3-4 JUNE, 2019

University of Oxford, UNITED KINGDOM

IEEE

Advancing Technology for Humanity

2019

Cyber Science 2019 Conference Programme

Cyber Situational Awareness for Predictive Insight and Deep Learning

C-MRiC.ORG

#Cyberscience @cmricorg

www.c-mric.org

Sponsors

the risk analyzer

Contents

Foreword

Cyber Science is the flagship conference of the *Centre for Multidisciplinary Research, Innovation and Collaboration* (C-MRiC), a multidisciplinary platform focusing on pioneering research and innovation in Cyber Situational 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 government departments and agencies. The purpose is to build bridges between academia and industry, and to encourage interplay of different cultures. Cyber Science invites researchers and industry practitioners to submit papers that encompass principles, analysis, design, methods and applications. It is an annual conference with the aim that it will be held in the future at various cities in different countries.

Cyber Science as a multidisciplinary and co-located event is gradually becoming a mainstream and notable conference, first, for its quality, second, for its uniqueness, and finally, for its structure, contributions and originality; something existing mainstream conferences do not normally possess. A testament to the significant interest Cyber Science has thus so far gained.

This year's conference is the fifth episode of the Cyber Science event, organised in partnership with the University of Oxford, University of Derby and SINTEF Digital, Norway, was held on June 3-4, 2019 at the Department of Computer Science, University of Oxford, Wolfson Building Parks Road, Oxford OX1 3QD, United Kingdom. At the conference, a Workshop organised by the Computer Science Department, University of Oxford, Oxford, UK, on Cyber Insurance and Risk Controls (CIRC 2019) was co-located with the CyberSA 2019 conference, while a Workshop organised by SINTEF Digital on Secure Software Engineering in DevOps and Agile Development (SecSE 2019) was co-located with the Cyber Security 2019 conference.

This Cyber Science 2019 conference proceedings is a collection of notable, topical and emerging contributions from researchers, practitioners and academics who submitted their papers to the four distinguished multidisciplinary and co-located conferences – CyberSA 2019, Social Media 2019, Cyber Security 2019 and Cyber Incident 2019, and in addition to papers received for the CIRC 2019 and SecSE 2019 workshops.

We received submissions from far and wide, from over 40 different countries. Following quality peer reviews, a total of 64 articles (i.e. 50 full papers, 7 extended abstracts and 7 posters) were accepted covering Social Media, IoT, Workload, Human Factors, Cognitive Psychology, CERTs, Machine Learning, Adaptive Cyber Defence, Ransomware, Cyber Security, Digital Protection, Web Analytics, Malware Economics and Advanced Ransomware Detection, Cyber Incident Response, Threat Intelligence, Crypto, Visualization, Game Theory, Adaptive Security, Policy, Legal, Compliance, Cyber Insurance, Measurement and Metrics, Social Media, Health Informatics and Social Media Analytics.

The Cyber Science 2019 conference was opened by the **Chair, IEEE United Kingdom & Ireland**, ***Professor Mike Hinchey***, and notable experts and keynote speakers from industry, academia and government who spoke at the 2-day event are:

- *Professor Sadie Creese* – Professor of Cybersecurity, University of Oxford, UK
- *Jean-Jacques Sahel – Managing Director, ICANN, Europe*
- *Professor Awais Rashid – Professor of Cyber Security, University of Bristol, UK*
- *Dr Aunshul Rege – Associate Professor, Department of Criminal Justice, Temple University, USA*
- *Simon Wilson – CTO, UK & Ireland for Aruba, a Hewlett Packard Enterprise Company*
- *John Crain – Chief Security, Stability & Resiliency Office, ICANN, USA*
- *Chrissy Morgan – Security Researcher, Cyber Security Challenge UK Team*

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

- *Ros Smith – Senior Product Manager, British Broadcasting Corporation (BBC)*

These internationally recognised domain experts in Cyber Situational Awareness, Cyber Security, Cyber Incident Response and Government Security spoke on a vast array of timely, topical and emerging topics including:

- Cyber Security Body of Knowledge (CyBOK)
- Cyber Situational Assessment, Cyber Security Operations Centres, Cybercrime and Threat Intelligence
- Policing, Cybercrime, Organised Criminals, Cyber Incident Response and Preparedness in the face of Nation State Sponsored Cyber Attacks
- Advanced Techniques for mitigating Enterprise-scale Cyber Attacks, including novel Machine Learning Algorithms for understanding behavioural and psychological cues for Cyber Situational Awareness
- Cyber-Value-at-Risk, Residual Risk and models for Systemic Cyber-Risk
- Case studies on the application and the transformational challenge of Identity and Access Management (IAM) at the BBC

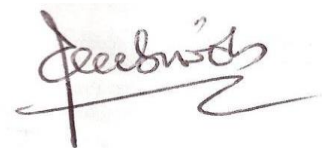
The 2-day event featured multiple plenary sessions that encouraged social interaction and engagement from all participants. Two evenings of drinks and dinner, group photographs and best paper and poster awards. Oxford is a beautiful city with cultural heritage, and provided an ideal experience for excursions and sightseeing. It was a great opportunity to network and learn great new and innovative things.

I would like to thank the Organisers, Programme Committee Members and the other Conference Reviewers for graciously contributing their time, assuring a scholarly fair and rigorous review process. I would also like to thank the IEEE UK and Ireland Computer Society Chair, Professor Frank Wang for accepting to become the Technical Co-Sponsor (TCS) of the Cyber Science 2019 joint conferences. I would like to thank Dr Arnau Erola for facilitating, and Professor Sadie Creese for her part in establishing our partnership and hosting the event at the Department of Computer Science, University of Oxford. I am grateful to Sarolta Mohaine Palfi, Industrial Research Partnerships Manager at the University of Oxford, for her efforts and time in promoting this event, without her last-minute efforts this event wouldn't have been widely accessible!

Thanks to our Platinum Sponsor – Aruba, HPE (https://www.arubanetworks.com) and our Gold Sponsor – Secudit (https://secudit.com/) whose financial support helped us put on a good show. Thanks to our media sponsors – Research Series Limited, IEEE Young Professionals (IEEE YP), the Institute of Information Security Professionals (IISP), University of Oxford Cyber Security Group (Cyber Security Oxford), Grayfield Solicitors and Aceobjects, for their support, too.

Special thanks to Professor Fatih Kurugollu and Dr Virginia N. L. Franqueira of the University of Derby, UK for their friendship, support, time and effort in contributing to and co-organising the 2019 Cyber Science conference.

Finally, I would like to thank the authors of papers and the delegates present at the event; there would be no conference without you!



Cyril Onwubiko, BSc, MSc, PhD

Secretary – **IEEE UK & Ireland**
Chair – **IEEE UK & Ireland Blockchain Group**
Chair – Cyber Science 2019 Steering Committee

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

Conference Venue

Department of Computer Science, University of Oxford, Wolfson Building

Parks Road, Oxford OX1 3QD, United Kingdom

The University of Oxford has been recognised in 2012 and again in 2017 as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR). Oxford is one of 14 universities recognised by the National Cyber Security Centre (NCSC) and the Engineering and Physical Sciences Research Council (EPSRC), based on review by a panel of experts.

Please use Oxford e-Research Centre (OeRC) entrance: 7 Keble Road, Oxford OX1 3QG

Main Contact: Telephone: +44 (0)1865 273838
Web: https://www.cs.ox.ac.uk/aboutus/contact.html

CyberSecurity@Oxford brings together the dynamic and vibrant community of researchers and experts working on Cyber Security at the University of Oxford. The network links the wide variety of research and education activities across the University, and provides an easy point of contact for engagement.

With experts working in over 20 units across the University, the network is able to address the difficult questions that cross the borders of traditional academic disciplines: what does 'good' cybersecurity look like, and how does that change in different contexts? How can technology interact gracefully with messy human realities?

Directions

By Car Postcode is OX1 3QD. Use the following navigation coordinates 51.759587, -1.258277	**From London Airports** From London Heathrow and Gatwick, take the Airline coach service. From London Stansted, take the Stansted Express train service to Liverpool Street and take the tube to either Paddington or Marylebone for direct trains to Oxford. (please ask for other airports)
By Train Direct services from London Paddington and London Marylebone.	

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

Please use Oxford e-Research Centre (OeRC) entrance: 7 Keble Road, Oxford OX1 3QG

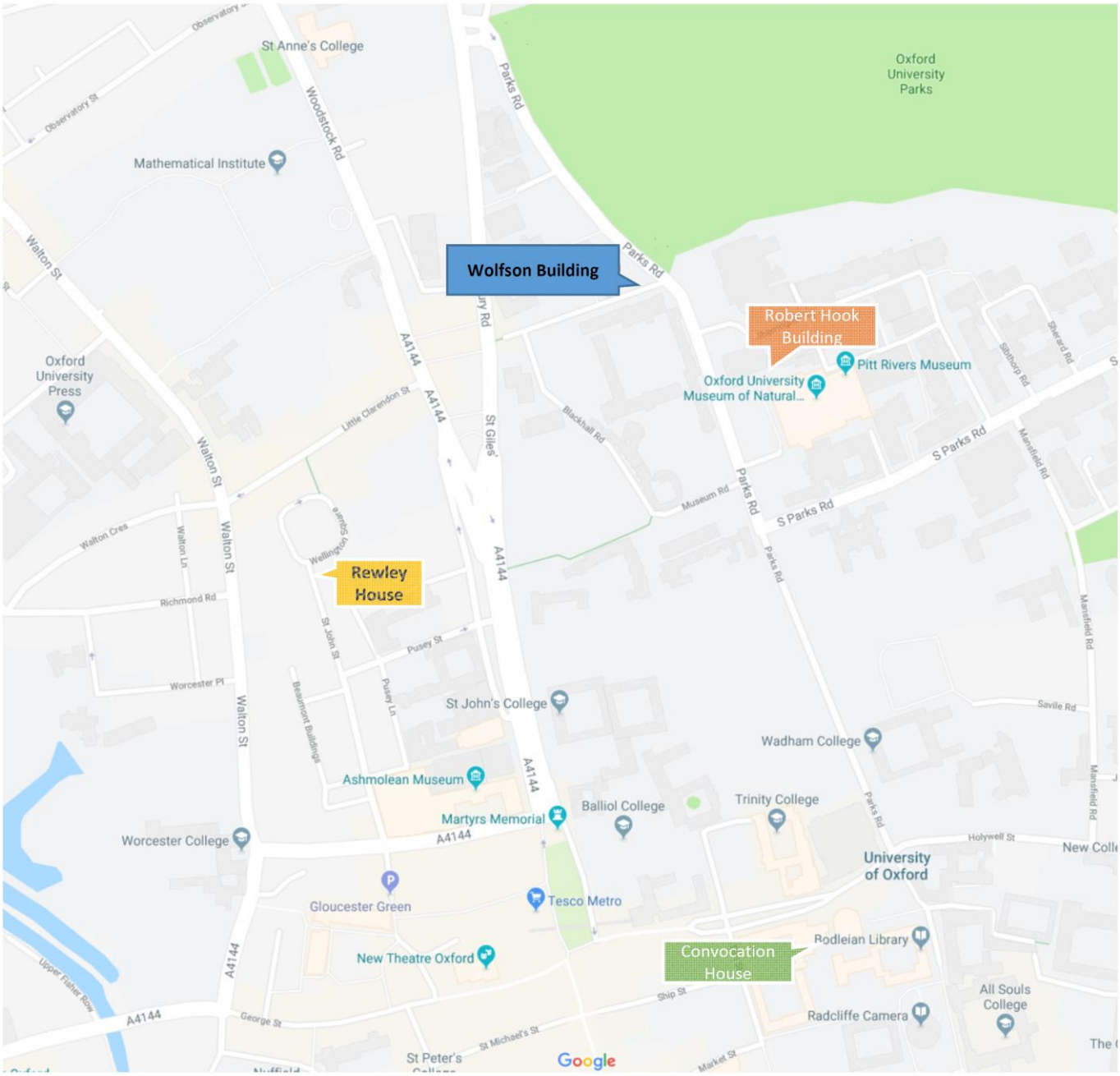


Figure 1: Map of Oxford and location of the conference venue

Keynote & Industry Speakers

Professor Sadie Creese

Professor Sadie Creese – Professor of Cyber Security, University of Oxford, UK

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 and how it emerges both for single organisations and for nations. She is Principal Investigator on the AXIS sponsored project "Analysing Cyber-Value-at-Risk, Residual Risk and models for Systemic Cyber-Risk" focused on developing a method for predicting potential harms arising from cyber-attacks in businesses. 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 is 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 Cyber Security Centre's Strategic Advisory Board.

Simon Wilson

Simon Wilson – Chief Technology Officer (CTO), UK & Ireland Aruba Networks, a Hewlett Packard Enterprise Company

Simon Wilson is ***CTO, UK & Ireland for Aruba***, a ***Hewlett Packard Enterprise Company***. In this role he works as a brand ambassador articulating the Aruba vision for experience driven infrastructure. Simon also works closely with Aruba customers and partners across all markets to design smart and secure workspaces that maximise business productivity. With over 25 years' experience in the networking industry, Simon joined HPE in March 2014.

