OWASP Cambridge Autumn Meeting -Tuesday 6th November 2018

Tuesday 6th November 2018 17:30 – 21:00, Lord Ashcroft Building (LAB003/LAB006), Anglia Ruskin University, Cambridge.

Hosted by the Cyber Security Networking & Big Data Research Group, Anglia Ruskin University, and OWASP (Open Web Application Security Project) Cambridge Chapter.

This evening is part of a series of evening events on raising awareness for local businesses & organisations on the issues of cyber security and cybercrime, what regulations and legislation do organisations need to be aware to protect themselves and what is considered best practice in these challenging times.

Background

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, Networking & Big Data** (**CSNBD**) 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.

Anglia Ruskin University

OWASP Open Web Application Security Project

Speaker Biographies & Abstracts

Guest Speaker: Dr. Grigorios Fragkos (@drgfragkos), Ernst &Young (EY)

Bio:

Dr. Grigorios Fragkos (aka Greg) is based in London and is currently part of the EY Cyber team in OTS/TAS, delivering excellence in a globally market-leading proposition that helps decision makers in multi-million investments to identify and quantify the risk-exposure in existing and emerging Cyber threats.

With 20 years of experience, Greg has engaged with companies around the world sharing his expertise and ensuring that business entities within different sectors (such as banking, payments, maritime, defense & space) have in place security-in-depth practices against emerging Cyber threats. His background includes thought-leading security research, experience in defending mission-critical systems and leading technical security assessments, exposure to the CyberDefense department of the military and, identifying security gaps in the payments industry (fintech) while protecting high-value assets.

He has a BSc in Software Engineering, an MSc in Computer Systems Security and designed the intelligent engine of a next-generation SIEM with "notional understanding" of network events (type of MachineLearning) for real-time Threat Assessment. His background, experience and studies, which include the acceptance at the Applied Cyber Security at MIT, are considered invaluable when it comes to identifying the hidden risks and safeguarding complex digital ecosystems.

Greg has been invited to present in a number of security conferences, workshops and summits over the years. Among other responsibilities, he is assisting ENISA as part of the NIS Experts in reviewing and designing incidents for Cyber Europe, he is the organizer for Security BSides Athens and Security BSides Amsterdam, and last but not least, part of the OWASP London Chapter leaders. Thinking ahead and outside-the-box when dealing with information security challenges, is one the key characteristics of his talks

Abstract: "A holistic view on Cyber Security in evolutionary terms (food-for-thought)"

The Red Queen hypothesis, also referred to as the Red Queen effect, is an evolutionary hypothesis which proposes that organisms must constantly adapt, evolve, and proliferate not merely to gain a reproductive advantage, but also simply to survive while pitted against ever-evolving rival

organisms in a continuously changing environment.

Let's explore under a Cyber lens this evolutionary hypothesis in contrast to the evolving (cyber)threats and our adaptation (as professionals) to equally evolve our Cyber Resiliency capabilities (as an industry). This presentation is an opportunity to explore as professionals our security mindset and draw some personal conclusions on our Cyber Security culture in order to better ourselves.

From user awareness all the way to Cyber Resilience, from developing by writing secure code to the effort it takes in breaking it, from gaps in hiring talents to hiring for the right reasons, this brief session is intended to spark a personal "eureka" moment in the mindmap of each security professional inside and outside the room.

Guest Speaker: Adrian Winckles, Director of Cyber Security, Networking & Big Data Research Group, Anglia Ruskin University.

Bio:

Adrian Winckles is Director for the Cyber Security, Networking & Big Data Research Group and Security Researcher at Anglia Ruskin University. He is OWASP Cambridge Chapter Leader, OWASP Europe Board Member and is involved in rebooting the Cambridge Cluster of the UK Cyber Security Forum. His security research programs include (in)security of software defined networks/everything (SDN/Sdx), novel network botnet detection techniques within cloud and virtual environments, distributed honeypots for threat intelligence, advanced educational techniques for teaching cybercrime investigation and virtual digital crimescene/incident simulation. He has successfully competed a contribution to the European FP7 English Centre of Excellence for Cybercrime training, research and education (ECENTRE). He is vice chair of the BCS Cyber Forensics Special Interest Group.

Abstract: “OWASP Web Honeypot Project - Web Application Threat Intelligence”

The goal of the OWASP Honeypot Project is to identify emerging attacks against web applications and report them to the community, in order to facilitate protection against such targeted attacks. Within this project, Anglia Ruskin University is leading the collection, storage and analysis of threat intelligence data.

The purpose of this part of the project is to capture intelligence on attacker activity against web applications and utilise this intelligence as ways to protect software against attacks. Honeypots are

an established industry technique to provide a realistic target to entice a criminal, whilst encouraging them to divulge the tools and techniques they use during an attack. Like bees to a honeypot. These honeypots are safely designed to contain no information of monetary use to an attacker, and hence provide no risk to the businesses implementing them.

The honeypots in VM, Docker or small computing profiles like Raspberry Pi, employ ModSecurity based Web Application Firewall technology using OWASP's Core Rule Set pushing intelligence data back to a console and be converted to STIX/TAXII format for threat intelligence or pushed into ELK for visualization.

One of the project's aim is to create honeypots that the community can distribute within their own networks. With enough honeypots globally distributed, we will be in a position to aggregate attack techniques to better understand and protect against the techniques used by attackers and be able to to create educational information, such as rules and strategies, that application writers can use to ensure that any detected bugs and vulnerabilities are closed.

Provisional Agenda

17:30 – 18:15 Registration & Refreshments (LAB006)

18:15 – 18:30 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University

18:30 – 19:15 "A holistic view on Cyber Security in evolutionary terms (food-for-thought)" - Dr. Grigorios Fragkos, Ernst & Young.

19:15 – 20:00 **"OWASP Web Honeypot Project - Web Application Threat Intelligence" – Adrian Winckles,** Director of Cyber Security & Networking Research Group, Anglia Ruskin University

20:00 – 20:45 Speaker tbc

20:45 – 21:00 Q & A & Close

Registration

To register for this free event, please register online at

https://goo.gl/1ryB1s

The event will be held in the Lord Ashcroft Building, Room LAB003 (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.

https://www.anglia.ac.uk/student-life/life-on-campus/cambridge-campus/travelling-to-our-cambridge-campus