LEVERHULME INTERDISCIPLINARY
NETWORK ON CYBERSECURITY
AND SOCIETY (LINCS)
NOW ACCEPTING APPLICATIONS
Institute for the Study of Conflict Transformation and Social Justice (ISCTSJ)
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES
The Leverhulme Trust

Guidance for Applicants, September 2016 entry

Contents

ABOUT THE PROGRAMME

The Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) at Queen's University Belfast has been established to support pioneering research at the interface between the social sciences and electronic engineering & computer science. LINCS brings together the Institute for the Study of Conflict Transformation and Social Justice (ISCTSJ) and the Centre for Secure Information Technologies (CSIT) to develop a distinctive cohort of doctoral students working across the boundaries of their disciplines who will open up new avenues of enquiry centred initially on the priority themes and specific PhD projects.

The deadline for applications to LINCS's is 5:00pm, Friday 17 June 2016.

WHAT IS AVAILABLE – 2 THREE YEAR STUDENTSHIPS

There are 2 fully funded, three year LINCS PhD studentships which includes;

- Full tuition fees at Standard UK Rates (£4,076 2016/17)[1] for three years
  Full stipend at Standard UK Research Council Rates (£14,198 for 2016/17)[2] for three years
- Research Training and Expenses £1,000 per annum for three years
- Access to additional research funding from a central LINCS research support fund

THERE ARE 4 PRIORITY THEMES

1. **Cybersecurity: Technology and Ethics**
2. **Cyberspace, Privacy and Data Protection** *(no projects available in this call)*
3. **Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspects**
4. **Borders, Security Technologies, Data Gathering and Data Sharing**

Step One:

Before you apply **you will need to explore with our Project Contacts (Professor Sakir Sezer and Dr Philip O'Kane)** whether your area of research interest can be supervised and supported. Please see the **lead supervisor** indicated beside each project.

PRIORITY THEMES AND SPECIFIC PROJECTS

1. THEME - Cybersecurity: Technology and Ethics

PROJECT: A novel application: Behaviour sensing technology for detecting malicious activities within a cloud environment

Lead Supervisor: Dr Philip O'Kane
Co Supervisor: Professor Sakir Sezer
Primary Location: CSIT

Cloud computing is the latest evolutionary step in computing. This evolutionary shift in technology presents a data-rich environment that can be attacked by cyber criminals using novel attack methods to compromise PCs and critical information that can be used to leverage greater profits than attacking conventional defensive barriers such as on premise enterprise network. Malware writers use an extensive range of cloud protocols to breach secure systems and attack internet users. These new attack approaches include bypass detection and geographic blacklisting by serving their malware from within a trusted Cloud provider such as Amazon or Google.

This cloud-based perimeter breach enables attacks to circumvent many of the traditional defence technologies, such as firewalls, intrusion prevention systems and anti-virus software. Hence, new detection technologies based on malicious behaviour is required to guarantee a secure Cloud environment for commerce and internet users alike.

[1] Fee rate for guidance purposes. Research Councils UK (RCUK) has not yet announced doctoral stipend levels and indicative fees for 2016.

[2] Stipend rate for guidance purposes. National Minimum Doctoral Stipend for 2015/16 is £14,057

This research seeks to address the need for new detection technologies by distinguishing between normal user/system behaviour and those would be malicious attack scenarios. In particular, the use of sophisticated anomaly detection algorithms that can be used to fuse multiple features (user and system properties) and behaviours to generate robust detection methods.

The research objectives are:

- Investigate existing detection algorithms and methods.
- Explore new types of quantifiable User behaviour and System behaviour that can be used to differentiate between malicious and benign behaviour.
- Derive anomaly detection algorithm, optimised for virtualized cloud computing environments.
- Prototype and validate the proposed malicious behaviour detection algorithm using the CSIT malware test lab facilities.

Primary Academic Discipline: Computer Science (Cybersecurity)

2. THEME: Cyberspace, Privacy and Data Protection

There are currently no projects in this theme available in this call.

