CRITERIA:

1. PhD in an area related to cyber security, digital twins, cyber-physical system security.
2. Good software development skills.
3. Academic research experience in application of analysis methods such as STRIDE, MITRE ATT&CK, Cyber Kill Chain, etc.
4. Experience related to digital twin development.
5. Experience in successful research with external partners (e.g. joint research publications or deliverables).