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 Naghmeh Moradpoor (Email: n.moradpoor@napier.ac.uk)
- 2ND SUPERVISOR: Dr Erisa Karafili

Subject Group: Cyber Security and System Engineering

Research Areas: Computer Science - Cyber Security

Project Title: An Electric Vehicle and Electric Vehicle Charging Station Incident Response Playbook

Project description:

In the rapidly evolving realm of electric vehicle technology, safeguarding the cybersecurity of both electric vehicles and their charging infrastructure has become fundamental. The integration of electric vehicles and their charging stations into the broader grid introduces complex cybersecurity challenges, necessitating robust incident response strategies. Traditional cybersecurity playbooks often fall short in addressing the unique vulnerabilities associated with electric vehicles and their charging systems. The lack of publicly available community playbooks tailored to these needs leaves the electric vehicle ecosystem vulnerable to cyber threats that could compromise user privacy, vehicle functionality, and grid stability. In response to this, the project aims to create a foundational playbook for electric vehicle and electric vehicle charging station incident response, addressing a significant void in current cybersecurity practices. This includes a comprehensive threat modelling to identify potential threats, vulnerabilities, and attack vectors, considering the specific risks to EVs and EVCs, to design more efficient incident response strategies.

References:

[1] Applebaum, A. et al. (2018) ‘Playbook oriented cyber response’, 2018 National Cyber Summit (NCS) [Preprint]. doi:10.1109/ncs.2018.00007.

[2] Banafshehvaragh, S.T. and Rahmani, A.M. (2023) ‘Intrusion, anomaly, and attack detection in smart vehicles’, Microprocessors and Microsystems, 96, p. 104726. doi:10.1016/j.micpro.2022.104726.

[3] TISZA, O. C. (2022). Federal Government Cybersecurity Incident & Vulnerability Response Playbooks.

[4] Johnson, J. et al. (2022) ‘Review of Electric Vehicle Charger Cybersecurity vulnerabilities, potential impacts, and defenses’, Energies, 15(11), p. 3931. doi:10.3390/en15113931.

[5] Muhammad, Z. et al. (2023) ‘Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability’, Energies, 16(3), p. 1113. doi:10.3390/en1603111

Candidate characteristics

Education:

A first degree (a minimum 2:1) in Cyber Security, Computing

Subject knowledge:

Cyber Security, Programming Knowledge

Essential attributes:

- Experience of fundamental cybersecurity
- Competent in software development and algorithmic design
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management