3. THEME - Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspects

PROJECT: Emerging Cyber Bordering Technologies

Named Supervisor: Professor Sakir Sezer
Co Supervisors: Dr Cathal McCall
Primary Location: CSIT

Securing cyberspace borders is a rapidly evolving and crucial area of interest for governments, private sector interests, and individual citizens. Defending cyberspace borders for the protection of critical infrastructure, key resources and sensitive information is a key concern for governments. Yet, as the Edward Snowden case revealed, governments are also deeply implicated in penetrating cyberspace borders for the purpose of information-gathering on friend and foe alike. Similarly, international corporations have a vital interest in securing internal networks, as well as a research and development compulsion to penetrate the cyberspace borders of competitors in the name of innovation.

Firewalls, network-based application and user detection technologies and URL black and white lists present essential technological tools for building borders in cyberspace and preventing cross-border access to web-content. For example, large scale filtering of URLs in China restricts the access of its citizens to many US and European websites. On the other hand, service providers of streamed content (e.g. live football matches, movies, shows etc.) restrict international cross-border access due to broadcast restrictions of licensed content. For example, except BBC News, all Internet-based access to UK TV programmes are restricted by a firewall, ensuring that access is permitted to users within UK jurisdictions only. However, new technologies, based on well-established Virtual Private

Networks (VPNs), and new VPN service providers (CyberGhost, Spotflux, Private Internet Access, Hotspot Shield, ProXPN, etc.) have evolved, providing encrypted anonymous tunnels, capable of penetrating virtual borders and providing anonymous access and hosting of unrestricted content via a country specific proxy server. The majority of these services are used for accessing terrorist or organised-crime related, copyright protected or illegal (offensive, abusive, sexual) content, stored or hosted in states with limited data protection and copyright laws.

The aim of this project is to explore various security, firewall and access control technologies that can be effectively used for policing and enforcing of cyber border policies. Many IT security technologies are developed for the Enterprise market and impose privacy and ethical concerns when they are used for bordering public cyber space. Scalability and global deployment pose technological challenges and potential misuse of intercepted and/or logged information as part of the policing process.

The research objectives are:

- Investigate and evaluate various security technologies that are suitable for cyber bordering and cyber border enforcements.
- In collaboration with AHSS, derive feature specification for cyber bordering technology for national cyber space and national cyber border protection.
- Explore technologies for policing encrypted VPN tunnels without violating user privacy or exposing intellectual property or trade secrets.
- Develop traffic analytics algorithms for cyber border policy enforcement.
- Prototype and validate traffic analytics algorithms and assess their suitability for cyber bordering.
- Assess the proposed analytics algorithms and developed bordering technology in terms of potential misuse for user privacy violation and ethical concerns.

Primary Academic Discipline: Computer Science

4. THEME: Borders, Security Technologies, Data Gathering and Data Sharing

PROJECT: The Internet of Things: Embedded Security Architecture

Lead Supervisor: Professor Sakir Sezer
Co Supervisor: Dr Xin Yang
Primary Location: CSIT

The Internet of Things (IoT) is a paradigm which allows a multitude of devices to be interconnected at any time and any place to gather, communicate, and share data and information across the network to achieve a specific purpose depending on the field of application. Hence, this gives rise to smart environments in various industries which includes transportation, medical and healthcare, energy management, building and home automation etc.

Cloud networks often serve as the backbone technology of IoT networks. IoT devices generally have limited computational and memory capabilities which often use lightweight authentication and identification processes when accessing the IoT networks. This presents a potential security concern of how these devices are accessing the network, and how these devices are being managed as the

IoT services are often being hosted on the cloud servers which could potentially compromise user privacy and data protection.

The aim of this project is to investigate the security aspects of IoT communication, protocols and systems, primarily targeting the vulnerabilities of resource-constrained embedded systems. The diversity and multitude of connected IoT devices requires a robust security framework building upon scalability and resilience.

The research objectives are:

- Investigate and evaluate various security technologies for resources constrained IoT technologies.
- In collaboration with AHSS, explore privacy challenges that IoT security may introduce.
- Explore the security and integrity of IoT communication, protocols and embedded systems
- Develop security architecture for IoT embedded systems.
- Prototype and validate the proposed security architecture.
- In collaboration with AHSS, assess the proposed IoT security architecture in terms of potential misuse.

