11-12 JUNE, 2018

Glasgow, Scotland, UNITED KINGDOM

IEEE
Advancing Technology for Humanity

2018

Cyber Science 2018 Conference Programme

Cyber Situation Awareness as a Tool for Analysis & Insight

C-MRiC.ORG®

Pioneering Research & Innovation in Cyber Situational Awareness

#Cyberscience @cmricorg

www.c-mric.org

C-MRiC.ORG

6/11/2018

Sponsors


IEEE
Advancing Technology for Humanity


GRAYFIELD
SOLICITORS


C-MRiC.ORG


e:(security group)
Information and Security Assurance


UNIVERSITY OF
OXFORD


CYBER
SECURITY
CENTRE


IEEE
computer
society


secudit
the risk analyzer


PRIVACYAZURE
The Privacy Impact Assessment Organisation


UNIVERSITY OF
OXFORD
DEPARTMENT OF
COMPUTER
SCIENCE


research series
...founded on research


IEEE
United Kingdom and Ireland Section


Abertay
University


aceObjects


LET GLASGOW FLOURISH

Contents

Conference Venue

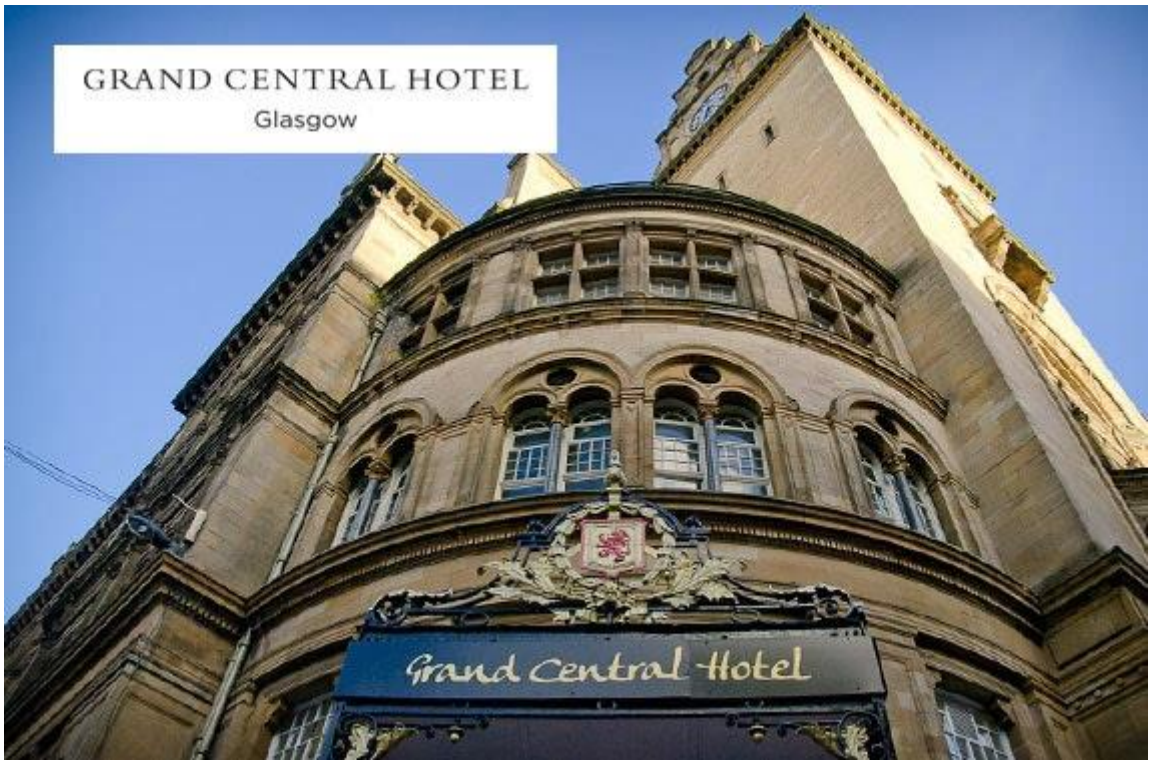
Hotel Information / Address

The Grand Central Hotel, Glasgow, (a.k.a. Principal) **99 Gordon Street, Glasgow, G1 3SF, Scotland**, United Kingdom

Central Reservations: Telephone: +44 (0)141 2403700
Web: https://www.phcompany.com/principal/glasgow-grand-central-hotel/

Grand Central Hotel, Glasgow is an iconic event venue in Central Glasgow, a 4-start landmark hotel adjoining Glasgow Central Station.

The Principal Grand Central Hotel, Glasgow was originally built in the late 19th-century as a great British railway hotel. One of the city's most prestigious buildings, the hotel has welcomed many famous guests including Frank Sinatra and Winston Churchill, throughout the years. Today, this iconic hotel is still a very much loved landmark in Glasgow's skyline, sat within the hub of the Style Mile and at the centre of the city's many attractions. At the restaurant, Tempus Restaurant & Bar, discover seasonal locally sourced food and drink that showcases the very best of Scottish cuisine and culture. The recently refurbished bar, Champagne Central, overlooks Central Station and evokes the golden age of travel, while Deli Central offers quick food on the go with a special focus on local favourites.



Directions

By Car Post code is G1 3SF. It's 5 minutes by M8. Use the following navigation coordinates 55.8604° N, 4.2585° W	**By Air** Glasgow International Airport is 7 miles away.
By Train Next to Glasgow Central Station.	

Figure 1: Regent Suite for Social Events

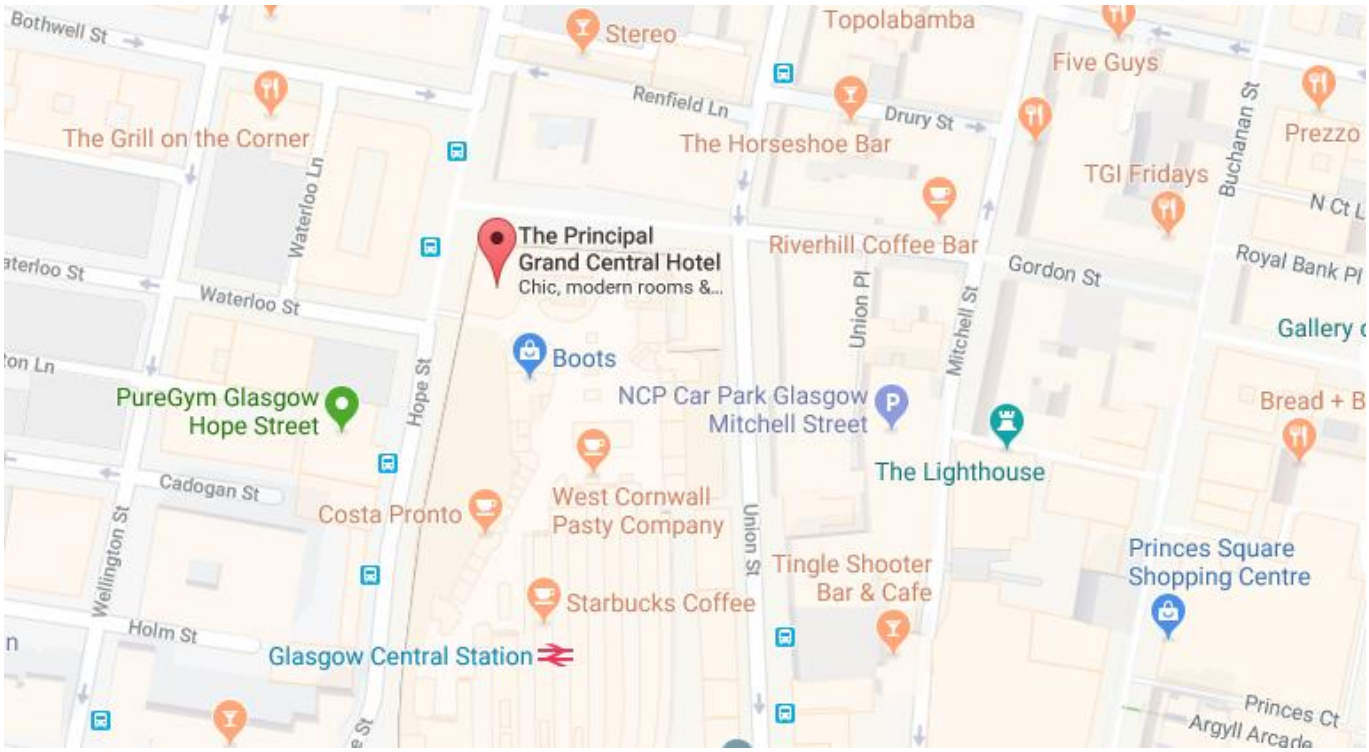


Figure 2: Map to the Conference Venue - Showing Glasgow Central Rail Station

Keynote Speakers

Mr Michael Matheson MSP – Cabinet Secretary for Justice, Member of the Scottish Parliament

Mr Michael Matheson MSP

Michael Matheson MSP is the Cabinet Secretary for Justice, and a Member of the Scottish Parliament. He studied at Queen Margaret College, Edinburgh where he obtained a BSc in Occupational Therapy. He also holds a BA and a Diploma in Applied Social Sciences from the Open University.

Prior to becoming an MSP Michael practised as a Community Occupational Therapist with Stirling Council, Central Regional Council, and Highland Regional Council. He was elected as the MSP for Falkirk West following the May 2007 elections. Before that he was a Regional MSP for Central Scotland from 1999-2007. Before being appointed Cabinet Secretary for Justice he was the Minister for Public Health. Michael was Vice Convenor of the European and External Relations Committee. He also sat on the Scottish Parliament's Health and Sport Committee, and previously served on the Justice and Enterprise and Culture Committees. He was re-elected at the May 5, 2011 election, and thereafter appointed Minister for Public Health.

Professor Sadie Creese – Professor of Cyber Security, Department of Computer Science, University of Oxford, UK

Professor Sadie Creese

Sadie Creese is a Professor of Cyber Security in the Department of Computer Science at the University of Oxford. She teaches threat detection, risk assessment and operational aspects of security. Her current research portfolio includes threat modelling and detection, visual analytics for cybersecurity, risk propagation logics and communication, resilience strategies, privacy, vulnerability of distributed ledgers, and understanding cyber-harm. She is Principal Investigator on the AXIS Insurance Company sponsored project "*Analysing Cyber Value-at-Risk*" focused on developing a method for predicting potential harms arising from cyber-attacks. She is a co-Investigator on the PETRAS EPSRC sponsored Internet of Things Research Hub project "*Cyber Risk Assessment for Coupled Systems"* which is developing a new risk assessment method aimed at helping organisations prepare for the threats and vulnerabilities we will face as the Internet of Things evolves. She was the founding Director of the Global Cyber Security Capacity Centre (GCSCC) at the

Oxford Martin School where she continues to serve as a Director conducting research into what constitutes national cybersecurity capacity, working with countries and international organisations around the world. She was the founding Director of Oxford's Cybersecurity network launched in 2008 and now called CyberSecurity@Oxford, and is a member of the World Economic Forum's Global Council on Cyber Security. Sadie is a Fellow of Worcester College, Oxford.

