Emerging Cyberspace Challenges and Solutions

Friday 11 January 2019
Og46, Old Sessions House, Canterbury Christ Church University

Keynote

David Rogers
Founder & CEO, **Copper Horse** *and Mobile Technology, Cyber Security & Standards Adviser,*
Department for Digital, Culture, Media & Sport (DCMS), UK

David is an adviser to DCMS in the UK on a number of technology and cyber security topics. He is the founder and CEO of Copper Horse Solutions Ltd, a software and security company based in Windsor, UK. His company is currently focusing on security and privacy research for the Internet of Things.

David chairs the Fraud & Security Group at the GSM Association and sits on the Executive Board of the Internet of Things Security Foundation. He is a Visiting Professor in Cyber Security and Digital Forensics at York St John University and teaches Mobile Systems Security at the University of Oxford.

He has worked in the mobile industry for 20 years in security and engineering roles. Prior to this he worked in the semiconductor industry. Most recently he authored the UK's 'Code of Practice for Security in Consumer IoT Products and Associated Services', in collaboration with DCMS, NCSC, ICO and industry colleagues.

David holds an MSc in Software Engineering from the University of Oxford and a HND in Mechatronics from the University of Teesside.

He blogs from https://mobilephonesecurity.org and tweets @drogersuk

****

Adrian Winckles, Chair, BCS Cybercrime Forensics Specialist Group
Anglia Ruskin University

Can IPFIX Improve Traffic Capture Techniques for Cyber Threat Intelligence

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.

Biography

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 vice chair of the BCS Cybercrime Forensics Special Interest Group.

****

Dr Nimmo Dragomelo, Senior Consultant
Quality World

Securing Auditing of Medical Suppliers and Devices

Briefly reviews the State of Medical Device vulnerability to cyberattack and examines how an effective audit approach can help in complying with the key regulations, for instance EU directive NIS, as well as identify vulnerabilities lowering cyber risks. BSC has been adopted to measure audit performance against pre-set KPIs. For ease of security auditing a set of modification for the audit management system of suppliers of medical devices have been reviewed and proposed an audit plan for audit execution in order to lower the cyber risks. Both ISO/IEC 27000-series entitled "Information Security Management System as well as ISO/IEC 80001" Application of risk management for IT-networks incorporating medical devices" have been included in the audit plan. Whilst auditing to enhance cyber security for medical devices and suppliers it is important to assure that healthcare organizations also do their part in managing cybersecurity risk. Responsibility cannot be held by the medical device manufacturer alone. The hospital or healthcare providers must ensure that medical device is deployed to an equally secure network system. Both parties. (Medical device manufacturers and Healthcare providers) need more visibility (details of their respective responsibilities with respect to the project scope) in order to manage risk and deliver quality products. From our research to date it tends to suggest that cyber security risk of medical devices could be lessened through (1) simplifying and centralizing regulatory requirements in order to achieve their more effective/efficient implementation (2) medical device development(improvement) by innovating, keeping up with trends, and meeting cyber security challenges as they pose.

****

Luc Poelmans, Telecom IT Security Expert, Belgium

Vehicle Forensics: Analysis of the SYNC3 (QNX6 based) Infotainment System of a Ford Kuga

If digital investigation of car accidents exists for about 30 years, modern cars are today important sources of information for the investigation of criminal activities like analysis of recovered vehicles or of hacked cars, but also for investigation of "usual" crimes: let's imagine that a car is found with a dead body in the trunk… Investigators might be interested by information about when and where the trunk has been opened, where the car has been parked during the last hours (to focus the

neighbourhood enquiries), where and when the car has been fuelled (to collect videos or indications about payment methods), etc.

The presentation will focus on the work performed by Luc, in the context of his Master Degree at University College Dublin, on a SYNC3 infotainment system installed on a Ford Kuga car.

After an overview of already published analysis and elements of guidance, specific artefacts are disclosed which could be of interest for criminal investigations. These artefacts are then compared with the data that could be found with a commercial tool used by Law Enforcement forces for automotive forensics.

Finally, he will also present some challenges that he will try to address in the near future.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

****

Ulf Bergum, Head of Education in Digital Forensics and Cybercrime Investigation & Detective Superintendent, Norwegian Police University College, Norway

Validation Techniques for Live Forensics Tools

In traditional computer forensics the forensic copy can be validated against the original disk. Normally such a validation process confirms the integrity of the forensic copy as the file system would not be mounted during the acquisition process. This is in contrast to LDF situations where the system is changing throughout the analysis. Being unable to verify acquisitions has an impact on the integrity of the seized data. As long as forensic readiness is not implemented to compensate for this, the only thing that can be done is to look into the acquisition process and try to make it as forensically sound as possible.

