Case for Support:
Academic Centre-of-Excellence in Cyber Security Research

University of Strathclyde

1 Expertise

The *Security Group* at the University of Strathclyde consists of the following permanent academic members:

Dr. Shishir Nagaraja Reader in Computer Security, who leads the group

Prof. Lilian Edwards Professor of Internet Law and Policy

Dr. James Irvine Reader

Dr. Robert Atkinson Senior Lecturer

Dr. George Weir Lecturer

Dr. Sotirios Terzis Lecturer

It also includes three staff researchers (Dr. Craig Hay, Dr. Greig Paul, Dr. Kinan Ghanem), two staff vacancies, and 27 PhD students.

1.1 Research expertise

The group leads research in the following areas:

- Network Security (Nagaraja, Terzis, Irvine, Atkinson)
- Privacy and Security (Nagaraja, Edwards, Terzis)
- Intrusion detection(Terzis, Nagaraja, Atkinson)
- Human factors and Socio-technical security (Weir and Terzis)
- Security governance (Edwards)
- Machine Learning and Security (Nagaraja, Atkinson)
- Network resilience (Irvine)
- Botnets and Malware (Nagaraja)

2 Background

2.1 Development in the last five years

The security group has been active since 2006. The group has steadily grown to its current size of eight permanent members, five postdocs and 27 PhD students over a period of ten years. The group has broad aims which covers significant aspects of the field of computer security. Its strength is in carrying out practical impact-led security research in close collaboration with real-world users.

2.2 Invited talks

Members of our group are frequently invited to give keynote talks. (nine in 2017, six in 2016).

2.3 Facilities

Due to its practical focus, the group has built and run a number of security testbeds.

The **Experimental Network ArChitectures Testbed (ENACT)** is a specialist testbed for enacting a variety of network-infrastructure scenarios, enabling networked systems research from low-level physical wiring to network protocols and applications, via a software-defined networking (SDN)-capable network testbed. ENACT is currently composed of 1056 switch ports and 96 server ports, using Pica8 3290N switches and Juniper 4500EX switches.

The **Ransom Architectures for Network and Systems Opportunistic Malware (RANSOM) Testbed** enables malware and vulnerability research for opportunistic malware on a cluster farm of desktop, mobile, and server class hardware. RANSOM is composed of an exclusive datacentre that hosts up to 100k virtual machines on a 40Gbps Mellanox network. The farm runs malware honeypots, experimental malware defences, and offensive technologies.

The **Power Network Demonstration Centre (PNDC) Testbed** is an AC electricity grid emulator that enables research on experimental architectures for secure power systems. It helps enact a variety of scenarios from bidirectional 500kVa to 1MVA power systems, thus providing a facility for studying the security of power systems in the face of adversaries. For instance, to create adversarial loads in power systems and adversarial interference in phase balancing mechanisms in high-voltage networks. It is composed of expandable Triphase modular power system hardware within two substations connected by fibre-optic cables, scada interface equipment connected via Cisco connected routers and managed via software-defined controllers.

2.4 Recent investments

Since 2006 the security group has acquired over £3.88 million in research funding, from EPSRC, VMWare, Samsung, IBM, Juniper, Brocade, Scottish Government, among many others. The group currently participates in projects having a total value of £9.886 million.

3 National Importance

The UK Government's Cyber Security Strategy identifies the need to strengthen resistance to cyber attacks and ensure service availability. Cyber attacks continue to create a Tier 1 risk as judged in the National Security Risk Assessment 2015. Cyber attacks have the potential to cause widespread damage, since most computer applications are based on the assumption of highly available information networks — an increasingly essential component of military operations, government communication systems, and businesses. The ability of these networks to cope with increasing demands on scale and performance, to perform efficiently in harsh operating environments, and to adapt to new applications and threats lies in the highly sophisticated and complex software making up their design. Unfortunately, the complexity of this software makes it prone to vulnerabilities and misconfigurations that can be targeted by attackers to gain access to network data, or disable network operation. This threat is growing increasingly severe with modern malware coordinating operations across a distributed network.

Academic impact: Our centre offers the potential for UK research to be at the forefront of academic research in selected sub-areas of cybersecurity. We expect rich interaction between UoS, other ACEs, and the wider cybersecurity community nationally and internationally. Particularly, via the secondment programme and the research workshops as part of the centre's activities.

