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: Rich Macfarlane (Email: R.Macfarlane@napier.ac.uk)
- 2ND SUPERVISOR: tbc

Subject Group: Cyber-Security and Systems Engineering

Research Areas: Cyber Security

Project Title: Behavioural Analysis for Ransomware and Extortion-based Attack Detection

Project description:

Edinburgh Napier University's Cyber Security and Forensics Research Group focuses on applied research in areas of threat analysis and detection, digital forensic triage, trust, identity and cryptography, and has had successful real world impact with several spin-out companies. A ransomware research group led by Rich Macfarlane has been working in the areas of ransomware attack analysis, detection and mitigation for several years.

Ransomware attacks include a range of behaviours at various stages of the attack model, including recon, data exfiltration, and data encryption, aimed at extortion from a victim. Crypto ransomware malware when used in attacks, typically locks user data, alongside double extortion which also involves exfiltration of sensitive data. A payment is typically then demanded from the victim in return for the safe return of access to their files and data. Over the last few years ransomware has become an ever growing threat to corporate as well as personal data, and has seen rapidly evolving tactics and techniques to evade detection and mitigation.

Research work aims to enhance and develop new methods of analysis and detection of extortion-based attacks, particularly focused on behavioural analysis early in the kill chain. A focus on pre-destructive activity detection and dynamic behaviour analysis, including methods to capture and model features such file interactions and staging of data for exfiltration. The scope of the work and focus of the individual project can be, to some extent, driven by the individual student. The work will be carried out within a small team of researchers here at Edinburgh Napier University working at the forefront of ransomware attack research, including various areas around analysis and datasets, detection and mitigation, for crypto ransomware and other extortion-based attacks.

A short research proposal of around 1,000 words outlining the specific project, is expected as part of the application. The project will be supervised by Associate Professor Rich Macfarlane (r.macfarlane@napier.ac.uk) and others from the team. Interested students are encouraged to contact Rich by email to discuss the proposal.

References:

[1] McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. ACM Computing Surveys (CSUR), 54(9), 1-36.

[2] Sihwail, R., Omar, K., & Ariffin, K. A. Z. (2018). A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), 1662.

[3] N. Hampton, Z. Baig, and S. Zeadally, “Ransomware behavioural analysis on windows platforms,” Journal of information security and applications, vol. 40, pp. 44–51, 2018.

[4] Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2023). Majority Voting Ransomware Detection System. Journal of Information Security, 14(4).

Candidate characteristics

Education:

A first degree (at least a 2.1) or MSc ideally in Computer Science-related area with a good fundamental knowledge of computer science and ideally cyber security.

Subject knowledge:

- Cyber Security, Threat Models, Malware Analysis, Dynamic Analysis, Ransomware, File Systems, Networking, Cryptography

Essential attributes:

- Strong focus on applied cyber security concepts, such as the attack kill chain, classification of threat information, offensive security, or dynamic analysis.
- Good written and oral communication skills.
- Strong motivation, with evidence of independent research skills.
- Good organisation and time management skills.

Desirable attributes:

- Research skills.
- Programming and software testing.
- Ransomware, and malware analysis.