ARU CSNRG, OWASP Cambridge, BCS Cybercrime "IoT & ICS/SCADA Forensics Workshop" 2018

Wednesday 10th January 2018 09:30– 14:00, Lord Ashcroft Building (LAB002), Anglia Ruskin University, Cambridge.

Hosted by the Cyber Security & Networking Research Group, Anglia Ruskin University, British Computer Society (BCS) Cybercrime Forensics Special Internet Group's and OWASP (Open Web Application Security Project) Cambridge Chapter.

Industry pundits have predicted that we are about to experience the fourth industrial revolution (Industry 4.0), which is the future of industrial production based on the "Internet of Things" (IoT). As with all previous industrial major transitions, this leads to exciting opportunities but also great challenges. The "perfect world" is that IoT, is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications. The interconnection of these embedded devices will potentially usher in automation in nearly all fields, resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. However, integrating IoT technologies within an organization means loosening access to the IT infrastructure, thus making it more susceptible to errors and vulnerable to attack. This is a scary proposition as intruders will not stop trying to find new ways of infiltrating business networks.

To better understand these infiltrations a cyber forensics program is necessary but this can be a challenging task when being applied to nontraditional environments, such as IoT and industrial control systems. Modern IT networks, through data exchange mechanisms, data storage devices and general computing components provide a good foundation for creating a landscape used to support effective cyber forensics. However, modern control systems environments are not easily configurable to accommodate forensics programs. Nonstandard protocols, legacy architectures that can be several decades old, and irregular or extinct proprietary technologies can all combine to make the creation and operation of a cyber forensics program anything but a smooth and easy process.

Cybercrime Forensics Specialist Group

OWASP
Open Web Application Security Project

Background

The British Computer Society (BCS) Cybercrime Forensics Special Interest Group (SIG) promotes Cybercrime Forensics and the use of Cybercrime Forensics; of relevance to computing professionals, lawyers, law enforcement officers, academics and those interested in the use of Cybercrime Forensics and the need to address cybercrime for the benefit of those groups and of the wider public.

OWASP (Open Web Application Security Project is a 501(c)(3) not-for-profit worldwide charitable organization focused on improving the security of application software. Their mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks.

The **Cyber Security and Networking** (**CSN**) Research Group at Anglia Ruskin University has close working strategic relationships with industry, professional bodies, law enforcement, government agencies and academia in the delivery of operationally focused applied information and application security research. We have strong international links with professional organisations such as OWASP, BCS, ISC2, IISP & the UK Cyber Security Forum amongst others. The primary aims of CSNRG are to help the UK and partner nations to tackle cybercrime, be more resilient to cyber attacks and educate its users for a more secure cyberspace and operational business environment. These will be achieved through the investigation of threats posed to information systems and understanding the impact of attacks and creation of cyber-based warning systems which gathering threat intelligence, automate threat detection, alert users and neutralising attacks. For network security we are researching securing the next generation of software defined infrastructures from the application API and control/data plane attacks. Other key work includes Computer forensic analysis, digital evidence crime scenes and evidence visualisation as well as Cyber educational approaches such as developing Capture the Flag (CTF) resources and application security programs.

Speaker Biographies

Ken Munro, Pen Test Partners

Ken is a regular speaker at events such as the ISSA Dragon's Den, (ISC)2 Chapter events and CREST (Council of Registered Ethical Security Testers), where he sits on the board. He's also an Executive Member of the "Internet of Things Security Forum", a body that aims to promote best security practice and the application of controls in smart device manufacturing, and spoke out on IoT security design flaws at the forum's inaugural event. He's also not averse to getting deeply techie, regularly participating in hacking challenges and demos at Black Hat, 44CON, DefCon and Bsides.

Ken has a wealth of experience in penetration testing but its the systems and objects we come into contact with on an everyday basis that really pique his interest. This has seen him hack everything from keyless cars and a range of Internet of Things (IoT) devices, from wearable tech to children's toys and smart home control systems. This has gained him notoriety among the national press, leading to regular appearances on BBC TV and BBC News online as well as the broadsheet press. He's also a familiar contributor to industry magazines, penning articles for the legal, security, insurance, oil and gas, and manufacturing press.

Aleksander Gorkowienko, Principal Cyber Security Consultant and Penetration Tester at PA Consulting/7Safe Ltd. (UK): "Securing sub-sea control systems from cyber-attack: vulnerabilities found by an experienced penetration tester"

In the IT industry since 1997, always being happy to play with various high-tech toys. With wide area of interests and rich business experience (development, design and maintenance of software, dealing with various IT systems) now deeply involved into IT Security area. For everyday helping to strengthen the security of business applications and corporate infrastructure for enterprises across the UK: banks, e-commerce, production, public sector, etc. Specially interested in databases and applications security (web applications and windows apps). Also responsible for preparing and delivering training courses (i.e. Certified Application Security Tester -CAST or Secure Coding for Web Developers) and creating a variety of hacking challenges.