4 Objectives and Methodology

Our vision for our Academic Centre of Excellence in Cybersecurity Research is to ensure cybersecurity delivers on its potential to be one of the key underpinning technologies that will drive our economic, social and scientific development in the decades ahead.

The Strathclyde Cyber Security Centre of Excellence will be hosted within the Strathclyde Centre for Doctoral Training in Cybersecurity. This is a multi-disciplinary centre spanning the Department of Computing and Information Sciences, the Department of Electrical Engineering, and the Department of Law. The centre involves one professor (Edwards), two Readers (Nagaraja, Irvine), one Senior Lecturer (Atkinson), and two Lecturers in Computer Security (Weir,Sotirios). The centre has a dedicated member of staff (Dr. William Wallace) to manage its flagship knowledge-exchange program and the extensive links it has with industry, NGO, and government organisations.

The centre is internationally renowned for its systems security focused research that bridges systems security (Nagaraja, Terzis, Irvine, Edwards, Atkinson), behavioural (Weir, Terzis) and legal aspects (Edwards, Weir) of cybersecurity research. These permanent members of staff are supported by three postdoctoral research associates (Hay, Paul, Ghanem). This research has been funded from a variety of sources including research councils (EPSRC, ESRC, AHRC), the European Commission, and direct investment from security organisations. Since 2006, the centre has received total research income of 3.88m from these sources. In addition, the centre has a thriving PhD program with 12 students completing their theses between April 2013 and March 2018 and another 27 current PhD students. Most of the staff and students are principally housed in the Department of Computing and Information Sciences.

Four key principles underlie the centre's research ethos that distinguish it from other centres: First, its focus on the ubiquitous and transformative nature of cybersecurity research spanning science, engineering, business and the social sciences; Second, its intersectorality drawing on leading academics across these Faculties, industry (large multinationals, SMEs, and start-ups), and third sector organisations (e.g. health providers, local government, police and armed forces); Third, the scale of its intended impact based upon around 75 companies who are already part of the Strathclyde Knowledge Exchange ecosystem; and Fourth, its focus on delivering end-to-end solutions including a strong focus on the legal, ethical and regulatory frameworks governing the use of cybersecurity.

Each aspect is crucial:

- Understanding the ubiquity of cybersecurity research is vital in developing the full spectrum of cybersecurity techniques as opposed to focussing on a limited sample of those techniques as often happens elsewhere;
- Intersectorality is vital in ensuring cybersecurity feeds into and is informed by diverse problems so as to gauge which techniques and approaches work best in which domains;
- Focussing on impact at scale is vital in ensuring our research can tackle significant real world problems; and
- Taking an end-to-end approach ensures we can not only perform core cybersecurity-interventions, but can also better choose which interventions are technically and ethically appropriate, and then translate the ensuing results into benefits for end-users. Crucially, research in the ethical, legal and regulatory framework will not only mean our results are fit-for-purpose, but also they help society fully embrace the benefits of cybersecurity. This ubiquitous and end-to-end approach significantly broadens the appeal of our vision. Thus, the Academic Centre for Excellence in Cybersecurity Research will be managed by leading academics, industry, business professionals, and policy makers who have been chosen to ensure expertise across the Centre.

Examples of the group's recent and ongoing work of this kind include:

- SDN security

- Malware and botnet detection
- Privacy-preserving computation
- Power networks security
- Massively parallel security defences with GPUs
- Privacy and digital anonymity in online social networks and cloud computing
- Copyright protection (adversarial) in machine-learning covering both legal and technological approaches
- Extremist content classification
- Cultural aspects of security
- Regulation of online intermediaries (Google, eBay, Facebook, etc.)
- Regulation of Robots, Autonomous Vehicles, and Digital Assets

The group's strengths are in *network security* (Nagaraja, Irvine, Atkinson); *access control* (Terzis); *cloud security* (Terzis, Edwards); *analysing attacks* (Nagaraja, Weir); *security design principles* (all); *human factors in security* (Weir, Terzis); *privacy, anonymity and security* (Edwards, Nagaraja); *malware and intrusion analysis* (Nagaraja, Atkinson); *security and privacy law* Edwards; *software-defined networks* (Nagaraja); *cyber-physical systems* (Irvine, Atkinson)

To ensure that cybersecurity delivers on its potential to be one of the key underpinning areas that will drive scientific, societal, and economic development, we have adopted a cross-disciplinary approach towards security research. This allows us to take a holistic view of security challenges; we work on foundational components (security protocols and privacy-preserving computation), to novel techniques (malware, SDN, power-networks, traffic analysis) that are sympathetic to the local context (for instance how cultural aspects influence information security). Crucially, research in the ethical, legal and regulatory framework will not only mean our results are fit-for-purpose, but also they help society fully embrace the benefits of cybersecurity. This ubiquitous and end-to-end approach significantly broadens the appeal of our vision.

