CRESTCON
SPECIAL
The Script Bulletin
FEBRUARY 2019

UPDATES:

An in depth look at the CRESTCon agenda

CRESTCon (**www.crestcon.co.uk**) takes place on 14th March at the Royal College of Physicians. A limited number of tickets are still available so please book now if you don't want to risk missing out. Contact **marketing@crest-approved.org** for information on free and discounted member tickets.

This is what you can expect to see in the three streams:

09:00 – 09:15 Welcome: Ian Glover, President, CREST & Mark Turner, Chairman, (Wolfson Theatre)

Ian Glover

Mark Turner

09:15 - 09:45 KEYNOTE Paul Midian, CISO Dixons Carphone plc: (Wolfson Theatre)

Paul Midian

Paul is an accomplished information and cyber security practitioner with over 20 years' experience; he is Chief Information Security Officer at Dixons Carphone plc. Previously, Paul was a director in the Cyber Security practice at PwC leading large scale information and cyber security improvement and transformation programmes. Prior to his role at PwC, Paul was a director at Information Risk Management Plc. During his tenure revenue increased by over 75% and the company won the Secure Computing 'Information Security Consultancy of the Year' 2013 award. Prior to working at IRM he was Head of Security Testing at Siemens Enterprise Communications (formerly Insight Consulting). Paul is a member of the BCS and of ISACA. He has been involved in the CREST organisation since its inception.

The Penetration Testing Stream – Wolfson Theatre

Stream Hosts – Mark Turner, NCC Group & Paul Midian, Dixons Carphone

09:55 – 10:25 Sarka Pekarova, Cybersecurity Consultant, SureCloud: The Pirate Queen's Techniques to social engineer her targets (and how you can too).

You can have great firewalls, IPS/IDS, have your perimeter locked down, your web applications secured, but it doesn't stand a chance against the social engineering tactics of Grace O'Malley, my social engineering alter ego and pirate queen from the 16th century! 91 % of today's cyberattacks start with social engineering.

Social engineering has many different faces; using open source intelligence (OSINT), phishing, vishing, smishing and all the other '-ishings', dropping weaponised USB flash drives and eventually getting right in middle of your target's own office to hack all things! There are many tools and almost all of them do not require any interaction with the target because it does not need you to leave your warm chair in front of your machine. But everyone wants to break into buildings like a pirate queen, am I right? To do that we will have to interact with our target directly and that requires certain knowledge and skills. I will describe how to use knowledge of facial expressions, body language, Chinese medicine, the whole psychology behind influence and persuasion and how to manipulate targets into believing my pretext and comply with my (evil) plans. I will also explain what some of the behaviours and pretexts to avoid are and I will step over to the defensive side as well and explain how to defend against the attacks I describe. Attendees will walk away knowing how to start working on their social engineering skills that can be used during social engineering engagements/ physical security, red teaming or at home. They will also have a better understanding of what to defend against.

This presentation is part of my unique series of talks on the deep dive into the psychology/body language reading to be used in social engineering. None of the talks are the same, I am building a deeper knowledge with every talk.

Grace O'Malley is a pirate queen from the 16th century that breaks into buildings, exfiltrates sensitive data and gets to places where she shouldn't be, manipulates people to comply with her demands…oh and **Sarka** is the nice one. She has been in IT for over 10 years and has a rich experience in blue team environment having worked in and managed SOC that guards national British infrastructure. Currently Sarka works as a pen tester for SureCloud where she tests everything from infrastructure, web apps to payment systems and specialises in social engineering.

11:00 – 11.45 Tabraiz Malik, Cyber Security Associate, PwC: Unorthodox Command and Control (C2) Channels

As technology progresses and malware evolves, cyber attackers continuously adopt new and innovative techniques to exploit current technologies, whilst also seeking to evade detection. The method in which an infected machine and attacker communicate – the "command-and-control" channel - is arguably the most critical aspect of its operation, allowing the attacker to remotely control malware and exfiltrate data remotely. By establishing a covert communication channel which bypasses a victim's logical defences, an attacker can increase the chances of making this channel persistent - a pivotal element of any successful attack campaign. Through developing novel channels which have not yet been widely adopted, Tabraiz will demonstrate how these seemingly innocuous technologies can be manipulated to achieve bilateral communication between an attacker controlled station and an unwitting victim. In order for organisations to take a proactive stance on combatting and minimising the adversarial threat in the increasing volatile digital realm, it is crucial that they are appropriately equipped with knowledge of unique C2 channels which could be abused by attackers.

Initially Tabraiz will aim to provide an analysis of unconventional C2 channels adopted in the wild by real threat actors in the modern age, such as X.509 and steganography. Notably he will give specific case studies of notorious strands of malware and provide commentary on the impact they have had on targets including the critical infrastructure of organisations and nation states. He will then proceed to explore a selection of original techniques that he has been actively researching and developing.

Tabraiz is an Ethical Hacker within the Cyber Threat Operations team in PwC's UK Cyber Security practice. Prior to joining PwC, he worked in the High-Performance Computing team at Rolls-Royce, developing in-house software. His research interests include remote C2 channels and SOC evasion techniques.

