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

PHD STUDENT PROJECT

Application instructions:
Detailed instructions are available at :
https://www.napier.ac.uk/research-and-innovation/doctoral-college/how-to-apply

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: Prof Emma Hart and Dr Z Tan

Subject Group: Computer Science

Research Areas: Computer Science

Project Title: Defeating complex families of malware using evolutionary based adversarial learning.

Project description:

Malicious attacks account for a significant portion of attacks to information assets and computer networks in organisations today. More specifically, dangerous groups of malware that transform their code structures between generations such as metamorphic malware, provide a greater attack surface for the perpetuation of cybercrimes. This group of malware evade detection by conventional Machine Learning models using a number of code obfuscation strategies thus making them hard to detect.

The proposed research will involves the use of evolutionary based adversarial learning approaches in defeating complex and dangerous malicious groups such as polymorphic and metamorphic malware. This involves the use of adversarial learning strategies in the generation of malicious mutants and the augmentation of training data with the produced mutants to improve the classification of such families of malware.

References:

[1] K. O. Babaagba, Z. Tan, and E. Hart, “Nowhere Metamorphic Malware Can Hide - A Biological Evolution Inspired Detection Scheme,” Commun. Comput. Inf. Sci., vol. 1123 CCIS, pp. 369–382, 2019.

[2] 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.

[3] K. O. Babaagba, Z. Tan, and E. Hart, “Improving Classification of Metamorphic Malware by Augmenting Training Data with a Diverse Set of Evolved Mutant Samples,” 2020 IEEE Congr. Evol. Comput. CEC 2020 - Conf. Proc., 2020.

[4] F. Wang, S. Yang, C. Wang, Q. Li, K.O. Babaagba and Z. Tan, “Toward machine intelligence that learns to fingerprint polymorphic worms in IoT,” International Journal of Intelligent Systems, March 27, 2022.

[5] L. Turnbull, Z. Tan, and K.O. Babaagba. “A Generative Neural Network for Enhancing Android Metamorphic Malware Detection based on Behaviour Profiling,” In 2022 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1-9. IEEE, 2022.

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:

- Knowledge of Evolutionary Computing