bcs The Chartered Institute for IT Cybercrime Forensics Specialist Group

OWASP Open Web Application Security Project

Anglia Ruskin University

ARU CSNRG, OWASP Cambridge, BCS Cybercrime Forensics “Cyber Threat Intelligence Workshop” 2019

Thursday 24th January 2019 10:00 – 15:30, Coslett Building (COS310), 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.

Threat intelligence has become one of the new cyber “buzzwords”, also known as cyber threat intelligence (CTI), is organized, analyzed and refined information about potential or current attacks that threaten an organization.

Its primary purpose is to help organisations understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. Although threat actors often include internal (or insider) and partner threats, the emphasis is on the types that are most likely to affect a particular organisation's operational environment. Threat intelligence includes in-depth information about specific threats to help an organisation protect itself from the types of attacks that could do them the most damage.

In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a component of security intelligence and, like SI, includes both the information relevant to protecting an organisation from external and inside threats as well as the processes, policies and tools designed to gather and analyze that information.

\

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

Nick Palmer, Technical Director, Europe, Attivo Networks "Deception technology, luxury item or life line?"

Abstract:

Abstract: Is deception technology only for mature security operations or is it an effective cyber security solution to help companies mature their capabilities? Organizations continue to build their security arsenal, yet advanced threats and insiders continue to breach networks and extract valuable data. Learn how deploying decoys throughout your environment can build the bridge strengthening all the levels in your security stack. Join us for this session where you'll hear about real-world deployment experiences, the value customers are realising, and what Red Teams are saying about deception-based threat detection.

Bio

Nick has been in and around the IT security industry for over 20 years. He has worked for Microsoft, IBM, HP and Symantec, as well as a number of smaller security start-ups. With a passion for assisting customers in protecting their intellectual property, customer data and commercial strategy, Nick believes that only a multi-partite security strategy will ever succeed. By empowering all stakeholder groups in the organisation to contribute to the security dialogue, and by working with user communities, the security-conscious enterprise can better align risk and expenditure and more effectively protect itself. In his current role with Attivo Networks, Nick is working with security teams to introduce Deception to their core IT security strategy. In this way, the economics of cyber warfare can be shifted and placed back on the attacker – where they belong!

Alan Melia, Principal Incident Response Investigator, Investigations & Incident Response – MWR InfoSecurity, "Conducting an APT Investigation"

Abstract

How do you go about conducting an APT investigation? This talk walks through the technical details of an actual APT investigation.

Tracking the investigation of the incident from detection point back across the client environment and through 9 separate compromised servers in 2 different domains and using 5 separate user accounts.

Details of the process, tools and techniques used by the investigators to follow the 'breadcrumbs' of evidence so as to identify the entry vector, establish a containment plan followed by remediation and recovery of the client estate.

While some of the details have been obfuscated, the process, tools and techniques used are very much real.

Bio

Alan is Principal Consultant with MWR, one of six providers for the government-sponsored CIR scheme for networks of national significance. He manages investigation and incidents for a wide range of international and domestic clients from small businesses to government agencies.

Such incidents include investigations into APT attacks, data breaches and ransomware attacks developing live response to rapidly evolving situations. With the advent of GDPR this includes advising clients on their responsibilities in reporting loss of PII along with other compliance and privacy legislation.

Previously a manager at EY, fourteen years at Microsoft in positions including Escalation Engineer (Internet Products) and Forensic Investigator, in 2009 he developed an alert-based application for mobile detection devices for a specialist equipment manufacturer.

Alan has an MSc in Forensic Computing, documenting how to convert Microsoft PE into a forensically sound platform for investigators, and most significantly, proving how and why it works so successfully.

Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University, "Can IPFIX improve Traffic Capture Techniques for Cyber Threat Intelligence?".

Abstract

IPFIX is the ratified standard for flow export. It was designed for security processes such as threat detection, overcoming the known drawbacks of network management based NetFlow. One major enhancement in IPFIX is template extensibility, allowing traffic capture at layers 3 through 7 of the OSI model. This talk introduces IPFIX and describes the creation of BotProbe - an IPFIX template specifically designed to capture botnet traffic communications from the analysis of almost 20 million botnet flows. BotProbe realises a 97% reduction in traffic volumes over traditional packet capture. Reduction of big data volumes of traffic not only opens up an opportunity to apply traffic capture in new areas such as pre-event forensics and legal traffic interception, but considerably improves traffic analysis times. Learn how IPFIX can be applied to botnet capture and other security threat detection scenarios.

Bio

Adrian Winckles is Director of the Cyber Security Research Group at Anglia Ruskin University, Cambridge. He is OWASP Cambridge Chapter Leader, European Board Member, holds joint meetings with IET, BCS, IISP & (ISC)^2 and was conference chair for OWASP AppSec Europe

2014 in Cambridge. He is also chair for the Cambridge Cluster of the UK Cyber Security Forum. 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 previously presented at international conferences including OWASP AppSec Europe, BSides (London), Cybercrime Forensics Education & Training (CFET) & Cyber Forensics. He is Chair of the BCS Cybercrime Forensics Special Interest Group.