Dr. Cyril Onwubiko – Cyber Security Intelligence, Research Series Limited, London, UK

Dr Cyril Onwubiko

Dr Cyril Onwubiko is the Secretary – IEEE UK & Ireland, and Director, Cyber Security and Intelligence at Research Series Limited, where he is responsible for directing strategy, IA governance and cyber security. Prior to Research Series, he had worked in the Financial Services, Telecommunication, Health, Government and Public services Sectors. He is experienced in Cyber Security, Security Information and Event Management, Data Fusion, Intrusion Detection Systems and Computer Network Security; and vastly knowledgeable in Information Assurance, Risk Assessment & Management. He holds a PhD in Computer Network Security from Kingston University, London, UK; MSc in Internet Engineering, from University of East London, London, UK, and BSc, first class honours, in Computer Science & Mathematics. He has authored several books including "**Security Framework for Attack Detection in Computer Networks" and "Concepts in Numerical Methods**.", and edited books such as "**Situational Awareness in Computer Network Defense: Principles, Methods & Applications**", and Cyber Science 2015 – International Conference on Cyber Situational Awareness, Data Analytics and Assessment. He has over 30 articles published in leading and most prestigious academic journals and conferences.

Eamonn Kane – Detective Inspector, Cybercrime Unit, Specialist Crime Division SCD, Police Scotland, UK

DI Eamonn Kane

Detective Inspector **Eamonn Keane** has worked with the Irish and Scottish Police for 33 years principally in the investigation of terrorism, serious crime, criminal investigation, public protection and most recently digital crime and forensic delivery.

His current portfolio is with the Cybercrime, Police Scotland, investigating all aspects of serious and organised crime across Scotland with particular emphasis on technology facilitated crime to include malware proliferation, cybercrime, acquisitive crime, child sexual exploitation, drug supply, and social network abuse**.**

Eamonn also works extensively with the Scottish Business Resilience Centre championing the ethos of prevention through preparation and intelligence sharing for the Scottish and UK business community.

Professor Karen Renaud – Professor of Cyber Security, University of Abertay, Scotland, UK

Professor Karen Renaud

Karen is a professor of Cyber Security at the University of Abertay, and Professor Extraordinarius, University of South Africa. She is a recipient of various awards including the Fulbright Cyber Security Scholarship.

Her research focuses on human-centred security, a branch of Human Computer Interaction (HCI). She is interested in the interplay between users and security in the context of societal and industrial use. She wants to work towards creating a natural easy yet secure interaction between humans and devices. Her work has a strong development, experimental and deployment focus, testing solutions in practical situations. She has come up with several novel solutions to improve usability in a wide range of situations; and has also done fundamental work in understanding people's mental models of security in a variety of applications and contexts.

She has a wide range of other interests, including electronic voting, accessible technology, mobile phone design for elderly users, knowledge visualisation and the use of email in organisations.

Professor Jens Myrup Pedersen – Aalborg University, Denmark

Professor Jens Myrup Pedersen

Jens Myrup Pedersen is Associate Professor at Aalborg University, Denmark. After finishing his M.Sc. in Mathematics and Computer science he did his PhD in the field of network planning, and through close collaboration with Danish ISPs the work developed into focusing on cyber security. Today his research is focusing mainly on security from a network point of view, and includes network-based detection of malicious activity using e.g. machine learning and DNS traffic analysis - still carried out in close collaboration with industrial partners. Together with his students he has been exploring the security weaknesses of a number of embedded and IoT devices, including demonstration of poor security in state-of-the art Industry 4.0 production lines. He is an active player in the development of cyber security educations in Denmark, and is currently leading the work of establishing a Danish National Training Platform. He has a strong interest in internationalisation of education and promotion of collaboration between students across countries and disciplines - an interest that has led to coordination of two Erasmus+ Strategic Partnerships. In addition to his employment at Aalborg University he works as external lecturer at Riga Technical University, Latvia, he is board member in companies related to energy and infrastructure, and he also sits on the board of the Society of Telecommunications within the Danish Society of Engineers.

Stu Hirst – Head of Security Operations (SecOps), UK Cyber, Capital One

Mr Stu Hirst

Stu is currently the Head of Security Operations & Infrastructure at leading UK credit card company Capital One.

He was instrumental in building Skyscanner's Security team from 2015-2017, having led them to the final of SC Magazine's Security Team of The Year 2017.

He has twice been nominated as a finalist for Cyber Evangelist of The Year at the Scottish Cyber Awards and runs one of Scotland's leading Tech Meet Ups; Security Scotland.

Stu has appeared at numerous leading Security events such as InfoSec Europe, Cloud Expo Europe and Future of Cyber Security.

Conference Chairs

Dr. Natalie Coull – Head of Division, Cyber Security, University of Abertay, Scotland, UK

Dr Natalie Coull

Dr Natalie Coull is the Head of Division, Cyber Security at the University of Abertay. She lectures Ethical Hacking in Abertay's School of Arts, Media & Computer Games and, in 2016, was honoured for her contribution to cyber security – winning the Outstanding Woman in Cyber prize at the inaugural Scottish Cyber Awards. Natalie has been a lecturer at Abertay since 2007 and is the Programme Leader for the MSc Ethical Hacking and BSc Digital Forensics. She is involved in several initiatives to increase the number of women studying computing. In her role as a STEM ambassador, she regularly visits schools to conduct workshops. Her research interests relate to the broad area of cyber security and cover issues such as utilising anti-patterns to embed security in the software development lifecycle and utilising steganographic techniques to address piracy.

Dr. Xavier Bellekens – Lecturer, University of Abertay, Scotland, UK

Dr Xavier Bellekens

Dr Xavier Bellekens is a Lecturer in the Division of Cyber-Security at the University of Abertay in Dundee, he is also the head of the Machine Learning Research Group. His current research interests include pervasive security and privacy for IoT devices in the context of eHealth as well as Machine Learning Techniques for Cyber-Security and Engineering, including automated malware forensics and related areas. Prior to joining the University of Abertay, Xavier was a Research Assistant and Associate in the Centre for Intelligent Dynamic Communications at the University of Strathclyde, Glasgow, working on cyber-physical security for critical infrastructures. He is also a reviewer for world leading academic conferences and journals.

Dr Arnau Erola – Research Fellow, Computer Science Department, University of Oxford, UK

Dr Arnau Erola

Dr Arnau Erola is a cyber security expert with strong background in data analytics, machine learning, data mining and information privacy. He is currently a Research Fellow at Cyber Security Oxford at the University of Oxford, working on enterprise security, defence systems and better understanding the cyber-threat landscape. Within his portfolio, Arnau has engaged with several UK authorities, determining their needs and providing state of the art innovative solutions. Dr Erola holds a Ph. D., M. Sc. and B.Sc. in Computer Science from the Rovira i Virgili University of Tarragona (URV). He is author of several international journal articles on online privacy, anonymity protocols and intrusion detection mechanisms.

Dr Lynsay Shepherd – Lecturer in Cyber Security, University of Abertay, Scotland, UK

Dr Lynsay Shepherd

Dr Lynsay A. Shepherd is a lecturer in Usable Security and works within the Division of Cyber Security, in the School of Design and Informatics. Lynsay studied at Abertay University, Dundee, and holds a PhD in Usable Security, an MSc in Internet Computing, and a BSc (Hons) in Computing. She is a member of the Security Research Group (SRG) within the school, and has joined the Human-Centred Security Research Group.

Her current research interests include: usable security, human-computer interaction, the human factors of cyber security, security awareness, affective feedback, and open-source intelligence.

Accepted Papers, Authors, Affiliations & Abstracts

Cyber SA 2018 Accepted Papers

Patrik Lif, Teodor Sommestad and Dennis Granåsen

Division for C4IS, Swedish Defence Research Agency, Linköping, Sweden

Title: *Development and evaluation of information elements for simplified cyber-incident reports*

Abstract: In cyber security incident handling one of the most important tasks is to report what has occurred. Several frameworks have been developed to support this reporting, all with their own pros and cons. As a first step in the development of a practically useful incident description standard, we set to determine the appropriateness of sixteen plausible information elements relating to traceability and analysis. The information elements were evaluated during an exercise with 30 participants in which the participants were instructed to report cyber threats and incidents in their assigned networks. The evaluation assessed the extent to which the proposed information elements were used in the reports, if the sixteen information elements correlate with the quality of the incident reports, and the participants' subjective experiences of using the elements. The results show that the usage ratio of information elements varies a lot both between different reporters and between incidents. Further, the number of information elements used in a report correlated with the exercise management's quality assessments. Finally, the results reveal that although the overall assessment of content relevance of the simplified cyber-incident reporting template was positive, there is need for further validation of the template.

Kay Michel and Michael King

Florida Institute of Technology, Floria, USA

Title: *Towards an Adaptable System-based Classification Design for Cyber Identity*

Abstract: As cybercrime activity continues to increase with significant data growth and the Internet of Things (IoT's), this research introduces a new proactive methodically designed approach vs. current reactive and specialized methods. A novel holistic identity classification scheme and information architecture is proposed with an adaptive, common cybernetic trait design to support a changing technological landscape and human behavior. Common cyber identity base trait dimensions for context, physical, cyber, and humans allow for systematic analysis of temporal evidence to help resolve a physical person's identity in a cybercrime. This research platform supports both broad and targeted identity analytics using advanced machine learning methods in addition to mixed media visualizations to facilitate Cyber Situational Awareness (SA). Early PhD experimentation with real-world use cases shows promise with regards to providing attributes and patterns of cyber activity that is unique to a person.

Adam Zibak and Andrew Simpson

University of Oxford, Oxford, UK

Title: *Can We Evaluate the Impact of Cyber Security Information Sharing?*

Abstract: Once concentrated on protecting critical infrastructure, cyber security information sharing efforts have evolved in recent years to include many industries and have resulted in the current complex constellation of situational awareness sharing efforts on national, regional and international levels. They have also yielded a plethora of cyber threat intelligence sharing technologies. Yet, despite the proliferation of these efforts and technologies, the literature on the ability to measure the value and the impact of cyber security information sharing remains limited. We aim to address the lack of empirical studies by using a triangulated mixed-methods research design to explore stakeholder attitudes towards cyber security information sharing benefits and risks, and to investigate the impact of this sharing on the productivity and performance of cyber security analysts.

Wei Xu[1], Yaodong Tao[2] and Xin Guan[3]

[1]University of Science and Technology of China
[2]Chinese Academy of Sciences
[3]Shanghai Ocean University

Title: *The Landscape of ICS Devices on the Internet*

Abstract: Industrial control systems are employed in numerous critical infrastructure assets. Originally designed for closed systems, these protocols do not have built-in security. If these systems receive a cyberattack, it will cause serious damage to the physical world, however, there are still many ICS devices connected directly to the Internet. To study the number, distribution and trend of these systems, we analyzed the Censys scanning data for the 5 protocols of Modbus, Siemens S7, DNP3, BACnet, Tridium Fox. We find that there are still many devices exposed on the Internet, distributed in more than 100 countries around the world, and the overall number of devices has been on the rise in the last two years. Separately, in the past two years, the number of Modbus and Siemens S7 protocol continued to grow rapidly, the number of DNP3 protocol devices has declined, and the number of BACnet and Tridium Fox protocol devices has basically remained unchanged. By analyzing the IP addresses of these devices, we find that some of the devices are continually exposed to the Internet, and some of the devices are temporarily exposed to the Internet. We also find some Conpot honeypot records in these data. We hope that our research will be able to promote the security of the industrial control system.

