Joint BCS DevSecOps/Cybercrime Forensics SGs and OWASP Cambridge “Social Media & Faux News Forensics” Mini Conference

Wednesday 11th October 2017 13:00 – 18:30, Lord Ashcroft Building (LAB003), Anglia Ruskin University, Cambridge.

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

As the digital world we knew continues to endlessly evolve, we must continue to adapt how we conduct cyber investigations. Evidence sources continue to grow rapidly. If we fail to keep up, the collection and validation of evidence during a cyber investigation will become a much more fraught task. For those investigators with a thorough understanding of how to leverage improvements in technology combined with the growing wealth of information available online, the evidence extracted during a digital forensic investigation ultimately created a more solid case.

Cyber investigations involving social media and social networks are becoming the norm. With new applications, links, techniques, and roadblocks discovered daily, social networks are rapidly progressing. Common platforms like Facebook, Twitter, and LinkedIn are becoming a smaller part of an ever growing and changing landscape. There are also many other evolving and changing social networks like Google Plus, Quora, Instagram, Groupon, Pinterest, and LoveIt and thats not even counting the thousands of blogs and special interest forums that exist.

With so much relevant evidence available on social media, there are also many new issues which are different from what investigators have traditionally dealt with in traditional digital forensics. In the past digital forensics investigators understood the terms and conditions for extracting digital evidence from a piece of hardware in the possession of the investigator, such as a computer hard drive or the flash memory on a smartphone. The evidence obtained could easily be corroborated by a third party if someone challenged how investigators had carried their work, a third party could easily corroborate the findings by reviewing the same hard drive which the investigator kept in an evidence store however this is certainly not the case with social media...

An alarming phenomenon of this rise in social media use is the growth of “faux or fake news” issue. While this concept has many synonyms - disinformation campaigns, cyber propaganda, cognitive hacking, and information warfare - it’s just one facet of a much larger problem:
the manipulation of public opinion to affect the real world. Due to global digital connectivity and platforms making it possible to share and spread information, traditional challenges such as physical borders and time/distance constraints no longer exist.

Even Mark Zuckerberg (CEO, Facebook) posted on his blog on Facebook on 21st September https://www.facebook.com/zuck/posts/10104052907253171?comment_id=356886588097117 about the large scale alleged fake news stories being published during last year’s US presidential election and the importance of this issue to protecting the security of the democratic process....

Fake news is the promotion and propagation of news articles via social media. These articles are promoted in such a way that they appear to be spread by other users, as opposed to being paid-for advertising. The news stories distributed are designed to influence or manipulate users’ opinions on a certain topic towards certain objectives. For example, by manipulating the balance of how a particular topic is reported (whether that concerns politics, foreign affairs or something more commercial), the views on that topic can be changed. This can be done either with inaccurate facts or with accurate ones twisted to favour a particular view or side.

**Background**

BCS DevSecOps Group fosters the awareness of tools and technologies regarding the acceleration and automation of code development to deployment, known as DevOps. It is both a work culture and complex, rapidly evolving toolchains both difficult to introduce and use effectively. It covers cultural, technical, management and security aspects.

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 Abstracts & Biographies**

**Dr Char Sample – Data Infidelity and Fake News: Software Security’s Soft Underbelly?**

**Biography - Dr Char Sample**

Dr Char Sample is cyber security researcher and fellow at ICF International, in Maryland, U.S. Her prior work includes as security solutions engineer with CERT, Carnegie-Mellon; and International Fellow at Warwick University.

Dr Sample is an academically and professionally experienced cyber security professional with over 19 years of experience in network security and software engineering. Her internet security experiences include threat intelligence research, cloud computing, security metrics, expertise with firewalls, IDS, IPS, Anomaly Detection, DNS, DNSSEC, Mail, routing, authentication, encryption, secure network architectures, cloud computing (IaaS, PaaS) and Unix internals. Dr Sample is internationally recognized as the leading expert in quantitative cultural cyber threat intelligence. Her publications include both academic and industry conferences and journals.

**Abstract**

Bad data can create more than just 'fake news.' Expert Dr Char Sample explains how cognitive hacking and weaponized information can undermine enterprise security.

One of the major security stories from the 2016 US Presidential election was not the breach of voter databases, the suspected hacking of the voting machines or even the vote counting. The
biggest security story was the use of weaponized information in support of cognitive hacking, defined in a 2002 Dartmouth College research paper as a cyberattack designed to change human users' perceptions and corresponding behaviors.

Disregarding the political dimensions of elections, the real reason for this interest is that security software is vulnerable to the same problem. That is, the data entered into security products, whether by a human or a machine, is trusted to be a faithful representation of reality.

**Dennis Ivory and Dr Diane Gan - Your Personal Information Stolen In Under 2 Minutes**

**Biography – Dennis Ivory**

Dennis Ivory recently graduated with a first class degree in BSc Computer Security and Digital Forensics from the University of Greenwich. He is currently employed as a post-graduate researcher within the Department of Computing and Information Systems, where he is undertaking research with the Cyber-SAFE security research team into security issues in the Internet of Everything.