11:50 – 12.35 Gabriel Gonzalez, Principal Security Consultant, IOActive: SATCOM: Attacker's Perspective

In 2014, IOActive presented "A Wake-up Call for SATCOM Security," and described several theoretical scenarios that could result from the disturbingly weak security posture of multiple SATCOM products. They are at CRESTCon now to prove those scenarios are real. Some of the largest airlines in the US and Europe had their entire fleets accessible from the Internet, exposing hundreds of in-flight aircraft. Sensitive NATO military bases in conflict zones were discovered through vulnerable SATCOM infrastructure. Vessels around the world are at risk as attackers can use their own SATCOM antennas to expose the crew to RF radiation. This time, in addition to describing the vulnerabilities, we will go one step further and demonstrate how to turn compromised SATCOM devices into RF weapons. This talk will cover new areas on the topic, such as reverse engineering, Radio Frequency (RF), SATCOM, embedded security, and transportation safety and security.

Gabriel has more than 15 years of working experience with embedded system mixing development and security from network equipment to satellite communication systems where he has actively exploited software and hardware vulnerabilities. Lately he has specialised in industrial equipment with a special mention to smart grid environments.

>>

UPDATES:

13:30 – 14:00 CISOs and Pen testers debate panel

Attack simulation, friend or foe? In this session we'll be exploring the want of the buyer to have a simulated attack and then the responsibility of the tester to help the customer.

Chair: Andrew Jutson, Director, Cyprotec Ltd

Andrew is an experienced Chief Information Security Officer, seasoned Information Security Consultant and Risk professional working across a number of industries including financial services, defence, retail and banking. Through his time in the industry I've had hands on experience interfacing with global regulators throughout the incident management, containment and response process.

CISOs: Neil Fowler Wright, Hitachi Rail Europe; Matt Gordon-Smith, Anglo-American; Denis Onuoha, Arqiva

Denis is the Chief Information Security Officer at Arqiva, a major UK infrastructure company which supports 40% of the UK's Critical National Infrastructure spanning the broadcast, telecommunications, finance, energy and utility sectors. He has the overall responsibility for Security Risk Management, Information Assurance and Cyber Security for the company and is at the forefront of its fight in defending against the latest media industry cyber-attacks. Denis holds a BSc in Computer and Network Security from the University of Hertfordshire and is close to completing the MSc in Information Security at Royal Holloway. Having completed his undergraduate studies, he commenced work in the financial sector with responsibilities for Risk and Information Security, subsequently making the move across to the broadcast industry. A proactive IT professional, Denis sits on three of UK's Centre for the Protection of National Infrastructure (CPNI) Government Information Security Exchanges, is the elected Chair of the AIB Cyber Security Working Group and is a member of the CREST industry advisory panel.

Matt is CISO at Anglo American, a FTSE100 mining company, managing information security requirements globally across both corporate and industrial IT; in-house and outsourced applications; and on-premise and cloud-based services. Matt began his career in Information Security over 18 years ago at IBM, before taking on global security leadership roles within several IT service providers, dealing with both internal and customer requirements across several different sectors, including Banking, FMCG, Media, Telecommunications and Local and Central Government. In 2014, Matt moved out of the IT managed services sector to take the role of Head of Security at URENCO, a highly-regulated global uranium enrichment company. Three years later, Matt took his current role in Anglo American to manage an increased investment in Cyber Security, leading the growth and development of the security team, processes and technology.

Neil Fowler Wright has a background developed through Legal Services, Financial Services (including FinTech), and Manufacturing; and has lead both large and small, but always highly dynamic, Information Risk/Security teams. Currently he is working for Hitachi Rail, overseeing all areas of their Information Security governance, and in doing so he covers areas as diverse as GDPR, Security… Design, Policy, Metrics, Compliance, Operations, Testing, Architecture, and Forensics. Whilst working closely with all the various business areas, from Manufacturing to Legal, and HR to Service and Maintenance, he is always focussed on how to deliver valuable security solutions that simultaneously protect and enable the business. Though he describes his primary role as that of translator between IT and business on those many areas of security governance and regulation. With more than 20 years' experience in Security, he is now enjoying working with a fast growing and young organization that is deeply embedded in our national critical infrastructure.

>>

UPDATES:

Penetration Testers: Gemma Moore, Director, Cyberis; Justin Clarke-Salt, Managing Director, Aon

Brian McGlone Regional Leader of X-Force Red

Gemma is an expert in penetration testing and simulated targeted attack. Having been a CHECK Team Leader since 2007, she holds CREST certifications in Infrastructure, Applications and Simulated Attack. Gemma has spent more than a decade working in the security consultancy industry and has helped customers across a wide range of industry sectors assess their risks and improve their security. Gemma is an engaging presenter and trainer who is passionate about helping her customers improve their own skills and experience. She delivers training and workshops to industry professionals, developers, operational teams and end users.

In recognition of her outstanding level of commitment to the technical information security industry and the highest level of excellence in CREST examinations, Gemma was selected to receive a CREST Fellowship award in 2017.