Provisional Agenda

10:00 – 10:30 Registration & Refreshments (COS313)

10:30 – 10:45 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University (COS310)

10:45 – 11:30 **Nick Palmer, Technical Director, Europe, Attivo Networks "Deception technology, luxury item or life line?"**

11:30 – 12:15 **Alan Melia, Principal Incident Response Investigator, Investigations & Incident Response – MWR InfoSecurity, "Conducting an APT Investigation"**

12:15 – 13:00 TBD – Recorded Future/Digitals Shadows

13:00 – 14:00 Lunch & Networking (COS313)

14:00 – 14:45 Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University, "Can IPFIX improve Traffic Capture Techniques for Cyber Threat Intelligence"

14:45 – 15:30 TBD – 7Safe/IT Governance

15:30 – 15:40 Roundup & Close

Registration

To register for this free event, please register online at

https://www.eventbrite.com/e/aru-csnrg-owasp-cambridge-bcs-cybercrime-forensics-cyber-threat-intelligence-workshop-2019-tickets-54753831183

The meeting will be held in the Coslett Building, Room COS310 (Breakout Room COS313 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

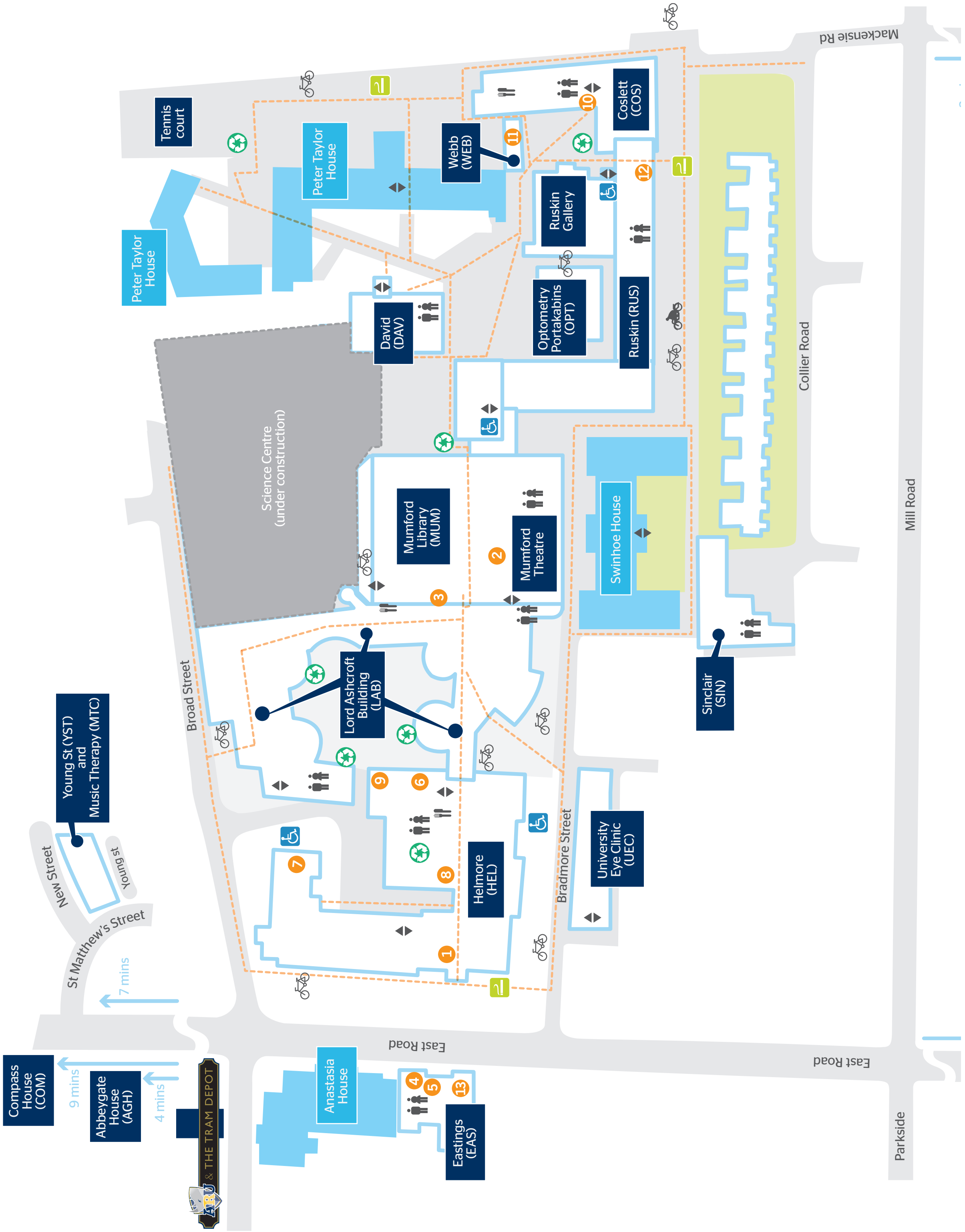
For a campus map to get to the Coslett Building please see:

bcs The Chartered Institute for IT

Cybercrime Forensics Specialist Group

OWASP Open Web Application Security Project

Anglia Ruskin University



Mackensie Rd
Tennis court
Peter Taylor House
Peter Taylor House
Webb (WEB)
Coslett (COS)
Ruskin Gallery
Optometry Portakabins (OPT)
Ruskin (RUS)
David (DAV)
Science Centre (under construction)
Mumford Library (MUM)
Mumford Theatre
Swinhoe House
Collier Road
Mill Road
Sinclair (SIN)
Broad Street
Lord Ashcroft Building (LAB)
Young St (YST) and Music Therapy (MTC)
New Street
Young st
St Matthew's Street
7 mins
Helmore (HEL)
Bradmore Street
University Eye Clinic (UEC)
East Road
East Road
Compass House (COM)
9 mins
Abbeygate House (AGH)
4 mins
ARU & THE TRAM DEPOT
Anastasia House
Eastings (EAS)
Parkside
1
2
3
4
5
6
7
8
9
10
11
12
13