Candidate Information

Position: Research Fellow in AI for Industrial Control System Security
School/Department: School of Electronics, Electrical Engineering and Computer Science
Reference: 24/112194
Closing Date: Monday 21 October 2024
Salary: £46,249 per annum.
Anticipated Interview Date: Wednesday 30 October 2024
Duration: Fixed term for 36 months

JOB PURPOSE:

To perform research in AI for industrial control system (ICS) security. The role involves gaining a deep understanding of how AI systems can be applied to secure ICS against malware and related advanced persistent threats (APTs) relevant to a partner company. A key requirement is to design explainable deep neural networks (DNNs), extending the latest state-of-the-art research into APT and anomaly detection using both proprietary and public datasets.

MAJOR DUTIES:

1. Undertake high-quality and novel research in deep-learning-based industrial control system (ICS) security. This will involve developing explainable anomaly detection and intrusion detection techniques that work with networking and industrial-process-based features and creating novel explainability techniques tailored to the ICS domain.
2. Design, develop, and refine experiments to evaluate deep-learning-based ICS security system performance and explainability.
3. Carry out analyses, critical evaluations, and interpretations using methodologies and other techniques appropriate to AI for ICS security.
4. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
5. Prepare material, often 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 in Computers and Communication Security.
6. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
7. Undertake supplementary duties relevant to the project's success, including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Normally have or about to obtain a PhD in engineering or physical sciences area.
2. Recent high quality research experience in machine learning/deep learning or cybersecurity, or both, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Proficient in Python. Experience using neural network libraries such as PyTorch, Keras, and/or TensorFlow.
4. Ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets.
5. Ability to assess and organise resources.
6. A consummate team player who is open-minded and is prepared to work closely with other members of a large multidisciplinary research and development team, as well as with industrial collaborators.
7. Evidence of being a strong communicator with excellent oral and written communication skills.
8. Demonstrate resilience and the ability to work in a fast-changing environment with competing priorities.
9. Demonstrates a high degree of integrity, honesty and openness in professional conduct.
10. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
11. On-site presence required for minimum 3 days per week.

DESIRABLE CRITERIA:

1. Normally have or about to obtain a PhD in the area of machine learning/AI, cybersecurity or cyberAI.
2. Experience with explainable AI techniques such as LIME, SHAP, and counter-factual explanations.
3. Experience in initiating and developing research plans.
4. Experience in collaborating with industry.
5. Experience in ICS operations, security, Programmable Logic Controllers, or protocols such as Modbus, Profinet, IEC60870 or IEC 61850.
6. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc).
7. Demonstrable commitment to the purpose and objectives of CSIT and Cyber AI Hub.