Before this, Simon was with Nortel/Avaya for sixteen years where he worked across product management, marketing and channel operations roles. His experience also spans network design and electronic engineering. Simon led the EMEA product marketing team and worked in Nortel's Global product marketing organisation in North America. Prior to that, he had worked in the SMB reseller market and in distribution. Simon holds a BTEC in Engineering from Croydon Technical College in the UK.

Professor Awais Rashid

Professor Awais Rashid – Professor of Cyber Security, University of Bristol, UK

Awais Rashid is ***Professor of Cyber Security at University of Bristol, UK***. His research focuses on security of large-scale connected infrastructures, software security and human behaviours (adversarial and non-adversarial) in these contexts. He leads projects as part of the UK Research Institute on Trustworthy, Interconnected Cyber-Physical Systems (RITICS) and UK Research Institute on Science of Cyber Security (RISCS), co-leads the Security and Safety theme within the UK Hub on Cyber Security of Internet of Things (PETRAS) and is a member of the UK Centre for Research and Evidence on Security Threats (CREST). He also leads the Cyber Security Body of Knowledge (CyBOK) project which aims to provide much needed foundations for education and training programmes in this area.

Dr Aunshul Rege

Dr Aunshul Rege – Associate Professor, Department of Criminal Justice, Temple University, USA

Aunshul Rege, PhD, is an ***Associate Professor with the Department of Criminal Justice at Temple University, USA***. She holds a PhD and MA in Criminal Justice, an MA and BA in Criminology, and a BS in Computer Science. She has been researching proactive cybersecurity in the context of cybercrimes against critical infrastructures for over 10 years. Specifically, her National Science Foundation funded research projects examine adversarial and defender behavior, decision-making, adaptations, modus operandi, and group dynamics. Dr. Rege's work employs qualitative approaches of observing real-time cybersecurity exercises to understand the behavior of adversaries and defenders. She intersects theoretical frameworks and methodologies from criminology with hard science approaches (time series analysis, graph theory, simulations, and machine learning) to foster innovative and multidisciplinary proactive cybersecurity research. Dr. Rege's has been published in the Journal of Information Warfare, Journal of Homeland Security and Emergency Management, the Security Journal, and the IEEE Intelligent Systems. She is also passionate about educating the next generation workforce across the social and hard sciences about the relevance of the human factor in cybersecurity.

Jean-Jacques Sahel

Jean-Jacques Sahel – Managing Director, Europe, ICANN

Jean-Jacques Sahel, ***Managing Director, Europe, ICANN***, has been involved in international government and regulatory affairs for over 15 years in both the private and government sectors. He was appointed Managing Director of ICANN's Brussels office in July 2017 to lead the organisation's corporate strategy and coordinate its operations across the European region. Since 2014 he has led ICANN's strategic plan for outreach, support and engagement with governments, private sector and user groups throughout Europe, and worldwide for civil society. Before joining ICANN, Mr Sahel headed government and regulatory affairs for Skype, then digital policy at Microsoft for the Europe, Middle-East & Africa regions. He had started his career in the City of London, before spending several years in the UK Government, leading in particular its international telecommunications policy.

Ex officio, Mr Sahel has chaired the UK Chapter of the International Institute of Communications (IIC) since 2009 and was a member of OSAB, the Spectrum Advisory Board of UK communications regulator Ofcom for 2 terms until 2016. He has authored articles and research in both mainstream media and academic publications particularly on Internet policy and governance.

Professor Mike Hinchey

Professor Mike Hinchey – Chair, IEEE UK & Ireland, and President, IFIP

Professor Mike Hinchey is ***Chair of IEEE UK & Ireland Section for 2018-2019***. He is President of IFIP, the International Federation for Information Processing (www.ifip.org) and is Emeritus Director of Lero-the Irish Software Research Centre and Professor of Software Engineering at University of Limerick, Ireland. Prior to joining Lero, Professor Hinchey was the Director of the NASA Software Engineering Laboratory. In 2009, he was awarded NASA's Kerley Award as Innovator of the Year and is recognized in the NASA Inventors Hall of Fame. Professor Hinchey holds a B.Sc. in Computer Systems from University of Limerick, an M.Sc. in Computation from University of Oxford and a PhD in Computer Science from University of Cambridge. Professor Hinchey is a Chartered Engineer, Chartered Engineering Professional, Chartered Mathematician and Charted Information Technology Professional, as well as a Fellow of the IET, British Computer Society and Irish Computer Society. He is Editor-in-Chief of Innovations in Systems and Software Engineering: a NASA Journal and Journal of the Brazilian Computer Society. In January 2018, he became an Honorary Fellow of the Computer Society of India.

John Crain – Chief Security, Stability & Resiliency Office, ICANN

John Crain

John Crain is ***Chief Security, Stability & Resiliency Office*** at *The Internet Corporation for Assigned Names and Numbers* (**ICANN**), responsible for establishing strategy, planning and execution for ICANN's external Security, Stability and Resiliency programs. He works on a cross functional basis with the ICANN executive team, staff and the community to enable and enhance capabilities that improve the overall security, stability and resiliency of the Internet's Identifier Systems and associated infrastructures and represents ICANN in operational and technical dialogues and forums to ensure the full communities' engagement with these programs.

Prior to his time at ICANN, John worked as part of the executive management team at the RIPE NCC in Amsterdam. The RIPE NCC is the Regional Internet Registry (RIR) that provides Internet resource allocations for Europe and surrounding areas. John has been directly involved in the administration of Internet Identifiers since his start at the RIPE NCC in 1995 and has worked in all areas of IP address administration. John also has extensive experience in the area of DNS administration and managing Internet infrastructure services. Currently he is responsible for the management of the L-Root server, one of the Internet's 13 "Root Servers". Before becoming involved in Internet Administration John worked as a Design Engineer in composite materials research and development. In that role John was also responsible for local area networking of Computer Aided Design Systems and for writing and developing custom software applications.

Ros Smith – Senior Product Manager in Identity and Access Management, BBC, UK

Ros Smith

Ros Smith, **Senior Product Manager**, **British Broadcasting Corporation (BBC)**, is relative newcomer to the world of Identity and Access Management (IAM). She has worked at the BBC for over 19 years. Until 2018 she worked on Production and Editorial side, having been a Radio Producer for Science Radio, Woman's Hour and The Big Toe Radio Show; Deputy Editor of the award winning BBC News School Report; Project Manager at BBC Media Action and most recently Acting Head of BBC Weather. She is now Senior Product Manager in Identity and Access Management, and has found a new found enthusiasm for the importance of IAM in the world... and has learnt more acronyms than she ever imagined possible.

Conference Chairs & Organisers

Dr Arnau Erola

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

Dr Arnau Erola is a cyber security researcher with strong background in data analytics, machine learning, data mining and information privacy. He is currently a Research Fellow at CyberSecurity@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.

Carolina Nogueira

Carolina Nogueira – Teaching Assistant and PhD Student, Distributed Computer Systems Group, Technische Universität Kaiserslautern, Germany

Carolina Nogueira is pursuing her PhD in the cyber-security field at TU Kaiserslautern. Her research focus is security in wireless communication for safety-critical embedded systems, and is part of a collaboration with armasuisse (Switzerland), where she was visiting researcher in 2018. She holds a M.Sc. in Electrical Engineering from the same university, and in 2016 she was awarded with the DAAD-Prize for outstanding achievement of a foreign student, due to her high academic achievement, and social and intercultural engagement. In addition to her academic experience, she has many years of practical experience in the industry, including tech leader of the first level infrastructure incident management team for a multinacional ISP (responsible region Latin America and Spain), and development of testing support tools focused in GNSS and radio systems for Asia, Europe and USA.

Dr Xavier Bellekens

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

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 Virginia Franqueira

Dr Virginia N. L. Franqueira – Senior Lecturer, Department of Electronics, Computing & Mathematics, University of Derby, UK

Dr Franqueira received a Ph.D. in Computer Science (focused on Security) from the University of Twente (Netherlands) in 2009, and a M.Sc. in Computer Science (focused on Optimization) from the Federal University of Espirito Santo (Brazil). Since June 2014, she holds a senior lecturer position in Computer Security and Digital Forensics at the University of Derby, UK. She has around 40 publications related to Security or Digital Forensics. She is a member of the British Computer Society and fellow of The Higher Education Academy.

Dr Martin G. Jaatun

Dr Martin Gilje Jaatun – Senior Scientist, SINTEF Digital, Trondheim, Norway

Martin Gilje Jaatun is a Senior Scientist at SINTEF Digital in Trondheim, Norway. He graduated from the Norwegian Institute of Technology (NTH) in 1992, and received the Dr.Philos degree in critical information infrastructure security from the University of Stavanger in 2015. He is an adjunct professor at the University of Stavanger, and was Editor-in-Chief of the International Journal of Secure Software Engineering (IJSSE). Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include software security, security in cloud computing, and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org), vice chair of the IEEE Technical Committee on Cloud Computing (TCCLD), an IEEE Cybersecurity Ambassador, and a Senior Member of the IEEE. Most of his published papers are available here: http://jaatun.no/papers

Hanan Hindy

Hanan Hindy – PhD Student, Division of Cyber Security, Abertay University, Dundee, Scotland, UK

Hanan Hindy is a second year PhD student at the Division of Cyber-Security at Abertay University, Dundee, Scotland, UK. Hanan received her bachelor with honours (2012) and masters (2016) degrees in Computer Science from the Faculty of Computer and Information Sciences at Ain Shams University, Cairo, Egypt.

Her research interests include Machine Learning and Cyber-Security. Currently, she is working on utilizing Deep Learning for Intrusion Detection Systems (IDS). https://hananhindy.com

Dr Thaddeus Eze

Dr Thaddeus Eze – Senior Lecturer Cyber Security, Department of Computer Science, University of Chester, UK

Thaddeus is a 2004 graduate of Anambra State University, Nigeria, with BSc (Upper 2nd Class) in Computer Science. He got a Diploma in Computer Networking and Management (with distinction) in 2006. He obtained his MSc (with distinction) in Mobile Computing and Communications in 2010 and his PhD in Trustworthy Autonomic Computing in 2014, both from the University of Greenwich, London. He is currently a Senior Lecturer in Cyber Security at the University of Chester. His research interests include Trustworthy Autonomics, MANET and Cyber Security (specifically, Return Oriented Programming, Policing the Cyber Threat and Cyber Education) and he has a number of publications in these areas.

Professor Fatih Kurugollu

Professor Fatih Kurugollu – Professor of Cyber Security, Department of Electronics, Computing and Mathematics, University of Derby, UK

Fatih Kurugollu obtained BSc and MSc in Computer and Control Engineering degree from Istanbul Technical University, Turkey, in 1989 and 1994, respectively. He was awarded with a PhD degree in Computer Engineering from the same university in 2000. He was employed as a research fellow by the Marmara Research Centre, which is the main governmental research unit of the Turkish Scientific Research Council (TUBITAK) in 1991. He joined the School of Electronics, Electrical Engineering and Computer Science at Queen's University, Belfast, in 2000, initially as a Post-Doctoral Research Fellow. In 2003, he was appointed to a lectureship at the same department and later on was promoted to Senior Lecturer in Computer Science. He is now a full Professor of Cyber Security at University of Derby.

His current research interests are centred around Security and Privacy in Internet-of-Things, Cloud Security, Imaging for Forensics and Security, Security related Multimedia Content Analysis, Big Data in Cyber Security, Homeland Security, Security Issues in Healthcare Systems, Biometrics, Image and Video Analysis.

He has been principal investigator and co-investigator of several projects funded by EPSRC, Royal Academy Engineering (RAEng), Leverhulme Trust, Action Medical Research as well as principal supervisor of KTP projects. He has supervised 11 PhD projects and he has authored more than 130 publications. He is Senior Member of IEEE, Member of Associate College of Engineering and Physical Sciences Research Council (EPSRC), Fellow of the Higher Education Academy (HEA), Voting member of IEEE Communication Society Multimedia Communications Technical Committee and Affiliate member of IEEE Signal Processing Society Information Forensics and Security Technical Committee.

Dr Cyril Onwubiko – Secretary, IEEE UK & Ireland and Chair, IEEE UK & Ireland Blockchain Group

Dr Cyril Onwubiko

Dr Cyril Onwubiko is the Secretary – IEEE UK & Ireland, Chair, IEEE UK & Ireland Blockchain Group, and Director, Cyber Security 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, Machine Learning, Data Fusion, Intrusion Detection Systems and Computer Network Defence. He has authored several books including "Security Framework for Attack Detection in Computer Networks" and "Concepts in Numerical Methods.", and edited several books including "Situational Awareness in Computer Network Defense: Principles, Methods & Applications".