The nature of LDF makes it difficult to test and verify tools for RAM acquisition. The constant changes of memory in a live system, make it challenging to ensure if the tools in use are able to acquire all data as there is no record of the data populating RAM. Recording the data present in RAM at all times, could be a way to improve the forensic soundness of the tools being used for RAM acquisition. Based on knowledge of the contents of RAM, it will be possible to change the way LDF tools are verified and lead to more accurate and trustworthy tools. This will raise the quality of the investigation and strengthen the legal protection for the all parties involved.

****

Yves Vandermeer, Chair, European Cybercrime Training & Education Group (ECTEG) and Norwegian Police University College, Norway

Electronic Evidence: Role of the First Responder in an IoT World

Increasing number of IoT devices result in the raise of potential electronic evidence contained in each of them. In this context, the role of First Responders, police patrol officers or investigators working on traditional crimes become essential. The presentation will start with a short overview of existing situation and identified issues related to identifying, protecting and, sometimes, acquiring electronic evidence. Yves Vandermeer will then explain how the cooperation between Lax Enforcement first responders and forensic experts and software developers delivered a set of dedicated tool and training allowing First Responders to play an active role on the crime scene.

Biography

"*After 30 years as police officer in the Belgian federal police, among which more than 15 years dedicated to computer forensics and cyber crime fighting, Yves Vandermeer is currently lecturer in the Norwegian Police University College.*

Master in Computer Forensics, and developer of software specialised in the computer forensics he performs currently a PhD focusing on the electronic evidence eco-system.

He is the chair of ECTEG, the European Cybercrime Training and Education Group, where he contributes to the creation of specialised lessons available for Law Enforcement in cooperation with Europol-EC3, CEPOL, Council of Europe and other EU cybercrime related projects.

His motto is an expert staying in his corner will soon become expert of only the corner."

****

Fida Hussain & Dr Man Qi
Canterbury Christ Church University

Smart home uses IoT for the purpose of home security, energy efficiency, convenience and an improved standard of life. In a smart home, everyday devices and sensors connect, communicate, transfer and process data. New Smart Home devices and services appear at a fast pace. Due to the interdependencies, numerous cyber threats appear with possible consequences on the life, health and safety of the inhabitants. Hence, it becomes important to enhance the security of smart home.

There are different wireless communication protocols for instance Wi-Fi, ZigBee, Bluetooth, Zwave etc. communication protocols used in Home Area Network (HAN) to exchange data from different devices. The threats and vulnerabilities to Smart Home security include modifying packets, injecting packets and men-in-the-middle. The research aims to tackle the men-in-the-middle and a passive attacker. For security and privacy, we propose a symmetric encryption algorithm before sending data and a hash function for unique token identification issued by UHG (Universal Home Gateway) for HAN appliances and also asymmetric encryption connection between HAN to outside world. We use UHG with unified API for heterogeneous appliances of HAN. Intrusion Detection System (IDS) is to analyse and monitor traffic on network. Hybrid Intrusion Detection System (HIDS) is proposed to detect, monitor and analyse traffic of the network. The hybrid intrusion detection system will help to significantly reduce attacks on smart home system. Our research will provide security and privacy schemes for smart devices to prevent intruder in the middle attacks so that smart devices can communicate safely in and outside smart home.

****

Jonathan Haddock, Network & Security Engineer
Local Government

The Threat of Security Knowledge Gaps

Cyber security is everyone's problem, not just the security team's, yet often there are avoidable basic gaps in knowledge that can prevent teams working well together. In this talk Jonathan discusses the importance of collaborating with other teams to help protect systems and data from would be attackers. With data breaches announced weekly, it's never been more important for all of an organisation's IT team to communicate to achieve this goal. Jonathan will examine these gaps and suggest ways to help reduce the problem, including the delivery of some basic training, in order to create "security allies". By reducing the knowledge gap, productive conversations can be had for the benefit of all.

Biography

Jonathan has worked in IT for over 15 years, recently moving to specialise in cyber security. Having gained qualifications in digital forensics, incident response and penetration testing, he now helps look after the security and network infrastructure of three local government authorities. He gained an MSc in Professional Computing from Staffordshire University and has given guest lectures and talks at universities. Previously he worked with the BCS Young Professionals Information Security Group (YPISG), speaking at a number of their penetration testing training days. Jonathan was a speaker at the first annual cyber conference organised by the Cyber Innovation Hub of Canterbury Christ Church University in January 2018.

He blogs about cybersecurity, development, IT administration and life at https://blog.jonsdocs.org.uk and tweets from @joncojonathan.