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: Prof. Bill Buchanan (Email: b.buchanan@napier.ac.uk)
- 2ND SUPERVISOR: Dr Jawad Ahmad

Subject Group: Cyber Security and System Engineering

Research Areas: Cyber Security, Data Science, Networks, Software Engineering

Project Title: zk-Cloud Forensics: Privacy-Aware and Tamper-proof Cloud Forensics using a Public Key Trust Infrastructure

Project description:

In order to detect contraband content within a cloud-based system, it is possible to sample fragments of data [1] and match them against hashed values. We can then use a Bloom filter to detect whether these fragments match to well-known contraband content [2]. With this, a Bloom filter can store the hash signatures of data fragments, and where the filter does not reveal the stored hash values. This approach preserves the privacy of the data contained in the filter, as opposed to using a hash-based table for matching. Unfortunately, the Bloom filter can be fairly large in its operation, and where it is difficult to fully secure the trustworthiness of the match. Along with this, the sharing of matches often does not have the required levels of trust and privacy.

This research work will investigate an integrated framework for the matching and sharing processes, and which is privacy-aware in its approach. Methods for this include a Multilayer Compressed Counting Bloom Filter [4], Public Key

Accumulators [3], and Zero-Knowledge Proofs (ZKPs) [5]. These can then be integrated into a trusted digital forensics data-sharing infrastructure, and where public key signing can be used to share trusted samples of fragments and associated proofs.

Research work will also look to integrate a permissioned blockchain infrastructure in the creation of a trusted infrastructure for public key management and identity provision.

Why undertake this PhD? The work will be undertaken with the Blockpass ID Lab at Edinburgh Napier and which is the first research lab in the world to focus on identity and trust, and is advancing in many areas of privacy-aware systems. This lab is led by Prof Bill Buchanan and who has a long track record of success in creating highly successful spin-out companies (Zonefox, Symphonic and Cyan Forensics), and in commercialising research work. This research work has the potential to build into a licencing or spin-out opportunity and is likely to involve collaboration with a range of law enforcement agencies.

References:

[1] Penrose, P., Macfarlane, R., & Buchanan, W. J. (2013). Approaches to the classification of high entropy file fragments. Digital Investigation, 10(4), 372-384.

[2] Penrose, P., Buchanan, W. J., & Macfarlane, R. (2015). Fast contraband detection in large capacity disk drives. Digital Investigation, 12, S22-S29.

[3] Ren, Y., Liu, X., Wu, Q., Wang, L., & Zhang, W. (2022). Cryptographic Accumulator and Its Application: A Survey. Security and Communication Networks, 2022.

[4] Ye, F., Zheng, Y., Fu, X., Luo, B., Du, X., & Guizani, M. (2022). TamForen: a tamper-proof cloud forensic framework. Transactions on Emerging Telecommunications Technologies, 33(4), e4178.

[5] Li, M., Lal, C., Conti, M., & Hu, D. (2021). LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Generation

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
- Software Development

Essential attributes:

- Experience of fundamental areas of cybersecurity, encryption and trust.
- 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.