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

PHD STUDENT PROJECT

Funding and application details

Funding status: Self funded students only

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: Mouad Lemoudden (Email: M.Lemoudden@napier.ac.uk)
- 2ND SUPERVISOR: Richard Macfarlane

Subject Group: Cyber-security and system engineering

Research Areas: Cyber Security

Project Title: Towards an Evolving Approach to Evaluate Security Monitoring Tools

Project description:

With continuing growth in the size of computer networks and applications, the potential damage that can be caused is increasing. Intrusion detection is a common cyber security mechanism used to detect malicious activities in host and/or network environments. Given the importance of intrusion detection, research and industry have designed and developed a variety of intrusion detection systems (IDS). Due to the lack of adequate datasets, in addition to the fundamental shortcomings of using them, anomaly-based approaches in intrusion detection systems lack a strong evaluation methodology.

From a scientific and operational point of view, it is necessary to evaluate detection solutions to understand their limits and to determine how to improve them. Traditionally, IDS are evaluated based on their detection performance against a labelled dataset that contains normal and malicious network traffic. Upon inspection, the datasets publicly available are usually obsolete in the span of a couple years in both anomaly types and background, benign Internet traffic. They also suffer from a lack of volume and diversity in traffic, and ultimately, lack of representativeness and realism.

In this PhD project, the successful candidate will explore the current state of the art on security monitoring evaluation and then develop a new approach for an evolving platform for IDS evaluation that solves many of the issues that exist in current methods. The approach will make use of state of the art generative tools in the field of artificial intelligence and apply them to generate normal and malicious traffic. The approach will provide a key solution to one of the biggest concerns of current Intrusion Detection Systems.

References:

[1] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147-167.

[2] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.

[3] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108-116.

Candidate characteristics

Education:

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

Subject knowledge:

- Cyber Security

Essential attributes:

- Experience of fundamental Computer Science
- Competent in Cyber Security
- Knowledge of Intrusion Detection
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Experience with artificial intelligence/machine learning would be beneficial