15-19 JUNE, 2020

Dublin City University, IRELAND

IEEE

Advancing Technology for Humanity

2020

Cyber Science 2020
Virtual Conference Programme

Advancing a Multidisciplinary Approach to Cyber Security

C-MRiC.ORG®

#Cyberscience2020 @cmricorg

www.c-mric.org

Sponsors


IEEE
Advancing Technology
for Humanity


IEEE
young
professionals


IEEE
computer
society


secudit
the risk
analyzer


DCU
DUBLIN CITY
UNIVERSITY


aruba
a Hewlett Packard
Enterprise company


research·series
... founded on research


dotLAB
The Irish Institute
of Digital Business


IEEE
United Kingdom and Ireland Section


SINTEF


CYBER
SECURITY
OXFORD


UNIVERSITY OF
OXFORD
DEPARTMENT OF
COMPUTER
SCIENCE

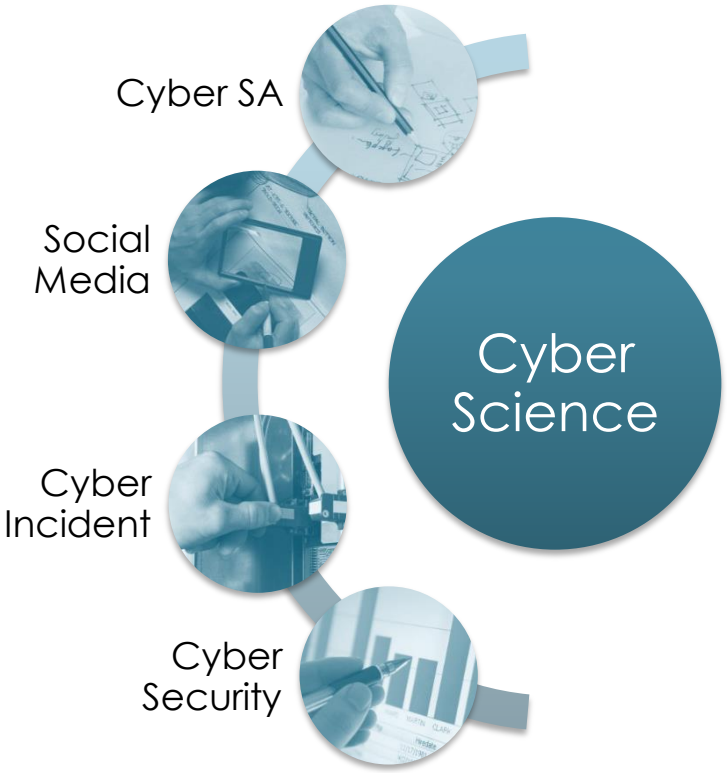

C-MRiC.ORG
Centre for Multidisciplinary Research,
Innovation and Collaboration

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. It is a platform for researchers and industry practitioners to present work encompassing principles, analysis, design, process, implementation, methods and applications.

