INTERNATIONAL CONFERENCE ORGANISED BY THE CYBERFORENSICS & SECURITY INNOVATION GROUP

‘Making the UK and Europe a Safer Place to Live and Work Online’

12 January 2018 | 9:30 – 17:00

Rg38 (Ramsey), Canterbury Campus

Sponsored by:
The British Computer Society Cybercrime Forensics Specialist Group

bcs The Chartered Institute for IT

Cybercrime Forensics Specialist Group

Canterbury Christ Church University

Welcome

I am delighted to extend a warm welcome to the delegates of the International Conference organised by the Cyberforensics & Security Innovation Hub in the School of Law, Criminal Justice and Computing. The conference theme "Making the UK and Europe a Safe Place to Live and Work Online" is very appropriate in today's context when 'cyber' is touching the lives of 7 billion people on this planet in one way or another. In view of this I am happy that an eminent panel of experts are with us today to share their experience. I am sure the delegates will immensely benefit from listening to them. While thanking the speakers I take this opportunity to wish everyone a very successful and useful conference.

Dr Abhaya Induruwa
Chair of the Conference Organising Committee

Conference programme

Time	Activity
09:30 – 09:45	Registration
	Session 1: Chair – Dr Abhaya Induruwa
09:45 – 10:00	Opening remarks by **Dr Abhaya Induruwa**, Conference Chair Welcome by **Prof. Robin Bryant** School of Law, Criminal Justice and Computing
10:00 – 10:45	**Cybercrime and Security Scenario – an overview** Prof Alastair Irons, Chair, BCS Cybercrime Forensics SG
10:45 – 11:30	**Virtual currencies – risks, possibilities and legal challenges** Jussi Aittola, National Bureau of Investigation, Finland
11:30 – 11:45	Tea/Coffee
	Session 2: Chair – Dr Paul Stephens (Director/ Dept of C,CF &CS, CCCU)
11:45 – 13:00	**Ransomware Forensics: an incident responder's perspective** Ian Howard, Cyber Threat Hunter, 7Safe
13:00 – 13:45	Lunch
	Session 3: Chair – Prof Alastair Irons (Chair/BCS CCF SG)
13:45 – 14:30	**Capacity building – a cooperative process** Yves Vandermeer, Chair, Europol ECTEG
14:30 – 15:15	**Open and Secure: present and future** Mike Bursell, Chief Security Architect, Red Hat
15:15 – 15:30	Tea/Coffee
	Session 4: Chair – Adrian Winckles (Vice Chair/BCS CCF SG)
15:30 – 16:15	**Security Framework for IoT** Floren Cabrera F. de Teresa, CEO, Bitbond Ltd
16:15 – 17:00	**Safer working in local government: a layered approach** Jonathan Haddock, Network & Security Engineer, Local Government
17:00	Closing remarks by **Dr Abhaya Induruwa** (Conference Chair)

Speakers' biographies and presentation abstracts

Prof Alastair Irons, Chair, BCS Cybercrime Forensics SG

Biography:

Professor Alastair Irons is Academic Dean for the Faculty of Computer Science at the University of Sunderland and a Professor of Computer Science. His subject interests focus on digital forensics and cybersecurity. Prior to joining the University in September 2008 he worked at ONE North East, Northumbria University and ICI having moved to the north east of England from Scotland after graduating in 1984 from Edinburgh University. Alastair became a National Teaching Fellow in 2010.

Alastair's current teaching focuses on computer forensics, digital forensics and cyber security. His research interests focus on cybersecurity and digital forensics – currently looking at threat sharing in cybersecurity, methods for digital investigations in "big data", digital investigations in journalism, gender issues in cybersecurity, as well as the role of computer forensics in South Africa. He is also active in research in academic and pedagogic issues in higher education with particular interest in student assessment and feedback. He has recently published books on Formative Feedback and on Learning and Teaching issues in Computing. He is currently leading a research project on Problem Based Learning in Cybersecurity. Alastair is a visiting scholar at the University of Cape Town in South Africa.

He serves on the management board of DYNAMO, the management board of Sphere North East, the Advisory Board of the North East Digital Catapult and on the management board of the North East Fraud Forum. He contributes to the British Computer Society through a number of roles and is chair of the BCS Academic Accreditation Committee, sits on the BCS Academy Board, chairs the BCS Cybercrime Forensics Special Interest Group and has recently been elected chair of the BCS NE England branch.

In his spare time Alastair participates in karate where he is a 2nd Dan black belt in Shokokai and is currently working towards his 3rd Dan black belt.

Abstract:

Cybercrime and Security in an Ever Changing World

The all-pervasive and ubiquitous nature of the computer and digital technology has made a profound mark on almost every aspect of our lives. The speed at which individuals, businesses, organisations and governments are utilising digital technology and generating data is increasing at an unprecedented rate.