Justin is one of the founders of Gotham Digital Science, and these days (post acquisition) is a Managing Director in Aon's Cyber Solutions Group. He is in charge of Aon's proactive business development and partnership efforts for EMEA. Justin has more than 20 years of experience providing organisations with security and risk management services, and on the CREST side of things he is a CREST Certified Tester (Infrastructure) and a CREST Certified Simulated Attack Manager. He is the lead author/technical editor of "SQL Injection Attacks and Defenses" (Syngress 2009 and 2012), co-author of "Network Security Tools" (O'Reilly 2005), and a contributing author to "Network Security Assessment, 2nd Edition" (O'Reilly 2007), as well as a speaker at various security conferences and events such as Black Hat, EuSecWest, ISACA, BruCON, OWASP, OSCON, RSA and SANS.

Brian is Regional Leader of IBM X-Force Red - UK & Ireland. His remit covers the selling, managing and delivering security services to a global client base. Brian has a wealth of experience in the Security Assessment and Audit fields. Brian was worked in America, Africa, and 10 countries across Europe; his work includes security assessments for all sectors. Brian has had many roles in IBM including ownership of Cyber Security & Intelligence UKI & Head of Security Assessment Services UKI. Primarily focussed on security technical assessments & consulting.

14:05 – 14:35 Imran Shaheem, Consultant, Cyberis: Quantum Cryptography

Quantum Cryptography has come along a great deal since scientific and mathematical interest in the field took off in the 90s. It has several consequences for classical cryptography and what will be considered the standard for secure communication in the near future. Successful trials that secure communication through the unique properties of quantum physics have already been undertaken. Progress in quantum technologies has been swift in the last decade; Quantum Key Distribution (QKD) systems have been tested by banks and governments, similar systems were deployed at the 2010 World Cup in South Africa. In 2017, researchers held a QKD-protected video conference between China and Austria using the quantum satellite Micius as a trusted relay, further strides and greater worldwide adoption is anticipated for the coming decade.

In this presentation we will begin by taking a broad look at quantum information and the ramifications it has on classical (current) cryptography. After which we shall be taking a dive into the interesting and counter intuitive world of quantum physics with regards to cryptography.

Imran joined Cyberis Limited in early 2018 following the successful completion of an MSc with Merit in Theoretical Physics (Gravity, Particles and Fields) at the University of Nottingham.

Prior to joining Cyberis, Imran participated in online bug bounty programs which led to private security research work for a Fortune 10 company. In conjunction to this, his work earned him BugCrowd's VIP researcher accolade in 2017, placing him in the top 300 of over 50,000 researchers who use the platform.

>>

UPDATES:

14:40 – 15:10 Justin Clarke -Salt, Managing Director, Aon: Let's Talk About Risk

As many folks are aware, Gotham Digital Science and Stroz Friedberg are now part of Aon. As part of the integration into what is a massive risk management professional services organisation, working with risk colleagues in other disciplines has highlighted how we look at risk wrong as pentesters, and how naive the traditional pentesting risk rating approach is.

In this talk I'll be covering some of the context of how we fit into a risk management structure, and how changing our awareness of risk can help to vastly improve the quality of advice we provide to our clients on what their true risks are.

15:45 - 16:30 Christopher Thomas, Solution Architect, IBM: Blockchain - conceptual and architectural security considerations and their potential associated risks.

Blockchain technology was first proposed in 1982, however it was never fully conceptualised until the end of 2008 with the creation of bitcoin. While its potential applications are now becoming known, there is a distinct shortage of knowledgeable individuals who understand the technology and even less who understand the risk and security aspects. A blockchain enabled environment is made up of many different components that can be built on-top of blockchain where it can be likened to building a house; if it is built on insecure foundations the house will always be at risk. This talk will embark on outlining conceptual and architectural security considerations and their potential risks associated with blockchain projects

Over the last 10 years, Chris Thomas has honed his skills within the information security industry and today is a Senior Managing Consultant at X-Force Red and part of the European management team. With a Bachelors (BSc) degree in Software Engineering and a Masters (MSc) degree in Computer Systems Security his responsibilities include managing the penetration testing network within the EMEA team, to mentor junior consultants and to perform a wide range of assessments ranging from infrastructure, web applications, code reviews, blockchain and architecture reviews.

Chris's experience with providing security assessments and advice spans a variety of industries include Finance, Government, Nuclear, Telecommunications and National Critical Infrastructure. Chris first started within the industry as a systems administrator of a penetration testing network where he eventually came to manage the same network while performing penetration testing activities. Chris likes to solve complex problems by either writing software or architecting systems/environments where he has built several enterprise grade solutions from the ground up that have spawned their own division.

