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: Professor Ashkan Sami (Email: a.sami@napier.ac.uk)
- 2ND SUPERVISOR: tbc

Subject Group: Computer Science

Research Areas: Software Engineering, Artificial Intelligence, Cyber Security, and Data Science

Project Title: Secure Code Generation with Foundation Models

Project description:

The PhD aims to evaluate the security of code generated by foundation models, with a primary focus on identifying vulnerabilities and potential threats that could pose risks to software systems and data. As the use of generated codes in software development becomes increasingly prevalent, ensuring the security of generated code is of paramount importance. This doctoral thesis embarks on an in-depth exploration of the security implications and vulnerabilities inherent in code generated by foundation models. As the adoption of AI in software development becomes increasingly widespread, the need for a comprehensive understanding of the security risks associated with generated code is paramount. This research project aims to provide valuable insights, tools, and guidelines to enhance the security of AI-assisted development.

Objectives:

The key objectives of this project include:

1) Analyzing the code generation process of foundation models to understand potential security implications. Identifying common vulnerabilities and coding errors present in generated code.
2) Developing a comprehensive set of security guidelines and best practices for using foundation model generated code.
3) Creating tools and automated processes so foundation model generated code are more secure.
4) Raising awareness about the potential security challenges associated with generated code.

Several researchers have identified even Large Language Models create vulnerabilities [1] and [2]. Our team is well known for its works on Software Security [3]. BBC, The Register has published articles on our researches and StackOverflow published blogs about them. We are to investigate how to use Foundation Models to create secure code.

The research is expected to yield a more efficient and secure approach to code generation in software development. This could potentially reduce the incidence of security vulnerabilities and improve the overall quality of software. Additionally, it could lead to the development of tools that assist developers in producing secure code more rapidly and with fewer errors.

References:

[1] [1] M. L. Siddiq, S. H. Majumder, M. R. Mim, S. Jajodia, and J. C. S. Santos, “An Empirical Study of Code Smells in Transformer-based Code Generation Techniques,” Limassol, Cyprus, Oct. 2022, (Accepted for Publication). [Online]. Available: https://s2e-lab.github.io/preprints/scam22-preprint.pdf

[2] [2] H. Pearce, B. Ahmad, B. Tan, B. Dolan-Gavitt, and R. Karri, “Asleep at the Keyboard? Assessing the Security of GitHub Copilot’s Code Contributions,” in 2022 IEEE Symposium on Security and Privacy (SP), May 2022, pp. 754–768, iSSN: 2375-1207.

[3] [3] M. Verdi, A. Sami, J. Akhondali, F. Khomh, G. Uddin and A. K. Motlagh, "An Empirical Study of C++ Vulnerabilities in Crowd-Sourced Code Examples," in IEEE Transactions on Software Engineering, vol. 48, no. 5, pp. 1497-1514, 1 May 2022, doi: 10.1109/TSE.2020.3023664.

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in Computer Science, Software Engineering, Cyber Security and Artificial Intelligence

Subject knowledge:

- Software Programming

Essential attributes:

- Experience of software engineering, AI and cyber security
- Competent in computer programming
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Expertise in Software Security