As the use of computing grows and the dependency on systems and the data held in those systems increases there are many opportunities and challenges for computer science. One of those challenges is dealing with cybercrime. In parallel with the growth of computing there is a growing threat from cybercrime. Cybercrime has reached pandemic proportions – global and never ending. The application of digital forensics techniques seeks to solve cybercrime after the event and the

application of cybersecurity seeks to develop robust computer systems and networks to prevent the cybercrime happening in the first place.

The cybersecurity domain is a challenging and complex one with technology developing at a fantastic speed and threats coming from all directions from national states to cybercriminals to individuals. Protecting the systems and using data in a safe and secure environment requires specialist understanding and awareness. There is a need for technical cybersecurity specialists to design, implement and maintain secure information systems, applications and networks.

There is however a paradox – there is a large skills gap in the cybersecurity domain and there is a demand for graduates and professionals with appropriate skills in cybersecurity. There is a challenge for educators to work with employers and government to provide programmes to address the skills gap in cybersecurity.

In this lecture Professor Irons, will examine the evolution of cybercrime and cybersecurity, the current environment of cybercrime, the challenges and threats in cybersecurity and the growth in demand for cybersecurity graduates.

****

Jussi Aittola, National Bureau of Investigation, Finland

Biography:

Mr. Jussi Aittola works in the National Bureau of Investigation Finland as an Inspector and is the project manager of 2 virtual currencies projects; Bitcoin-JIT and TERHA. Mr. Aittola has been active in the field of virtual currencies since 2010, and has an extensive knowledge of different virtual currencies. The focus on Bitcoin-JIT ja TERHA projects is to analyze and gather information of the misuse of virtual currencies and gather information on cases where virtual currencies has been used in terrorism financing. Mr. Aittola has 2 degrees in IT and is currently studying law in Finland. He is also responsible for training, supporting investigations, creating best practices, doing strategic, operational and tactical analyses for the Finnish Police related to virtual currencies, he also lectures for international law enforcement agencies and in different European Union projects.

Abstract:

Virtual Currencies – risks, possibilities and legal challenges

Bitcoin and other virtual currencies have lately gained a lot of popularity. Especially Bitcoin has been widely adopted and the price has risen to over 16 000 euros. In my presentation I will explain briefly what is Bitcoin and why it is the preferred choice in criminal to criminal payments. Also through a very simple example we will see why it is so often used in typical small payment frauds. The European union is preparing the new anti money laundering law and in this act virtual currencies will be regulated in the EU. The new AML law will regulate the virtual currency companies to know their customers, make due diligence and file suspicious activity reports. The private to public relationships is essential to be able to find the criminals who misuse virtual currencies in all kind of crimes.

****

Ian Howard, Cyber Threat Hunter, 7Safe

Biography:

Ian has over 13 years in digital forensics and incident response. Initially a forensic investigator in Hertfordshire Constabulary, progressing to be their Investigation Manager, before moving to 7Safe. In his current role, Ian delivers incident response, threat hunting and digital forensic investigations and is a registered expert witness. He also designs and delivers practical training in digital forensics and cyber security.

Ransomware Forensics: An incident responder's perspective

Abstract:

Incident responder Ian Howard will draw on experience from real incidents to examine ransomware attacks; from initial infection with live demonstrations of attack techniques including drive-by-downloading, to possible data recovery with forensic methods. How to take a proactive approach to not just ransomware but malware and cyber breaches in general will be discussed by gaining a better understanding of cyber threat hunting.

****

Yves Vandermeer, Chair, Europol ECTEG

Biography:

"After 30 years as a police officer in the Belgian Judicial Police, during which Yves spent 20 years working on computer forensics and computer crime topics, Yves is now a full-time lecturer at the Norwegian Police University College and a lecturer in Advanced Computer Forensics at Dublin University.

Also involved in forensic software development, researching computer forensic software validation for his PhD thesis. Yves is chairing the European Cybercrime Training & Education Group."

Capacity building – a cooperative process

Abstract:

"Since years Law Enforcement is struggling with Computer Crime capacity building. Europol, CEPOL, ECTEG are now involved in a new training governance model, aiming to provide to Law Enforcement quality training materials created and updated by saving the few available human resources. To

allow training deployment at national level and guarantee a sound education approach, several issues were addressed.

Today presentation will explain how existing materials may be deployed at national level and how reach sustainability.

****

Mike Bursell, Chief Security Architect, Red Hat

Biography:

Mike Bursell joined Red Hat in August 2016, following previous roles at Intel and Citrix working on security, virtualisation and networking. After training in software engineering, he specialised in distributed systems and security, and has worked in architecture and technical strategy for the past few years. His responsibilities at Red Hat include forming security and blockchain strategy, external and internal visibility and thought leadership. He regularly speaks at industry events in Europe, North America and APAC.