16.35 – 17:05 Rewanth Cool, Payatu Software Labs LLP: Creating browser extension to hunt low hanging fruits

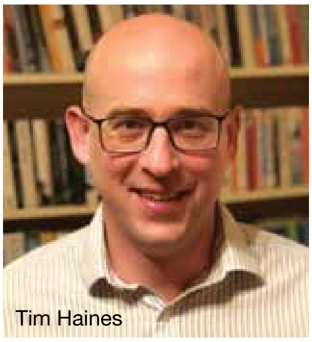
With the recent advancements in technology, more people are aware of the importance of security. More companies started paying huge rewards to protect the sensitive information of their customers. This Firefox extension is a first of its kind and an open source product. The Firefox extension is capable of detecting header related vulnerabilities by analysing the request and response headers. The browser extension requires no special configurations, easy to install, easy to use, low false positives and capable of finding vulnerabilities in all the endpoints the user visits in a fraction of seconds. The web application firewall doesn't block the requests crafted by the browser extension (due to legit traffic) yielding better results compared to other existing tools. Github link of the tool - **https://github.com/rewanth1997/vuln-headers-extension**

As of today, the browser extension is capable of detecting CORS misconfiguration, Host Header Injection, Clickjacking and missing secure flags/headers vulnerabilities. I found vulnerabilities in Bugcrowd, Hotstar, Medium, Signup.com, Chargify etc using this minimal browser extension. People from across the globe (India, Sri Lanka, Taiwan, Philippines, Nepal, Denmark, etc) found this tool to be helpful, **https://github.com/rewanth1997/vuln-headers-extension/stargazers**. In this 30minute talk, we will be focusing on creating your own minimal smart scanner as browser (Firefox ESR) extension to detect header related vulnerabilities. This extension monitors the request and response headers passing through your browser and detects vulnerabilities in them. The browser extension is capable of detecting CORS misconfigurations, host header injections, and clickjacking vulnerabilities. In the process, you will be learning about basic header vulnerabilities like CORS misconfiguration, host header injection, clickjacking and exploitation scenarios, detection methods and the biggest bounties earned through simplest detection techniques for each of the above vulnerabilities. By the end of the talk, you will be capable of writing your own browser extension to hunt low hanging fruits.

Rewanth started his career as a fullstack/backend developer building applications before moving to the security field. He is currently working as a security consultant at Payatu and has been a speaker at Null Pune and a trainer at MIT Pune. Rewanth participates in numerous Capture-the-Flags (CTF) and enjoys participating in private bug bounty programs. He is a programmer and open source contributor as well as an active Hack The Box player. Currently, his focus is on vulnerability research, web application security and contribution to security tools. He collaborated with Daniel Miller a.k.a bonsaviking and added 17,000 lines of code to Nmap which includes puncode support, enumeration of openwebnet protocol, remote smb services, optimisation of exploitation scripts etc.

>>

UPDATES:



Tim Haines

Rob Dartnall

Threat Intelligence Stream – Seligman Theatre

Stream Hosts: Rob Dartnall, Security Alliance & Tim Haines, NCC Group

Sponsored by:

SECURITYALLIANCE

09:55 – 10:25 Thomas V. Fischer, Security Advocate & Threat Researcher, FVT SecOps Consulting: Building a Personal Data Focused Incident Response Plan to Address Breach Notification

The era of the data breach is upon us. In a traditional incident response investigation, the focus is often on attribution and how it was done, with an aim of quickly containing. Change needs to occur and organisations need to be able to quickly identify and understand what personal data is affected. Using the SANS six primary phases of incident response as a base, this talk will explore practical steps to rebuild the incident response plan with a personal data focus. By using and understanding Information Asset registries, data mappings and data protection impact assessments, the preparation phase can be enhanced to support personal data protection coverage in the IR plan. The goal to engage ideas and thoughts on how to improve the identification phase where detection and determination needs to quickly identify an event and subsequent incident where a potential personal data breach is occurring.

Thomas has over 30 years of experience in the IT industry ranging from software development to infrastructure and network operations and architecture to settle in information security. He has an extensive security background covering roles from incident responder to security architect at fortune 500 companies, vendors and consulting organisations. He is currently a security advocate and threat researcher focused on advising companies on understanding their data protection activities against malicious parties not just for external threats but also compliance instigated.

Thomas is also an active participant in the InfoSec community not only as a member but also as director of Security BSides London, ISSA UK chapter board member and speaker at events like SANS DFIR EMEA, DeepSec, Shmoocon, and various BSides events.

11:00 – 11:45 Matt Lorentzen, Principal Security Consultant, Trustwave: Sheepl – Automating People for Red and Blue Team Tradecraft

While there is a wealth of information out there about how to build environments that can be used for training, offensive tradecraft development and blue team response detection, a vital part of these environments is hard to emulate. A computer network is more than a collection of connected computer resources, it is a platform for communications and productivity between people. So the focus becomes how do you properly emulate people within a network environment? In this presentation Matt will share his research into developing more realistic user behaviour and how it can be used to improve red team and blue team tradecraft. Windows based lab environments are vital in developing a cohesive team strategy and exploring new attack vectors, but static environments don't offer the opportunities to experience 'real world' stimulus and therefore diminish learning objectives. Matt's wanted to look at how he could replicate more natural end user behaviour in a portable, but less predictable way.

His solution to this challenge is a new open source tool called 'Sheepl' that can be used to emulate the tasks that people could perform within a network whilst addressing some of the shortfalls of traditional script-based approaches to emulating user behaviour. Matt will demonstrate how the tool allows the creation of 'Sheepl' who execute tasks over a defined period of time.