4.1 Research culture

The centre carries out research collaboratively with other academic partners including Universities of Edinburgh, Newcastle, Glasgow, Abertay, Manchester, UCL, Kings College, University of Illinois at Urbana-Champaign (UIUC), Stanford University, UC Berkeley, and Princeton University. The group has hosted numerous speakers and visiting scholars from these universities as well as from Bristol, Cambridge, and Oxford. Recent industrial speakers have included the Scottish Police, NPL, Morgan Stanley, NHS Scotland, Previse, Samsung, VMWare, Juniper, among others. The group regularly conducts workshops, organises monthly reading groups, and a hacking club. Members of the group are regularly invited as visiting professors. Nagaraja is Adjunct Professor at UIUC and previously Visiting Professor at EPFL; Edwards is Visiting Professor at U. Edinburgh, and previously at UC Berkeley and Stanford University; and, Weir is Adjunct Professor at Simon-Fraser University.

4.2 Planned Activities 2018–2022

As part of making Strathclyde "a place of useful security research", the centre will initiate a major expansion of our outreach programme by way of creating a Strathclyde Cybersecurity Network. The main thematic area of focus will be secure industrial informatics. This will involve a number of workshops

as well as site visits to organisations in sectors whose operational security is critical to the integrity of UK national infrastructure. We will initially leverage the Strathclyde knowledge-exchange ecosystem but we will go well beyond that. The goal is to take research into the core of industrial processes and bring practitioner-wisdom into our research. The security group will complete the process of of creating the network of organisations by 2019. This network will include companies (driven by Industry 4.0 priorities), NGOs, governments, and policy think tanks who face complex cybersecurity challenges that demand a collaborative response.

The second major activity will be a secondments programme. The group's ethos is to carry out research of importance to society including industry and government. Because of this ethos, the group is naturally financially self-sustaining: it shifts its focus in line with national importance. In line with this, we need to develop close working relationships with a select group of organisations. We will ensure this by hosting them within the ACE-CSR or by providing opportunities for Strathclyde staff and students to spend a period of secondment at stakeholder sites. This will maximise the potential of transferring knowledge, tools, and techniques from the ACE-CSR to the industry and practice.

Third, we plan to hold a number of UK all-hands meetings at periodic internvals which will enable direct meetings with stakeholders and organisations, these are designed to maximise impact from academia to industry and vice-versa.

Fourth, we have grown by about four people per year for the last five years, and we anticipate further growth of three people per year for another four years, reaching a steady-state size of 45 people.

4.3 Planned impact

The centre's activities are focused on a number of organisations in industry, policing, and government who are interested in cybersecurity. The centre's objective is to maximise impact from ACE-CSR funds and status. As such a number of activities have been planned with this objective in mind. The creation of a network on the cybersecurity of industrial informatics will lead to the creation of a focused group of stakeholders. Further, the secondments programme builds upon the initial networking phase and is designed to develop close working relationships via reciprocal staff exchanges. This will maximise the knowledge transfer from the ACE-CSR to practitioners as well as be a pathway for ensuring that practitioner concerns are adequately reflected in the research we pursue.

The ACE will not operate in isolation and there is an extensive network of industry, practice and community contacts open to us through existing projects. Further, the ACE will have access to 75+ companies within the Strathclyde Knowledge Exchange ecosystem who have said to us that they are keen to engage with us on cybersecurity. All of these will provide invaluable pathways to impact for research. The ACE-CSR status will enable us to harmonise these various contacts into a systematic approach for maximising impact from our cybersecurity research.

5 Management

The PI will provide leadership to the centre and take day-to-day charge of the centre's activities and harmonise the efforts by members into a systematic approach for maximising impact from our cybersecurity research. The VC's office will provide oversight on the centre's activities and on its strategic direction.