Accepted Papers, Extended Abstracts & Posters

Cyber Science 2019 Accepted Papers

MANiC: Multi-step Assessment for Crypto-miners

Jonah Burgess, Domhnall Carlin, Philip O'Kane and Sakir Sezer
Centre for Secure Information Technologies, Ireland, UK

Abstract: Modern Browsers have become sophisticated applications that provide a portal to the web. Browsers host a complex mix of interpreters such as HTML and JavaScript which allow the user's browser to perform malicious activities, this threat is known as browser-hijacking. These types of attacks can be particularly difficult to detect as they usually operate within the scope of normal browser behaviour. CryptoJacking is a form of browser-hijacking which has emerged as a result of the increased popularity and profitability of cryptocurrencies and the introduction of new cryptocurrencies that promote CPU-based mining. This paper proposes MANiC (Multi-step AssessmeNt for Crypto-miners); a system to detect CryptoJacking websites. It uses regular expressions compiled in accordance with the API structure of different miner families to detect crypto-mining scripts and extract parameters that could be used to detect suspicious behaviour associated with CryptoJacking. When MANiC was used to analyse the Alexa top 1m websites, it detected 887 malicious URLs containing miners from 11 different families and demonstrated strong results when compared to related CryptoJacking research. We propose that MANiC can be used to provide insights into this new threat, identify new potential features of interest and establish a ground-truth dataset to assist future research.

Efficient and Interpretable Real-Time Malware Detection Using Random-Forest

Alan Mills, Theodoros Spyridopoulos and Phil Legg
Department of Computer Science and Creative Technologies, The University of the West of England, Bristol, UK

Abstract: Malicious software, often described as malware, is one of the greatest threats to modern computer systems, and attackers continue to develop more sophisticated methods to access and compromise data and resources. Machine learning methods have potential to improve malware detection both in terms of accuracy and detection runtime, and is an active area within academic research and commercial development. Whilst the majority of research focused on improving accuracy and runtime of these systems, to date there has been little focus on the interpretability of detection results. In this paper, we propose a lightweight malware detection system called NODENS that can be deployed on affordable hardware such as a Raspberry Pi. Crucially, NODENS provides transparency of output results so that an end-user can begin to examine why the classifier believes a software sample to be either malicious or benign. Using an efficient Random-Forest approach, our system provides interpretability whilst not sacrificing accuracy or detection runtime, with an average detection speed of between 3-8 seconds, allowing for early remedial action to be taken before damage is caused.

Destructive Attacks Detection and Response System for Physical Devices in Cyber-Physical Systems

Peyman Kabiri[1] and Mahdieh Chavoshi[2]
[1]Sheffield Hallam University, Sheffield, UK
[2]Iran University Science & Technology, UK

Abstract: Nowadays, physical health of equipment controlled by Cyber-Physical Systems (CPS) is a significant concern. However, there are few researches reported in this area. This paper reports a work, in which, a hardware is placed between Programmable Logic Controller (PLC) and the Actuator as a solution. The proposed hardware operates in two conditions, i.e. passive and active. Operation of the proposed solution is based on the repetitive operational profile of the actuators. The normal operational profile of the actuator is fed to the protective hardware and is considered as the normal operating condition. In the normal operating condition, the middleware operates in its passive mode and simply monitors electronic signals passing between PLC and Actuator. In case of any malicious operation, the proposed hardware operates in its active mode and both slowly stops the actuator and sends an alert

to SCADA server initiating execution of the actuator's emergency profile. Thus, the proposed hardware gains control over the actuator and prevents any physical damage on the operating devices. Two sample experiments are reported in which, results of implementing the proposed solution are reported and assessed. Results show that once the PLC sends incorrect data to actuator, the proposed hardware detects it as an anomaly. Therefore, it does not allow the PLC to send incorrect and unauthorized data pattern to its actuator. Significance of the paper is in introducing a solution to prevent destruction of physical devices apart from source or purpose of the encountered anomaly and apart from CPS functionality or PLC model and operation.

Big Social Data - Predicting Users' Interests from their Social Networking Activities

Alexiei Dingli and Bernhardt Engerer
Department of AI, Faculty of ICT, University of Malta, Malta

Abstract: The amount of data produced by Social Network users, whether through direct content creation or as a by-product of their Social Network usage, is ever increasing. This research presents an approach to predicting unknown user interest in entities based on Entity Extraction from User Generated Content and through the use of a Potential Link Prediction algorithm for recommendations. An algorithm was developed which is able to extract relevant entities from the microtext forming the metadata of Facebook pages liked by a user. These entities are then used in order to suggest other potentially interesting pages to the user. Additionally, crowd-sourced knowledge is used in order to automatically filter out entities which are likely to be irrelevant to future users based on past ratings. Using these filtered entities and by having at least 10 interests disclosed by a user, it is possible to predict further entities of interest to a user, with at least 80% confidence in the predictions.

Forensic Readiness within the Maritime Sector

Kimberly Tam and Kevin Jones
Plymouth University, UK

Abstract: Forensic investigation is an essential response strategy following a cyber-related incident, and forensic readiness is the capability to gather critical digital information and maximize its use as evidence. The effectiveness of this data is highly dependent on the readiness, quality, and trustworthiness of the data itself. Far from a passive post-analysis tool, there have been many instances where an organization has benefited from gathering, and using, digital evidence to improve their cyber-security and mitigate future incidents. This article examines the forensic readiness of the maritime sector, a core component of global trade and a unique combination of information/operational technology and people, to understand its investigation and mitigation capabilities. Once the readiness of maritime forensic investigation has been better understood, by comparing it to other sectors and using risk scenarios, this paper proposes actions toward improvement. These steps are built from established attempts to increase investigation capabilities and improve maritime cybersecurity, but address the maritime sector specifically.

A cost-efficient Protocol for Open Blockchains

Chunlei Li[1], Chunming Rong[2] and Martin Gilje Jaatun[2]
[1]Daeprtment of Informatics, University of Bergen, Bergen, Norway
[2]Dept. of Electrical Engineering and Computer Science, University of Stavanger, Stavanger, Norway

Abstract: Current proof-of-work blockchains are not sustainable in terms of energy needed to run them. In this paper we propose a new scheme that avoids wasted proof-of-work by a dynamic probabilistic method, where the consensus algorithm can be adjusted according to the parties' required assurance levels.

Factors Affecting Cyber Risk in Maritime

Kimberly Tam and Kevin Jones
Plymouth University, UK

Abstract: To ensure the safety of ships and ports, groups and individuals, at all levels of the maritime sector, use analysis to identify potential hazards and their outcomes. One of the most relied upon methods is using a risk

assessment tool to define and prioritise threats. A disadvantage of most existing assessment frameworks, however, is their inability to update risks dynamically as factors, such as the environment, change. In the maritime sector, a range of dynamic factors is needed to measure risks, but most conventional frameworks are unable to use them to revise and update their risk profiles. In addition to static and dynamic, maritime operational risks can be affected by elements classified as cyber, cyber-physical, or physical in nature. This demonstrates the relatively equal presence of information and operational technology (i.e. IT/OT) used, however most quantitative risk assessment frameworks are normally limited to one or the other. This article explores the full range of cyber-related risk factor types within maritime in order to evaluate applicable risk frameworks and suggest improvements that could help each of those tools assess maritime-cyber risks specifically.

Keystroke Dynamics using Auto Encoders

Yogesh Patel[1], Karim Ouazzane[2], Vassil Vassilev[2], Ibrahim Faruqi[2] and George Walker[2]
[1]Callsign, London, UK
[2]London Metropolitan University, London, UK

Abstract: In the modern day and age, credential based authentication systems no longer provide the level of security that many organisations and their services require. The level of trust in passwords has plummeted in recent years, with waves of cyber attacks predicated on compromised and stolen credentials. This method of authentication is also heavily reliant on the individual user's choice of password. There is the potential to build levels of security on top of credential based authentication systems, using a risk based approach, which preserves the seamless authentication experience for the end user. One method of adding this security to a risk based authentication framework, is keystroke dynamics. Monitoring the behaviour of the users and how they type, produces a type of digital signature which is unique to that individual. Learning this behaviour allows dynamic flags to be applied to anomalous typing patterns that are produced by attackers using stolen credentials, as a potential risk of fraud. Methods from statistics and machine learning have been explored to try and implement such solutions. This paper will look at an Autoencoder model for learning the keystroke dynamics of specific users. The results from this paper show an improvement over the traditional tried and tested statistical approaches with an Equal Error Rate of 6.51%, with the additional benefits of relatively low training times and less reliance on feature engineering.

A Comparison of Machine Learning Approaches for Detecting Misogyny Speech in Urban Dictionary

Theo Lynn[1], Patricia Takako Endo[1], Pierangelo Rosati[1], Ivanovitch Silva[2], Guto Leoni[3] and Debbie Ging[4]
[1]Irish Institute of Digital Business, Dublin City University, Ireland
[2]Digital Metropolis Institute, Federal University of Rio Grande do Norte, Natal, Brazil
[3]Universidade Federal de Pernambuco, Recife, Brazil
[4]Institute for Future Media and Journalism, Dublin City University, Ireland

Abstract: Recent moves to consider misogyny as a hate crime have refocused efforts for owners of web properties to detect and remove misogynistic speech. This paper considers the use of deep learning techniques for detection of misogyny in Urban Dictionary, a crowdsourced online dictionary for slang words and phrases. We compare the performance of two deep learning techniques, Bi-LSTM and Bi-GRU, to detect misogynistic speech with the performance of more conventional machine learning techniques, logistic regression, Naive-Bayes classification, and Random Forest classification. We find that both deep learning techniques examined have greater accuracy in detecting misogyny in the Urban Dictionary than the other techniques examined.

Examining the Roles of Muhajirahs in the Islamic State via Twitter

Aunshul Rege and Scott Vanzant
Department of Criminal Justice, Temple university, USA

Abstract: This qualitative study examines the experiences and roles of Western migrant women, muhajirahs, after their arrival to the Islamic State through their Twitter discourse. A total 763 tweets, from 2014 to 2016, were analyzed. This study found that IS women encouraged identity, sisterhood, and oneness; offered recruitment and migration information; and promoted IS ideology and celebrated violence. The muhajirahs were also highly tech-savvy,

exhibited regenerative traits to maintain their online presence, and were well-versed in the use of secure communications as an alternate to Twitter. While these women embraced the IS ideology, their language, cultural memes, food, and social habits indicated that they still subscribed to western ideologies and influence. Finally, these muhajirahs experienced several hardships, such as cultural alienation, differential treatment, freedom and movement restrictions, and some even expressed a desire to return. This paper also discusses the dualities and contradiction in the muhajirahs' twitter discourses. The paper concludes by making a case for the relevance of qualitative research in an era of big data; and how the former can (and should) inform big data research.

Cyber Onboarding is 'Broken'

Cyril Onwubiko[1,2] and Karim Ouazzane[2]
[1]Cyber Security Intelligence, E-Security, Research Series, London, UK
[2]Cyber Security Research Centre (CSRC), London Metropolitan University, London, UK

Abstract: Cyber security operations centre (CSOC) is a horizontal business function responsible primarily for managing cyber incidents, in addition to cyber-attack detection, security monitoring, security incident triage, analysis and coordination. To monitor systems, networks, applications and services the CSOC must first on-board the systems and services onto their security monitoring and incident management platforms. Cyber Onboarding (a.k.a. Onboarding) is a specialist technical process of setting up and configuring systems and services to produce appropriate events, logs and metrics which are monitored through the CSOC security monitoring and incident management platform. First, logging must be enabled on the systems and applications, second, they must produce the right set of computing and security logs, events, traps and messages which are analysed by the detection controls, security analytics systems and security event monitoring systems such as SIEM, and sensors etc.; and further, network-wide information e.g. flow data, heartbeats and network traffic information are collected and analysed, and finally, threat intelligence data are ingested in real-time to detect, or be informed of threats which are out in the wild. While setting up a CSOC could be straightforward, unfortunately, the 'people' and 'process' aspects that underpin the CSOC are often challenging, complicated and occasionally unworkable. In this paper, CSOC and Cyber Onboarding are thoroughly discussed, and the differences between SOC vs SIEM are explained. Key challenges to Cyber Onboarding are identified through the reframing matrix methodology, obtained from four notable perspectives – Cyber Onboarding Perspective, CSOC Perspective, Client Perspective and Senior Management Team Perspective. Each of the views and interests are discussed, and finally, recommendations are provided based on lessons learned implementing CSOCs for many organisations – e.g. government departments, financial institutions and private sectors.

Does the NIS implementation strategy effectively address cyber security risks in the UK?

Meha Shukla, Shane Johnson and Peter Jones
University College London (UCL), London, UK

Abstract: This research explored how cyber security risks are managed across UK Critical National Infrastructure (CNI) sectors following implementation of the 2018 Networks and Information Security (NIS) legislation. Being in its infancy, there has been limited study into the effectiveness of this national framework for cyber risk management. The analysis of data gathered through interviews with key stakeholders against the NIS objectives indicated a collaborative implementation approach to improve cyber-risk management capabilities in CNI sectors. However, more work is required to bridge the gaps in the NIS framework to ensure holistic security across cyber spaces as well as non-cyber elements: cyber-physical security, cross-sector CNI service security measures, outcome-based regulatory assessments and risks due to connected smart technology implementations alongside legacy systems. This research proposes ten key recommendations to counter the danger of not meeting the NIS key strategic objectives. In particular, it recommends that the approach to NIS implementation needs further alignment with its objectives, such as bringing a step-change in the cyber-security risk management capabilities of the CNI sectors.

Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation

Erik Moore, Steven Fulton, Roberta Mancuso, Tristen Amador and Dan Likarish
College of Computer and Information Sciences, Regis University, Denver, Colorado, USA

Abstract: In the United States, the State of Colorado's Department of Transportation successfully defended and recovered from a recent severe malware attack. The 2018 attack at the Colorado Department of Transportation was mitigated by a rapid multi-agency incident response. This is the first case in the United States where a state's National Guard responded to a governor's declaration of a cyber emergency response. In anticipation of advanced threats to Colorado citizens, Regis University has hosted collaborative exercises with government, organizations, and industry as part of a larger Collaborative Training Response Community (CTRC) effort to facilitate collaborative physical exercises, governmental policy development, and relationship building. The resulting capabilities allowed for an effective response to this incident. The authors present a new incident response model, based on this case in the context of existing cybersecurity organizations extant in the U.S., that may be useful to private and public sector communities where collaborative incident response is appropriate.

Online Anomaly Detection of Time Series at Scale

Andrew Mason[1], Yifan Zhao[1], Hongmei He[1], Raymon Gompelman[2] and Srikanth Mandava[2]
[1]Manufacturing Department, Cranfield University, Cranfield, UK
[2]iDirect, Cranfield, UK

Abstract: Cyber breaches can result in disruption to business operations, reputation damage as well as directly affecting the financial stability of the targeted corporations, with potential impacts on future profits and stock values. Automatic network-stream monitoring becomes necessary for cyber situation awareness, and time-series anomaly detection plays an important role in network stream monitoring. This study surveyed recent research on time-series analysis methods in respect of parametric and non-parametric techniques, and popular machine learning platforms for data analysis on streaming data on both single server and cloud computing environments. We believe it provides a good reference for researchers in both academia and industry to select suitable (time series) data analysis techniques, and computing platforms, dependent on the data scale and real-time requirements.

Domain Identification for Commercial Intention-holding Posts on Twitter

Yuanyuan Zhu[1], Mee Chi So[1] and Paul Harrigan[2]
[1]Southampton Business School, University of Southampton, UK
[2]University of Western Australia, Perth, Australia

Abstract: Today, more people use social networking platforms to convey their desires and recent needs. Actually, there are numerous daily posts carrying commercial intention. The detection of these kinds of user intention would be quite valuable, especially for the platform itself. Firstly, it could help the platform provide precise and instant recommendations to users for its own business interests. Secondly, intention mining works may help link users' needs by detecting potential buyers and sellers and their specific intentions which can benefit users by optimizing the resources in their hand and increase functional richness.
The whole intention mining process generally includes three main stages: user commercial intention filtering, intention domain identification and specific intention words extraction. In this work, the first stage was simplified using keywords-based automatic filter followed by a manual screening. The main focus of this paper is the second stage, assigning the intention-holding posts into their own single domain. Three machine learning models and two deep learning models were proposed to solve this text classification problem. The proposed methods have been evaluated on a dataset containing 5500 real-time intention-holding tweets collected from Twitter. In general, the experimental results showed impressive performance with the highest classification accuracy of 96% achieved by Long short-term memory.

Adaptive and Intelligible Prioritization for Network Security Incidents

Leonard Renners[1], Felix Heine[1], Carsten Kleiner[1] and Gabi Dreo Rodosek [2]
[1]University of Applied Sciences and Arts Hanover, Germany
[2]Universität der Bundeswehr München, Germany

Abstract: Incident prioritization is nowadays a part of many approaches and tools for network security and risk management. However, the dynamic nature of the problem domain is often unaccounted for. That is, the prioritization is typically based on a set of static calculations, which are rarely adjusted. As a result, incidents are incorrectly prioritized, which leads to an increased and misplaced effort in the incident response. A higher degree of automation could help to address this problem. In this paper, we explicitly consider flaws in the prioritization an unalterable circumstance. As a result, we propose an adaptive incident prioritization, which allows to automate certain tasks for the prioritization model management in order to continuously assess and improve a prioritization model. At the same time, we acknowledge the human analyst as the focal point and propose to keep the human in the loop, among others by treating understandability as a crucial requirement.

Security awareness escape room - a possible new method in improving security awareness of users

Eszter Diána Oroszi
National University of Public Services, Budapest

Abstract: Security awareness escape room is a new method of security awareness improvement. This program uses gamification elements to highlight information security risks and problems for users, for example bad habits of employees which could be exploited by a possible attacker. According to my experiences, users like the “learning-by-experience” better than classroom trainings, presentations or even online courses, because in this case participants can identify their own weaknesses and change their daily practices.

Threat Modeling of Connected Vehicles: A privacy analysis and extension of vehicleLang

Wenjun Xiong and Robert Lagerström
KTH Royal Institute of Technology, Sweden

Abstract: Modern vehicles contain more than a hundred Electronic Control Units (ECUs) that communicate over different in-vehicle networks. These ECUs are often connected to the Internet, which makes them vulnerable to various cyber attacks. Besides, large amounts of data are generated and communicated through vehicular networks, and some of them are sensitive for the vehicle drivers. Previously, a threat modeling language named vehicleLang was proposed for security analysis of vehicles, however, privacy issues of the vehicular data have not been thoroughly addressed. To fill the gap, this paper proposes a privacy-focused enhancement of vehicleLang, and the suggested privacy extension is evaluated by threat modeling with test cases running through the Meta Attack Language (MAL) compiler.

Ethereum Blockchain for Securing the Internet of Things: Practical Implementation and Performance Evaluation

Subhi Alrubei, Jonathan Rigelsford, Callum Willis and Edward Ball
The University of Sheffield, Sheffield, UK

Abstract: Blockchain technology is a distributed database "distributed ledger" and offers features such as autonomous, decentralisation and a trustless environment. These features make blockchain suitable to be applied to different applications within the Internet of Things (IoT) realm. This paper provides a practical implementation of Proof of Authority (PoA) Ethereum blockchain on an IoT system in a real-world use case. This implementation was practically accomplished in order to investigate and highlight some of the possible problems and issues that could affect the integration of blockchain with IoT, to lay the ground for future research and possible solutions to these issues.

Brexit Impact on Cyber Security of United Kingdom

Muntaha Saleem
Queen Mary University of London, London, UK

Abstract: In 2017, cyber-attacks alone cost UK businesses £32.2 million. Cyber security is laced with various key social, political and economic challenges of the 21st century. The attack on UK health services, NHS, last year signifies that there is a strong need to focus on improving cyber defence of the country. With Brexit in view, it is imperative to understand its impacts on UK's cyber security. The cyber defence military relations of UK will remain same with Five Eyes and NATO. But the cyber security industry could be affected by Brexit in various ways. Moreover, Brexit could also affect government's cyber laws and policies. In the midst of Brexit negotiations, UK and EU should not forget their mutual interest and focus on maintaining efficient and effective cyber security system, as their nation's stability relies on it.

Pattern discovery in intrusion chains and adversarial movement

Nima Asadi, Aunshul Rege and Zoran Obradovic
Computer and Information Sciences, Temple University, Philadelphia, USA

Abstract: Capturing the patterns in adversarial movement can present crucial insight into team dynamics and organization of cybercrimes. This information can be used for additional assessment and comparison of decision-making approaches during cyberattacks. In this study, we propose a data-driven analysis based on time series analysis and social networks to identify patterns and alterations in time allocated to intrusion stages and adversarial movements. The results of this analysis on two case studies of collegiate cybersecurity exercises is provided as well as an analytical comparison of their behavioral trends and characteristics. This paper presents preliminary insight into complexities of individual and group level adversarial movement and decision-making as cyberattacks unfold.

Organizational formalization and employee information security behavioral intentions based on an extended TPB model

Yuxiang Hong[1] ***and Steve Furnell***[2,3,4]
[1]Hangzhou Dianzi University, Hangzhou, China
[2]University of Plymouth, United Kingdom
[3]Edith Cowan University, Australia
[4]Nelson Mandela University, South Africa

Abstract: Information security is a worldwide problem, and the psychological and behavioral factors of users are some of the most important reasons for the occurrence of information security incidents. Although many previous studies have discussed the influencing factors of information security behaviors, few have considered the impacts of organizational structures. In this study, the formation mechanism of information security behavioral intention was studied by integrating the Theory of Planned Behavior (TPB) and organizational formalization. Data analysis was performed using the Structural Equation Model (SEM) analysis, based on a survey of 261 company employees. The empirical results showed that organizational formalization had significant effect on cognitive processes theorized by TPB, and TPB was still applicable to predict and explain the information security behavioral intention. This study suggests that more formalized rules, procedures, and communications should be designed in order to increase employees' information security behavioural intentions.

Towards a Conversational Agent for Threat Detection in the Internet of Things

Christopher McDermott and John Isaacs
Robert Gordon University, Scotland

Abstract: A conversational agent to detect anomalous traffic in consumer IoT networks is presented. The agent accepts two inputs in the form of user speech received by Amazon Alexa enabled devices, and classified IDS logs stored in a DynamoDB Table. Aural analysis is used to query the database of network traffic, and respond accordingly. In doing so, this paper presents a solution to the problem of making consumers situationally aware when their IoT devices are infected, and anomalous traffic has been detected. The proposed conversational agent

addresses the issue of how to present network information to non-technical users, for better comprehension, and improves awareness of threats derived from the *mirai* botnet malware.

A Scalable Attribute Based Encryption for Secure Data Storage and Access in Cloud

Kamalakanta Sethi, Ankit Pradhan, Punith. R and Padmalochan Bera
Indian Institute of Technology Bhubaneswar, India

Abstract: Today a large volume of data is stored in cloud that requires fine grained accessibility for heterogeneous users. Ciphertext policy attribute based encryption (CP-ABE) has evolved into a promising solution for secure data storage with fine grained access control. In CP-ABE, the ciphertext is associated with an access policy (set of rules) and users can access the data if their attributes satisfies the access policy. However, existing CP-ABE schemes fail to perform in presence of large number of users and hierarchical relationships among them. Moreover, a majority of the CP-ABE schemes require large computational overhead for light weight applications. In this paper, we present a hierarchical attribute based cryptosystem by introducing hierarchical dependency between the users and thereby achieving multi-layer verification for fine grained data access. Moreover, our proposed cryptosystem is seamless to user revocation. The efficiency and security of our proposed cryptosystem have been analyzed and reported. Further we implement the proposed cryptosystem in Charm to demonstrate its practicality.

A Social Engineering Course Project for Undergraduate Students Across Multiple Disciplines

Aunshul Rege, Katorah Williams and Alyssa Mendlein
Computer and Information Sciences, Temple University, Philadelphia, USA

Abstract: Social engineering is defined as any act that influences individuals to take an action that may or may not be in their best interests. In fact, social engineering is a key tactic used in the reconnaissance stage of cyberattacks, a stage that takes up roughly 50-75% of the overall attack. Yet, social engineering education in the undergraduate curriculum is limited. This paper shares a social engineering project developed for an undergraduate course that caters to students across multiple disciplines. It details the project design and implementation across two semesters, and also shares student and educator experiences and lessons learned.

A Novel Method to Prevent Phishing by using OCR Technology

Yunjia Wang and Ishbel Duncan
University of St Andrews, UK

Abstract: Phishing is one of the most common attacks in the world, especially with the increasing usage of mobile platforms and e-commerce. Although many users are weary of phishing attacks from suspicious paths in the URL address, phishing still accounts for a large proportion of all of malicious attacks as it is easy to deploy. Most browser vendors mainly adopt two approaches against phishing; the blacklist and the heuristicbased. However, both have related limitations.
In this paper, a novel method was proposed to protect against phishing attacks. By using image recognition (OCR) technology, phishing attacks can be distinguished from the actual website by reading the logos on the website and comparing with the site URL. An easy to implement prototype demonstrated a high accuracy of detection in the experimental trials.

Arithmetic Circuit Homomorphic Encryption and Multiprocessing Enhancements

Ruitao Kee, Jovan Sie, Rhys Wong and Chern Nam Yap
Cyber & Digital Security, Temasek Polytechnic, Singapore

Abstract: This is a feasibility study on homomorphic encryption using the TFHE library in daily computing using cloud services. A basic set of arithmetic operations namely - addition, subtraction, multiplication and division were created from the logic gates provide. This research peeks into the impact of logic gates on these operations such as latency of the gates and the operation itself. Multiprocessing enhancement were done for multiplication operation using MPI and OpenMP to reduce latency.