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 for 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. Matt has spoken at CRESTCon Asia, 44Con London and presented at various university and IT events.

>>

UPDATES:

Nancy Strutt

Kimberly Bucholz

11:50 – 12.35 Nancy Strutt & Kimberly Bucholz, Accenture: VBA and Macro-Document Analysis & Case Studies

This presentation looks at the VBA code and obfuscation techniques used by APT groups (i.e. APT32) and other groups/actors (i.e. FIN7). This presentation will discuss analysis techniques and tools and demonstrate their use on specific samples. This presentation will show how to perform analysis on malicious macro-based documents and follow-on payloads, such as powershell scripts, through common analysis tools such as Microsoft Word VBA Debugger, Didier Steven's oledump.py, Process Explorer, Python, and more. Applicable examples will be shown from various APT actors, as well as other groups.

Kim is a member of the Cyber Espionage team. She has more than 11 years of experience in IT, including a Bachelor of Science degree in Computer Science and Master of Science in Information Security. Since 2011, she has been focused on incident response and malware analysis. This focus has included crimeware, as well as targeted threats. Her main areas of interest are in reverse engineering malware, and using the information obtained to pivot and find unknown threats.

Nancy joined iDefense in 2011 as a malware analyst whose focus was primarily web-based malware. Currently she works for the Malware Analysis and Countermeasures team, where she looks at and dissects many different types of malware. Her specialities in malware analysis have included exploit kits, ransomware, wipers, and information stealers. Prior to iDefense, she analysed spyware as a research engineer for PestPatrol, CA, and HCL. Before 2004, Nancy had an extensive career as a software engineer. Nancy holds a B.S. degree in Computer Science and a M.S. in Information Systems and Telecommunications Management as well as several humanities degrees. Her other research interests include digital forensics and finding common code bases between malware.

13:30 – 14:00 Oliver Church, CEO of Orpheus & Chair of CTIPs: Introducing the CREST Threat Intelligence Practitioners group – what are we doing and why?

In order to contribute to the further development of the cyber threat intelligence specialism, CREST has established the CREST Threat Intelligence Professionals group (CTIPs). CTIPS represents cyber threat intelligence companies and professionals globally, and some of the work being undertaken by CTIPs includes accreditation of leading cyber threat intelligence companies, developing certifications for individuals and acting as a lightning rod for communication. Oliver Church, current Chair of CTIPS, will provide an overview of CTIPs, what we are doing and why.

Oliver is CEO of Orpheus, a specialist cyber security company. Oliver is a passionate believer in the importance of intelligence-led security, and has previously established successful cyber security teams and capabilities at major global companies. He has a wide portfolio of risk management and security experience, developed working for a diverse range of large and small organisations over the last 17 years. Oliver is an elected member of the Executive Committee for CREST, and has led the establishment of the CREST Threat Intelligence Professionals (CTIPs) group with the purpose of developing the Cyber Threat Intelligence sector worldwide. Oliver is also a CREST Certified Cyber Threat Intelligence Manager (CCTIM), and an Assessor of the CCTIM exam. An expert in cyber risk management and cyber resilience testing, Oliver has been involved in developing intelligence-led cyber resilience testing frameworks such as CBEST, and has extensive experience leading teams to conduct the testing itself.

>>

UPDATES:

14:05 – 14:35 Paula Hancock, Senior Intelligence Lead, Cyber Tech and Threats, BT Cyber Threat Intelligence: Out of the trough of disillusionment and up the slope of enlightenment

Threat intelligence has become one of the recent buzzwords of the last 5 years. It became a "must have" for businesses to protect against cyberattacks. Organisations rushed to fill their intelligence gaps with "threat intelligence feeds" which in reality are little more than lists of indicators which quickly become outdated and useless, as criminals quickly adapt to security defences. Organisations then question the effectiveness of the threat intelligence that they have invested in, and after all the hype and peak of inflated expectations, the inevitable disappointment in the quality of service follows.

The market is currently awash with vendors claiming to provide a holistic approach to threat intelligence, but in reality there is simply no one-stop shop solution. Organisations find it difficult to navigate the minefield of threat intelligence providers, where the range of content and expertise means it is virtually impossible to compare services and match them against their needs, which in themselves are likely to be poorly understood.

"Threat intelligence" as a term is also widely misused and misunderstood. What vendors claim to provide may not necessarily align with an organisation's expectation or interpretation of threat intelligence. So how does an organisation fully leverage the capabilities of threat intelligence? And how does threat intelligence as a discipline, climb out of this trough of disillusionment and up the slope of enlightenment?

Paula is a Senior Security Specialist within BT Security's Threat Intelligence and Investigations team. She leads a team of Cyber Intelligence Analysts to proactively protect BT and its customers from the myriad of cyber threats faced by global organisations every day. With over 14 years' experience in operational intelligence environments, Paula has seen first-hand how proactive intelligence is crucial in mitigating and preventing threats, allowing organisations to focus on their core business. Having joined BT from Hampshire Constabulary in 2010, Paula has worked in a variety of intelligence areas including physical security, fraud and now cybercrime. With experience as an intelligence analyst in law enforcement, Paula has brought a wealth of knowledge on the various methodologies and processes to help BT successfully adopt a new approach to intelligence-led security. Paula has a BA (hons) degree in Geography and an MSc in Social Research Methods, is a qualified Intelligence Analyst and currently she is working towards the CREST Threat Intelligence Manager accreditation.

