Joint OWASP Cambridge, BCS Cybercrime Forensics SIG UK Cyber Security Forum – Cambridge Cluster "Cyber Security & AI Day" 2018

Thursday 18th January 2018 9:30– 17:00, 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, UK Cyber Security Forum Cambridge Cluster and OWASP (Open Web Application Security Project) Cambridge Chapter

Over the past couple of year's 2016-17 significant advancements in artificial intelligence in self-driving cars, language translation, and big data have been observed. However, during the same time period, we have also witnessed the rise of ransomware, botnets, and attack vectors as popular forms of malware attack, with according to Malware Byte's State of Malware report, cybercriminals continually expanding their methods of attack (e.g., attached scripts to phishing emails and randomization), To complement the skills and capacities of human analysts, organizations are turning to machine learning (ML) in hopes of providing a more forceful deterrent. ABI Research forecasts that "machine learning in cybersecurity will boost big data, intelligence, and analytics spending to $96 billion by 2021."

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.

The **Cambridge Cyber Security Cluster** is an affiliate **UK Cyber Security Forum**, a government and industry led partnership which will look at how the region can develop the skills and infrastructure to combat cyber security threats.

Speaker Biographies

Dave Palmer & Andrew Tsonchev, Director of Technology, Darktrace "How unsupervised machine learning can be used successfully to provide cyber defence to small or large organisations"

Dr Ali Dehghantanha Marie-Curie International Incoming Research Fellow in Cyber-Forensics Cyber Threat Hunting and Intelligence in IoT Environments

Dr. Ali has served for more than a decade in a variety of industrial and academic positions with leading players in Cyber-Security, Forensics and Threat Intelligence. He has long history of working in different areas of computer security as security researcher, malware analyzer, penetration tester, security consultant, professional trainer, and university lecturer. Ali is imminently qualified in the field of cyber security; he has an EU Marie Curie post-doctoral fellowship in cyber forensics, Ph.D in Security in Computing and a number of professional

qualifications namely GXPN, GREM GCFA, CISM, CCFP and CISSP. Ali is a fellow of the UK Higher Education Academy (HEA) and a senior IEEE-UK member.

Abstract:

Cyber Threat Hunting and Cyber Threat Intelligence are growing fields of practice in cyber security. This presentation first looks at meaning of these terms and where and how relevant technologies should be utilised. Afterwards, suitability of using artificial intelligence techniques for threat hunting and intelligence in IoT environments is discussed through analysing several case studies of using machine learning classification and deep learning techniques in attack detection. The presentation is concluded by suggesting some future works and opportunities for further collaboration.

Nikola Milosevic , Research Associate University of Manchester, **Machine learning aided Android malware classification**

Nikola Milosevic is a research associate at the University of Manchester, Manchester Institute of Innovation Research, where his research topics focus around machine learning and natural language processing. Previously he was doing a PhD at the School of Computer Science, the University of Manchester. He is involved with OWASP (Open Web Application Security Project) as a founder of OWASP Serbia local chapter, OWASP Manchester local chapter leader and a project leader of OWASP Seraphimdroid mobile security project, as well as contributing to several other projects.

Abstract:

The widespread adoption of Android devices and their capability to access significant private and confidential information have resulted in these devices being targeted by malware developers. Existing Android malware analysis techniques can be broadly categorized into static and dynamic analysis. In this paper, we present two machine learning aided approaches for static analysis of Android malware. The first approach is based on permissions and the other is based on source code analysis utilizing a bag-of-words representation model. Our permission-based model is computationally inexpensive, and is implemented as the feature of OWASP Seraphimdroid Android app that can be obtained from Google Play Store. Our evaluations of both approaches indicate an F-score of 95.1% and F-measure of 89% for the source code-based classification and permission-based classification models, respectively.

Richard Dennis, Security Researcher, Nettitude, "Machine Learning for the Bad Guys – Attack on Bitcoin"

Richard obtained a Masters in Computer information security, with a grade of distinction from the university of Portsmouth in 2013 and is currently at the writing stage of his PhD examining scalability solution to blockchain networks. Richard taught as a lecturer of Cryptography at the school of computing at Portsmouth University from 2017, being the youngest cryptographer lecturer in the United Kingdom. Currently Richard is undertaking research within Nettitude on vulnerabilities in public / private key generation in cryptocurrencies as well looking at use cases of blockchain technology.