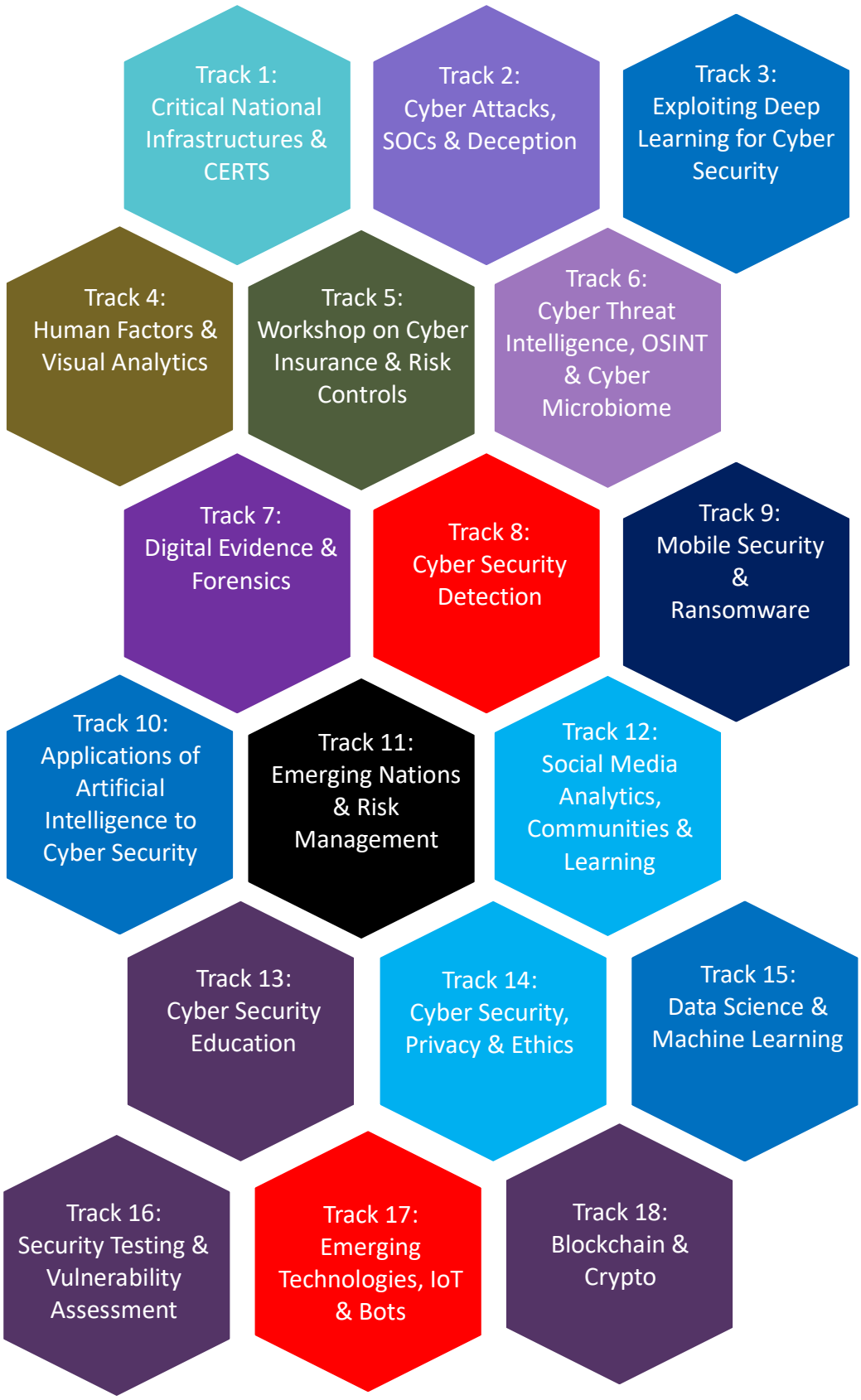
It is a yearly conference held at various cities; the first three meetings have been in London, followed by Glasgow, Scotland in 2018, University of Oxford, England in 2019, and Dublin City University, Dublin, Ireland in 2020 (now held virtually due to COVID-19).



The overall theme for Cyber Science 2020 is:

Advancing a Multidisciplinary Approach to Cyber Security

Cyber Science 2020 Thematic Tracks



Contents

Conference Venue

This conference was planned to be hosted at the Dublin City University, Dublin, Ireland, but due to the novel coronavirus (COVID-19), this conference is now being held online (virtually).

Dublin City University, Dublin, Ireland

Dublin City University (http://www.dcu.ie) was founded in 1981 and comprises three campuses and over 16,000 students including over 2600 postgraduate students. Having grown its student population by more than 50% in the past five years, DCU is Ireland's most innovative university and fastest growing university. In 2016 it delivered more than 200 programmes across its five faculties – Humanities and Social Sciences, Science and Health, Engineering and Computing, DCU Business School and DCU Institute of Education.