14:40 – 15:10 Louise Taggart, Manager, & Keith Short, Senior Analyst, PwC: A Quartermaster for Compromise

PwC Cyber Threat Operations staff will present on an ongoing series of campaigns conducted by multiple threat actors using a common document builder. We examine some of the more interesting lures, and cover overlaps between documents and groups. We will also examine the targeting from a strategic point of view and suggest some potential geo-political reasons for the threat actor's interest.

Louise is a manager in PwC UK's Threat Intelligence team, responsible for tracking political and defence/security developments and analysing their implications for cyber security, with a particular focus on the Former Soviet Union region. Before joining PwC, Louise worked as head of the intelligence department at a political risk and security consultancy firm. She holds an MA (Hons) in Russian, an MSt (Oxon) in Slavonic Studies and an MA in Politics, Security and Integration.

Keith is a technical analyst on PwC's Cyber Threat Intelligence team based in London, UK. Specialising in malware analysis, Keith has also previously delivered a talk on how to track Threat Actors at the BSides London rookie track in 2018, which focussed on the activities of a threat actor commonly known as Dark Caracal. He has worked at PwC following his graduation from a Computer & Information Security course at Plymouth University in 2016.

UPDATES:

15:45 – 16:30 Lesley Kipling, Lead Investigator & Chief Cybersecurity Advisor, Microsoft: What is the first thing you do when you are faced with a security incident? Do you have a plan?

What is the first thing you do when you are faced with a security incident? Do you have a plan? Join Microsoft Lead Investigator and Chief Cyber Security Advisor Lesley Kipling to find out what the first thing the Microsoft response team does when they get to site. This session will showcase some of the common attacks against Azure through a demonstration of Azure Security Center, discuss changes Microsoft are seeing in the incident response world and how to protect, detect and respond to those attacks. Objectives are to: Gain an understanding of common attacks against cloud workloads; Learn how to leverage Microsoft built-in cloud services to detect, investigate and contain attacks; Understand how to harden cloud environments to be resilient to common attacks.

Previously the lead investigator for Microsoft's detection and response team (DaRT), Lesley has spent more than 16 years responding to our customers' largest and most impactful cybersecurity incidents. As Chief Cybersecurity Advisor, she now provides customers, partners and agencies around the globe with deep insights into how and why security incidents happen, how to harden defences and more importantly, how to automate response and contain attacks with the power of the cloud and machine learning. She holds a Master of Science in Forensic Computing from Cranfield University in the United Kingdom.

16:35 – 17:05 Nick Hayes, Global Head of Technical Direction, BSI: Safely Assessing Operational Technology (OT) Environments

The Operation Technology (OT) security landscape is traditionally one which has been significantly lagging behind that of the IT world. With a huge emphasis on safety and availability over confidentiality and integrity, a need for further divergence and an elevated threat profile from nation states it is imperative that OT environments are adequately assessed from a security point of view. Many of those same OT environments however, are not safe to perform fully offensive testing against. In this talk, Nick will explore the different methods BSI have employed in recent times to assess SCADA/ OT networks whilst maintaining operational safety and availability. This includes the development of a bespoke risk assessment methodology and framework providing a holistic view, targeted testing within test/development environments and a full penetration test of a production gas network.

Nick is an experienced and well-rounded security consultant with 7 years of industry experience and over 750 delivery days completed to-date. Working for two of the largest security consultancies before BSI, Nick gained valuable experience and skills working across a large number of industries, being exposed to a wide variety of technologies and assessment types and leading teams of all sizes. In a previous life, Nick was also a SCADA design engineer before moving into the security world. Nick is currently the Global Head of Technical Direction at BSI with the remit of ensuring that BSI are at the forefront of the industry and delivering high quality consultancy.

>>

UPDATES:

Samantha Alexander

Andrew Juston

Training stream – Lineker Room

Stream hosts: Samantha Alexander and Andrew Juston

09:55 – 10:25 Costas Senekkis, Senior Security Analyst, ICSI: Mandatory Access Control Essentials with SELinux

It is very important for technical people to understand the importance of Mandatory Access Control and why it should be enforced in an organisation. Standard permissions are not enough to protect a system thus by using more sophisticated rules in a case of compromise, mandatory access control (enforced by using SELinux) will protect user data from the compromised service.

Costas is an experienced pen tester and security consultant and has delivered several penetration tests across several countries. He leads the Penetration Testing team at ICSI LTD UK and is passionate about Linux Security. He has also delivered penetration testing courses across the globe.

Costas is now working with companies to help management to understand the technical issues that will arise if their employees (technical and non-technical) do not have have not a security awareness consciousness.

11:00 – 11:30 Tom Huckle, Head of Cyber Training and Development, Crucial Academy: An overview of CREST Registered Threat Analyst Training

Tom is the Head of Cyber Training & Consultancy at Crucial Academy and a specialist in defensive security, threat intelligence and information assurance. Tom is a former Royal Marines officer and Mountain Leader. He joined Crucial Academy from Barclays SOC Cyber Operations Team and is responsible for the strategic direction and delivery of Crucial Academy’s training and consultancy capability.

11:35 – 12:05 Tony Reeves, Director of Level 7 Expertise Ltd and QA Partner: Hacking Drones… Or not?

Hacking Drones….or not” is presented by Tony Reeves, the Level 7 Expertise Ltd principal consultant for drones and Unmanned Aerial Systems (UAS). Tony is an air defence and electronic warfare expert and has worked on a variety of military drone projects from mini UAS through to ScanEagle in the maritime domain, and up to large UAS such as the MQ-9 Reaper. More recently Tony has been involved in vulnerability analyses and the provision of counter-drone workshops to Government and Industry clients. The presentation will address the following areas:

- A typical airborne drone system architecture
- Areas in which drones might be vulnerable
- Countering Drones – Deter, Detection, Defeat and Response
- Where next? Cyber and drones – drones delivering cyber effect?

Tony’s company is soon to undergo accreditation for CAA Permission for Commercial Operations, which will include such as operations as the use of drones for disruptive experiments and assessments, and ethical penetration testing.

>>

UPDATES:

Tony is an experienced Unmanned Aerial Systems (UAS or "drone") and cyber security principal consultant, with over 23 years in the Royal Air Force and 9 years in Industry. Tony has worked for SMEs and large international Defence Primes, but for the past two years has been a director and co-owner of Level 7 Expertise Ltd, a small business based in Northamptonshire. Tony has worked on or with most of the UK MOD's current and recent portfolio of UAS, and also has experience in a number of international programmes. He has experience of enterprise audit and insider threat programmes, and comes from a strong military intelligence background. More recently, he has been involved in Cyber Vulnerability Investigations across a number of platforms and capabilities, and through his chairmanship of a number of high-profile Counter-Drone conferences is recognised as a leading proponent in his field. As part of Level 7's Corporate Social responsibility activity. He has started an education programme for business owners and local government, seeking to improve their cyber security and business resilience.

12:05 – 12:35 Miguel Rego, CEO of iHackLabs: Cyber Training 4.0: How to face dynamic environments training

Miguel Rego will outline some of the guiding principles of the iHackLabs ground-breaking approach to cybersecurity education and its cyber-range, which covers the whole spectrum of training platforms and simulation solutions. He will explain the dilemmas that companies face with the lack of professionals in the sector and how iHackLabs helps the public and private sector with its solutions.

Miguel is CEO of iHackLabs, a cybersecurity training company, specialising in cyber-range platforms for training, drills and performance evaluation. From 2013 to October 2016 he was General Director of the Institute National Cybersecurity Agency (INCIBE), a centre designated by the Government of Spain to provide cybersecurity services to citizens, businesses and critical infrastructure operators, and for the development of cybersecurity talent and entrepreneurship. Miguel collaborates with the Organization of American States as an international expert, having participated in the definition of the national cybersecurity strategies in Peru, Paraguay and the Dominican Republic. In Spain, Miguel contributed to the definition of the National Cybersecurity Plan and the derived plans. He is currently a professor at the War College of Colombia, within the Cybersecurity and Cyber Defense Master's Degree, and the Business School IE, in its Master of Cybersecurity. Miguel has been Cyber Security Leader at EY, Director of Technological Risks at Deloitte, Director of Security and Corporate Risks at ONO company, and held several positions related to cybersecurity in the Ministry of Defense of Spain. Miguel is Lieutenant Colonel of the Spanish Navy and has different postgraduate courses and certifications related to the governance and management of ICTs and cybersecurity.

13:30 – 14:00 Max Vetter, Chief Cyber Officer, Immersive Labs: Criminal Innovation and Cyber Threat Intelligence

Immersive Labs has partnered with digital shadows to bring practical labs on the latest cyber threat intelligence. When the latest threat intelligence is received, we work with Digital Shadows to produce lab exercises that give users hands on experience of the malware, threat or exploit just released.

In this training we will go through a few stages of the cyber threat intelligence cycle; from the intelligence collection on the darknet to seeing the malware activate on a live system, how to detect and mitigating it.

Before joining Immersive Labs, Max spent seven years in London with the Metropolitan Police Service. He worked as a police officer, intelligence analyst and covert internet investigator, while also spending time in Scotland Yard's money laundering unit. Max spent seven years with the Commercial Crime Services and Federation Against Copyright Theft too, investigating commercial crime, fraud and serious organised crime groups. Most recently, Max trained the private sector and government agencies in ethical hacking and open source intelligence, specialising in darknets and cryptocurrencies. This included three years teaching the GCHQ Cyber Summer School.

>>

UPDATES:

14:05 – 14:35 Martin Jordan, Austerbury: Iranian cyber threat briefing

Austerbury will deliver a briefing on Iran's Cyber capabilities, likely targets and modus operandi. They will also discuss the broader state of Cyber Resilience across the Middle East.