Yogachandran Rahulamathavan[1], Xuewen Yao[2], Rahulamathavan Sutharsini[3], Muttukrishnan Rajarajan[4] and Kanapathippillai Cumanan[5]

[1]Loughborough University, UK
[2]Georgia Institute of Technology, USA
[3]Techinspire LTD, UK
[4]City University, London, UK
[5]University of York, York, UK

Title: *Redesign of Gaussian Mixture Model for Efficient and Privacy-preserving Speaker Recognition*

Abstract: This paper proposes an algorithm to perform privacy-preserving (PP) speaker recognition using Gaussian mixture models (GMM). We consider a scenario where the users have to enrol their voice biometric with the third-party service providers to access different services (i.e., banking). Once the enrolment is done, the users can authenticate themselves to the system using their voice instead of passwords. Since the voice is unique for individuals, storing the users' voice features at the third-party server raises privacy concerns. Hence, in this paper we propose a novel technique using randomization to perform voice authentication, which allows users to enrol and authenticate their voice in the encrypted domain, hence privacy is preserved. To achieve this, we redesign the GMM to work on encrypted domain. The proposed algorithm is validated using the widely used TIMIT speech corpus. Experimental results demonstrate that the proposed PP algorithm does not degrade the performance compared to the non-PP method and achieve 96:16% true positive rate and 1:77% false positive rate. Demonstration on Android smartphone shows that the algorithm can be executed within two seconds with only 30% of CPU power.

Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh and Moosung Park

Agency for Defense Development, South Korea

Title: *Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture*

Abstract: Over a decade, intelligent and persistent forms of cyber threats have been damaging to the organizations' cyber assets and missions. In this paper, we analyze current cyber kill chain models that explain the adversarial behavior to perform advanced persistent threat (APT) attacks, and propose a cyber kill chain model that can be used in view of cyber situation awareness. Based on the proposed cyber kill chain model, we propose a threat taxonomy that classifies attack tactics and techniques for each attack phase using CAPEC, ATT&CK that classify the attack tactics, techniques, and procedures (TTPs) proposed by MITRE. We also implement a cyber common operational picture (CyCOP) to recognize the situation of cyberspace. The threat situation can be represented on the CyCOP by applying cyber kill chain-based threat taxonomy.

Zahid Maqbool[2], V.S. Chandrasekhar Pammi[1] and Varun Dutt[2]

[1]Centre of Behavioural and Cognitive Sciences, University of Allahabad, India
[2]Indian Institute of Technology Mandi, India

Title: *Cybersecurity: Influence of patching vulnerabilities on the decision-making of hackers and analysts*

Abstract: Patching of vulnerabilities on computer systems by analysts enables us to protect these systems from cyber-attacks. However, even after patching, the computer systems may still be vulnerable to cyber-attacks as the patching process may not be full proof. Currently, little is known about how hacker's attack actions would be influenced by the varying effectiveness of the patching process. The primary objective of this study was to investigate the influence of the patching process on the attack-and-defend decisions of hackers and analysts. In this study, we used a 2-player zero-sum stochastic Markov security game in a lab-based experiment involving participants performing as hackers and analysts. In the experiment, participants were randomly assigned to two between-subjects patching conditions: effective (N = 50) and less-effective (N = 50). In effective patching, the probability of the network to be in a non-vulnerable state was 90% after patching by the analyst; whereas, in less-effective patching, the probability of the network to be in the non-vulnerable state was 50% after patching by the

analyst. Results revealed that the proportion of attack and defend actions were similar between effective and less-effective conditions. Furthermore, although the proportion of defend actions were similar between vulnerable and non-vulnerable states, the proportion of attack actions were smaller in the non-vulnerable state compared to the vulnerable state. A majority of time, both players deviated significantly from their Nash equilibria in different conditions and states. We highlight the implications of our results for patching and attack actions in computer networks.

Arun Lakhotia[1,2], Vivek Notani[2] and Charles LeDoux[2]
[2]Cythereal Inc, USA
[1]University of Louisiana at Lafayette, USA

Title: *Malware Economics and its Implication to Anti-Malware Situational Awareness*

Abstract: Malware, like any other software, is developed iteratively, improved in incremental versions over a long period of time. Malware economics requires amortizing the cost of malware development over several attacks. Even though the classic indicators of attacks, such as, domain names, file names, IP addresses, etc., are parameterized and often changed over versions, the malware code itself is carried through versions, albeit transformed and obfuscated. Recent breakthrough in automated malware analysis and code debofuscation makes it possible to overcome the challenges imposed by obfuscated code and create new anti-malware tools that use the malware code itself as an immutable indicator in anti-malware defense. The resulting technologies can be used to provide situational awareness of the dynamic threat profile of an organization. Persistent adversaries intending to penetrate a particular organization send morphed variant of malicious content to a large number of people in an organization. Such attack campaigns may be executed over weeks or months. By correlating malware generated from the same code base, one can detect such persistent campaigns against an organization from the malware blocked by an anti-virus. Results from the field demonstrate that this approach has promise in detecting targeted attacks as the attacks are in progress, giving the defender's enough time to take preventing actions.

Shane Miller, Kevin Curran and Tom Lunney
Ulster University, Northern Ireland, UK

Title: *Multilayer Perceptron Neural Network for Detection of Encrypted VPN Network Traffic*

Abstract: There has been a growth in popularity of privacy in the personal computing space and this has influenced the IT industry. There is more demand for websites to use more secure and privacy focused technologies such as HTTPS and TLS. This has had a knock-on effect of increasing the popularity of Virtual Private Networks (VPNs). There are now more VPN offerings than ever before and some are exceptionally simple to setup. Unfortunately, this ease of use means that businesses will have a need to be able to classify whether an incoming connection to their network is from an original IP address or if it is being proxied through a VPN. A method to classify an incoming connection is to make use of machine learning to learn the general patterns of VPN and non-VPN traffic in order to build a model capable of distinguishing between the two in real time. This paper outlines a framework built on a multilayer perceptron neural network model capable of achieving this goal.

Nima Asadi[1], Aunshul Rege[2] and Zoran Obradovic[1]

[1]Computer and Information Sciences Department, Temple University, USA
[2]Department of Criminal Justice, Temple University, USA

Title: *Analysis of Adversarial Movement Through Characteristics of Graph Topological Ordering*

Abstract: Capturing the patterns in adversarial movement can provide valuable information regarding how the adversaries progress through cyberattacks. This information can be further employed for making comparisons and interpretations of decision making of the adversaries. In this study, we propose a framework based on concepts of social networks to characterize and compare the patterns, variations and shifts in the movements made by an adversarial team during a real-time cybersecurity exercise. We also explore the possibility of movement association with the skill sets using topological sort networks. This research provides preliminary insight on adversarial movement complexity and linearity and decision-making as cyberattacks unfold.

Hanan Hindi[1], Elike Hodo[2], Ethan Bayne[1], Amar Seeam[3], Robert Atkinson[2] and Xavier Bellekens[1]

[1]Abertay University, Scotland, UK
[2]University of Strathclyde, Scotland, UK
[3]Middlesex University, Mauritius

Title: *A Taxonomy of Malicious Traffic for Intrusion Detection Systems (Short Paper Ph.D. Track)*

Abstract: With the increasing number of network threats it is essential to have a knowledge of existing and new network threats to design better intrusion detection systems. In this paper we propose a taxonomy for classifying network attacks in a consistent way, allowing security researchers to focus their efforts on creating accurate intrusion detection systems and targeted datasets.

Yara Bayoumy[1], Per Håkon Meland[2] and Guttorm Sindre[1]

[1]Norwegian University of Science and Technology, Norway
[2]SINTEF Digital, Norway

Title: *A Netnographic Study on the Dark Net Ecosystem for Ransomware*

Abstract: For more than a decade, businesses and private citizens alike have been tormented by an online phenomenon that has changed our stance on cyber security. Ransomware, malicious software that demands payment in exchange for a stolen functionality, has grown beyond expectations. The development and distribution of ransomware is stimulated by social networks active in the Dark Net. From the cyber criminal perspective, this is an ideal platform to participate in a business ecosystem, either as an author, vendor or distributor of ransomware. Within the Dark Net, they can find forums and marketplaces that offer complete secrecy and concealment of the user's identity. Studying the activities taking place within the Dark Net sites can improve our situational awareness on upcoming threats and how we can defend against them. In this research, a netnographic study was done to obtain useful data such as observations of the marketplace economies and reflections on the social interactions between the different stakeholders involved in the creation and distribution of ransomware.

Zachary Hills, David Arppe, Amin Ibrahim and Khalil El-Khatib
University of Ontario Institute of Technology, Canada

Title: *Compound Password System for Mobile*

Abstract: Authentication on mobile devices deviates from the traditional text-based password system. The choice to use alternative password systems comes at a cost and in this paper, we explore the current issues with said systems and propose a new method for authentication on mobile devices. In this paper we explore the current landscape of mobile authentication. The mobile authentication systems, Personal Identification Number and Pattern passwords both have issues which makes them weak to attacks. Our goal is to create a scheme that can strengthen the security of mobile passwords by combining both methods of authentication. When a new security system is implemented there is two factors that determine the system's success, the complexity of the system and the usability or feasibility of the system. This paper looks to define the complexity of our scheme in terms of security.

Karen Renaud and Lynsay Shepherd
Abertay University, Scotland, UK

Title: *How to Make Privacy Policies both GDPR-Compliant and Usable*

Abstract: It is important for organisations to ensure that their privacy policies are General Data Protection Regulation (GDPR) compliant, and this must be done by the May 2018 deadline. However, it is also important for these policies to be designed with the needs of the human recipient in mind. We carried out an investigation to find out how best to achieve this. We commenced by synthesising the GDPR requirements into a checklist-type format. We then derived a list of usability design guidelines for privacy notifications from the research literature. We augmented the recommendations with other findings reported in the research literature, to confirm the guidelines. We conclude by providing a usable and GDPR-compliant privacy policy template for the benefit of policy writers.

Eliana Stavrou
University of Central Lancashire, Cyprus

Title: *Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools*

Abstract: Password cracking can enhance the cyber situational awareness of defenders, e.g. cyber security/IT professionals, with regards to the strength of text-based authentication mechanisms utilized in an organization. Auditing results can proactively indicate if weak passwords exist in an organization, decreasing the risks of compromisation. Password cracking is a typical and time-consuming way to perform password auditing. Given that defenders perform password auditing within a specific evaluation timeframe, the cracking process needs to be optimized to yield useful results. Existing password cracking tools do not provide holistic features to optimize the process. Therefore, the need arises to build new password auditing toolkits to assist defenders to achieve their task in an effective and efficient way. Moreover, to maximize the benefits of password auditing, a security policy should be utilized. Currently the efforts focus on the specification of password security policies, providing rules on how to construct passwords. This work proposes the functionality that should be supported by next-generation password auditing toolkits and provides guidelines to drive the specification of a relevant password auditing policy.

