School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Funding and application details

Funding status: Fully funded project (worldwide)

Application instructions:
Detailed instructions are available at https://blogs.napier.ac.uk/scebe-research/available-phd-student-projects/

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- DIRECTOR OF STUDY: Kehinde Oluwatoyin Babaagba (Email: K.Babaagba@napier.ac.uk)
- 2ND SUPERVISOR: Dr N Moradpoor and Dr Oluwaseun Bamgboye

Subject Group: Computer science

Research Areas: Computer Science

Project Title: Adversarial Learning for Industrial Control Systems

Project description:

Cyber-attacks are increasingly posing more and more threat to information assets and computer systems in general. This is particularly so in industrial control systems which refer to a generalized group of automation systems employed in controlling and keeping track of industrial and manufacturing facilities [1]. The preservation of such safety critical systems against cyber-attacks is germane as there are far reaching effects of these systems being compromised as such attacks can affect physical objects and potentially lead to accidents and in some cases claiming human lives.

Adversarial learning has been proposed as a means of protecting industrial control systems from cyber-attacks [2] and [3]. This method is designed to generate malware that takes advantage of the loopholes in ML models. It usually uses deep convolutional neural network to collect data employed in the analysis of malicious software, particularly in the categorization of samples as either clean or malicious. A different network is designed to generate malicious samples to be identified by the initial network as benign. At first, the network performs poorly but with more iterations, this leads to an increased ability of the malware created to go undetected [4].

In the proposed research, an adversarial learning approach would be used in detecting attacks to industry control systems. This would involve the creation of adversarial attacks and the training of ML models in detecting the generated attacks in a competition setting.

References:

[1] E. D. Knapp and J. T. Langill, “Chapter 2 - about industrial networks,” in Industrial Network Security (Second Edition), second edition ed., E. D. Knapp and J. T. Langill, Eds. Boston: Syngress, 2015, pp. 9–40.

[2] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, “Adversarial attacks on machine learning cybersecurity defences in industrial control systems,” Journal of Information Security and Applications, vol. 58, p. 102717, 2021.

[3] S. K. Alabugin and A. N. Sokolov, “Applying of generative adversarial networks for anomaly detection in industrial control systems,” in 2020 Global Smart Industry Conference (GloSIC). IEEE, 2020, pp. 199–203.

[4] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” in Advances in Neural Information Processing Systems 27, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, Eds. Curran Associates, Inc., 2014, pp. 2672–2680.

[5] K. O. Babaagba, Z. Tan, and E. Hart, “Automatic Generation of Adversarial Metamorphic Malware Using MAP-Elites,” in 23rd European Conference on the Applications of Evolutionary and bio-inspired Computation, pp. 1–16, 2020.

Candidate characteristics

Education:

A first-class honours degree, or a distinction at master level, or equivalent achievements in Computer Science, Cyber Security or Artificial Intelligence.

Subject knowledge:

A good fundamental knowledge of Cybersecurity, Artificial Intelligence, Machine Learning and Malware Analysis.

Essential attributes:

- Experience of fundamental software engineering and cybersecurity
- Competent in one or more programming languages
- Knowledge of Machine Learning and interested in Malware Detection techniques
- Good written and oral communication skills

- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes: