Conference Programme[1]

23 August 2016 (Workshops)

Time	Event	Room
08:30 - 09:00	Registration and Coffee	Foyer
09:00 - 09:20	Welcome	Seminar Room
09:30 - 11:30	***Detection and Forensics of ICS Cyber-attack – Hands-on Cyber Range Training*** **(CyberBit)** *To most people SCADA protocols and ICS environments are a black-hole. Engineering team entrusted with managing ICS networks are struggling with knowledge, control and visibility gaps that don't allow them to respond to ICS threats efficiently and on time. In this workshop, we will explain and teach about Modbus Protocol and show how attackers can utilize its weaknesses to their advantage. Throughout this workshop, we will utilize CYEBRBIT Cyber Range technology, to simulate a real ICS environment, attack it using CVE's and protocol vulnerabilities, and provide the participants with several tools to conduct root cause analysis and forensics to understand the attack vector and how to remediate it.*	Seminar Room
11:30 - 12:30	**Cyber Forensics and Incident Response for ICS/SCADA (Airbus Group)** *Cyber Forensics and Incident Response for ICS/SCADA is an emerging field as control operators begin to implement incident response plans and teams to respond appropriately to cyber events. The application to traditional IT forensics processes and tools is not directly transferrable to an ICS environment due to the requirements, conditions, and constraints of an operating ICS environment. This seminar will present some of the leading thinking in the ICS Forensics domain, based on published work "Developing Cyber Forensics for SCADA Industrial Control Systems" whilst using real application of investigation techniques to validate the process and tools usage presented.*	Seminar Room
12:30 - 13:00	Working Lunch	Seminar Room
13:00 - 14:30	**Assessing & Exploiting ICS Vulnerabilities -- Hands-On (Limes Security)** *This short workshop is an extract of a larger training provided by Limes Security. In the first half of this 90-minute section, common pitfalls when testing ICS will be discussed, as well as recommendations on getting around them. Furthermore, a quick overview will be given what*	Seminar Room

[1] Subject to change

	functions common security testing tools do offer ICS-wise today. In the second half of this course, attendees will have the chance to experiment with and conduct a number of real-world ICS exploits and attacks themselves such as shutting down a PLC remotely, triggering ICS protocol functions and creating a DoS against a BACnet server. To participate in the hands-on section, attendees should bring a Laptop with a remote desktop client (any Windows Client version such as Win7, Win8, Win10) will work.	
14:30 - 15:00	Coffee	1st Floor Bridge
15:00 - 17:00	**SCIPS -- Simulated Critical Infrastructure Protection Scenarios (DMU)** *is a 'gamified' table-top learning environment for senior executives developed as part of ongoing research into cyber security awareness in the sector and human decision making. SCIPS positions the cyber threat as a strategic issue and presents a scenario in which a privatised critical infrastructure facility must protect its operations from capable a threat actor whilst also preserving market confidence and shareholder value. Through the course of the game the players discuss strategies to balance competing requirements and budgets, ultimately drawing their own conclusions as to the reality and impact of cyber attacks, learning from their own experiences. Players form up into teams and randomly select senior leadership roles within a Combined Cycle Gas Turbine (CCGT) electric power generation plant. They are presented with a set of budgets and commitments from their fictitious company's annual report, and must reallocate funds from these in order to purchase security capabilities from a set of cards that offer security mechanisms and services.*	Seminar Room

24 August 2016 (Conference Day 1)

Time	Event	Room
09:00 - 09:30	Registration and Coffee	Foyer
09:30 - 09:45	Chairs' Welcome	Seminar Room
09:45 - 10:45	**Keynote** (Eeiran Leverett, Cambridge) ***Attackers are magic, but defense is science.*** *Unknown unknowns. Information asymmetry. Composable insecurity. Incomposable security. Embodied vulnerabilities. Software Liability. Firmware as a critical infrastructure. Anything could happen.*	Seminar Room
10:45 - 11:15	Coffee Break	1st Floor Bridge
11:15 - 12:40 **Session 1**	Gundars Kalns, Simin Nadjm-Tehrani and Maria Vasilevskaya. **Trading off latency against security in open energy metering infrastructures** Rob Antrobus, Sylvain Frey, Ben Green and Awais Rashid. **SimaticScan: Towards A Specialised Vulnerability Scanner for Industrial Control Systems** Ivo Friedberg, Paul Smith, Kieran Mclaughlin and Markus Wurzenberger. **Towards a Resilience Metric Framework for Cyber-Physical Systems**	Seminar Room
12:40 - 13:40	Lunch	Foyer
13:40 - 15:10 **Session 2**	Antoine Lemay, Jonathan Rochon and José M. Fernandez. **A Practical flow white list approach for SCADA systems** Christopher Tebbe, Karl-Heinz Niemann and Alexander Fay. **Ontology and life cycle of knowledge for ICS security assessments** Andrew Wain, Stephan Reiff-Marganiec, Helge Janicke and Kevin Jones. **Towards a Distributed Runtime Monitor for ICS/SCADA Systems**	Seminar Room
15:10 - 15:40	Coffee	1st Floor Bridge
15:40 - 16:40 **Session 3**	Manuel Cheminod, Luca Durante, Marcello Maggiora, Adriano Valenzano and Claudio Zunino. **Performance of Firewalls for Industrial Applications** Peter Eden, Andrew Blyth, Peter Burnap, Yulia Cherdantseva, Kevin Jones, Hugh Soulsby and Kristan Stoddart. **Forensic Readiness for SCADA/ICS Incident Response**	Seminar Room

16:40	End of Day, Bus Transport provided to City Centre	Foyer
18:15	Tour of the City Hall (Optional - collect ticket at registration desk)	Belfast City Hall
18:45	Drinks Reception and Welcome	Belfast City Hall
19:30	Conference Dinner	Belfast City Hall

25 August 2016 (Conference Day 2)

Time	**Event**	**Room**
08:30 - 09:00	Coffee and Networking	Foyer
09:00 - 10:00	**Keynote** (Kevin Jones, Airbus Group) **The Factory of the Future with a Next Generation ICS** *Protection of manufacturing Industrial Control Systems from cyber-attack is of critical importance for Europe's leading manufacturing companies which requires innovative security solutions. However, as such manufacturing systems move towards Industry 4.0 / Factory of the Future interconnected, digitalised, and automated environments security risks are further increased. This presentation will discuss the future of manufacturing in Factory of the Future and consider the cyber security requirements, risks, and innovation to come.*	Seminar Room
10:00 - 10:30	Coffee Break	1st Floor Bridge
10:30 - 12:30 **Track**	**Cyber Security of Industrial Control Systems for Smart Grid** (Chair: Kieran McLaughlin) Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty and Sakir Sezer**. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid** Jan Wolf, Gerhard Hansch, Felix Wieczorek, Norbert Wiedermann, Frank Schiller and Martin Hutle. **Adaptive Modelling for Security Analysis of Networked Control Systems** Sarita Paudel, Paul Smith and Tanja Zseby. **Data Integrity Attacks in Smart Grid Wide Area Monitoring**	Seminar Room
Track	**Cyber Security Awareness** (Chair: Ulrik Franke) Allan Cook, Richard Smith, Leandros Maglaras and Helge Janicke. **Using Gamification to Raise Awareness of Cyber Threats to**	Board Room

	Critical National Infrastructure Elisa Canzani, Helmut Kaufmann and Ulrike Lechner. **Characterising Disruptive Events to Model Cascade Failures in Critical Infrastructures** Allan Cook, Richard Smith, Leandros Maglaras and Helge Janicke. **Measuring the Risk of Cyber Attack in Industrial Control Systems**	
12:45 - 13:45	Lunch	Foyer
13:45 - 15:15 **Session 4**	Justyna Chromik, Boudewijn Haverkort and Anne Remke. **Improving SCADA security of a local process with a power grid model** Boojoong Kang, Kieran Mclaughlin and Sakir Sezer. **Towards A Stateful Analysis Framework for Smart Grid Network Intrusion Detection** Andrew Fielder, Tingting Li and Chris Hankin. **Defense-in-depth vs. Critical Component Defense for Industrial Control Systems**	Seminar Room
15:15 - 15:30	Final Remarks	Seminar Room
15:30	Conference Close	

Please note that the programme is still subject to changes.

SPARKS - Workshop (Friday 26th August 2016)
We are also pleased to announce that the SPARKS project is running a co-located workshop following ICS-CSR'16. The workshop can be booked separately through the SPARKS website: https://project-sparks.eu/events/workshop-on-european-smart-grid-cybersecurity-emerging-threats-and-countermeasures/

In this half-day workshop — the third in a series that is organised by the EU-funded SPARKS project — we examine the emerging cybersecurity threat to electrical energy systems and the future smart grid, presenting the research-driven security and resilience countermeasures that can be applied to address these threats. In particular, the workshop will focus on the emerging cyber-physical threat, as seen in the Ukraine in December, 2015, wherein cyber-attacks result in operational consequences, such as blackouts or equipment damage. A highlight of the programme will the demonstration of a multi-stage cyber-physical attack and an intrusion detection system that can detect the manipulation of SCADA protocols.

Travel Information

George Best Belfast City Airport is three miles from Belfast city centre (area around City Hall).

- The Airport Express 600 bus service runs from the airport terminal to the city centre every 20 minutes (05.30 - 22.05) Monday to Friday. Full service information at www.translink.co.uk

- Taxis from the airport are operated by Value Cabs. Debit/credit card payment is available. Costs to the city centre are in the region of £10, so a taxi is recommended if you are part of a group. There is a Value Cabs kiosk in the terminal. If you are travelling from City Airport directly to ECIT, a taxi is the best option. Tel: +44 28 9080 9080. Web: www.valuecabs.co.uk

Belfast International Airport is 30 minutes from Belfast city centre.

- The Airport Express 300 service operates between the airport and Belfast city centre every 15 minutes Monday to Friday. Full service information at www.translink.co.uk

More travel and tourism information available at: http://visitbelfast.com/home/page/getting-here

Conference Location

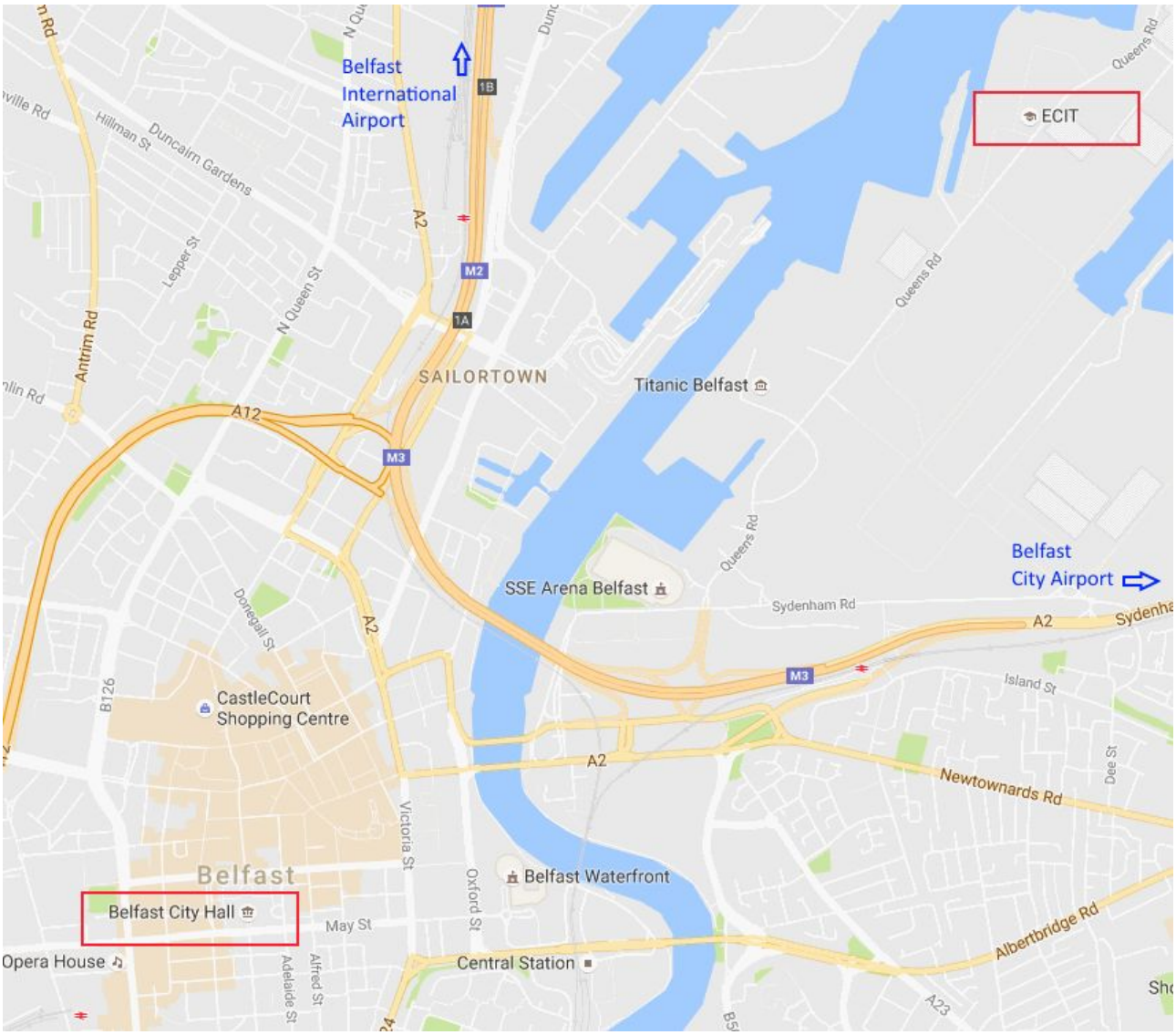
The conference is located at Queen's University's ECIT building (top right in the map below):

ECIT
Northern Ireland Science Park
Queen's Road,
Belfast
BT3 9DT

Web: http://www.ecit.qub.ac.uk/Contactus/ Tel: +44 28 9097 1700

Travel from city centre hotels (bottom left in the map below):

- A taxi is the simplest way to travel to the venue, and will cost £6 - £8.
- Taxi providers include Value Cabs, Tel: +44 28 9080 9080, FonaCab, Tel: +44 28 9033 3333
- Bus number 26B departs from Donegall Square North, opposite the front of City Hall, and stops at the Science Park. Timetable available from http://www.translink.co.uk/Services/Metro-Service-Page/Timetables/


Belfast
International
Airport
ECIT
Duncairn Gardens
Hillman St
Lepper St
N Queen St
Antrim Rd
A2
M2
1B
1A
SAILORTOWN
Titanic Belfast
A12
M3
Queens Rd
Belfast
City Airport
SSE Arena Belfast
Sydenham Rd
Donegall St
CastleCourt
Shopping Centre
B126
Island St
Dee St
Newtownards Rd
Victoria St
Oxford St
Belfast Waterfront
Belfast
Belfast City Hall
May St
Opera House
Adelaide St
Alfred St
Central Station
Albertbridge Rd
A23