Excellence in DCU education and research activities has led to its ranking in the top of 1.5% of universities in the world. The University is consistently ranked among the top young universities globally, appearing in the 2020 QS Top 70 under 50, and 2019 Times Higher (THE) Top 100 under 50. DCU has twice been named Sunday Times 'University of the Year' (2004, 2010).

The 2017 QS World University Rankings by Subject feature DCU in the top 250 of more than 4,438 universities worldwide in the areas of Communications and Media Studies, Business and Management Studies and Modern Languages. DCU is also now ranked in the top 300 universities in the world for both 'arts and humanities' and 'social sciences'. The 2018 Times Higher Education World University Rankings placed DCU amongst the top 300 universities in the world in the area of Life Sciences.

Conference Structure / Organisation

- The conference will be held online from **Monday June 15 through to Friday June 19, 2020**.
- There are six keynote speakers, a keynote speaker per day, except on Tuesday 16th June when two keynote speakers will be speaking at different times of the day.
- There are two industry panel sessions on **Thursday 18th June** and **Friday 19th June**. Keynote speakers and industry panellist are notable subject matter experts from government departments and agencies, industry and academia. This is deliberately done so to offer variety, coverage and quality for our audience.
- Keynotes and industry panel discussions will not be held in parallel sessions in order to allow everyone to attend keynotes and industry discussions.
- There are two parallel sessions per day (for authors' paper presentations and posters). The choice of which session to attend is entirely up to the attendee to decide based on the conference timetable, which can be found towards the end of this programme and on the conference website. Attendees are equally allowed to 'mix and match' and are free to leave one session to attend the other. Further, all talks, presentations and keynote speeches will be recorded to give people the opportunity to watch them on demand.
- The conference timetable is structured with ample free times in between to allow our audience who may be working from home to do their work, while still being able to join in on a wide variety of the talks and keynotes.

Keynote & Industry Speakers

Dr Ruoyi Zhou

Dr Ruoyi Zhou, Director of IBM Research Ireland

Dr Ruoyi Zhou is the Director of IBM Research – Ireland with the responsibilities to drive innovation and grow a world-class industrial research organization in AI, Internet of Things (IoT), high performance computing, mathematical modeling, quantum computing, and other cutting-edge sciences and technologies.

Prior to her current role, she served as the Director of IBM Accessibility Research where she oversaw development of advanced technology to enable accessibility for IBM products, solutions, and services; creation of AI-powered assistive technology for people with disabilities; and exploration of IoT-based AI solutions for Aging. She also served on the Industry Advisory Council at the Colorado University College of Engineering & Applied Science and on the Board of Advisors for G3ict. She initiated and launched the Accessibility track at the Grace Hopper Conference and served as a committee member. Additionally, Ruoyi was the Co-Director of AI for Healthy Living, a joint research center between IBM and the University of California, San Diego.

Previously, **Ruoyi** was the Director responsible for the partnership between IBM Research and IBM Global Business Services. In this role, she led a global team and grew services revenue by applying differentiating technologies to solve challenging business problems. During her tenure as a senior research manager, Ruoyi led a cross-disciplinary team in tackling one of the most difficult problems in IBM's strategic outsourcing business: forecasting deal cost and pricing, using complex mathematical modeling and predictive analytics. Before stepping into research management, Ruoyi served as the Chief of Staff in the Lab Director's office at IBM's Almaden Research Center. Ruoyi

spent the early part of her career in IBM's Storage Systems Group as an engineer designing magnetic recording heads and developing thin-film disk technology. Prior to joining IBM, Ruoyi was a postdoctoral researcher at the Los Alamos National Laboratory, where she studied and researched process and characterization of high-temperature superconductors.

Ruoyi holds a Ph.D. in Materials Science from Rutgers University. She has over 30 publications and is the recipient of several patents. She was a YWCA TWIN Award honoree, one of the most prestigious awards in the United States, recognizing successful women executives for their outstanding achievements.

