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://www.napier.ac.uk/research-and-innovation/research-degrees/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: Bill Buchanan (Email: B.Buchanan@napier.ac.uk)
- 2ND SUPERVISOR: La Spada, Luigi

Subject Group: Cyber-security and system engineering

Research Areas: Artificial Intelligence, Cyber Security, Data Science, Machine Learning, Networks

Project Title: Large Language Models (LLMs) for Cryptographic and Cybersecurity Threat Model Building

Project description:

LLMs can be applied to cryptography and cybersecurity by taking weakly structured definitions in written English and then matching these to formal models. This includes structured definitions for cryptographic methods and then matching to cryptographic primitives [10]. With cybersecurity, it is also possible to match LLMs to formal models, such as with the MITRE framework [1-7] and to take a stateful approach to matching network traffic profiles to threat actors and associated campaigns [8]. This PhD aims to thus match vague abstractions of a cybersecurity threat, and link these to more formal models, and then into associated mitigation techniques, including how adversaries could modify threats to overcome existing network defences.

References:

[1] A. Happe and J. Cito, “Getting pwn’d by ai: Penetration testing with largelanguage models,” arXiv preprint arXiv:2308.00121, 2023.

[2] U. Iqbal, T. Kohno, and F. Roesner, “Llm platform security: Applying a systematic evaluation framework to openai’s chatgpt plugins,” arXiv preprint arXiv:2309.10254, 2023.

[3] P. Charan, H. Chunduri, P. M. Anand, and S. K. Shukla, “From text to mitre techniques: Exploring the malicious use of large language models for generating cyber attack payloads,” arXiv preprint arXiv:2305.15336, 2023.

[4] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, “Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping,” in 2020 Resilience Week (RWS), pp. 106–112, IEEE, 2020.

[5] W. Xiong, E. Legrand, O. ˚Aberg, and R. Lagerstr¨om, “Cyber security threat modeling based on the mitre enterprise att&ck matrix,” Software and Systems Modeling, vol. 21, no. 1, pp. 157–177, 2022.

[6] V. Mavroeidis and S. Bromander, “Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence,” in 2017 European Intelligence and Security Informatics Conference (EISIC), pp. 91–98, IEEE, 2017.

[7] E. Garza, E. Hemberg, S. Moskal, and U.-M. O’Reilly, “Assessing large language model’s knowledge of threat behavior in mitre att&ck,” 2023.

[8] R. Fayyazi and S. J. Yang, “On the uses of large language models to interpret ambiguous cyberattack descriptions,” arXiv preprint arXiv:2306.14062, 2023.

[9] S. Moskal, S. Laney, E. Hemberg, and U.-M. O’Reilly, “Llms killed the script kiddie: How agents supported by large language models change the landscape of network threat testing,” arXiv preprint arXiv:2310.06936, 2023

[10] Dong Kwon, Minjoo Sim, Gyeongju Song, Minwoo Lee, and Hwajeong Seo. Novel approach to cryptography implementation using chatgpt. Cryptology ePrint Archive, 2023

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in a Computer Science-related area or Electronic Engineering with a good fundamental knowledge of software development.

Subject knowledge:

- Cybersecurity

Essential attributes:

- Experience of fundamental areas of cybersecurity.
- Competent in software development
- Knowledge of cloud-based systems.
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Strong interest in encryption and cryptography.