Christopher McDermott, Andrei Petrovski and Farzan Majdani

Robert Gordon University, UK

Title: *Towards Situational Awareness of Botnet Activity in the Internet of Things*

Abstract: An IoT botnet detection model is designed to detect anomalous attack traffic utilised by the mirai botnet malware. The model uses a novel application of Deep Bidirectional Long Short-Term Memory based Recurrent Neural Network (BLSTMRNN), in conjunction with Word Embedding, to convert string data found in captured packets, into a format usable by the BLSTM-RNN. In doing so, this paper presents a solution to the problem of detecting and making consumers situationally aware when their IoT devices are infected, and forms part of a botnet. The proposed model addresses the issue of detection, and returns high accuracy and low loss metrics for four attack vectors used by the mirai botnet malware, with only one attack vector shown to be difficult to detect and predict. A labelled dataset was generated and used for all experiments, to test and validate the accuracy and data loss in the detection model. This dataset is available upon request.

Andrea Cullen and Lorna Armitage

University of Bradford, UK

Title: *A Human Vulnerability Assessment Methodology*

Abstract: Organisations are struggling to keep pace with the threats posed to their information security by hackers and the growing sophistication of both technical and non-technical cyber-attacks. Many countermeasures have been discussed, developed and deployed, yet the human element remains the least understood and a significant weak link within the system. With this in mind, the social engineer uses a combination of tactics to exploit the vulnerabilities each individual has to gain access to systems and sensitive information. This paper demonstrates that not all individuals are susceptible to the same attack, but instead that each of us is likely to succumb to a different type of tactic. The focus here is therefore to understand these differences and to identify the attacker tactics likely to be the most successful in each case. Social engineering tactics are designed to attack specific vulnerabilities in individuals in much the same way as a technical attack is designed to target the vulnerabilities in specific technologies. The objective of this research is to combine personality preference and attackers' tactics to develop a vulnerability assessment methodology for the human within the system. In this way, we look to improve the effectiveness of training and awareness raising within this context.

Anthony Arrott[1], Arun Lakhotia[2], Ferenc Leitold[3] and Ledoux Charles[2]

[1]CheckVir
[2]Cythereal
[3]Veszprog

Title: *Cluster analysis for deobfuscation of malware variants during ransomware attacks*

Abstract: Risk managers attempting to reduce cybersecurity vulnerability in enterprise IT networks rely on the "malware detection rate" as a primary measure at each layer of protection (e.g., network firewalls, breach detection systems, secure mail-servers, endpoint security suites). However, to be directly usable in risk assessments, separate malware detection rates are required for different malware categories that are quantitatively related to specific impacts of infection. A three-tier hierarchy of malware classification is formulated to assist cyber-risk decision-making. Malware is first categorized by victim impact (e.g., adware, data exfiltration, ransomware); second by malware technique (e.g., malware families), and third by evasion and obfuscation variants within individual

malware families (e.g., polymorphs, metamorphs). The three-tier hierarchy is applied to a specific vertical: ransomware (impact); ransomware family (technique); and malware binary variants within one family, WannaCry (obfuscation and evasion).

Cyril Onwubiko
Cyber Security Intelligence, e-Security Group, Research Series Limited, London

Title: *CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process*

Abstract: A cybersecurity operations centre ontology for analysis (CoCoa) is proposed which aligns to the NIST cybersecurity framework. The proposed CoCoa is used to map the CSOC analysis processes, which in turn provides cyber security analysts situational awareness of the vital aspects of the CSOC. The process ontology offers a fundamental shift from log collection to the analysis of five overarching threat intelligence and information sources (namely – events and logs, network information, structured digital feed, semi and unstructured feed and threat intelligence), which should allow the CSOC to provide proactive monitoring, and detection of inflight, emerging and complexity threats that would not have ordinarily been detected through only events and logs. Further, and most importantly, the proposed ontology is then used to identify how cyber incidents can be realized and detected through ontology-based knowledge graph.

Social Media 2018 Accepted Papers

Jason Koepke and Siddarth Kaza

Towson University, USA

Title: *Information flow on Twitter surrounding regional events*

Abstract: The purpose of this study is to identify how valid information spreads across Twitter based on user activity levels surrounding regionalized events. The types of events analyzed include sporting events, natural disasters, political events and other types of events. We use a regionalized dataset captured from Twitter, social analysis techniques, and a concrete definition of an event to analyze communication patterns of users and their associated social networks. The anticipated outcome of this study is to confirm that users increased their activity levels on social media during the timeframe of an event which results in an increased spread of valid information amongst their peers.

Cyber Security 2018 Accepted Papers

Sean Mckeown, Gordon Russell and Petra Leimich

Edinburgh Napier University, Scotland, UK

Title: *Sub-file Hashing Strategies for Fast Contraband Detection*

Abstract: Traditional digital forensics processes do not scale well with the huge quantities of data present in a modern investigation, resulting in large investigative backlogs for many law enforcement agencies. Data reduction techniques are required for fast and effective digital forensics triage, and to reduce the time taken to conduct an investigation. This work explores the potential of sub-file cryptographic hashing strategies, where small fragments of files are hashed in lieu of processing the file in its entirety, for contraband detection. Results show that sub-file hashing techniques perform well, particularly on solid state media, while also retaining a high degree of discriminating power. Such strategies may offer an opportunity to take advantage of the performance characteristics of non-mechanical media, streamlining future investigations and greatly reducing investigation times.

Halldis Søhoel[1], Martin Gilje Jaatun[2] and Colin Boyd[3]

[1]BEKK Consulting, Norway
[2]SINTEF Digital, Norway
[3]NTNU, Norway

Title: *OWASP Top 10 - Do Startups Care?*

Abstract: In a cut-throat world where time-to-market can be the difference between success and failure, it can be tempting for startups to think ``let's get it to work first, and then we'll worry about security later." However, major security flaws have killed more than one startup. This paper studies a small sample of 5 IT startups that offer services via the web, to determine to what extent they are aware of and can handle the OWASP top 10 threats.

Ensar Seker and Hasan Huseyin Ozbenli

NATO CCD COE, Estonia

Title: *The Concept of Cyber Defence Exercises: Planning, Execution, Evaluation*

Abstract: This paper discusses the concept of cyber defence exercises (CDXs) that are very important tool when it comes to enhancing the safety awareness of cyberspace, testing an organization’s ability to put up resistance and respond to different cyber events to establish the secure environment, gathering empirical data related to security, and looking at the practical training of experts on this subject. The exercises can give ideas to the decision makers about the precautions in the cybersecurity area and to the officials, institutions, organizations, and staff who are responsible on the cyber tools, techniques, and procedures that can be developed for this field. In the cyber defense exercises, the scenarios that are simulated closest to reality which provides very important contributions by bringing together the necessity of making the best decisions and management capabilities under the cyber crisis by handling stress and coordinated movement as a team. The objective of this paper is to address the issue from a scientific point of view by setting out the stages of planning, implementation, and evaluation of these exercises, taking into account and comparing international firefighting exercises. Another aim of the work is to be able to

reveal the necessary processes that are required for all kind of cyber exercises, regardless of the type, although the processes involved vary according to the target mass of the planned exercise.

Mirko Bottarelli, Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas and Haider Al-Khateeb

University of Wolverhampton, UK

Title: *Quantisation feasibility and performance of RSS-based secret key extraction in VANETs*

Abstract: Vehicular Ad Hoc Networks (VANETs) has emerged as a unique implementation of Mobile Ad Hoc Networks (MANETs). These networks promise to increase road safety and improve the driving experience by exploiting recent advances in wireless technologies for both intra-vehicle and inter-vehicle communications. Physical layer security is a promising alternative approach to secure communication in VANETs where physical and applications' constraints encourage the use of lightweight and fast cryptographic algorithms. Our work focuses on the quantisation stage of the secret generation process, by reviewing existing schemes in the public domain and associated performance metrics. Evaluations are done through simulation with the aid of a wireless channel model which includes three-dimensional scattering and scatterers' mobility. Preliminary findings show that RSS-based algorithms do not perform efficiently in the proposed vehicular stochastic wireless model. Hence they are not able to satisfy the typical low latency required in safety-related broadcasting messaging. We conclude that more research is desirable to design protocols capable of taking advantage from the nodes' high-mobility and the consequent variability of both coherence intervals and level crossing rates, to further improve secret bit extraction throughput.

Daniel Fraunholz, Daniel Krohmer, Carolina Nogueira and Hans Dieter Schotten

German Research Center for Artificial Intelligence, Germany

Title: *Introducing Falcom: A Multifunctional High-Interaction Honeypot Framework for Industrial and Embedded Applications*

Abstract: Falcom is a high-interaction honeypot that provides a full fledge operating system, maximizing its interaction with an attacker, aiming at embedded architectures. Since poorly secured embedded devices and internet of things applications form a profitable matrix for criminal activity, a deeper understanding of the existent risks is needed. Threat intelligence is crucial to increase the security in terms of prevention, detection and mitigation of attacks. Honeypots are a well establish technology that provide more insights about the behavior of adversaries by luring attacks into a monitored decoy. Any interaction with this decoy is suspicious and forwarded for further investigation. By analyzing the observed attack parameters, it is possible to reveal recent trends, new attack vectors and ongoing intrusion attempts. Since embedded systems are the focus of the proposed honeypot, CPU architectures, as well as system resources are chosen to imitate embedded devices. In the reference implementation, brute-force and dictionary attacks against the authentication mechanism are implemented as vulnerability.

Baskoro Adi Pratomo, Pete Burnap and George Theodorakopoulos

Cardiff University, Wales, UK

Title: *Unsupervised Approach for Detecting Low Rate Attacks on Network Traffic with Autoencoder*

Abstract: Most approaches to network intrusion detection look only at the header part of network packets. These approaches are able to detect high-rate attacks, such as Denial of Service or probing, with high degrees of accuracy. However, it remains to be seen whether they are also able to detect more subtle attacks, such as when adversaries try to exploit a vulnerability or plant a backdoor. In these cases, the attributes of network packets are usually very similar to the legitimate traffic which presents a limitation for header-only intrusion detection methods. Such attacks present an increasing problem to network security, especially given the rise of Internet of Things (IoT) and the rapidly increasing number of devices that can be exploited through low-intensity attacks. To address this problem, we propose the use of the Autoencoder method for network intrusion detection. Autoencoder is a deep learning architecture that has the capability to identify outliers in a dataset. Thus, it does not need labelled datasets which contain both legitimate and malicious traffic for training purposes. Through our experiments, we show that the proposed approach was able to detect 100% of low rate attack traffic with an average false positive rate of 8.01%. To demonstrate the improvement over the state of the art we have compared our results to a number of other similar works and our proposed method gave at least 32.81% better in detection rate.

