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: Dr Nikolaos Pitropakis (Email: n.pitropakis@napier.ac.uk)
- 2ND SUPERVISOR: Dr Sana Ullah Jan

Subject Group: Cyber Security and Systems Engineering

Research Areas: Cyber Security, Artificial Intelligence, Machine Learning

Project Title: Exploring cyberattacks against AI and their real-world impact

Project description:

Artificial Intelligence (AI) applications have invaded every aspect of daily life, significantly expanding the threat landscape and making AI systems prime targets for malicious actors. These adversaries aim to compromise AI systems by maliciously altering training data (poisoning attacks) or test data (evasion attacks). This project seeks to identify new attack vectors across various application domains, highlighting their vulnerabilities to AI-targeted attacks and their potential impact on everyday activities. Furthermore, the project will develop and test countermeasures to enhance the robustness of AI systems against such cyberattacks. Ultimately, a novel testbed framework will be established to support the global cybersecurity community in the ongoing arms race against these malicious parties.

References:

Pitropakis, N., Panaousis, E., Giannetsos, T., Anastasiadis, E., & Loukas, G. (2019). A taxonomy and survey of attacks against machine learning. Computer Science Review, 34, 100199.

Gallagher, M., Pitropakis, N., Chrysoulas, C., Papadopoulos, P., Mylonas, A., & Katsikas, S. (2022). Investigating machine learning attacks on financial time series models. Computers & Security, 123, 102933.

Papadopoulos, P., Thornewill von Essen, O., Pitropakis, N., Chrysoulas, C., Mylonas, A., & Buchanan, W. J. (2021). Launching adversarial attacks against network intrusion detection systems for iot. Journal of Cybersecurity and Privacy, 1(2), 252-273.

Kantartopoulos, P., Pitropakis, N., Mylonas, A., & Kylilis, N. (2020). Exploring adversarial attacks and defences for fake twitter account detection. Technologies, 8(4), 64.

Marchand, B., Pitropakis, N., Buchanan, W. J., & Lambrinoudakis, C. (2021). Launching Adversarial Label Contamination Attacks Against Malicious URL Detection. In Trust, Privacy and Security in Digital Business: 18th International Conference, TrustBus 2021, Virtual Event, September 27–30, 2021, Proceedings 18 (pp. 69-82). Springer International Publishing.

Candidate characteristics

Education:

Minimum 2:1 degree in Computer Science, Cyber Security

Subject knowledge:

Artificial Intelligence, Machine Learning, Cyber Security

Essential attributes:

- Competence in one or more programming languages
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Competence in Python
- Competence in C++
- Fundamental knowledge of CUDA library