Deepinder Singh – Principal Consultant at Verizon Consulting and Advisory Services, AI Challenges of Cyber Big Data

Deepinder (Deep) works as a Principal Consultant at Verizon Consulting and Advisory Services. He challenges, educates and engages with his audiences on many keys issues of cybersecurity and digital transformation. He encourages innovative thinking to generate actionable strategies that help business thrive in a VUCA world. He believes that poor quality decision-making skills significantly contribute towards insecure systems resulting in security breaches and compromises. He has worked with many of the worlds' largest organisations across numerous industries. In his twenty-year business career, he has held senior leadership positions in large and medium-sized organisations.

He has addressed several conferences and events on the wide-ranging topics of Cybersecurity, GRC, GDPR, Big Data Analytics and Artificial Intelligence.

Deep has attended Harvard Business School and holds a Post Graduate Diploma in Business Management along with various industry qualifications including ISO/IEC 27001 Lead Auditor, CISSP, CISM, CRISC and CGEIT. He is currently pursuing Professional Doctorate at the University of East London.

Deep actively engages in voluntary work. He is the Vice-President of ISACA London Chapter and Secretary of Verizon Reading Toastmasters Club. In the past, he has served as Secretary for BCS-IRMA Specialist Group and a judge for SC Magazine (Europe) Awards.

Abstract: AI Challenges of Cyber Big Data

Nathan Benaich, LondonAI, "Using Machine Learning to reduce reduce cyber data analysis" - TBC

Chris Woods, Founder & CEO CyberSparta, Neil Passingham (CISO) & Kari Lawler "Machine Learning in the Security Operations Centre, SOCaaS" –

Biography: Chris Woods Founder & CEO CyberSparta

An experienced leader within the cyber security realm, Chris Woods is also the founder and director of CyberSparta – an award winning cyber security startup in the UK. Having previously managed elite security teams at the European Space Agency, HP and Fujitsu, Chris brings over 20 years of pure cyber Security experience developed within the EU and MENA regions.

Whilst at HP, Chris developed and led a cyber security practice, culminating in the acquisition of ArcSight for $1.5b. With the creation of CyberSparta, Chris is now leading a passionate team of cyber and business professionals, developing the next generation of security solutions within the Big Data and Machine Learning realms.

Chris is a committed Information Security Champion and frequent speaker at international conferences and events.

Biography: Neil Passingham Chief Information Security Officer [CISO]

Neil is a highly-experienced technical and business consultant, solutions architect, client adviser and innovator with 32 years' IT experience (17 focused on security). Neil is a former CLAS consultant and has worked on securing accreditation for major government clients whilst leading the government accreditation department at HP.

His experience is wide and deep including business development, pre-sales, solution architecture, application development, testing (including ethical hacking), implementation, security assessment/accreditations, metrics/KPIs and often acting as "trusted advisor" for clients.

Provisional Agenda

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

10:00 – 10:15 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University, (LAB002)

10:15 – 11:00 "How unsupervised machine learning can be used successfully to provide cyber defence to small or large organisations" - Dave Palmer & Andrew Tsonchev, Director of Technology, Darktrace

11:00 – 11:45 "Cyber Threat Hunting and Intelligence in IoT Environments" Dr Ali Dehghantanha Marie-Curie International Incoming Research Fellow in Cyber-Forensics

11:45 – 12:30 "Machine learning aided Android malware classification", Nikola Milosevic , Research Associate University of Manchester,

12:30 – 13:15 Lunch & Networking (LAB006)

13:15 – 14:00 "AI Challenges of Cyber Big Data", Deepinder Singh – Principal Consultant at Verizon Consulting and Advisory Services

14:00 – 14:45 "Machine Learning for the Bad Guys – Attack on Bitcoin", Richard Dennis, Security Researcher, Nettitude,

14:45 – 15:15 Refreshments (LAB006)

15:15 – 16:00 "Using Machine Learning to reduce reduce cyber data analysis", Nathan Benaich, LondonAI, - TBC

16:00 – 16:45 "Machine Learning in the Security Operations Centre", Chris Wood, CEO Cyber Sparta, Neil Passingham [CISO] & Kari Lawler

16:45 - 17:00 Session Wrap Up & Close

Registration

To register for this free event, please register online at

http://ow.ly/ca8Z30hoaPU

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