Paul Wortman, Fatemeh Tehranipoor and John Chandy

University of Connecticut, USA

Title: *An Adversarial Risk-based Approach for Network Architecture Security Modelling and Design*

Abstract: Network architecture design and verification has become increasingly complicated as a greater number of security considerations, implementations, and factors are included in the design process. In the design process, one must account for various costs of interwoven layers of security. Generally, these costs are simplified for evaluation of risk to the network. The obvious implications of adding security are the need to account for the impacts of loss (risk) and accounting for the ensuing increased design costs. The considerations that are not traditionally examined are those of the adversary and the defender of a given system. Without accounting for the view point of the individuals interacting with a network architecture, one cannot verify and select the most advantageous security implementation. This work presents a method for obtaining a security metric that considers not only the risk of the defender, but also the probability of an attack originating from the motivation of the adversary. We then move to a more meaningful metric based on a monetary unit that architects can use in choosing a “best fit” solution for a given network critical path design problem.

Martin Gilje Jaatun[1], Marie Moe[2] and Per Erik Nordbø[3]

[1]SINTEF Digital, Norway
[2]SINTEF, Digital Norway
[3]BKK Nett, Norway

Title: *Cyber Security Considerations for Self-healing Smart Grid Networks*

Abstract: Fault Location, Isolation and System Restoration (FLISR) mechanisms allow for rapid restoration of power to customers that are not directly implicated by distribution network failures. However, depending on where the logic for the FLISR system is located, deployment may have security implications for the distribution network. This paper discusses alternative FLISR placements in terms of cyber security considerations, concluding that there is a case for both local and centralized FLISR solutions.

Vladimir Eliseev and Olga Eliseeva

JSC InfoTeCS, Russia

Title: *Lightweight Distributed Attack Detection and Prevention for the Safe Internet of Things*

Abstract: The paper investigates the causes of widespread use by cybercriminals of the Internet of Things for organizing distributed network attacks including DDoS and other illegal use. An analysis of existing approaches and technologies for protecting network computer devices is presented, as well as the main factors that prevent their use in the world of Internet of Things. An original approach is suggested that ensures the integration of lightweight protective mechanisms directly into the construction of Smart Things with the defense on the side of a telecom operator. Variants of technology implementation are considered. Key aspects and potential ways of implementation of the proposed approach are noted. Advantages and disadvantages are discussed.

Egon Kidmose, Matija Stevanovic and Jens Myrup Pedersen

Department of Electronic Systems, Aalborg University, Denmark

Title: *Detection of malicious domains through lexical analysis*

Abstract: Malicious domains play an important role for many malicious operations: For example, botnets use them for avoiding hardcoded IP addresses when connecting to command-and-control servers, and they are heavily used by criminals when distributing SPAM and phishing emails. Being able to identify malicious domains and block the harmful traffic is therefore one of the keys to create a more secure cyber environment. In this paper we demonstrate how the lexical analysis of domain names can contribute to increasing precision and decreasing the number of false positives when combined with other basic domain features.

Domhnall Carlin, Phillip O'Kane and Sakir Sezer

Centre for Secure Information Technologies, Northern Ireland, UK

Title: *Dynamic Opcode Analysis of Ransomware*

Abstract: The explosion of ransomware in recent years has served as a costly reminder that the malware threatscape has moved from that of socially-inept hobbyists to career criminals. This paper presents an extension of previous work, with a new dataset of cryptoransomware dynamic run-traces, the largest of its kind in the literature. We release this to the wider research community to foster further research in the field. The analyses presented here demonstrate that a short run- length of 32k opcodes can provide highly accurate detection of ransomware (99.56%) compared to benign software. Further, our model offers a distinct advantage over other models in the literature, in that it can detect benign encryption (i.e. file zipping) with 100% accuracy against not only ransomware, but non- encrypting benignware too. Our work demonstrates that dynamic opcode tracing is capable of detecting ransomware in comparable times to static analysis, without being thwarted by obfuscation tactics.

Bob Duncan

Aberdeen University, UK

Title: *Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis*

Abstract: Many attackers constantly threaten the very survival of all organisations. No-one is safe, no-one is immune. They will attack any and every IT component of every organisation, whether financial, industrial, retail, service, educational, charita- ble or governmental, using whatever means they can to breach these systems. They ignore legislation, all laws, regulations or standards, do not care who they inconvenience, or hurt. They have no moral scruples and will have no compunction about attacking the weakest link in any organisation — the people. Who or what could be more destructive than these people? The answer is Carcharodon Carcharias Moderator Europa Universalis: The European Regulator with a global appetite potentially greater than that of the Great White Shark. We refer, of course, to the regulator for the European Union General Data Protection Regulation, which came into effect on 25th May, 2018. Weak- nesses in hardware, software, networks, systems, procedures, people and all attackers are the regulator's friends. Even the organisations at risk are the regulator's friends. They are obliged by regulation to report any breach within 72 hours of discovery, thus awakening the potentially voracious appetite of the regulator to feast remorselessly upon their weakened carcass. In this paper, we highlight the need for all organisations who are liable to comply with this new regulation to be aware of the serious pitfalls they face when considering the impact of this regulation should they fail to be compliant. We make some sensible suggestions for actions that organisations might take to mitigate their risk now. We also outline our plans for a test study to determine how effective our suggestions might be.

Farhad Foroughi and Peter Luksch

University of Rostock, Germany

Title: Observation Measures to Profile User Security Behaviour

Abstract: Recognising user behaviour in real time is an important element of providing appropriate information and help to take suitable action or decision regarding cybersecurity threats. A user's security behaviour profile is a set of structured data and information to describe a user in an interactive environment between the user and computer. The first step for behaviour profiling is user behaviour model development including data collection. The data collection should be transparent as much as possible with minimum user interaction. Monitoring individual actions to obtain labelled training data is less costly and more effective in creating a behaviour profile. The most challenging issue in computer user security can be identifying suitable data. This research aims to determine required observation measures to capture user-system interactions to understand user's behaviour and create a user profile for cybersecurity purposes.

Kimberly Tam and Kevin Jones
Plymouth University, UK

Title: Cyber-Risk Assessment for Autonomous Ships

Abstract: As a $183.3 Billion industry controlling 90% of all world trade, the shipping community is continuously looking for methods to increase profits while still considering human and environmental safety. As a result of developing technologies and policy that make autonomy a feasible solution, at least three separate organizations are aiming to produce and sail their first autonomous ships by 2020. Thus, it is essential to begin assessing their cyber-risk profiles in order to rank and mitigate any vulnerabilities. As existing risk models for physical ship safety and autonomous cars do not adequately represent the unique nature of cyber-threats for autonomous vessels within the maritime sector, this article applies a model-based risk assessment framework named MaCRA which had previous only been used to model existing ships, not those of the near-future.

André Sørensen, Maxime Jerome Remy, Nicolaj Kjettrup, Rasmi Vlad Mahmoud and Jens Myrup Pedersen

Aalborg University, Denmark

***Title:** An Approach to Detect and Prevent Cybercrime in Large Complex Networks*

Abstract: Recently, the Danish defense department announced that research institutes are prominent targets for cybercrime. To better protect these organizations, an approach to prevent and detect cybercrime in large complex computer networks is needed. This paper contributes by a proof of concept of such an approach, based on a combination of Penetration test (Pen test) and Domain Name System (DNS) analysis. Pen test is a method to assess a network's current security state, thereby detecting vulnerabilities and misconfigurations before they are being abused. On the other hand, DNS analysis can be used to detect ongoing cybercriminal activities. The combination of the Pen test and DNS analysis can give an administrator a crucial overview of vulnerabilities present in the system as well as already compromised parts. The methods were tested on the network of Aalborg University, and they were both able to identify ongoing cybercrime or vulnerabilities. While the feasibility was demonstrated, further developments are needed before it could be implemented at a larger scale.

Martin Span, Logan Mailloux and Michael Grimaila

United States Air Force Institute of Technology, USA

***Title:** A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems*

Abstract: Today's highly interconnected and technology reliant environment places greater emphasis on the need for dependably secure systems. This work addresses this problem by detailing a systems security analysis approach for understanding and eliciting security requirements for complex cyber-physical systems. First, a readily understandable description of key architectural analysis definitions and desirable characteristics is provided along with a survey of commonly used security architecture analysis approaches. Next, a tailored version of the System-Theoretic Process Analysis approach for Security (STPA-Sec) is detailed in three phases which supports the development of functional-level security requirements, architectural-level engineering considerations, and design-level security criteria. In particular, these three phases are aligned with the systems and software engineering processes defined in the security processes of NIST SP 800-160. Lastly, this work is important for advancing the science of systems security by providing a viable systems security analysis approach for eliciting, defining, and

analyzing traceable security, safety, and resiliency requirements which support evaluation criteria that can be designed-for, built-to, and verified with confidence.

Anastasios Balaskas and Virginia N. L. Franqueira

University of Derby, UK

Title: *Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges*

Abstract: Bitcoin has introduced a new concept that could feasibly revolutionise the entire Internet as it exists and positively impact on many types of industries including, but not limited to, banking, public sector and supply chain. This innovation is grounded on pseudo-anonymity and strives on its innovative decentralised architecture based on the Blockchain. Blockchain is pushing forward a race of transaction-based applications with trust establishment without the need for a centralised authority, promoting accountability and transparency within the business process. However, a Blockchain ledger (e.g., Bitcoin) tend to become very complex and specialised tools, collectively called "Blockchain Analytics", are required to allow individuals, agencies and service providers to search, explore and visualise it. Over the last years, several analytical tools have been developed with capabilities that allow, e.g., to map relationships, examine flow of transactions and filter crime instances as a way to enhance forensic investigations. This paper discusses the current state of Blockchain analytical tools and presents a thematic taxonomy model based on their applications. It also examines open challenges for future development and research.

Shuai Fu and Nizar Bouguila

Concordia University, Canada

Title: *An Intrusion Detection Model based on Asymmetric Gaussian mixtures with Reversible Jump MCMC*

Abstract: This paper presents our work on a novel intrusion detection classifier based on asymmetric Gaussian mixture (AGM) model and reversible jump Markov chain Monte Carlo (RJMCMC) learning algorithm. Previous efforts reveal the fact that AGM overperforms classic Gaussian mixture model (GMM) by taking asymmetric datasets into consideration which provides more flexibility. Our RJMCMC implementation is based on a hybrid sampling-based approach which takes advantages of both Metropolis-Hastings (MH) and Gibbs sampling methods, therefore, simplifies mathematical complexity and extends adaptability of the model. Moreover, without giving a fixed components number in advance, RJMCMC applies a dynamic data-based strategy to identify the optimal components number throughout iterations which makes the model learning a self-adaptive process. Since the model is nondeterministic, Laplace approximation based marginal likelihood will be calculated for multiple runs as model selection procedure to improve the correctness and fitting accuracy. Both synthetic and challenging intrusion detection datasets are applied to our model to discover its merits.