Analysis of Obfuscated Code with Program Slicing

Mahin Talukder[1], Syed Islam[2] and Paolo Falcarin[1]
[1]University of East London, London, UK
[2]University College London, London, UK

Abstract: In Man-At-The-End (MATE) attacks, the user is the attacker having full control over the device, and they are able to violate intellectual property by means of malicious reverse engineering, software piracy, and software tampering. Obfuscation is a technique that is widely adopted by developers to mitigate this problem. Obfuscation increases the complexity of software code by obscuring the structure of code and data in order to thwart the reverse engineering process. However, it is possible to reverse engineer obfuscated code with hard determination and the right tools, but it is very time-consuming. Resilience of obfuscated code is the percentage of obfuscated code that is not removed by automated de-obfuscation tools, and it is usually considered an empirical method to assess the strength of obfuscated code. In this paper, we introduce a novel approach to measure the resilience of obfuscated C code using program slicing. Given a variable of interest, that might be part of a code region used to manipulate the crypto key or license number, program slicing can mimic the attacker behaviour by trying to remove the code unrelated to that variable, acting as a new type of de-obfuscator.

BATSense: Anomalous Security-Event Detection using TBATS Machine Learning

Pranshu Bajpai, Tyler Olsen, Seth Edgar, Rob McCurdy and Richard Enbody
Michigan State University, USA

Abstract: The BATSense anomaly detection methodology has been running in a large university (~50k students) successfully detecting anomalies across ~300k devices for a year. We use machine learning, specifically the TBATS forecasting algorithm, to predict future trends for the number of events per second for a variety of device types. The forecasted values are compared against actual observations to alert security personnel of significant deviations. Anomalies are detected based on logs relevant to security events; they may be a system change, a system failure or a football game. Forecasts are never perfect, but when measured over 51 days of use we have shown that false positives can be manageable (1 per week) for true positives of 1 per day. The result is a methodology that is useful to security personnel because the detected anomalies are based on logs of interest to them.

Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators

Florian Skopik and Stefan Filip
AIT Austrian Institute of Technology, Austria

Abstract: The timely exchange of information on new threats and vulnerabilities has become a cornerstone of effective cyber defence in recent years. Especially national authorities increasingly assume their role as information brokers through national cyber security centres and distribute warnings on new attack vectors and vital recommendations on how to mitigate them. Although many of these initiatives are effective to some degree, they also suffer from severe limitations. Many steps in the exchange process require extensive human involvement to manually review, vet, enrich, analyse and distribute security information. Some countries have therefore started to adopt distributed cyber security sensor networks to enable the automatic collection, analysis and preparation of security data and thus effectively overcome limiting scalability factors. The basic idea of IoC-centric cyber security

sensor networks is that the national authorities distribute Indicators of Compromise (IoCs) to organizations and receive sightings in return. This effectively helps them to estimate the spreading of malware, anticipate further trends of spreading and derive vital findings for decision makers. While this application case seems quite simple, there are some tough questions to be answered in advance, which steer the further design decisions: How much can the monitored organization be trusted to be a partner in the search for malware? How much control of the scanning process should be delegated to the organization? What is the right level of search depth? How to deal with confidential indicators? What can be derived from encrypted traffic? How are new indicators distributed, prioritized, and scan targets selected in a scalable manner? What is a good strategy to re-schedule scans to derive meaningful data on trends, such as rate of spreading? This paper suggests a blueprint for a sensor network and raises related questions, outlines design principles, and discusses lessons learned from small-scale pilots.

Security-Related Stress: A Perspective on Information Security Risk Management

Martin Lundgren and Erik Bergström
Luleå University of Technology, University of Skövde, Sweden

Abstract: In this study, the enactment of information security risk management by novice practitioners is studied by applying an analytical lens of security-related stress. Two organisations were targeted in the study using a case study approach to obtain data about their practices. The study identifies stressors and stress inhibitors in the ISRM process and the supporting ISRM tools and discusses the implications for practitioners. For example, a mismatch between security standards and how they are interpreted in practice has been identified. This mismatch was further found to be strengthened by the design of the used ISRM tools. Those design shortcomings hamper agility since they may enforce a specific workflow or may restrict documentation. The study concludes that security-related stress can provide additional insight into security-novice practitioners' ISRM challenges.

What makes for effective visualisation in Cyber Situational Awareness for Non-Expert Users?

Fiona Carroll[1], Phil Legg[2] and Adam Chakof[2]
[1]CardiffMet University, Cardiff, Wales
[2]University of West of England, UK

Abstract: As cyber threats continue to become more prevalent, there is a need to consider how best we can understand the cyber landscape when acting online, especially so for non-expert users. Satellite navigation systems provide the de facto standard for many modern-day navigation tasks in the physical domain, so we consider the question of how one could navigate the online domain using similar concepts. In this paper, we study the design of a cyber sat nav for improving situational awareness of non-expert users. We focus on three core tasks: understanding where we are in cyber space, understanding how we got there, and understanding future states that we may traverse to. To support understanding, we explore the use of visualisation techniques to portray complex online activities in clear and engaging formats for non-expert users.

In wolf's clothing: Complications of threat emulation in contemporary cyber intelligence practice

Jd Work
Marine Corps University and Columbia University, USA

Abstract: The dramatic expansion of threat intelligence in private practice has created a challenging multi-stakeholder environment in which cyber incidents now play out, including incidents which are not hostile intrusion or attack but rather the simulated modeling of such events for the purposes of Red Team exercise and assessment. The increasing complications of the interactions between these legitimate functions, against the backdrop of evolving adversary capabilities and deception tactics, gives rise to a number of potential consequences - including degraded warning posture. Mature organizations' intelligence, digital forensics / incident response (DFIR), and threat emulation functions must be prepared to address these issues in the course of time sensitive crisis management.

Secure Chaotic Maps-based Authentication Scheme for Real-Time Data Access in Internet of Things

Wenting Li, Haibo Cheng and Ping Wang
Peking University, China

Abstract: User authentication plays an important role in generic IoT networks that prevents malicious parties from gaining access to various services offered by remote servers. As user-end IoT devices are typically resource-constrained, how to design secure and efficient multi-factor authentication schemes remains hard to tackle. Very recently, instead of using traditional asymmetric encryption algorithms such as RSA, ElGamal encryption, a number of attempts have been made to employ chaotic maps as building blocks to design multi-factor authentication schemes for IoT environments. In this paper, we first revisit two foremost chaotic maps based multi-factor user authentication schemes presented by Roy et al. and Truong et al., and show that, despite being armed with a formal security proof, none of them can achieve the essential goal of "truly multi-factor security". Besides, we find Roy et al.'s scheme fails to achieve the claimed feature of forward secrecy, while Truong et al.'s scheme suffers from stolen verifier attack and user anonymity violation attack. Further, we figure out how to fix these identified weaknesses and suggest an enhanced protocol with better security and reasonable efficiency. Security and efficiency analysis suggest that our scheme outperforms existing schemes and is practical for real applications of IoT environments.

A Preliminary Exploration of Uber Data as an Indicator of Urban Liveability

Aguinaldo Bezerra[1], Gisliany Alves[1], Ivanovitch Silva[1], Pierangelo Rosati[2], Patricia Takako Endo[2] and Theo Lynn[2]
[1]Digital Metropolis Institute, Federal Univ. of Rio G. do Norte, Brazil
[2]Irish Institute of Digital Business, Dublin City University, Ireland

Abstract: Urban liveability is a key concept in the New Urban Agenda (NUA) adopted by the United Nations (UN) in 2016. The UN has recognized that effective benchmarks and monitoring mechanisms are essential for the successful implementation of the NUA. However, the timely and cost-effective collection of objective international quality of life urban data remains a significant challenge. Urban liveability indexes are often complex, resource intensive and time consuming to collect, and as a result costly. At the same time, competing methodologies and agendas may result in subjective or non-comparable data. Historically, transit has been a central organizing factor around which communities have been built. This paper explores the use of Uber data as a simple real-time indicator of urban liveability. Using data from the Uber Ride Request (URR) API for the Brazilian city of Natal, our preliminary findings suggest that Uber Estimated Time to Arrive (ETA) data is strongly correlated with selected quality of life indicators at a neighborhood and region level. Furthermore, unlike other urban liveability indicators, our findings suggest that Uber ETA data is context-sensitive reflecting daily and seasonal factors thereby providing more granular insights. This preliminary study finds strong evidence that Uber data can provide a simple, comparable, low cost, international urban liveability indicator at both city and neighborhood level for urban policy setting and planning.

Longitudinal performance analysis of machine learning based Android malware detectors

Suleiman Yerima and Sarmadullah Khan
De Montfort University, UK

Abstract: This paper presents a longitudinal study of the performance of machine learning classifiers for Android malware detection. The study is undertaken using features extracted from Android applications first seen between 2012 and 2016. The aim is to investigate the extent of performance decay over time for various machine learning classifiers trained with static features extracted from date-labelled benign and malware application sets. Using date-labelled apps allows for true mimicking of zero-day testing, thus providing a more realistic view of performance than the conventional methods of evaluation that do not take date of appearance into account. In this study, all the investigated machine learning classifiers showed progressive diminishing performance when tested on sets of samples from a later time period. Overall, it was found that false positive rate (misclassifying benign samples as malicious) increased more substantially compared to the fall in True Positive rate (correct classification of malicious apps) when older models were tested on newer app samples.

Cyber KPI for Return on Security Investment

Cyril Onwubiko[1] and Austine Onwubiko[2]
[1]Cyber Security Intelligence, E-Security Group, Research Series Limited, London, UK
[2]School of Computing, Engineering & Physical Sciences, University of the West of Scotland (UWS) Scotland, UK

Abstract: Cyber security return on investment (RoI) or return on security investment (RoSI) is extremely challenging to measure. This is partly because it is difficult to measure the actual cost of a cyber security incident or cyber security proceeds. This is further complicated by the fact that there are no consensus metrics that every organisation agrees to, and even among cyber subject matter experts, there are no set of agreed parameters or metric upon which cyber security benefits or rewards can be assessed against. One approach to demonstrating return on security investment is by producing cyber security reports of certain key performance indicators (KPI) and metrics, such as number of cyber incidents detected, number of cyber-attacks or terrorist attacks that were foiled, or ongoing monitoring capabilities. These are some of the demonstrable and empirical metrics that could be used to measure RoSI. In this abstract paper, we investigate some of the cyber KPIs and metrics to be considered for cyber dashboard and reporting for RoSI.

Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management alignment

Abraham Althonayan and Alina Andronache
Brunel University, London, UK

Abstract: Rethinking organisations' risk resiliency against cyber risks has been found both successful and lacking because it is more challenging when organisations mirror past siloed approaches. In pursuit of effectiveness and resiliency, this paper examines the antecedents of Cybersecurity Management (CsM) to explore how siloed risk controls influence business effectiveness. At the same time, it explores the additional strengths in enhancing CsM through alignment with Enterprise Risk Management (ERM) to ensure that handling risk is proactively, strategically, and comprehensively managed. To explore the problem, this research commenced by considering both secondary and primary qualitative data to determine the current state of strategic foresight of organisations. The authors found evidence of a granular legacy, stranded in different security domains and siloed strategic approaches.

Towards Better Understanding of Cyber Security Information Sharing

Adam Zibak and Andrew Simpson
Department of Computer Science, University of Oxford

Abstract: There is an increased recognition of the importance of information sharing within cyber security. Nevertheless, and despite the widespread use of the term "information sharing", it is difficult to associate a precise meaning with it — not least because it is used to describe a range of different activities that are driven by a variety of goals. Furthermore, when it comes to distinguishing between the various forms of information-sharing efforts, there is evidence of a degree of inconsistency between stakeholders. In this paper we seek to understand the various definitions of cyber security information sharing; we also seek to develop a better categorisation of its different forms. In addition, we try to assess the extent to which practitioners are willing to engage in each of the derived categories. A literature review, combined with an online survey, were used to capture stakeholders' perspectives. We analyse the data with a view to establishing a more nuanced conceptualisation of information sharing. The hope is that our findings will have the potential to serve as a basis for future studies.

Cyber Security Supervision in the Insurance Sector: Smart Contracts and Chosen Issues

Remy Zgraggen
Financial Supervisory Authority, Liechtenstein & EPFL Lausane, Zurich, Switzerland

Abstract: There are still many open issues and questions concerning the supervision and the legal and regulatory assessment of cyber security issues in the insurance sector, especially regarding smart insurance contracts and similar issues. In the present case the focus shall be on the underlying legal framework in the European Union and in Switzerland, including the most relevant ordinances and circulars as well as public and private guidelines, followed

by an outlook and some general ideas how Brexit could potentially have an impact on the general recognition and acceptation of smart contracts within the legal and regulatory framework and the society in general.

