AI and Cyber Security for Cyber Physical Systems

Contact: Dr. Mujeeb Ahmed, Mujeeb.ahmed@newcastle.ac.uk

1. **Recovery from Cyber Attacks in Cyber-Physical Systems**

This position focuses on the recovery from cyber attacks in Cyber-Physical Systems (CPS). This research will delve into the unique challenges and open problems associated with this critical aspect of cybersecurity. Unlike traditional IT systems, CPS integrate computational and physical components, making them inherently more complex. This complexity, coupled with the real-world impact of these systems, makes recovery from cyber attacks a challenging task. The interconnected nature of CPS means that an attack on one component can have cascading effects, complicating the recovery process. This studentship offers a unique opportunity to contribute to a cutting-edge field of study and make significant advancements in the security of Cyber-Physical Systems. Applicants should have a strong background in computer science, electrical engineering, or a related field, and a keen interest in cybersecurity.

2. **Side channel based IoT malware detection**

In the realm of Internet of Things (IoT) systems, side-channel based malware detection presents a promising approach to enhance security. This method leverages the fact that malware, alters certain secondary characteristics of the system, such as power consumption, heat generation, or processing time. By monitoring these side-channels, it is possible to detect anomalous patterns indicative of malware activity. This approach does not require the malware to be active to be detected, making it a powerful tool for proactive defense. It holds significant potential for safeguarding IoT devices, which are often the targets of sophisticated cyber-attacks due to their ubiquitous nature and the valuable data they hold.

3. **Global Scale Digital Forensics for CyberPhysical Systems**

Forensics often takes place in a local context. However, to detect attacks, protect systems, recover operations, and identify attackers in cyberphysical systems requires cooperation across a number of defenders -- the cyberphysical network and the core. Indeed ISP networks have visibility into 60-70% of network traffic however, they don't have the intelligence or the context of the local cyberphysical system in order to attribute attacks or detect stepping stones. Specifically, this project aims to develop methods and tools to address the challenges of visibility, scale, privacy, false-positives, and cooperation.

4. **AI/LLMs in Cybersecurity**

This topic focuses on the exploration of Language Learning Models (LLMs) in the field of cybersecurity. This research will delve into the dual nature of LLMs, examining both their positive contributions and potential threats to security and privacy, as well as addressing the open challenges in this field. On the positive side, LLMs have shown significant promise in enhancing code security and data security, outperforming traditional approaches in areas such as secure coding, test case generation, vulnerable code detection, malicious code detection, and code fixing. They have also been instrumental in ensuring data integrity, confidentiality, reliability, and traceability. However, LLMs also have offensive applications, including hardware-level attacks, OS-level attacks, software-level attacks, network-level attacks, and user-level attacks. This studentship offers a unique opportunity to contribute to this cutting-edge field of study, and we invite applications from candidates with a strong interest in AI, LLMs, and cybersecurity.

Successful students will be associated with the edge AI hub https://edgeaihub.co.uk/ and the Network and Distributed Systems Security Lab in the School of Computing.