Andres Robles-Durazno, Naghmeh Moradpoor, James McWhinnie and Gordon Russell

Edinburgh Napier University, Scotland, UK

Title: *A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system*

Abstract: Industrial Control Systems are part of our daily life in industries such as transportation, water, smart cities, etc. Technological development over time have improved their components including operating system platforms, hardware capabilities, and connectivity with networks inside and outside the organization. Consequently, the Industrial Control Systems components are exposed to sophisticated threats with weak security mechanism in place. This paper proposes a supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. A testbed of such a system is implemented using the Festo MPA Control Process Rig. The machine-learning algorithms; SVN, KNN and Random Forest, perform classification tasks process in three different datasets obtained from the testbed. The algorithms are compared in terms of accuracy and F-measure. The results show that Random Forest presents a better performance over KNN and SVM with small and large datasets. Regarding to time taken to build the model, KNN presents the best performance, although the difference compared with Random Forest is smaller compared with SVM.

Mahdi Madani and Camel Tanougast

University of Lorraine, France

Title: *Combined and Robust SNOW-ZUC Algorithm Based on Chaotic System*

Abstract: SNOW-3G and ZUC are two stream ciphers standardized by the 3GPP (3rd Generation Partnership Project) organization to ensure the LTE (Long Term Evolution of radio networks) security. Unfortunately, these algorithms present some weaknesses. The main objective of this study is to design and implement an enhanced algorithm combining the functionalities of standard SNOW-3G and ZUC algorithms to provide security of the LTE network. A chaotic generator has been used to increase the randomness and robustness of generated keystreams. The proposed architecture was implemented on Xilinx virtex-5 FPGA technology and its security was evaluated using many security tests (generated key-stream distribution, key sensitivity, key space, and NIST statistical tests). The experimental results show that the proposed design allows to encrypt data in two operating modes (SNOW-3G and ZUC modes) using limited hardware resources, power consumption, while ensuring more resistance against cryptanalysis attacks.

Yassine Lemmou and El Mamoun Souidi

Mohammed V University in Rabat Faculty of Sciences, LabMIA, BP 1014 RP, Rabat, Morocco

Title: *Infection, Self-reproduction and Overinfection in Ransomware: The Case of TeslaCrypt*

Abstract: Security experts observed between 2015 and 2017 an exponential increase in the number of advanced threats via ransomware. They confirm that ransomware continues to make organizations suffer. This situation is announced in SophosLabs malware forecast 2018 which mentioned that the history of 2016/2017 is a revolution of ransomware. For Kaspersky this situation will not be different in 2018, ransomware will remain king and its destructive attacks will continue to rise, leveraging its status as the most visible type of cyberwarfare. In this work, we present a model of infection, self-reproduction and over-infection in a particular ransomware, it is TeslaCrypt

in its version 3.1. We describe these concepts and we discuss about some indicators for TeslaCrypt and ransomware detection according to some recent works on ransomware.

Obinna Omego, Eckhard Pfluegel, Martin Tunnicliffe and Charles Clarke

Kingston University, London, UK

Title: *Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol*

Abstract: In recent years, mobile banking has been enjoying a tremendous increase in popularity. Sophisticated mobile apps allow a convenient and secure conduct of banking instructions for users worldwide. However, the use of SMS for mobile banking does not require a fast Internet connection, nor an expensive smart-phone and is an alternative approach, popular in many countries in the world. Due to the existence of vulnerabilities in GSM, this approach is lacking security. In this paper, we improve a recently published SMS banking protocol, which is based on steganography and the use of several communications channels. After analysing the security of this prototype protocol, we address the threat of a multi-channel replay attacks by introducing server-side nonces and making the protocol interactive. We postulate that the resulting, strengthened protocol is secure and robust for use in real-world scenarios.

Trushna Parida and Suvrojit Das

National Institute of Technolgy, Durgapur, India

Title: *Detecting Pure and Impure Programs Through Memory Based Signature Analysis*

Abstract: Physical memory forensics has gradually evolved from simple string and regular expression searching to many complex methods of analysis that can reveal ample of information about live systems. However, the inadequacies suffered by analysis tools while analyzing critical information from physical memory and rapid evolution of anti-forensics techniques, are now making both acquisition and analysis much more challenging. So an integral part of physical memory forensics is an in-depth analysis of the critical set of programs, their data and intended behavior in order to trace any suspicious behavior. The approach of program analysis has been emerging in the research community to properly analyze the intended behavior of programs which are now becoming the powerful weapon to obstruct a meaningful analysis of the live systems. This paper aims to propose an approach of program signature-based analysis that can differentiate between normal behavior and anomalous behavior of a program and can help to find traces of malicious codes injected within the program, with the aim of thwarting the analysis. The proposed approach can model an anomaly detection mechanism by analyzing program's structure and normal operational traffic and can detect any kind of suspicious behavior the program may exhibit when compromised.

Santhosh Parampottupadam and Arghir-Nicolae Moldovan

National College of Ireland, Ireland

Title: *Cloud-based Real-time Network Intrusion Detection Using Deep Learning*

Abstract: Deep learning has increased in popularity with researchers and developers investigating and using it for various use cases and applications. This research focuses on real-time network intrusion detection by making use of deep learning. A cloud-based prototype system was developed to investigate the capability of deep learning

based binomial classification and multinomial regression to detect network intrusions in real-time. An evaluation carried out using the NSL-KDD dataset showed that the deep learning models outperform traditional machine learning models like random forest. The evaluation showed that the deep learning based binomial classification model achieved the highest performance with 99.82% accuracy, followed by the multinomial regression model with 99.05% accuracy.

Dimitrios Kavallieros, Christina Chalanouli, Georgios Kokkinis, Anastasios Papathanasiou, Efthimios Lissaris, Georgios Leventakis, Georgios Giataganas and Georgios Germanos

Center for Security Studies-KEMEA, Greece

Title: *Searching for crime on the web: Legal and Ethical perspectives*

Abstract: The TENSOR and SAINT projects, funded under the European Commision's financial instrument Horizon 2020, are developing cutting edge technologies and technical tools to fight serious and organised crime on the web. These projects are examined as a showcase to highlight the fact that technological advancements do not always adhere to Legal and Ethical Requirements. Compliance with a complex framework, consisting of European Union Regulations, Directives, National Laws, International Regulations and policies is mandatory for all cybercrime fighting solutions. The necessity of a harmonized regulatory framework for Law Enforcement Agencies across all member states is emphasized, especially in cases of cross-border cooperation. Current operational procedures of European cyber security practitioners are examined for similarities, Legal adherence and effectiveness to suppress evolving cybercrime.

Sean Mckeown, Gordon Russell and Petra Leimich

Edinburgh Napier University, Scotland, UK

Title: *Reducing the Impact of Network Bottlenecks on Remote Contraband Detection*

Abstract: Cloud based storage is increasing in popularity, with large volumes of data being stored remotely. Digital forensics investigators examining such systems remotely are limited by bandwidth constraints when accessing this kind of data using traditional tools. This paper explores the potential for sub-file hashing strategies to decrease the time taken to detect contraband on networked storage devices, while maintaining a high degree of accuracy. Results show that sub-file hashing is faster than full file hashing for both LAN and Internet server configurations, with reduced bandwidth heavily favouring sub-file strategies.

Cyber Incident 2018 Accepted Papers

Terézia Mézešová[1] and Hayretdin Bahsi[2]

[1]Institute of Computer Science, Pavol Jozef Šafárik University, Košice, Slovak Republic
[2]Department of Software Science, Tallinn University of Technology, Estonia

Title: *Expert Knowledge Elicitation for Skill Level Categorization of Attack Paths*

Abstract: Attack graphs deduce the attack paths based on the identified vulnerabilities, the existing network topology and the applied network access controls. The exploitation likelihood of the paths derived from the Common Vulnerability Scoring System (CVSS) values of the vulnerabilities provides an important input to risk assessments. This paper focuses on the identification of attacker skill levels required for exploiting the attack paths. First, expert knowledge is elicited for the determination of skill level categories and their detailed descriptions. Second, elicited knowledge is systematically applied to the attack graphs. This skill level categorization method can provide a significant contribution to the design of hands-on offensive cyber games as it enables to balance the skills of participants and difficulty of game tasks. It also improves the threat analysis capability of organizations by demonstrating the possible infiltration ways of threat actors depending on their skill levels.

Basil Alothman

De Montfort University, UK

Title: *Network Traffic Data Preparation for Automatic Botnet Detection by Incident Response Teams*

Abstract: Monitoring network traffic and trying to detect malicious activities is one of the high significance tasks carried out by a Computer Security Incident Response Team (CSIRT). The team usually use tools to monitor and collect network traffic data, analyse the data and perform the necessary procedures if a dangerous activity is detected. However, this captured network traffic data is in raw format and must be transformed into a format that data analysis tools and platforms can process and analyse.

In this paper we provide a detailed explanation of several steps required to make sure the data is in good shape for analysis and automatic detection of malicious traffic. We explain the steps in a tutorial like manner and support it by executing them to analyse a publicly available network traffic dataset that contains safe and malicious data. Our steps and analysis illustrate that the steps we take help in making tasks such as automatic classification and clustering easy.

Cyber Insurance and Risk Controls (CIRC) Workshop 2018 Accepted Papers

Erin Kenneally, Lucien Randazzese and David Balenson

U.S. Department of Homeland Security; International Computer Sciences Institute, USA

Title: *Cyber Risk Economics Capability Gaps Research Strategy*

Abstract: This paper introduces a forthcoming publication produced in conjunction with the Cyber Risk Economics Program at the U.S. Department of Homeland Security that presents an overarching strategy for cyber security risk economics applied research and advanced development intended to address some of the most pressing capability gaps in government and industry.

Per Håkon Meland[1] and Fredrik Seehusen[2]

[1]SINTEF, Norway
[2]Norwegian Defence Research Establishment, Norway

Title: *When to Treat Security Risks with Cyber Insurance*

Abstract: Transferring security risk to a third party through cyber insurance is an unfamiliar playing field for a lot of organisations, and therefore many hesitate to make such investments. Indeed, there is a general need for affordable and practical ways of performing risk quantification when determining risk treatment options.
To address this concern, we propose a lightweight, data-driven approach for organisations to evaluate their own need for cyber insurance. A generic risk model, populated with available industry averages, is used as a starting point. Individual organisations can instantiate this model to obtain a risk profile for themselves related to relevant cyber threats. The risk profile is then used together with a cyber insurance profile to estimate the benefit and as a basis for comparing offers from different insurance providers.

Daniel W Woods and Andrew C Simpson

University of Oxford, Oxford, UK

Title: *Towards Integrating Insurance Data into Information Security Investment Decision Making*

Abstract: Making security investment decisions involves comparing a variety of risks. However, there is little robust empirical evidence that can be used to support this process. This paper builds a road-map for incorporating cyber insurance data into existing security investment models. We propose an approach for using this data as an input for one investment model and introduce three distinct methods for evaluating the effectiveness of a new investment. We then describe a road-map for improving the insurance data collection process that aims to improve data utility for researchers. This approach could benefit those trying to justify an investment at all levels by providing evidence for the return on security.