A Combined Attack-Tree and Kill-Chain Approach to Designing Attack-Detection Strategies for Malicious Insiders in Cloud Computing

Adrian Duncan, Sadie Creese and Michael Goldsmith
Cybersecurity Centre, Department of Computer Science, University of Oxford, UK

Abstract: Attacks on cloud-computing services are becoming more prevalent with recent victims including Tesla, Aviva Insurance and SIM-card manufacturer Gemalto. The risk posed to organisations from malicious insiders is becoming more widely known about and consequently many are now investing in hardware, software and new processes to try to detect these attacks. As for all types of attack vector, there will always be those which are not known about and those which are known about but remain exceptionally difficult to detect - particularly in a timely manner. We believe that insider attacks are of particular concern in a cloud-computing environment, and that cloud-service providers should enhance their ability to detect them by means of indirect detection. We propose a combined attack-tree and kill-chain based method for identifying multiple indirect detection measures. Specifically, the use of attack trees enables us to encapsulate all detection opportunities for insider attacks in cloud-service environments. Overlaying the attack tree on top of a kill chain in turn facilitates indirect detection opportunities higher-up the tree as well as allowing the provider to determine how far an attack has progressed once suspicious activity is detected. We demonstrate the method through consideration of a specific type of insider attack - that of attempting to capture virtual machines in transit within a cloud cluster via use of a network tap, however, the process discussed here applies equally to all cloud paradigms.

TrapMP: Malicious Process Detection by Utilising Program Phase Detection

Zirak Allaf, Mo Adda and Alexander Gegov
University of Portsmouth, UK

Abstract: Hardware and software have failed to securely man-age the sensitive elements of cryptographic algorithms in computational environment due to memory contentions. This opened new opportunities for hackers to carry out side channel attacks on a system and steal sensitive data. Existing Side-channel attack techniques show that attackers can exploit the microarchitecture and OS vulnerabilities. The recent Meltdown[1] attack for instance, using Flush+Reload technique, exploits program execution attributes such as “outof-order execution” to break the logical isolation between the memories and processes. In this paper, we have developed a real-time detection and identification system against side-channel attacks. Unlike previous works, the proposed approach does not rely on synchronisation between the attackers and victims. This is realised by taking a course of program phase analysis, through performance counters, to extract Malicious Loop (ML). Simulation has shown that the proposed approach attained higher accuracy for up to 99% and efficient detection of Flush+Reload activities, through classification methods. Furthermore, the detection process, in native and cloud systems, unlike others, takes shorter execution time without additional costs, and the model benefits from very low overhead performance of approximately less than 1% of the host system.

Cyber Science 2019 Accepted Extended Abstracts

Cyber attacks real time detection: towards a Cyber Situational Awareness for naval systems [Extended Abstract]

Olivier Jacq, David Brosset, Yvon Kermarrec and Jacques Simonin
Naval Cyber Defense Chair - Ecole Navale, IMT Atlantique, France

Abstract: Over the last years, the maritime sector has seen an important increase in digital systems on board. Whether used for platform management, navigation, logistics or office tasks, a modern ship can be seen as a fully featured, complex and moving information system. Meanwhile, cyber threats on the sector are real and, for instance, the year 2018 has seen a number of harmful public ransomware attacks impacting shore and ashore assets. Gaining cyber situation recognition, comprehension and projection through Maritime Cyber Situational Awareness is therefore a challenging but essential task for the sector. However, its elaboration has to face a number of issues, such as the collect and fusion of real-time data coming from the ships and an efficient visualization and situation sharing across maritime actors. In this paper, we describe our current work and results for maritime cyber situational awareness elaboration. Even if its development is still going on, the first operational feedback is very encouraging.

The Future of Cyber Analytics: Identity Classification for Systematic and Predictive Insight [Extended Abstract]

Mary C. (Kay) Michel and Michael C. King
Florida Institute of Technology, USA

Abstract: The Internet's constant-changing infrastructure and technology calls for broader, more robust methods that can adapt and aid in establishing/strengthening linkages between a physical person and an online persona based on representative use cases with time, human, and cyber-physical system dimensions. This research introduces a novel identity classifier system comprised of a defined scheme, salient features, and mathematical axiom-based model logic of mapped type patterns utilizing contextual reasoning over time for consistent, long-term analysis. This holistic multi-discipline approach was designed with real-world case simulated evidence data to determine a mapped identity type. Ph.D. experimentation has proven effective design aspects for demographic profiles and more targeted identities. The bio-inspired, system-based design was also intended to support emerging and/or learned features, and help determine human characteristics or a person's unique signature. Experiment trials are promising and have yielded insightful visualizations and feedback for improved Situational Awareness. This paper focuses on evaluation of holistic identity classification system prototyped design with enhanced aspects of communication and automated control systems in both machines and living things which has revealed interesting types of human vs. non-humans. We leverage prior effective design features for contextual salience, and assess innovative living and non-living cybernetic identity classification features for systematic and predictive insight.

Cyber Threat Intelligence for "Things" [Extended Abstract]

Thomas D. Wagner
ETAS GmbH (Bosch Group), Germany

Abstract: Cyber Threat Intelligence (CTI) programs have gained momentum across the cyber security community. Whether they are vendor based or open source solutions, practitioners should be able to find an appropriate solution to enhance security for their IT infrastructure. The tangible world, i.e. (I)IoT products and embedded components have not been considered yet in the CTI world with few exceptions from industry specific vendors and Information Sharing Analysis Centres (ISACs). This extended abstract presents a work in progress to establish a CTI program for "things", especially the generation, consumption and distribution of product specific CTI.

Empowering Citizen Data Scientists [Extended Abstract]

Lakshmi Prayaga
University of West Florida, USA

Abstract: The use of social media, wearable devices generating high volume of structured and unstructured data is increasing exponentially. However, it is becoming increasingly difficult to obtain information from this volume of data due to lack of trained professionals. In this context, we describe a set of tools and processes that encourage and empower citizen data scientists to make use of the information available from the abundance of data and obtain a better return on investment for their organizations, institutions and or personal decisions.

The determinants of individual cyber security behaviours [Extended Abstract]

Bertrand Venard
Oxford Internet Institute, University of Oxford, UK
Audencia Business School, France

Abstract: The aim of the article is to study the determinants of individual cyber security behaviours, using a qualitative approach with face-to-face interviews of students in France. Based on our interviews, we will stress that cyber security behaviours could be explained by: self-efficacy, perceived personal susceptibility to digital threat, guardianship and conformity.

Facebook Data: Sharing, Caring, and Selling [Extended Abstract]

Renate Schubert[1] and Ioana Marinica[2]
[1]Chair of Economics, ETH Zurich, Zurich, Switzerland
[2]Collegium Helveticum, ETH Zurich, Zurich, Switzerland

Abstract: We investigate privacy concerns, privacy literacy, privacy behavior, the efficacy of privacy education and people's willingness to sell data in what is, to our knowledge, the first study to analyze subjects' entire Facebook data package in laboratory conditions. In pilot sessions with 46 participants we have found that subjects hold moderately high levels of privacy concern, have high knowledge of technical aspects of data protection and of protection strategies, yet only low to moderate knowledge of institutional practices and legislation. In line with the literature on the privacy paradox, high levels of privacy concern do not appear to be associated with a more parsimonious use of the social network site. Subjects having watched a video aimed at increasing their levels of privacy concern have sent fewer private messages, have effectively stopped sending pictures via private message and have rejected more friend requests compared to the control group in the two weeks after the session. They have, however, logged in on more devices, liked more pages and posts and posted more compared to the control group. Lastly, 63% of the subjects were willing to sell their Facebook data package to us, 79% of which did so for 10 US Dollars or less. Results from a more in-depth study with 300 participants are due to follow.

Practical approach for measuring the level of user behaviour [Extended Abstract]

Ferenc Leitold
SECURDIT, Hungary

Abstract: User behaviors danger the operation of an organization much more than any technical vulnerability does. A lot of technical solutions exist against attacks using technical security holes. The technical part of the IT security is well-grown, however dealing with the human factor is still in its infancy. In this paper the possible methods for the user behavior assessments are discussed. The presentation focuses on some useful observation possibilities for user behavior measurement. The input sources what we can use can be from the workstation used by the particular user, from the network traffic and from the application logs, especially from protection logs. Using these input sources, a couple of very useful metric can be defined for the user classification as well. Once we can measure the level of the user behavior, we can use it for improving the IT security at the given organization.

Cyber Science 2019 Accepted Posters

Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination [Poster]

***Marios Ioannou*[1]*, Eliana Stavrou*[1] *and Maria Bada*[2]**
[1]University of Central Lancashire, Cyprus
[2]University of Cambridge, UK

Abstract: This study aims to identify the factors related to developing a cybersecurity culture at an organizational context and the difficulties faced in communicating and cooperating within a CSIRT. Specifically, our aim is to identify: 1) The issues which may limit the communication and the coordination of incident management process inside a CSIRT, 2) the issues which may limit the cooperation from top management to employees and reverse and 3) approaches towards addressing the issues that limit the communication and the cooperation of a CSIRT. The research was conducted using an online survey and the study participants were experts within the existing CSIRT community. In total, 25 participants responded to the questionnaire, from 23 different countries in the world. The questions of the survey queried the personal knowledge and experience of participants regarding CSIRTs. In our analysis, issues such as communication, cooperation, coordination, trust and information sharing are discussed as crucial factors that affect the development of a cybersecurity culture. Several issues and weaknesses in terms of communication, coordination and cooperation within CSIRT are outlined and a set of recommendations and key elements are defined.

Leveraging Existing IT Resources for Insider Threat Risk Mitigation [Poster]

William Claycomb and Daniel Costa
Carnegie Mellon University (CMU) CERT, USA

Abstract: Detecting observable indicators of insider risk from organizational use of information technology (IT) relies heavily on collection of relevant data and configuration of specific criteria to monitor within that data. One valuable set of data for this task are those that represent an employee's interaction with corporate IT systems. Some organizations choose to deploy software specifically for this type of data collection, but others are unable to do so, either for cost reasons, lack of support resources, etc. In this extended abstract, we discuss how organizations can leverage existing IT resources to provide meaningful data for insider threat risk mitigation.

Classifying Phishing Email Using Machine Learning and Deep Learning [Poster]

***Sikha Bagui*[1]*, Debarghya Nandi*[2]*, Subhash Bagui*[1] *and Robert Jamie White*[3]**
[1]University of West Florida
[2]University of Illinois at Chicago
[3]AppRiver, Pensacola, FL

Abstract: In this work, we applied deep semantic analysis, and machine learning and deep learning techniques, to capture inherent characteristics of email text, and classify emails as phishing or non -phishing.

Indicator Development for Insider Threat Risk [Poster]

William Claycomb and Daniel Costa
Carnegie Mellon University (CMU) CERT, USA

Abstract: Developing useful indicators for assessing risk of insider threat activity in the workplace is a challenge faced by security practitioners seeking to mitigate counterproductive workplace behaviors. In this poster paper, we discuss different types of potential risk indicators for insider activity, how to create effective indicators, and how to measure indicator performance. Our goals are to combine findings from previous empirical research on insider threat cases with experience developing and testing real threat indicators to provide useful information for security practitioners and begin to develop a baseline for future insider threat indicator research.

Tools and Techniques for Improving Cyber Situational Awareness of Targeted Phishing Attacks [Poster]

Phil Legg and Tim Blackman
University of the West of England, UK

Abstract: Phishing attacks continue to be one of the most common attack vectors used online today to deceive users, such that attackers can obtain unauthorised access or steal sensitive information. Phishing campaigns often vary in their level of sophistication, from mass distribution of generic content, such as delivery notifications, online purchase orders, and claims of winning the lottery, through to bespoke and highly-personalised messages that convincingly impersonate genuine communications (e.g., spearphishing attacks). There is a distinct trade-off here between the scale of an attack versus the effort required to curate content that is likely to convince an individual to carry out an action (typically, clicking a malicious hyperlink). In this short paper, we conduct a preliminary study on a recent real-world incident that strikes a balance between attacking at scale and personalised content. We adopt different visualisation tools and techniques for better assessing the scale and impact of the attack, that can be used both by security professionals to analyse the security incident, but could also be used to inform employees as a form of security awareness and training. We pitched the approach to IT professionals working in information security, who believe this may provide improved awareness of how targeted phishing campaigns can impact an organisation, and could contribute towards a pro-active step of how analysts will examine and mitigate the impact of future attacks across the organisation.

A Novel Machine Learning Based Malware Detection and Classification Framework [Poster]

Kamalakanta Sethi, Rahul Kumar and Padmalochan Bera
Indian Institute of Technology IIT Bhuabaneswar, India

Abstract: As time progresses, new and complex malware types are being generated which causes a serious threat to computer systems. Due to this drastic increase in the number of malware samples, the signature-based malware detection techniques cannot provide accurate results. Different studies have demonstrated the proficiency of machine learning for the detection and classification of malware files. Further, the accuracy of these machine learning models can be improved by using feature selection algorithms to select the most essential features and reducing the size of the dataset which leads to lesser computations. In this paper, we have developed a machine learning based malware analysis framework for efficient and accurate malware detection and classification. We used Cuckoo sandbox for dynamic analysis which executes malware in an isolated environment and generates an analysis report based on the system activities during execution. Further, we propose a feature extraction and selection module which extracts features from the report and selects the most important features for ensuring high accuracy at minimum computation cost. Then, we employ different machine learning algorithms for accurate detection and fine-grained classification. Experimental results show that we got high detection and classification accuracy in comparison to the state-of-the-art approaches.