Professional interests include: Linux, Open Source Software, security, distributed systems, blockchain, NFV, SDN, virtualisation (including Linux Containers and hypervisors).

Mike has an MA from the University of Cambridge and an MBA from the Open University.

Abstract:

Long gone are the days of open source being the poor cousin to proprietary software: open source is a staple part of infrastructure in markets from banking to the public sector, from supply chain to healthcare. Open source software is big business, too: support and maintenance for open source products is not dependent on the proverbial teenager in his or her parent's basement anymore. Experts in cybersecurity and cyberforensics are likely not only to be examining systems based on open source software, but also using it for their own tools.

What are some of the security-related questions around using and maintaining open source software, and what might the future hold?

Beyond that, what is there that open source can provide that proprietary maybe cannot? Finally, what are some other areas where "open-ness" is taking hold such as open data, open intelligence and open organisations which may have an impact on how we work in cybersecurity?

****

Floren Cabrera F. de Teresa, CEO, Bitbond Ltd

Abstract:

Security Framework for the Internet-of-Things

As an SME equipped with a UK patent pending initiative for IoT devices, we provide a whistle-stop review of some key problems and options for delivery of a new highly secure IoT environment for the UK and Europe. We propose a vision for a new UK and European "IoT Security Framework" in which new generation IoT "meta-nodes" are retro-fit, proving new hardware and firmware credentials and security protocols, so as to prevent system-wide hacks (in a large-scale attack, hacking smart devices one-by-one would be required) since the network "nodes" or "clients" would become a lot more capable IoT devices.

Vehicular networks are expected to be one of the major new application areas for wireless and IoT services. There are more than 600 million vehicles worldwide and many of these will be networked to achieve improvements to safety, traffic management, navigation, and user convenience[1]. The "Internet of Cars" is one of the greatest opportunities for implementation of advanced "blockchain" technologies, including "smart contracts" that will determine the behavior of smart things according to rules implemented by Artificial Intelligence and will record transactions in an alterable encrypted ledger.

Industry observers estimate £4.5 trillion will be invested over the next five years, in "Internet-of-things" solutions by businesses, governments and consumers, producing up to £11.3 trillion in economic value worldwide by 2025, according to McKinsey[2].

Biography:

I am an Entrepreneur, trained as political science analyst and as a debt arbitrage trader, having worked for over 15 years in Wall Street. My corporate training was followed by many years as an inventor and IoT system architect, with an emphasis in embedded systems' architecture and related mainframe systems. I filed for a U.S. patent filings for Optical through the air communications using electrical lighting systems and other applications involving AC smart buildings. In that IoT experience, we prototyped very large populations of IoT devices, which led to confidential insights into cyber-security for IoT.

https://patents.google.com/patent/US20040164950A1/en

During the last couple of years, I founded BitBond Ltd, formed a group of Investors and have filed two UK patents for an entirely disruptive and completely secure family of devices for the Internet of things, especially for the Internet-of-Cars.

1 Dipankar Ray Chaudhuri and Mario Gerla "Emerging Wireless Technologies and the Future Mobile Internet"

2 https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

Jonathan Haddock, Network and Security Engineer, local government

Biography:

Jonathan has worked in IT for almost 20 years, recently moving to specialise in cyber security. Having gained qualifications in digital forensics, incident response and penetration testing, he now helps look after the security and network infrastructure of three local government authorities.

He gained an MSc in Professional Computing from Staffordshire university and has given guest lectures and talks at a few universities. Previously he worked with the BCS Young Professionals Information Security Group (YPISG), speaking at a number of their penetration testing training days.

Abstract:

Safer working in local government: a layered approach

Expensive technologies and the most advanced firewalls can still be defeated by a single person. This talk looks at the various techniques used to help protect local government, from user training to next generation firewalls. People are often an organisation's greatest defence, so it's important to bring them on the cyber security journey.

****

Conference organising committee

- Dr Abhaya Induruwa (Chair) - CCCU
- Hannah Bygraves - CCCU
- Georgina Humphries - CCCU
- Prof Alastair Irons - BCS Cybercrime Forensics SG/University of Sunderland
- Nigel Jones MBE - CCCU
- Ian Kennedy - CCCU
- Reza Mousoli - CCCU
- Dr Paul Stephens - CCCU
- Yves Vandermeer - Norwegian Police University College/ECTEG
- Joseph Williams - CCCU
- Adrian Winckles - BCS Cybercrime Forensics SG/Anglia Ruskin University

bcs The Chartered Institute for IT
Cybercrime Forensics Specialist Group

Canterbury Christ Church University