Ganbayar Uuganbayar, Artsiom Yautsiukhin and Fabio Martinelli

CNR, Italy

Title: *Cyber Insurance and Security Interdependence: Friends or Foes?*

Abstract: cyber insurance is a cyber risk treatment option which allows transferring losses to another party for a fee. Although researchers and practitioners see cyber insurance as a desirable practice, the new market faces several practical (e.g., lack of data) and theoretical (effect of security interdependency) challenges. One of the most important questions from the cyber security point of view is whether cyber insurance is an incentive to self-protection investments. Several studies have shown that with cyber insurance available, agents are more willing to buy insurance than investing in self-protection.

In this study, we investigate how security interdependence affects the incentive of agents to invest in self-protection with/without cyber insurance available to them. In particular, we are interested in comparing the investments with and without insurance available for agents when the degree of interdependence changes. In the study, we model a competitive cyber insurance market and assume no information asymmetry.

Best Paper Awards

Best papers are selected through a rigorous and transparent process for each conference based on the double or multiple peer reviews scores. Scores are computed based on the average score, weighted against reviews by reviewers' confidence, in additional further criteria for contribution of originality and relevancy.

	Cyber SA 2018 – Joint Best Papers
1	Christopher McDermott, Andrei Petrovski and Farzan Majdani Robert Gordon University, UK Title: *Towards Situational Awareness of Botnet Activity in the Internet of Things*
2	Zahid Maqbool[2], V.S. Chandrasekhar Pammi[1] and Varun Dutt[2] [1]Centre of Behavioural and Cognitive Sciences, University of Allahabad, India [2]Indian Institute of Technology Mandi, India Title: *Cybersecurity: Influence of patching vulnerabilities on the decision-making of hackers and analysts*
3	Patrik Lif, Teodor Sommestad and Dennis Granåsen Division for C4IS, Swedish Defence Research Agency, Linköping, Sweden Title: *Development and evaluation of information elements for simplified cyber-incident reports*
	Cyber Security 2018 – Joint Best Papers
4	Domhnall Carlin, Phillip O'Kane and Sakir Sezer Centre for Secure Information Technologies, Northern Ireland, UK Title: *Dynamic Opcode Analysis of Ransomware*
5	Ensar Seker and Hasan Huseyin Ozbenli NATO CCD COE, Estonia Title: *The Concept of Cyber Defence Exercises: Planning, Execution, Evaluation*
	CIRC 2018 – Best Paper
6	Per Håkon Meland[1] and Fredrik Seehusen[2] [1]SINTEF, Norway [2]Norwegian Defence Research Establishment, Norway Title: *When to Treat Security Risks with Cyber Insurance*

Cyber Science 2018 Thematic Tracks

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Cyber Science 2018 Conference Presentation Timetable

Day 1: June 11, 2018

Cyber Science 2018	
Comprising	
International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2018)	
International Conference on Social Media, Wearable and Web Analytics (Social Media 2018)	
International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018)	
International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident 2018)	
International Work on Cyber Insurance and Risk Controls (CIRC 2018)	
Grand Central Hotel, Glasgow, Scotland, United Kingdom June 11- 12, 2018	

Cyber Science 2018

Monday, June 11, 2018	
08:00 – 09:00	**Day 1** **Registration, Networking and Refreshments in the Victoria Suite**
09:00 – 09:05	**Welcome Session** **Dr Cyril Onwubiko** – Chair, Cyber Security Intelligence, Research Series, London, UK
09:05 – 09:10	**Announcements & Introduction** **Dr Xavier Bellekens – Conference Chair** **Dr Natalie Coull – Conference Chair** **Dr Lynsay Shepherd – Conference Chair** **Dr Arnau Erola – Conference Chair**
09:15 – 09:45	**Keynote: Opening Session** **Mr Michael Matheson MSP** – Cabinet Secretary for Justice, Scottish Member of Parliament, UK
10:00 – 10:30	**Keynote:** **Professor Sadie Creese** – Professor of Cyber Security, Department of Computer Science, University of Oxford, UK
10:30 – 10:40	**Coffee Break & Social Networking**

10:40 – 11:10	**Keynote: Describing a CyberSA Analysis Model** **Dr Cyril Onwubiko** – Chair, Cyber Security Intelligence, Research Series, London, UK		
11:10 – 11:40	**Keynote: The Challenge to Policing in Investigating Cybercrime** **DI Eamonn Keane** – Cybercrime Unit, Specialist Crime Division SCD, Police Scotland, UK		
11:40 – 11:50	**Coffee Break & Social Networking**		
Conference in Suites	**Cyber Security 2018 in Victoria Suite**	**Cyber Security 2018 in Wellington Suite**	**Cyber Security 2018 in Buchanan Suite**
Track	**Track 7a: Cyber Defence Exercise, Planning & Recovery**	**Track 9a: Cyber Physical Systems, Deep Learning and Cloud Computing**	**Track 18a: Cyber Security, Legal and Ethics**
11:50 – 12:10	**The Concept of Cyber Defence Exercises: Planning, Execution, Evaluation** *Ensar Seker and Hasan Huseyin Ozbenli*	**Observation Measures to Profile User Security Behaviour** *Farhad Foroughi and Peter Luksch*	**Sub-file Hashing Strategies for Fast Contraband Detection** *Sean Mckeown, Gordon Russell and Petra Leimich*
12:10 – 12:30	 **Group Conference Photographs at the Victoria Suite**		
12:30 – 13:30	**Lunch (in the Regent Suite)** 		
Conference in Suites	**Cyber SA 2018 in Victoria Suite**	**Cyber Security 2018 in Wellington Suite**	**Cyber SA 2018 in Buchanan Suite**
Tracks	**Track 1: Adaptive Cyber Defense Operations**	**Track 2: Machine Learning for Cyber Security Operations**	**Track 3: CyberSA Emerging Tools and Techniques**
13:30 – 13:50	**Development and evaluation of information elements for simplified cyber-incident reports**	**Detection of malicious domains through lexical analysis** *Egon Kidmose, Matija Stevanovic and Jens Myrup Pedersen*	**Analysis of Adversarial Movement Through Characteristics of Graph Topological Ordering**

	Patrik Lif, Teodor Sommestad and Dennis Granåsen		*Nima Asadi, Aunshul Rege and Zoran Obradovic*
13:50 – 14:10	**Towards an Adaptable System-based Classification Design for Cyber Identity** *Kay Michel and Michael King*	**A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system** *Andres Robles-Durazno, Naghmeh Moradpoor, James McWhinnie and Gordon Russell*	**Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools** *Eliana Stavrou*
14:10 – 14:30	**Can We Evaluate the Impact of Cyber Security Information Sharing?** *Adam Zibak and Andrew Simpson*	**Unsupervised Approach for Detecting Low Rate Attacks on Network Traffic with Autoencoder** *Baskoro Adi Pratomo, Pete Burnap and George Theodorakopoulos*	**Compound Password System for Mobile** *Zachary Hills, David Arppe, Amin Ibrahim and Khalil El-Khatib*
14:30 – 14:50	**The Landscape of ICS Devices on the Internet** *Wei Xu, Yaodong Tao and Xin Guan*	**Combined and Robust SNOW-ZUC Algorithm Based on Chaotic System** *Mahdi Madani and Camel Tanougast*	**Towards Situational Awareness of Botnet Activity in the Internet of Things** *Christopher McDermott, Andrei Petrovski and Farzan Majdani*
14:50 – 15:00	**Coffee Break & Social Networking**		
Conference in Suites	**Cyber SA 2018 in Victoria Suite**	**Cyber Security 2018 in Wellington Suite**	**CIRC Workshop 2018 in Buchanan Suite**
Tracks	**Track 5: Malware Economics and Advanced Ransomware Analysis**	**Track 4: Ransomware Cryptanalysis and Crypto Systems**	**Track 16: Collaborative Insurance Data for Strategic Investment Risk Decisions**
15:00 – 15:20	**Cluster analysis for deobfuscation of malware variants during ransomware attacks** *Anthony Arrott, Arun Lakhotia, Ferenc Leitold and Ledoux Charles*	**Dynamic Opcode Analysis of Ransomware** *Domhnall Carlin, Phillip O'Kane and Sakir Sezer*	**Towards Integrating Insurance Data into Information Security Investment Decision Making** *Daniel W Woods and Andrew C Simpson*
15:20 – 15:40	**Malware Economics and its Implication to Anti-Malware Situational Awareness** *Arun Lakhotia, ivek Notani and Charles LeDoux*	**Quantisation feasibility and performance of RSS-based secret key extraction in VANETs** *Mirko Bottarelli, Dr Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas and Haider Al-Khateeb*	**When to Treat Security Risks with Cyber Insurance** *Per Håkon Meland and Fredrik Seehusen*

15:40 – 16:00	**A Netnographic Study on the Dark Net Ecosystem for Ransomware** *Yara Bayoumy, Per Håkon Meland and Guttorm Sindre*	**Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol** *Obinna Omego, Eckhard Pfluegel, Martin Tunnicliffe and Charles Clarke*	**Cyber Risk Economics Capability Gaps Research Strategy** *Erin Kenneally, Lucien Randazzese and David Balenson*
16:00 – 16:20	**Cybersecurity: Influence of patching vulnerabilities on the decision-making of hackers and analysts** *Zahid Maqbool, V.S. Chandrasekhar Pammi and Varun Dutt*	**Infection, Self-reproduction and Overinfection in Ransomware: The Case of TeslaCrypt** *Yassine Lemmou and El Mamoun Souidi*	**Cyber Insurance and Security Interdependence: Friends or Foes?** *Ganbayar Uuganbayar, Artsiom Yautsiukhin and Fabio Martinelli*
16:20 – 16:30	**Coffee Break & Social Networking**		
Conference in Suites	**Cyber Security 2018 in Victoria Suite**	**Social Media 2018 in Wellington Suite**	**Cyber Security 2018 in Buchanan Suite**
Tracks	**Track 7b: Cyber Defence Exercise, Planning & Recovery**	**Track 6: Health Informatics and Social Media Analytics**	**Track 18b: Cyber Security, Legal and Ethics**
16:30 – 16:50	**An Approach to Detect and Prevent Cybercrime in Large Complex Networks** *André Sørensen, Maxime Jerome Remy, Nicolaj Kjettrup, Rasmi Vlad Mahmoud and Jens Myrup Pedersen*	**Information flow on Twitter surrounding regional events** *Jason Koepke and Siddarth Kaza (Via Skype)*	**Searching for Crime on the Web: Legal and Ethical Perspectives** *Dimitrios Kavallieros, Christina Chalanouli, Georgios Kokkinis, Anastasios Papathanasiou, Efthimios Lissaris, Georgios Leventakis, Georgios Giataganas and Georgios Germanos*
16:50 – 17:10	**Cyber Security Considerations for Self-healing Smart Grid Networks** *Martin Gilje Jaatun, Marie Moe and Per Erik Nordbø*	**Introducing Falcom: A Multifunctional High-Interaction Honeypot Framework for Industrial and Embedded Applications** *Daniel Fraunholz, Daniel Krohmer, Carolina Nogueira and Hans Dieter Schotten*	**Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis** *Bob Duncan*
17:10 – onwards	**Social Evening: Drinks, Chat and Social Networking - at the City Council** 		