Hardware Implementation of Secured Socket Communication based on Chaotic Cryptosystem [Poster]

Belqassim Bouteghrine, Mohammed Rabiai, Camel Tanougast and Said Sadoudi
Université Lorraine, France

Abstract: Over the last decades, Field Programmable Gate Array (FPGA) boards have seen their use widely spread in different research topics. This can be explained by their low power consumption, their ability of enhancing the performances, and the numerous functions that can be integrated in those circuits. One major function delivered by FPGA boards is to be reconfigurable which helps during the development and validation stages, since it is always possible to correct just the program and to reload it in the circuit. Exploiting these advantages and functions was the main stone of our work. In this paper, we will show how to design and to implement a Pseudorandom-Key-Generator that can be used to secure a socket-based communication. The proposed key-generator, created by solving the Lorenz chaos-system, has the main task of delivering at each opened channel a new 32-bit key that is used for encrypting/decrypting data. The proposed solution is implemented and tested using Xilinx Zync702 Boards.

International Workshop on Cyber Insurance and Risk Controls (CIRC) Accepted Papers

Two simple models of business interruption accumulation risk in cyber insurance

Ulrik Franke[1] and Joachim Draeger
[1]RISE, Sweden

Abstract: As modern society becomes ever more dependent on IT services; risk management of cyber incidents becomes more important. Cyber insurance is one tool, among others, for such risk management that has received much attention in the past few years. One obstacle to well-functioning cyber insurance, however, is the fact that cyber accumulation risk remains poorly understood, despite efforts from practitioners and scientists. In this article, we address the accumulation risk of business interruption incidents, an area that has received less attention than the accumulation risk of data breach incidents. Two simple models are introduced: First, a model that takes the insurer's perspective and explores the impact on aggregated claims cost from incidents that are unintentionally transferred between firms. Second, a model that takes the insured's perspective, considering the impacts of limited incident management capacity and showing that there is sometimes an economic case for collectively funding additional incident managers. The paper is concluded with some reflections on the models and an outlook.

Quantile based risk measures in cyber security

Maria Francesca Carfora[1] and Albina Orlando[1]
[1]Consiglio Nazionale delle Ricerche (CNR), Italy

Abstract: Measures and methods used in financial sector to quantify risk, have been recently applied to cyber world. The aim is to help organizations to improve risk management strategies and to make better decisions about investments in cyber security. On the other hand, they are useful instruments for insurance companies in pricing cyber insurance contracts and setting the minimum capital requirements defined by the regulators. In this paper we propose an estimation of Value at Risk (VaR), referred to as Cyber Value at Risk in cyber security domain, and Tail Value at risk (TVaR). The data breach information we use is obtained from the “Chronology of data breaches” compiled by the Privacy Rights Clearinghouse.

Demand side expectations of cyber insurance

Ulrik Franke[1] and Per Håkon Meland[2]
[1]RISE, Sweden
[2]SINTEF, Norway

Abstract: Cyber insurance has attracted much attention from both practitioners, policymakers and academics in the past few years. However, it also faces some challenges before it can reach its full potential as a tool for better cyber risk management. One such challenge is the gap between what customers expect and what insurers really offer.
This paper investigates this gap empirically, based on interviews with informant companies in Norway and Sweden considering cyber insurance. The expectations expressed in the interviews are compared to anonymized incident claims reports and claims statistics for 2018 from a global insurance intermediary.
The results show no obvious pattern of discrepancies between different domains. However, informant expectations on business interruption coverage is much greater than one would expect from its share of claims. In this respect, informant expectations on business interruption coverage are more aligned with some recently published scenarios on possible major business interruptions.

Cyber Insurance and Time-to-Compromise: An Integrated Approach

Ganbayar Uuganbayar[1,2], Fabio Massacci[2], Fabio Martinelli[1] and Artsiom Yautsiukhin[1]
[1]Consiglio Nazionale delle Ricerche (CNR), Italy
[2]University of Trento, Italy

Abstract: Fast-growing numbers of technologies and devices make cyber security landscape more complicated and require a more accurate model. This complexity challenges cyber security experts to devise a better solution to manage cyber risks. One of the promising methods is to find the best distribution of security expenditure for risk mitigation and transfer (i.e. cyber insurance) options.
In this work, we propose a solution to find the optimal security investments when there is a cyber insurance option by applying a time-to-compromise metric to the probability of attack computation. In particular, we find the best set of countermeasures which decreases the maximum number of vulnerabilities to increase the required time to compromise a system. Our approach is based on a multiple-objective knapsack problem for the selection of countermeasures and we find the best distribution of security expenditure by computing the time-to-compromise metric which eventually defines the probability of attack.

Analysing cyber-insurance claims to design harm-propagation trees

Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith and Sadie Creese
University of Oxford, UK

Abstract: With a continuously changing threat landscape, companies must be prepared for the most unforeseen cyber events. Harm originating from cyberspace varies in magnitude and type, with potential for systemic consequences. While the adoption of security controls may partially mitigate the impact of cyber-attacks, a nuanced understanding of how events unfold during and after an incident will help organisations to better estimate the risk they face and implement advanced incident response strategies. A better estimation of risk is of particular importance to the insurance community because the costs from claims due to cyber-events vary significantly. Towards this end, we collected and analysed more than 70 claims against an insurance company, extracting different types of harm and their characteristics. We then reconstructed the claims based on these types of harm in order to obtain patterns of how cyber-harm propagates. The result is a graph indicating the most common paths that harm follows on multiple events. The findings can help policy-makers and insurance companies to understand how harm propagates, estimate more accurately the value-at-risk and adopt the necessary controls to mitigate these harms.

International Workshop on Secure Software Engineering in DevOps and Agile Development (SecSE 2019) Accepted Papers

Keynote: Practically Teaching the Next Generation

Chrissy Morgan
IT Security Operations for a Close Protection (Bodyguard) Company, UK

Abstract: In order to mitigate for the future, we must find innovative ways in which to train the next generation of application developers and security professionals, on how to spot issues and rectify. This should come before entering their professional careers, ideally at university. Students are actively taught on how to attack, however there is improvements to be made with the current state of practical mitigation teaching tools. Chrissy, having researched this subject matter for her master's dissertation will present the key research findings, the areas that need improvement, providing insight on how we can better teach our students. A realistic view looking everywhere for inspiration from Academia through to the internet underground.

Security Risk Assessment and Management as Technical Debt

Kalle Rindell and Johannes Holvitie
University of Turku, Finland

Abstract: The endeavor to achieving software security consists of a set of risk-based security engineering processes during software development. In iterative software development, the software design typically evolves as the project matures, and the technical environment may undergo considerable changes. This increases the work load of identifying, assessing and managing the security risk by each iteration, and after every change. Besides security risk, the changes also accumulate technical debt, an allegory for postponed or sub-optimally performed work. To manage the security risk in software development efficiently, and in terms and definitions familiar to software development organizations, the concept of technical debt is extended to contain security debt. To accommodate new technical debt with potential security implications, a security debt management approach is introduced. The selected approach is an extension to portfolio-based technical debt management framework. This includes identifying security risk in technical debt, and also provides means to expose debt by security engineering techniques that would otherwise remained hidden. The proposed approach includes risk-based extensions to prioritization mechanisms in existing technical debt management systems. Identification, management and repayment techniques are presented to identify, assess, and mitigate the security debt.

Threat modelling and agile software development: Identified practice in Norwegian organisations

Karin Bernsmed and Martin Gilje Jaatun
SINTEF Digital, Norway

Abstract: Threat modelling is considered a key activity in secure software engineering. However, despite its documented benefits it has not (yet) been widely adopted by agile software development projects. In this paper we present results from a qualitative study of how it is performed in practice by three different organisations. The findings show that, even though they all consider threat modelling to lead to a more secure product, they all struggle with practical aspects of the established theory.

Attack Surface Identification and Reduction Model Applied in Scrum

George Yee
Carleton University, Canada

Abstract: Today's software is riddled with security vulnerabilities that invite exploitation. Attackers are particularly attracted to software systems that hold sensitive data with the goal of compromising the data. For such systems, this paper proposes a modeling method especially suited for Scrum to identify and reduce the attack surface, which arises

due to the locations containing sensitive data within the software system and the accessibility of those locations to attackers. The method reduces the attack surface by changing the design so that the number of such locations is reduced. The method performs these changes on a graphical model of the software system. The changes are then considered for application to the actual system to improve its security.

An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps

Nora Tomas[1], Jingyue Li[1] and Huang Huang[2]
[1]NTNU, Norway
[2]Nanjing University, China

Abstract: Programmers are central agents in creating secure applications. However, software engineering and software security have historically worked in separate silos. DevSecOps is the practice of breaking down silos between development, operations, and quality assurance of security. To understand the state of art and challenges of DevSecOps, we interviewed six developers about their DevSecOps practices. We asked interview subjects about their security practices rooted in the four pillars of DevOps, namely culture, automation, sharing, and measurement. Results were analyzed by using qualitative methods. The results of the study show that it is necessary first to create a security culture. Several interviewees identified the importance of caring about security and issues in existing culture, such as how developers feel attacked by security engineers if they create vulnerable code. After establishing a security culture in the organization, development and operations need the necessary training and knowledge so that security automation tools can be utilized effectively. Measurements need to be applied continuously to keep track of identified vulnerabilities, the amount of training staff has received, and staffs general opinions regarding security.

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 Science 2019 – Best Papers
1	Examining the Roles of Muhajirahs in the Islamic State via Twitter ***Aunshul Rege and Scott Vanzant*** Temple University, Department of Criminal Justice, Temple university, USA
2	Adaptive and Intelligible Prioritization for Network Security Incidents ***Leonard Renners[1], Felix Heine[1], Carsten Kleiner[1] and Gabi Dreo Rodosek [2]*** [1]University of Applied Sciences and Arts Hanover, Germany [2]Universität der Bundeswehr München, Germany

Cyber Science 2019 Thematic Tracks

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

Cyber Science 2019 Conference Presentation Timetable

Cyber Science 2019
Comprising
International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2019)
International Conference on Social Media, Wearable and Web Analytics (Social Media 2019)
International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019)
International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident 2019)
International Workshop on Cyber Insurance and Risk Controls (CIRC 2019)
International Workshop on Secure Software Engineering in DevOps and Agile Development (SecSE 2019)

Day 1: Monday 3 June, 2019

Department of Computer Science, University of Oxford	
08:00 – 09:00	**Registration, Networking and Refreshments in the Atrium**
09:00 – 09:05	**Welcome Session – Lecture Theatre B (LTB)** **Dr Cyril Onwubiko** – Chair, Cyber Security Intelligence, Research Series, London, UK
09:05 – 09:15	**Announcements & Introduction (LTB)** **Dr Xavier Bellekens – Conference Chair** **Dr Arnau Erola – Conference Chair** **Dr Martin Gilje Jaatun – Conference Chair** **Dr Hongmei (Mary) He – Session Chair**
09:15 – 09:45	**Keynote (LTB): Opening Session** **Professor Mike Hinchey** – Chair, IEEE United Kingdom & Ireland & President, IFIP
09:45 – 10:15	**Keynote (LTB):** **Jacques Sahel** – Managing Director, ICANN, Europe **John Crain** – Chief Security, Stability & Resiliency Office, ICANN, USA
10:15 – 10:35	**Coffee Break & Social Networking (Atrium)**

Suites	Lecture Theatre B	Conference Room (278)	Access Grid Room (277)
	Track 1: Machine Learning for Cyber Security	**Track 7: Cyber Threat Intel Sharing & Return on Investment**	**Track 3: Maritime CyberSA**
10:50 – 11:10	**Efficient and Interpretable Real-Time Malware Detection Using Random-Forest** *Alan Mills, Theodoros Spyridopoulos and Phil Legg*	**Cyber Threat Intelligence for "Things"** *Thomas Daniel Wagner*	**Factors Affecting Cyber Risk in Maritime** *Kimberly Tam and Kevin Jones*
11:10 – 11:30	**TrapMP: Malicious Process Detection by Utilising Program Phase Detection** *Zirak Allaf, Mo Adda and Alexandar Gegov*	**In wolf's clothing: Complications of threat emulation in contemporary cyber intelligence practice** *Jd Work*	**Cyber attacks real time detection: towards a Cyber Situational Awareness for naval systems** *Olivier Jacq, David Brosset, Yvon Kermarrec and Jacques Simonin*
11:30 – 11:50	**A Novel Method to Prevent Phishing by using OCR Technology** *Yunjia Wang and Ishbel Duncan*	**Cyber KPI for Return on Security Investment** *Cyril Onwubiko and Austine Onwubiko*	**Forensic Readiness within the Maritime Sector** *Kimberly Tam and Kevin Jones*
11:50 – 12:10	**Industry Speaker** **Simon Wilson** – *CTO UK & Ireland, Aruba Networks, a HPE Company*	**Longitudinal performance analysis of machine learning based Android malware detectors** *Suleiman Yerima and Sarmadullah Khan*	**Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators** *Florian Skopik and Stefan Filip*
12:20 – 12:30	**Group Conference Photographs at the Convocation House**		
12:30 – 13:30	**Lunch at the Convocation House** 		
14:00 – 14:30	**Keynote (LTB):** **Professor Awais Rashid** – Professor of Cyber Security at University of Bristol, UK		

