

Department	School of Computing
Supervisors	Dr. Kehinde Oluwatoyin Babaagba, Prof Emma Hart and Dr Thomas Tan
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 involve 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.

Prospective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisors.

Academic qualifications

A first degree (at least a 2.1) ideally in Computer Science, Cyber Security or Artificial Intelligence with a good fundamental knowledge of Cybersecurity, Artificial Intelligence, Machine Learning and Malware Analysis.

English language requirement

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. [Full details of the University's policy](#) are available online.

Essential attributes:

- Experience of fundamental software engineering and malware analysis
- Competent in one or more programming languages
- Knowledge of Malware Detection techniques, Machine Learning and Adversarial Learning
- 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 and experience using Evolutionary Algorithms

Indicative Bibliography	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Enquiries	For informal enquiries about this PhD project, please contact k.babaagra@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process