Primary Academic Discipline: Computer Science

HOW TO APPLY

Step Two: Complete an Online Application Form

All applications must be made via the Queen's University Applications Portal.

You must include the code **LINCS16** on your application form to indicate that you wish to be considered for a LINCS award.

Applicants should chose the option "**I wish to be considered for external funding**" and then enter **LINCS16** in the free text box which follows.

COMPLETING YOUR APPLICATION

- All applicants must provide an up-to-date CV; this should be uploaded to the Admissions Portal as a separate document.[3]
- All applicants are required to provide a **100-400** word statement detailing how their PhD will address the interdisciplinary aspects of the LINCS programme.
- Applicants wishing to propose an interdisciplinary PhD topic of their own, that aligns with one or more of the LINCS priority themes, **must upload a 400 word research proposal** that describes the topic as a separate document. [4] This research proposal must **clearly identify** a potential supervisory team and which of the themes it relates to.
- Applicants must provide the name of an Academic Referee in support. **Failure to provide a referee will result in the application being rejected.**

[3] Please note that **only one document can be uploaded**, you must combine your CV and Research Proposal into one document (word or PDF).

[4] As above note.

- **Please note, failure to include the reference LINCS16 in the free text box may result in your application not being allocated or considered for funding.**

The deadline for applications to LINCS's 2016 competition is **5:00pm, Friday 17 June 2016**.

Please read the applicant guidance notes carefully, which sets out the eligibility criteria and application guidance notes for people wishing to apply for a fully funded, three year LINCS PhD studentship.

ELIGIBILITY CRITERIA AND GUIDANCE NOTES

- Applicants must hold a minimum 2nd Class Upper Degree (2:1) or equivalent qualification in a relevant Technology, Social Science or Humanities Based subject.

- Applicants must be a UK or EU citizen.

- Applications from non-UK or non-EU citizens may be accepted on an exceptional basis but additional funding to cover International student fees is not available and must be secured by the applicant prior to starting.

- Applicants must be proficient in both writing and speaking in English.

- Successful applicants must be prepared to live and work in Northern Ireland for the duration of their studies.

- Interested candidates **must** consult the main topic contact at the earliest possible opportunity to discuss their research plans and application.

THE ONLINE APPLICATION

- Applicants must complete an online application through the Queen's University Applications Portal before the closing date of **5:00pm, Friday 17 June 2016**.

- Please note that **only one document can be uploaded**, you must combine your CV and Research Proposal into one document (word or PDF).

- Failure to include the reference **LINCS16** in the **free text box** may result in your application not being allocated or considered for funding.

APPLY NOW

PROGRAMME CONTACTS

Programme Coordinator	Dr Cathal McCall c.mccall@qub.ac.uk
Training & Skills Coordinators	**CSIT:** Fatih Kurugollu f.kurugollu@qub.ac.uk **AHSS:** Brice Dickson b.dickson@qub.ac.uk
Internationalisation Coordinator	Prof Weiru Liu w.liu@qub.ac.uk
Placements and Partnerships Coordinators	**CSIT:**Dr Kieran McLoughlin kieran.mclaughlin@qub.ac.uk **AHSS:** Dr Muiris MacCarthaigh m.maccarthaigh@qub.ac.uk
Pastoral Support Coordinator	Prof John Morison j.morison@qub.ac.uk
Programme Reporting Coordinator	Dr Cathal McCall c.mccall@qub.ac.uk
Supervisory Teams Coordinators (Theme)	*Cybersecurity: Technology and Ethics* **Prof Sakir Sezer** sakir.sezer@qub.ac.uk *Cyberspace, Privacy and Data Protection* **Dr Tom Walker** tom.walker@qub.ac.uk *Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspects* **Dr Debbie Lisle** d.lisle@qub.ac.uk *Borders, Security Technologies, Data Gathering and Data Sharing* **Prof Hastings Donnan** h.donnan@qub.ac.uk
Research Ethics Officer	Dr Tom Walker tom.walker@qub.ac.uk
Programme Administrator	Mrs Teresa Cotton t.cotton@qub.ac.uk