Suites	Lecture Theatre B	Conference Room (278)	Access Grid Room (277)
	Track 4: National Directives & Cyber Policy	**Track 6: Cyber Foresight & Risk Management**	**Track 10: Crypto System & Cloud**
14:40 – 15:00	**Does the NIS implementation strategy effectively address cyber security risks in the UK?** *Meha Shukla, Shane Johnson and Peter Jones*	**Security awareness escape room - a possible new method in improving security awareness of users** *Eszter Diána Oroszi*	**Analysis of Obfuscated Code with Program Slicing** *Mahin Talukder, Syed Islam and Paolo Falcarin*
15:00 – 15:20	**Facebook Data: Sharing, Caring, and Selling** *Renate Schubert and Ioana Marinica*	**Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation** *Erik Moore, Steven Fulton, Roberta Mancuso, Tristen Amador and Dan Likarish*	**A Scalable Attribute Based Encryption for Secure Data Storage and Access in Cloud** *Kamalakanta Sethi, Ankit Pradhan, Punith. R and Padmalochan Bera*
15:20 – 15:40	**Towards Better Understanding of Cyber Security Information Sharing** *Adam Zibak and Andrew Simpson*	**A Social Engineering Course Project for Undergraduate Students Across Multiple Disciplines** *Aunshul Rege, Katorah Williams and Alyssa Mendlein*	**Arithmetic Circuit Homomorphic Encryption and Multiprocessing Enhancements** *Ruitao Kee, Jovan Sie, Rhys Wong and Chern Nam Yap*
15:40 – 16:00	**BATSense: Anomalous Security-Event Detection using TBATS Machine Learning** *Pranshu Bajpai, Tyler Olsen, Seth Edgar, Rob McCurdy and Richard Enbody*	**Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management alignment** *Abraham Althonayan and Alina Andronache*	**Cyber Security Supervision in the Insurance Sector: Smart Contracts and Chosen Issues** *Remy Remigius Zgraggen*
16:00 – 16:30	**Coffee Break & Social Networking (Atrium)**		
16:30 – 17:00	**Keynote (LTB):** **Ros Smith** – Senior Product Manager in Identity and Access Management, BBC, UK		
from 17:00	**Poster Discussion**		
19:00	**Social Evening Dinner & Drinks - Rewley House** 		

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

Day 2: June 04, 2019

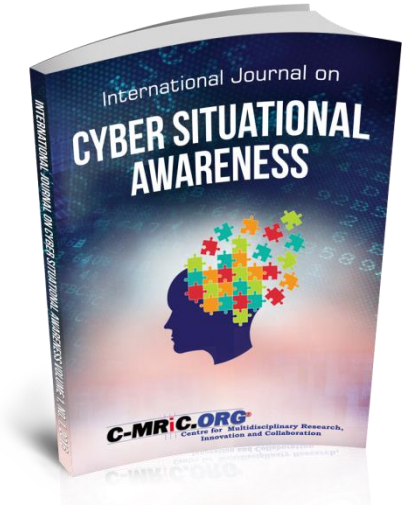
Department of Computer Science, University of Oxford			
08:00 – 09:00	**Registration, Networking and Refreshments in the Atrium**		
Suites	**Lecture Theatre B**	**Conference Room (278)**	**Access Grid Room (277)**
	Track 11: Visual Analytics & CyberOps	**Track 2: Blockchain Applications**	**Track 9: Human Factors & Cognition**
09:00 – 09:20	**What makes for effective visualisation in Cyber Situational Awareness for Non-Expert Users?** *Fiona Carroll, Phil Legg and Adam Chakof*	**MANiC: Multi-step Assessment for Crypto-miners** *Jonah Burgess, Philip O'Kane, Domhnall Carlin and Sakir Sezer*	**Organizational formalization and employee information security behavioral intentions based on an extended TPB model** *Yuxiang Hong and Steve Furnell*
09:20 – 09:40	**The Future of Cyber Analytics: Identity Classification for Systematic and Predictive Insight** *Mary C. (Kay) Michel and Michael C. King*	**A cost-efficient Protocol for Open Blockchains** *Chunlei Li, Chunming Rong and Martin Gilje Jaatun*	**Practical approach for measuring the level of user behavior** *Ferenc Leitold*
09:40 – 10:00	**Threat Modeling of Connected Vehicles: A privacy analysis and extension of vehicleLang** *Wenjun Xiong and Robert Lagerström*	**Ethereum Blockchain for Securing the Internet of Things: Practical Implementation and Performance Evaluation** *Subhi Alrubei, Jonathan Rigelsford, Callum Willis and Edward Ball*	**Security-Related Stress: A Perspective on Information Security Risk Management** *Martin Lundgren and Erik Bergström*
10:00 – 10:20	**Online Anomaly Detection of Time Series at Scale** *Andrew Mason, Yifan Zhao, Hongmei He, Raymon Gompelman and Srikanth Mandava*	**Secure Chaotic Maps-based Authentication Scheme for Real-Time Data Access in Internet of Things** *Wenting Li, Haibo Cheng and Ping Wang*	**Big Social Data - Predicting Users' Interests from their Social Networking Activities** *Alexiei Dingli and Bernhardt Engerer*
10:20 – 10:40	**Coffee Break & Social Networking (Atrium)**		

11:00 – 11:30	**Keynote (Convocation House):** **Dr Aunshul Rege** – Associate Professor, Department of Criminal Justice, Temple University, USA		
11:30 – 12:00	**Keynote (Convocation House):** **Professor Sadie Creese** – Professor of Cyber Security, Department of Computer Science, University of Oxford, UK		
12:00 – 12:10	**Group Conference Photographs at the Convocation House**		
12:10 – 13:10	**Lunch in the Convocation House** 		
13:10 – 13:20	**Group Plenary Discussion & Bidding to host Cyber Science 2020**		
Suites	**Lecture Theatre B**	**Lecture Theatre A**	**Access Grid Room (277)**
	Track 13: SecSE Workshop	**Track 12: Cyber Insurance & Risk Controls (CIRC) Workshop**	**Track 14: Data Science & Social Analytics**
13:30 – 14:00	**Keynote: Chrissy Morgan** **Practically Teaching the Next Generation**	**13:40 - 14:00** **Two simple models of business interruption accumulation risk in cyber insurance** *Ulrik Franke and Joachim Draeger*	**Examining the Roles of Muhajirahs in the Islamic State via Twitter** *Aunshul Rege and Scott Vanzant*
14:00 – 14:20	**Security Risk Assessment and Management as Technical Debt** *Kalle Rindell and Johannes Holvitie*	**Quantile based risk measures in cyber security** *Maria Francesca Carfora and Albina Orlando*	**Domain Identification for Commercial Intention-holding Posts on Twitter** *Yanyuan Zhu, Mee Chi So and Paul Harrigan*
14:20 – 14:40	**Threat modelling and agile software development: Identified practice in Norwegian organisations** *Karin Bernsmed and Martin Gilje Jaatun*	**Cyber Insurance and Time-to-Compromise: An Integrated Approach** *Ganbayar Uuganbayar, Fabio Massacci, Fabio Martinelli and Artsiom Yautsiukhin*	**A Comparison of Machine Learning Approaches for Detecting Misogyny Speech in Urban Dictionary** *Theo Lynn et al.*
14:40 – 15:10	**Attack Surface Identification and Reduction Model Applied in Scrum**	**Demand side expectations of cyber insurance**	**The determinants of individual cyber security behaviours**

	George O. M. Yee	*Ulrik Franke and Per Håkon Meland*	*Bertrand Venard*
15:10 – 15:30	**An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps** *Nora Tomas, Jingyue Li and Huang Huang*	**Analysing cyber-insurance claims to design harm-propagation trees** *Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith and Sadie Creese*	**A Preliminary Exploration of Uber Data as an Indicator of Urban Liveability** *Aguinaldo Bezerra, Gisliany Alves, Ivanovitch Silva, Pierangelo Rosati, Patricia Takako Endo and Theo Lynn*
15:30 – 16:00	**Coffee Break & Social Networking (Atrium)**		
Suites	**Lecture Theatre B**	**Lecture Theatre A**	**Access Grid Room (277)**
	Track 13: SecSe Industrial	**Track 5: National Cyber Fusion Centres**	**Track 8: Adversarial Cyber Defence**
16:00 – 16:20	**Industry Speaker** **Frank Aakvik** – *Capture*	**Cyber Onboarding is 'Broken'** *Cyril Onwubiko and Karim Ouazzane*	**A Combined Attack-Tree and Kill-Chain Approach to Designing Attack-Detection Strategies for Malicious Insiders in Cloud Computing** *Adrian Duncan, Sadie Creese and Michael Goldsmith*
16:20 – 16:40	**Industry Speaker** **Marco Constantino** – *Kongsberg Digital*	**Adaptive and Intelligible Prioritization for Network Security Incidents** *Leonard Renners, Felix Heine, Carsten Kleiner and Gabi Dreo Rodosek*	**Pattern discovery in intrusion chains and adversarial movement** *Nima Asadi, Aunshul Rege and Zoran Obradovic*
16:40 – 17:00	**Industry Speaker** **Nick Murison –** *Synopsys*	**Towards a Conversational Agent for Threat Detection in the Internet of Things** *Christopher D. McDermott et al.*	**Destructive Attacks Detection and Response System for Physical Devices in Cyber-Physical Systems** *Peyman Kabiri and Mahdieh Chavoshi*
17:00 – 17:20	**Industry Speaker** **Thomas Frederik Düllmann –** *ISTE, University of Stuttgart, Germany*	**Brexit Impact on Cyber Security of United Kingdom** *Muntaha Saleem*	**Keystroke Dynamics using Auto Encoders** *Yogesh Patel, Karim Ouazzane, Vassil Vassilev, Ibrahim Faruqi and George Walker*
	Closing remarks & Thank you by Dr Cyril Onwubiko in Lecture Theatre B		
17:40 – onwards	**Networking (Atrium)**		

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

Editor-in-Chief: Dr Cyril Onwubiko

Associate Editors:
Professor Frank Wang
Professor Karen Renaud

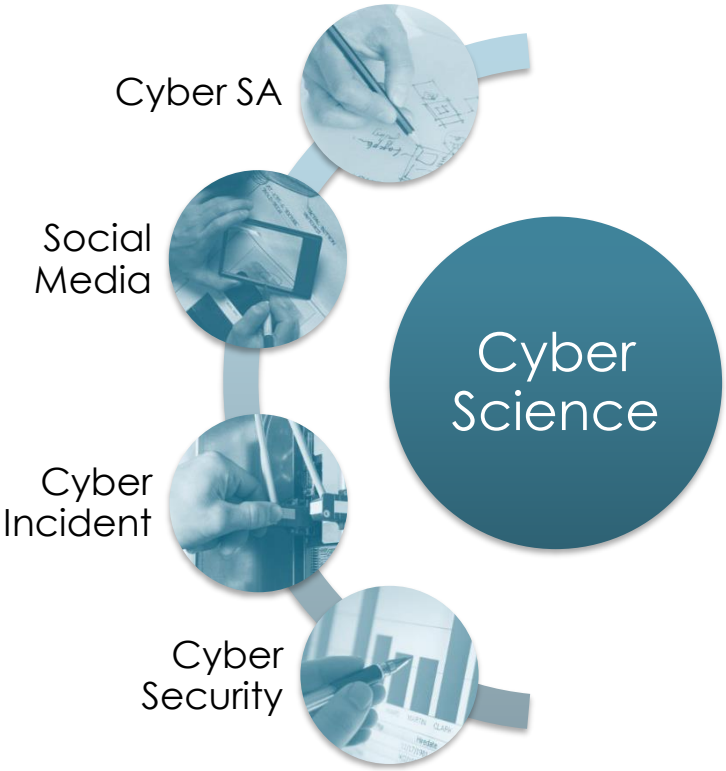
C-MRiC Other Services

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

Cyber Science 2020

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, implementation, methods and applications. It is a yearly conference held at various cities; the first three meetings have been in London, followed by Glasgow, Scotland in 2018, University of Oxford, England in 2019.



The theme for Cyber Science 2020 is:

Theme – Machine Learning for insight in Cyber Security and Situational Awareness

Dates: **Cyber Science 2020 will be held on Monday 15th to Wednesday 17th June 2020.**

Venue: **TBC**

Request to host Cyber Science 2020

To bid to host the Cyber Science 2020 joint & co-located multidisciplinary and internationally refereed conferences, or to organise a workshop or seminar as part of the Cyber Science 2020, please contact us immediately, it's first come first served, however, all bids will be assessed fairly. A decision will be made in **September 2019**. All bids must be submitted via email to submission@c-mric.org

Thank-you!

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

Notes

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 @cmricorg

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

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