Day 2: June 12, 2018

Cyber Science 2018

Comprising

International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2018)
International Conference on Social Media, Wearable and Web Analytics (Social Media 2018)
International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018)
International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident 2018)
International Work on Cyber Insurance and Risk Controls (CIRC 2018)

Grand Central Hotel, Glasgow, Scotland, United Kingdom

June 11- 12, 2018

Tuesday, June 12, 2018

08:00 – 09:00	**Day 2** **Registration, Networking and Refreshments in the Victoria Suite**
09:00 – 09:05	**Welcome Session** **Dr Cyril Onwubiko** – Chair, Cyber Security Intelligence, Research Series, London, UK
09:05 – 09:10	**Announcements & Introduction** **Dr Xavier Bellekens – Conference Chair** **Dr Natalie Coull – Conference Chair** **Dr Lynsay Shepherd – Conference Chair** **Dr Arnau Erola – Conference Chair**
09:10 – 09:40	**Keynote: Getting Real about the Reasons for Insecure Behaviours** **Professor Karen Renaud** – Professor of Cyber Security, University of Abertay, Scotland, UK
09:40 – 10:20	**Keynote: Internet of Things – A Hacker Perspective** **Professor Jens Myrup Pedersen –** Aalborg University, Denmark

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

10:20 – 10:50	**Keynote: An Imposter's Journey into Infosec** **Mr Stu Hirst** – Head of Security Operations (SecOps), UK Cyber, Capital One, UK	
10:50 – 11:00	**Coffee Break & Social Networking**	
Conference in Suite	**Cyber Security 2018 in Victoria Suite**	**Cyber Security 2018 in Wellington Suite**
Track	**Track 11: Situational Awareness, Cyber Kill Chain, Threat Intel and CyberOps**	**Track 17: Blockchain, IoT and Emerging Cyber Techniques, Tools and Concepts**
11:00 – 11:20	**CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process** *Cyril Onwubiko*	**Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges** *Anastasios Balaskas and Virginia N. L. Franqueira*
11:20 – 11:40	**A Taxonomy of Malicious Traffic for Intrusion Detection Systems (Short PhD Track)** *Hanan Hindi, Elike Hodo, Ethan Bayne, Amar Seeam, Robert Atkinson and Xavier Bellekens*	**An Intrusion Detection Model based on Asymmetric Gaussian mixtures with Reversible Jump MCMC** *Shuai Fu and Nizar Bouguila*
11:40 – 12:00	**Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture** *Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh and Moosung Park*	**Detecting Pure and Impure Programs Through Memory Based Signature Analysis** *Trushna Parida and Suvrojit Das*
12:00 – 12:20	**Multilayer Perceptron Neural Network for Detection of Encrypted VPN Network Traffic** *Shane Miller, Kevin Curran and Tom Lunney*	**Lightweight Distributed Attack Detection and Prevention for the Safe Internet of Things** *Vladimir Eliseev and Olga Eliseeva*
12:20 – 12:50	**Best Paper Awards &** **Group Conference Photographs at the Victoria Suite** 	
12:50 – 13:50	**Lunch (in the Regent Restaurant) Grand Central Hotel** 	

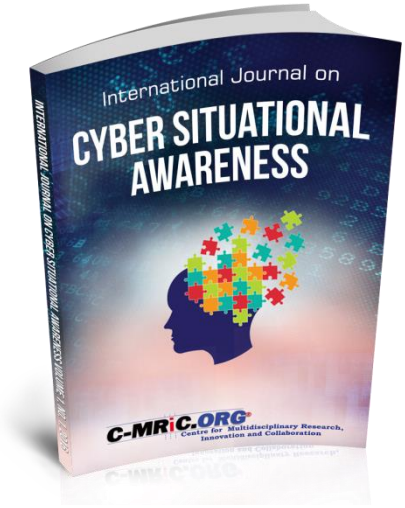
13:50 – 14:00	**Plenary Group Session for all Conference Participants at the Victoria Suite**	
Conference in Suite	**Cyber SA 2018 in Victoria Suite**	**Cyber Security 2018 in Wellington Suite**
Tracks	**Track 14: Machine Learning & Blockchain in Cyber SA**	**Track 9b: Cyber Physical Systems, Deep Learning and Cloud Computing**
14:00 – 14:20	**Redesign of Gaussian Mixture Model for Efficient and Privacy-preserving Speaker Recognition** *Yogachandran Rahulamathavan, Xuewen Yao, Rahulamathavan Sutharsini, Muttukrishnan Rajarajan and Kanapathippillai Cumanan*	**A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems** *Martin Span, Logan Mailloux and Michael Grimaila*
14:20 – 14:40	**Reducing the Impact of Network Bottlenecks on Remote Contraband Detection** *Sean Mckeown, Gordon Russell and Petra Leimich*	**Cloud-based Real-time Network Intrusion Detection Using Deep Learning** *Santhosh Parampottupadam and Arghir-Nicolae Moldovan*
14:40 – 15:00		**OWASP Top 10 - Do Startups Care?** *Halldis Søhoel, Martin Gilje Jaatun and Colin Boyd*
15:00 – 15:10	**Coffee Break & Social Networking**	
Conference in Suite	**Cyber Incident 2018 in Victoria Suite**	**Cyber Security 2018 in Wellington Suite**
Tracks	**Track 10: Expert Knowledge in Cyber Incident Response**	**Track 15: Cyber Risk Assessment & Management**
15:10 – 15:30	**Expert Knowledge Elicitation for Skill Level Categorization of Attack Paths** *Terézia Mézešová and Hayretdin Bahsi*	**Cyber-Risk Assessment for Autonomous Ships** *Kimberly Tam and Kevin Jones*
15:30 – 15:50	**Network Traffic Data Preparation for Automatic Botnet Detection by Incident Response Teams** *Basil Alothman*	**An Adversarial Risk-based Approach for Network Architecture Security Modelling and Design** *Paul Wortman, Fatemeh Tehranipoor and John Chandy*
Conference in Suite	**Cyber SA 2018 in Victoria Suite**	
Tracks	**Track 12: Human Factors, Cognition, Cyber Policy & Compliance**	
15:50 – 16:10	**A Human Vulnerability Assessment Methodology** *Andrea Cullen and Lorna Armitage*	

16:10 – 16:30	**How to Make Privacy Policies both GDPR-Compliant and Usable** *Karen Renaud and Lynsay Shepherd*
16:30	**Thanks & Closing Remarks (at the Victoria Suite)** **Dr Cyril Onwubiko on behalf of Centre for Multidisciplinary Research, Innovation & Collaboration (C-MRiC.ORG) & IEEE TCS**
16:30 – onwards	**Social Evening and Dinner at The Corinthian Club, Glasgow, Scotland, UK** 191 Ingram St, Glasgow G1 1DA **http://www.thecorinthianclub.co.uk/**   

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

International Journal on Cyber Situational Awareness (IJCSA)

ISSN: (Print) **2057-2182** ISSN: (Online) **2057-2182, DOI: 10.22619/IJCSA**



The **International Journal on Cyber Situational Awareness (IJCSA)** is a comprehensive reference journal, dedicated to disseminating the most innovative, systematic, topical and emerging theory, methods and applications on Situational Awareness (SA) across Cyber Systems, Cyber Security, Cyber Physical Systems, Computer Network Defence, Enterprise Internet of Things (EIoT), Security Analytics and Intelligence to students, scholars, and academia, as well as industry practitioners, engineers and professionals.

https://www.c-mric.com/journals/ijcsa

C-MRiC Other Services

We provide a number of other and interrelated services, such as:

- Innovation, Research & Development ranging from national cyber security programmes, enterprise security management, information assurance, protection strategy & consultancy
- Customised & Professional Training
- Technology-inspired programmes, and undertake independent bespoke technology-based & survey-based research engagements
- Security Testing and Lab Experimentations
- Conference Organisation
- Printing and Publications
- Consultancy & Consortium-led collaborations

Notes:

Cyber Science 2019

Cyber Science is the flagship conference of the Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC) focusing on pioneering research and innovation in Cyber Situation Awareness, Social Media, Cyber Security and Cyber Incident Response. It is an IEEE technically co-sponsored conference. Cyber Science aims to encourage participation and promotion of collaborative scientific, industrial and academic inter-workings among individual researchers, practitioners, members of existing associations, academia, standardisation bodies, and including government departments and agencies. The purpose is to build bridges between academia and industry, and to encourage interplay of different culture. Cyber Science invites researchers and industry practitioners to submit papers that encompass principles, analysis, design, methods and applications. It is a yearly conference held at various countries in the world; the first three meetings have been in London, UK, while the 2017 will be held in Glasgow, Scotland.

The theme for Cyber Science 2019 is:

Theme – Cyber Situational Awareness for Predictive Insight and Deep Learning

Dates: **Cyber Science 2019 will be held on Monday 3rd to Tuesday 4th June 2019.**

Venue: TBC

2019 Call for Papers and Workshops

Should wish to host a workshop or a seminar for the Cyber Science 2019, then please contact us immediately via email to submission@c-mric.org

Thank-you!

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

Organiser / Contact Us

Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC.ORG)

Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC) is a nonprofit non-governmental organisation.

The aim is to participate, encourage and promote collaborative scientific, industrial and academic inter-workings among individual researchers, practitioners, members of existing associations, academia, standardisation bodies, and including government departments and agencies.

The purpose is to build bridges between academia and industry, and to encourage interplay of different cultures.

C-MRiC is committed to outstanding research and innovation through collaboration, and to disseminate scientific and industrial contributions through seminars and publications. Its products range from conferences on advanced and emerging aspects of societal issues, ranging from Cyber security to environmental pollution, and from Health IT to Wearable, with the best of breeds of such contributions featuring in our journal publications.

C-MRiC is reliant on individual and corporate voluntary and free memberships to support its activities such as peer reviews, editorials, participating, organising and promoting conference and journal publications.

We collaborate with academia, industries and government departments and agencies in a number of initiatives, ranging from national cyber security, enterprise security, information assurance, protection strategy, climate control to health and life sciences.

We participate in academic and industrial initiatives, national and international collaborative technology-inspired programmes, and undertake independent bespoke technology-based & survey-based research engagements.

C-MRiC is free membership to both individuals and corporate entities; it is voluntary, open and professional.

Membership to C-MRiC entitles you free access to our publications, early sightings to research and innovations, and allows you to submit, request and pioneer research, conference or journal project through us. Members are selected based on expertise to support some of our activities on a voluntary basis, such as peer reviews, editorials, participating, organising and promoting conference and journal publications.

Address: C-MRiC.ORG
1 Meadway, Woodford Green, Essex, IG8 7RF, UK
Email: submission@c-mric.org

Twitter: Follow @cmricorg

Web: http://www.c-mric.org

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration