University of Strathclyde Security Group

1 Profile

The Strathclyde Security Group spans the Department of Computing and Information Sciences, the Department of Electrical Engineering and the Department of Law. It 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

Dr. Robert Atkey Lecturer

The group is internationally known for its systems focus 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 five postdoctoral research associates (Hay, Paul, Ghanem, two vacancies), and 27 Phd students. 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 group has received total research income of 3.88m from these sources. The group 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 group has a thriving PhD program with 12 students completing their theses between April 2013 and March 2018 and 27 current PhD students. Most of the staff and students are principally housed in the Department of Computing and Information Sciences.

1.1 Development in the last five years

Since 2008, staffing levels have steadily grown to the current size of eight permanent members, five postdocs (including two vacancies) 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. The group's strengths are in *network security* (Nagaraja, Irvine, Atkinson); *access control* (Terzis); *verification* (Atkey); *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); *information flow* (Nagaraja, Atkey); *security law and governance* Edwards; *software-defined networks* (Nagaraja); *cyber-physical systems* (Irvine, Atkinson)

1.2 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. ENACT membership includes Juniper, Brocade, VMWare, Samsung, InMon, and Fortinet.

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. PNDC membership includes SSE, SPEN, UKPN, Vodafone, Cisco.

1.3 Recent investments

Since 2008 the group has acquired over £1.482 million in research funding, from research councils, government, and industry. The group currently participates in projects having a total value of £9.886 million.

1.4 Strategy and vision

Our vision for excellence in security 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.

Four key principles underlie the group's research ethos that distinguish it from similar groups: 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.

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
- Regulation of online intermediaries (Google, eBay, Facebook, etc.)
- Regulation of Robots, Autonomous Vehicles, and Digital Assets
- Extremist content classification
- Cultural aspects of security

1.5 Engagement with government and industry

Nagaraja leads an international consortium involving Brocade, Juniper, VMWare, Samsung, and Fortinet on SDN security; Nagaraja has four patents in trust and security. His work on the FLAIM lightweight secure distributed database is currently running on tens of thousands of production servers at large banks and media houses. He also works closely with a number of NGOs including the Tibetan Govt-in-exile on defences against targeted malware attacks; Weir works closely with the Scottish Police and the Scottish Policing Research Institute on extremist content detection; Irvine works closely with a consortium of electricity suppliers such as Scottish Power and equipment manufacturers such as Triphase; Edwards has advised the House of Lords Select Committee (on security and law), the European Parliament and the European Commission on digital rights, privacy, and civil liberties. She has worked closely with MPs, Lords, and policy makers in her role as (advisory) board member of the Open Rights Group and the Foundation for Internet Privacy Research; Atkinson's collaboration with Cisco has lead to the adoption of a data-provenance solution into Ciscos routers. Atkey works with banks and trading firms to detect potential concurrency attacks in distributed computing environments.

1.6 Research culture

We carry 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.