**Abstract**

One of the single biggest threats to personal security is a targeted social engineering attack. Attackers are becoming more sophisticated at tricking people into giving away their personal details by using these types of attacks gained from information harvested from social media (Twitter, Facebook, etc.). More people than ever have an online presence, with 2.34bn people (37% of the world population) now using some form of social media [Statista. 2017]. Many of these users are either new to these platforms or are unaware of the seriousness of adding a lot of personal information about themselves on, for example, their Facebook page. This research set out to determine how people perceive their own online privacy and how this relates to what is actually available to anyone searching about them online who had no connection with them via their social media sites.

A survey was conducted to identify how individuals perceived their own online security and to determine what they had knowingly published online. There were 252 volunteer responders. The vast majority of these volunteers were students at the University of Greenwich but only 43% were studying computing degrees. The split of female (58%) to male (42%) participants was reasonably balanced and the largest age range was 18 to 23, as expected in a university population. The second phase of this work was to investigate what information could actually be found online about each of these participants. Searches were conducted on each person using Facebook, Twitter and the
Google search engine. The fastest search found the subject’s full name, picture and the places that they had visited in the last few days in 14 seconds. The vast majority of these investigations (166) took less than 2 minutes to gain access to a significant amount of the subject’s personal information, including details which they did not think could be found online. This presentation presents the results of this experiment.

**Stuart Clarke – Nuix - Relationship Centric Data Analysis using Social Media and Other Forensic Sources**

**Biography – Stuart Clarke**

Stuart is an internationally respected information security expert who is responsible for the overall security and intelligence strategy and delivery at Nuix. During his time at the company, Stuart has advised the United Nations’ peak cybersecurity body ITU and provided cybersecurity training for over 60 computer emergency response teams. He led the development of Nuix Investigation & Response, an innovative investigative tool used to delve into the causes and scope of data breaches. He also currently leads the development of Nuix Insight Analytics & Intelligence, a powerful security intelligence platform.

Stuart has a deep understanding of the Nuix technology and capabilities. Prior to joining Nuix, he used Nuix offerings extensively in breach response. He brings that understanding together with a vision for the cybersecurity needs of Nuix’s current and prospective clients. He holds a Bachelor of Science degree with honors in Computer Forensics and a Master’s Degree in Business Administration. He has developed and delivered training for a Master of Science program in Computer Security and Forensics, has contributed to a book covering evidence preservation as well as published several industry-recognized white papers.

**Abstract**

The traditional item centric and linear approach to digital evidence is effective, however is straining under the ever-increasing volume and variety of data that individuals generate. Social media and mobile data is now overtaking traditional computer based sources of evidence and it is becoming key for forensic investigators to correlate disparate pieces of information that reveal a bigger picture.

This session will explore how relationship centric analysis can accelerate investigations and
provide a deeper level of visibility and understanding of various investigative scenarios. We will see how analysts can use advanced technologies to find hidden connections from something as simple as an account handle or alias and turn what’s outwardly disparate into a clear picture.

Dr. Ali Dehghantanha - Digital Forensics in Social Internet of Things: Opportunities and Challenges

Biography - Dr. Ali Dehghantanha

Dr. Ali Dehghantanha is a Marie-Curie International Incoming Fellow in Cyber Forensics, a fellow of the UK Higher Education Academy (HEA) and an IEEE Sr. member. He has served for many years in a variety of research and industrial positions. Other than Ph.D in Cyber Security he holds several professional certificates such as GXPN, GREM, GCFA, CISM, and CISSP. His main research interests are cyber threat intelligence, threat hunting and digital forensics.

Abstract

IoT as a world-wide network of interconnected and uniquely addressable objects would soon pervade all aspects of our life from managing our home temperature to thinking cars and smart management of the cities. The Social Internet of Things (SIoT) stands beyond IoT as environments in which information gained from IoT nodes are merged with social networking principles to enable social driven human to device interactions. SIoT concept facilitates social interactions by enabling smart devices to play a more active social role. While there are many challenges in realizing the SIoT vision, digital forensics is probably the least discussed issue! This talk would first start with describing architecture and developing technologies to materialise SIoT vision. Moreover, it sheds light on challenges a forensics investigator would face in identification, collection, preservation and analysis of evidences in a SIoT environment. Finally, some ideas are suggested for future development of tools, techniques and procedure to possibly overcome forensics challenges in SIoT environments.
Provisional Agenda

13:00 – 14:00 Registration & Refreshments (LAB006)

14:00 – 14:05 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University

14:05 – 14:55 Dr Char Sample - Data Infidelity and Fake News: Software Security’s Soft Underbelly?

14:55 – 15:45 Dr Diane Gan & Dennis Ivory – Your Personal Information Exposed in under 2 Minutes

15:45 – 16:15 Refreshments, Networking & Industry Demo’s

16:15 - 17:00 Dr Ali Dehghantanha – Digital Forensics in Social Internet of Things: Opportunities and Challenges

17:00 – 17:45 Stuart Clarke – Nuix - Relationship Centric Data Analysis using Social Media and Other Forensic Sources

17:45 – 18:30 Industry Panel & Round up
Registration & Arrival

Please register online using the following URL:


The meeting 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.

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