Abstract: "Securing sub-sea control systems from cyber-attack: vulnerabilities found by an experienced penetration tester"

7Safe has recently helped to remediate serious security vulnerabilities in a sub-sea control system for a global provider of industrial solutions of oil and gas that will be deployed on a Floating, Production, Storage and Offloading vessel (FPSO).

Aleksander 'Aleks' Gorkowienko conducted simulated attacks - demonstrating that an attacker could connect to the network and carry out Man-In-The-Middle attacks, change time data coming from the ship GPS system and to intercept and modify network traffic whilst remaining virtually unnoticed. As a result, the client was satisfied that we had enabled them to significantly harden their system and in so doing protect their prestigious reputation in the Oil & Gas industry.

Aleks will outline how he approached this task in collaboration with the development engineers and what lessons have been learned from penetration testing.

Karl Williams, Principal Consultant - PA Consulting, "ICS Demonstrator"

Karl Williams is a Principal Consultant with PA Consulting's Energy & Utilities Cyber team and has extensive experience in conducting and delivering complex assignments on Industrial Control Systems (ICS) across energy and transport Critical National Infrastructure (CNI) clients.

Abstract: ICS Demonstrator

The PA Consulting Energy & Utilities Cyber team developed the ICS Demonstrator to support industry operating with ICS in place. The tool uses real life ICS equipment and networks to provide demonstrations of potential cyber-attacks, security testing of ICS/OT devices and the integration and testing of security solutions. Currently the OT on the rig has been configured to simulate the cooling process found within a nuclear reactor but its flexible architecture means that it can be changed to simulate other industrial processes much like those found in gas and power generation plants. Combined with our test rig and our CREST approved cyber security arm 7safe we have the capability to carry out comprehensive testing on a range of products, devices and systems, highlight where vulnerabilities lie and recommend risk reducing controls. The demonstrator rig has already been In front of various multi-sector clients, government bodies and regulators and has been well received at many industry conferences and workshops this year.

Maxim Silin, Technical Architect , GSK - TBC

Maxim Silin is a CTO and Committee Member with International Operational Technology Security Association (IOTSA). Maxim has extensive experience in ICS Cyber Security consultancy and solutions in Automation Industry (Power, Nuclear, Utilities, Chemical, Oil& Gas and Pharma) across worldwide.

Maxim is ENISA ICS CERT member focusing on red team scenarios and advising organizations how to protect their OT environment from attacks. He is visiting lecture within different r training organizations, including universities in Scotland and other countries focusing on network and security programmes for OT Environment and researcher with numbers of cyber security programmes like ENISA FP7 framework (Cockpit CI, Atena and more). He likes to cook and active outdoors activities: hiking and mountain climbing.

The International Operational Technology Security Association (IOTSA) and like-minded partners from the public and private sectors are working together and collaborating to reduce the risk of a significant compromise of our Operational Technology, ICS, SCADA, IT and IoT environments.

Provisional Agenda

09:30 – 10:00 Registration & Refreshments (LAB006)

10:00 – 10:05 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University (LAB002)

10:05 – 11:00 Ken Munro, Pen Test Partners.

11:00 – 11:30 Aleksander Gorkowienko, PA Consulting & 7Safe: "Securing sub-sea control systems from cyber-attack: vulnerabilities found by an experienced penetration tester"

11:30 – 12:00 Karl Williams, PA Consulting "Live hacking Industrial Control Systems with the ICS Demonstrator"

12:00 – 13:00 Maxim Silin, Technical Architect, GSK - TBC

13:00 – 14:00 Lunch & Networking (LAB006)

Registration

To register for this free event, please register online at

https://www.eventbrite.com/e/aru-csnrg-owasp-cambridge-bcs-cybercrime-forensics-iot-icsscada-forensics-workshop-10th-january-2018-tickets-41515777809

The meeting will be held in the Lord Ashcroft Building, Room LAB002 (Breakout Room LAB006 for networking & refreshments).

Please enter through the Helmore Building and ask at reception.

Anglia Ruskin University
Cambridge Campus
East Road
Cambridge
CB1 1PT

Please note that there is no parking on campus. Get further information on travelling to the university.

http://www.anglia.ac.uk/ruskin/en/home/your_university/anglia_ruskin_campuses/cambridge_campus/find_cambridge.html