Anglia Ruskin University

OWASP
Open Web Application Security Project

OWASP Cambridge Christmas Meeting –

Tuesday 4th December 2018

Tuesday 4th November 2018 17:30 – 21:00, Lord Ashcroft Building (LAB107/LAB109), 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.

Speaker Biographies & Abstracts

Guest Speaker: Matt Lorentzen ~ Principal Security Consultant @ SpiderLabs

Bio:

Matt has 20 years IT industry experience working within government, military, finance, education and commercial sectors. He is a principal security consultant and penetration tester at Trustwave SpiderLabs with a focus on red team engagements.

Before joining SpiderLabs, he worked with Hewlett Packard Enterprise as a CHECK Team Leader delivering penetration testing services to a global client list. Prior to HPE, Matt ran his own IT consultancy company for 7 years.

Abstract: "Red Teaming : From Battlefield to Bunker"

Red Teaming is a fairly recent approach to delivering digital security assessments within the Information Security sector but the ethos of Red Teaming stems from the military and a successful operation is organized in the same way. In this talk I will be covering some aspects of Red Teaming to give an insight into how an operation is performed from the initial planning and preparation through to the delivery of the outcomes for the operation. I also introduce ways in which operators can maintain a constantly evolving skillset.

A high level summary will introduce:

- Operational Infrastructure and organization
- Open Source Intelligence
- Attacking a target
- The importance of Reporting
- Skills evolution

Guest Speaker: Etienne Greeff, CTO, SecureData

Bio:

Etienne Greeff is one of the early pioneers of the information security industry. He has spent over 20 years promoting the innovative use of technology and services to solve complex customer issues: founding, growing and successfully exiting a number of information security businesses. As CTO of SecureData, Etienne is passionate about cementing its status as a complete security services provider. He is a graduate of the University of the Witwatersrand in South Africa with a BSc in Electrical Engineering.

Abstract: "Machine Learning, Cyber & Application Security"

This talk isn't a detailed technical talk and does not require prior knowledge of Artificial Intelligence (Al) & Machine Learning (ML). After introducing core AI & ML concepts this presentation takes a high level look at the state-of-the-art in machine learning and AI with respect to Cybersecurity. We will examine where ML is effective and where it isn't effective in protecting us against those pesky hackers. I will share some practical insights in how my business uses Machine Learning to detect threats that would be difficult to detect in other ways. This presentation does not pull any punches however in debunking some myths around wild claims of how AI will automatically defend us by somehow becoming "smarter" on their own. The presentation finishes by predicting where all this may lead and the impact on application security.

Guest Speaker: Michael Koczwara - Associate Director, SecOps:Purple Team (Monitoring & Incident Response), CLS Group.

Bio:

Michael is a Senior Cyber Security professional, involved in various Cyber Security projects, managing teams and engaging with senior management to meet objectives and maximising defences against sophisticated APT cyber attacks. He has conducted penetration tests/red/purple team engagements and cybercrime investigations.

(incident response) in various FTSE100 companies/Financial Services.

Specialities - Experience:

- Offensive/Defensive Technical Cyber Security Services - SOC, Threat Hunting, Penetration Testing, Red Teaming/Purple Teaming, Threat Response, Threat Intelligence.
- Project Management/Assurance.
- Red/Purple Team Operations/APT Adversary Emulation.
- Incident Response, Threat Detection, Security Monitoring/Attack Analysis.
- Exploit Development (OllyDbg, Mona, WinDbg, IDA, Immunity, ROP, GDB).
- Software Engineering/Programming.
- Application Security/SecDevOps/SDLC - Static Code Analysis (HP Fortify, Checkmarx).

He has been acknowledged by Sony, Apple, BlackBerry, Dell, ESET, SkyTV, Bitcasa Cloud, General Motors, CERT-US and CERT-EU

Abstract: (tbc) Hedge Fund Investigation Case Study

Provisional Agenda

17:30 – 18:15 Registration & Refreshments (LAB109)

18:15 – 18:30 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University (LAB107)

18:30 – 19:15 "Red Teaming : From Battlefield to Bunker"- Matt Lorentzen ~ Principal Security Consultant @ SpiderLabs (LAB107)

19:15 – 20:00 “Machine Learning, Cyber & Application Security” – Etienne Greeff, CTO, SecureData (LAB107)

20:00 – 20:45 “Hedge Fund Investigation Case Study” - Michael Koczwara - Associate Director, SecOps:Purple Team (Monitoring & Incident Response), CLS Group. (LAB107)

20:45 – 21:00 Q & A & Close

Registration

To register for this free event, please register online at

https://goo.gl/W6F1ri

The event will be held in the Lord Ashcroft Building, Room LAB107 (Breakout Room LAB109 for networking & refreshments).

Please enter through the Helmore Building and ask at reception.

Lord Ashcroft Building (1st Floor) Room 107/109
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