Security Group

University of Strathclyde

External research funding and impact of projects

Robustness-as-evolvability (Competitive)
Principal investigator: Shishir Nagaraja
Dates: 04/2015 – 03/2019
Funding agency: EPSRC
Financial value: £790,000 (EPSRC contribution) (£294000 for the University of Strathclyde) Lead institution
Main outcomes: Dr. Nagaraja and his team published three peer-reviewed papers with two more papers in submission. With the support of UK Govt. and industry, we created the ENACT and RANSOM testbeds as part of this project. The testbed is used by the team and the industrial partners on the project. In terms of impact, Brocade is currently considering the quorum control architecture for productisation, while Juniper's product management is considering the adoption of SDN cache defences within their EX series switches.
Summary: Dr. Nagaraja leads an international consortium of five universities and five industry partners on SDN security. This project explores novel architectures for secure control in IoT, SDN, and NFV environments. These environments present unique management challenges due to the sheer scale, complexity, dynamicity, and the substantial attack surface that must be defended. This project has developed a novel dynamic quorum primitive and applied it to build a scalable distributed control architecture that can defend against insider attackers. The project involves the extensive application of machine learning primitives at all levels of router design - from smart caching algorithms in switches to adversarial measurement techniques to adversary-resistant controllers.

CREATe (Competitive)
Principal investigator: Lilian Edwards
Dates: 10/2012–08/2017
Funding agency: AHRC,ESRC,EPSRC
Financial value: £4,169,477 (EPSRC contribution) (£206,025 for the University of Strathclyde)
Main outcomes: Prof. Edwards and her team published six peer-reviewed papers on legal aspects of cyber-security
Summary: Prof. Edwards as Deputy Director, co-leads the CREATe consortium of 7 universities and 80-plus industry, public sector and policy partners, for a programme of more than 80 work packages over 4 years, funded for 5m, plus 3m industry contribution. Prof. Edwards has general responsibility for the digital security side of the centre and also in charge of 7 funded packages, running for various periods over the four years, including work on digital copyright enforcement and its security economics; adversarial data mining; privacy of digital assets; data-protection in networked technologies; privacy and security in smart cities; privacy, trust, and confidence in digital services; Privacy and Disclosure on Twitter feeds.

SHAWN: Secure High availability Avionics Wireless Networks (Competitive)
Principal investigator: R Atkinson
Other investigators: I Andonovic, C Michie, D Harle
Dates: 1/14–06/17
Funding agency: Technology Strategy Board
Financial value: £723,965 UKRI contribution (£162,724 for the University of Strathclyde)

Main outcomes: The project led to the development of advanced security features within GE's aircraft network systems including the design of secure antennas to resist DoS attacks, eavesdropping attacks, and malicious corruption of data on the network.
Summary: This project focused on the security of wireless networks used to interconnect different components on aircrafts. While wireless brought weight savings and greater flexibility in these systems, contributing to reduced fuel burn and less instances of unscheduled maintenance, the use of insecure wireless technology can compromise flight safety. Instead of confidentiality, the core requirement was availability. This project had two objectives which were both achieved: developing aircraft wireless networks that were (a) intrusion-tolerant and (b) jamming resistant. The core innovation from Strathclyde was the development of security mechanisms that leverage channel redundancy to achieve denial-of-service resistance.

Power Systems Security (Competitive)
Principal investigator: J Irvine
Other investigators: R Atkinson
Dates: 06/2017–01/2019
Funding agency: Innovate UK
Financial value: £200,000
Main outcomes: The main outcomes with be the implementation of a secure PC environment that can be used in an OT environment. Through PNDC (see 2-description-of-applicant.pdf) member links to ENA, this will be disseminated in the UK utility sector more generally, and through Strathclyde's membership of EE-ISAC, utilities in Europe.
Summary: This project will survey the UK utility sector to identify from a landscape of potential incidents to identify the capacity needed to respond and recover to cyber security events. This will include considering the necessary functions that need to be maintained during an attack and assessing the levels of incident handling that can be carried out by DNOs. An incident response framework will be developed that enables identification of the capabilities and redundancy back-up that are required to withstand an attack and manage recovery. This project considers mechanisms to encourage the achievement of cyber security across organisational boundaries and throughout supply chains in electricity distribution. Due to the growing attack surface and increase in volume of attacks, a more efficient deployment and ongoing assurance of security controls will be investigated. The project also considers the security of vendor equipment and vendor interactions with operational systems through the design of secure and verifiable software environments which can be audited.

Privacy-preserving computation on the Cloud (Competitive)
Principal investigator: Sotirios Terzis
Other investigators: Cheng Dong
Dates: 04/13–03/17
Funding agency: EPSRC DTG
Financial value: £11,948
Main outcomes: This project developed three security protocols for private set-intersection. The first protocol ensures confidentiality under a honest-but-curious adversary using homomorphic cryptosystems. The second protocol is a significant improvement in terms of security, as it assumes an active adversary, whilst also doing away with homomorphic cryptosystems resulting in a more efficient solution. The third protocol, adds verifiability and formal proofs of security. The project outputs were published in respectable peer-reviewed journals and conferences.
Summary: This project focused on scalable private set-intersection. A problem of longstanding interest within the security community; given a number of encrypted sets, how can a cloud operator (or a set of distributed participants) reliably compute the intersection of these sets without learning any information about non-intersecting elements of the sets.