Martin has been in IT for over 30 years, having worked at Oracle, Defcom Information Security and KPMG were headed up the ethical hacking team for ten years. Martin now runs his own company, Austerbury, focusing cyber intelligence training and bespoke cyber assessments. Martin spends his spare time buying and restoring Land Rover Defenders, his latest project is a 94' TDi 300.

14:40 – 15:10 Mark Hutchings, QA: The challenge of cloud security and penetration testing

This presentation takes a look at some of the challenges facing those wishing to perform penetration tests of cloud based applications and functions, whether it's something simple like understanding the naming conventions used by cloud providers, or something more complicated like understanding the different constraints enforced by different providers, a gap in your, or your teams knowledge and skills may exist. Are penetration testing qualifications keeping pace with these requirements?

Mark joined QA after a 23 year career in the Royal Air Force (RAF), Mark started his career as a Telecommunications Technician progressing through the ranks. In 2007 Mark was commissioned as an Officer and after completing Initial Officer Training and Engineer Officer Training went on to Command the Command and Control, Computer, Communications and Intelligence Flight at RAF Honnington. Mark then worked as a Service Manager in the Logistics Information Technology System Project Team. Following these tours Mark completed a Master's Degree in Computing and Information Network Systems before seeing out the rest of his service career teaching at the Defence School of Communications and Information Systems as lead instructor in the Information Systems department of Engineer Officer Training. Mark is a Network and Telecommunications specialist (including mobile, cryptography and Radio Frequency Networks), also has UNIX and Windows administration experience, has coded and published iPhone applications, has spent the last few years teaching digital footprint and Open Source Intelligence

15:45 – 16:30 Ask the Assessors Panel: A specially assembled panel of experienced assessors will be answering questions on CREST examinations.

>>

UPDATES:

Breaks and Networking sessions

08:30 – 09:00 Registration, coffee and pastries (exhibition halls)

10:25 – 11:00 Coffee & networking (exhibition halls) -

Sponsored by AON

12:35 – 13:30 Lunch (exhibition halls)

Sponsored by AON

15:10 – 15:45 Coffee & networking (exhibition halls) -

Sponsored by AON

17:15 – 18:15 Sponsors and VIP guest networking drinks –

Sponsored by PEN TEST PARTNERS

18:00 – 22:00 Networking drinks and canapés -

Sponsored by AON

A big thank you to our sponsors

CREST would like to take the opportunity to thank all our Sponsors this year for supporting at CRESTCon. Without the input of our Sponsors CREST would not be able to put such a great event together for the industry to attend.

The sponsors can be found spanning out over two halls at the venue, please make sure that you take the time to visit them at their stands, you can also get your card stamp and the chance to win a experience voucher!

Platinum

AON
Empower Results®

Gold

ixia
A Keysight Business

Silver

pwc

REDSCAN™

Bronze

NETTITUDE
A member of the Lloyd's Register group

CheckSec

OBRELA
SECURITY INDUSTRIES

VERSPRITE

TITANIA

Training Providers

AUSTERBURY

ICSI

IMMERSIVELABS

QA

CRUCIAL

PGI

iHackLabs

Academia

ROYAL HOLLOWAY UNIVERSITY OF LONDON

CYBSAFE

Demonstrations

NETTITUDE
A member of the Lloyd's Register group

Try Hack Me

Student Room Sponsor

context

>>

UPDATES:

Student Networking Drinks Sponsor

PEN TEST PARTNERS

Evening Drinks, Lunch and Coffee Breaks

AON
Empower Results®

Incident Response and Threat Intelligence Stream

SECURITYALLIANCE

Community

44CON

PTSD Resolution
Forces' Veterans Mental Health

TECHVETS

Bob's Business
Cyber Security Awareness Training

CERIS
INFORMED ETHICAL PROFESSIONAL

ISSA UK

A focus on our students demo area

This year, CRESTCon boasts a dedicated student demonstration room, sponsored by Context Information Security. Students from Bournemouth University, Cardiff Metropolitan University, Keele University, National College of Ireland, University of East London, University of Greenwich and University of the West of England will be showcasing pieces of their research to interested delegates. Stop in to see the talent of the future.

Also, in the main demonstration room two students from University of Portsmouth will be promoting TryHackMe – an online platform they developed that runs capture the flag events along with cyber security workshops, training and online courses, to teach cyber security in an enjoyable and interactive way. The hope is that it will be used by universities and companies globally, to attract and train more people for careers in cyber-security.

The CREST Gulf region focused event

This event is being held with the support of the Department of International Trade to showcase the UK's technical cyber security services industry and takes place on 14th March 2019, running alongside CRESTCon. The intention is to demonstrate the UK's ability to support the development of a country's eco system to increase capacity, capability and consistency in cyber security. There are still a few places available and people who are involved with the region and would like to attend can find out more and register here: **https://crestgccevent.eventbrite.co.uk**

>>

BUILDING
CONFIDENCE
in a WORLD of
UNCERTAINTY

Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG
CREST is a not for profit company registered in the UK, CREST (Int) company number 09805375