Steven B. Lipner is executive director of SAFECode

Prof. Steven B. Lipner

Steven B. Lipner is executive director of SAFECode, a non-profit industry organization dedicated to improving software assurance and is an adjunct professor of computer science at Carnegie Mellon University. He has almost fifty years' experience as a researcher, engineering manager, and general manager in cybersecurity. Lipner retired in 2015 as partner director of software security at Microsoft, where he created and led Microsoft's Security Development Lifecycle (SDL) team and was responsible for the definition, tools development and company-wide execution of Microsoft's internal SDL process and for tools and programs that made the SDL available to organizations beyond Microsoft. Lipner was also responsible for Microsoft's corporate strategies and policies for supply chain security and for strategies related to government security evaluation of Microsoft products. He served as the Microsoft member and board chair of SAFECode.

Steven has been involved throughout his career as a contributor to the development of government policies related to cybersecurity. He is now serving his third term on the United States Information Security and Privacy Advisory Board and currently serves as the board chair. He was elected to the National Academy of Engineering in 2017 and has served on numerous National Academies committees. He was elected to the National Cybersecurity Hall of Fame in 2015. Lipner holds twelve U.S. patents for inventions in the field of computer and network security. He received an S.B. and S.M. in civil engineering from MIT and attended the Harvard Business School's Program for Management Development.

Wayne Bursey, Industrial Cyber Security Lead at Siemens Ltd Dublin

Wayne Bursey

Wayne Bursey is the Industrial Cyber Security Lead with Siemens Ltd., Dublin, focusing on OT (Operational Technology) Security for our customers Industrial Control Systems and Environments. In the age of Digitalisation, Cyber Security and Networks are the core pillars to deliver this evolution.

Wayne has worked with Siemens for 20 years serving industrial customers, distribution partners and OEMs to deliver solutions and services in automation, networking, digitalization and data driven IoT platforms within Industry 4.0; and holds a BTEC in Industrial Control Systems.

Paul C Dwyer

Paul C Dwyer, CEO of Cyber Risk International, Ireland

Paul C Dwyer is recognised as one of the world's foremost experts on cyber security, risk and privacy. As CEO of Cyber Risk International he specialises in corporate and enterprise security, development of cyber defence programs, and business operations protection for CRI clients. With responsibility for the protection of trillions of euros in global money movement and critical infrastructure technologies that protect hundreds of thousands of companies' and governments' interests in more than 100 countries.

He has been certified an industry professional by the International Information Security Certification Consortium (ISC2) and the Information System Audit and Control Association (ISACA) and selected for the IT Governance Expert Panel. Approved by the National Crime Faculty and the HTCN High Tech Crime Network.

Paul has worked extensively around the world and his diverse career spans more than 25 years working with military, law enforcement, and the commercial sector.

Valerie Lyons

Valerie Lyons**,** COO at BH Consulting, Ireland

Valerie Lyons is COO of BH Consulting, where she designs and delivers projects across a vast range of topics such as GDPR, Data Protection, ISO 27001, Cyber Strategy, Enterprise Security Risk and Incident Response. Prior to BH Consulting, she spent almost 15 years as Head of Information Risk in KBC Bank and has extensive senior-level experience in the financial services sector. Her background spans compliance, corporate and ICT governance, data protection, information privacy, cyber auditing, cyber risk management, cyber strategy and team leadership.

Valerie has an in-depth knowledge of GDPR and is frequently invited to speak at industry conferences, most recently keynoting at COSAC's International Security Conference 2019. Valerie is currently pursuing a PhD in DCU's Business School (under a scholarship award from the Irish Research Council) researching the effectiveness of organizations' privacy protection orientations. A certified CISSP for almost 20 years, she holds a Master of Science in Business Leadership from University College Cork and a BSc in Information Systems from Trinity College Dublin.

Vincent Blake

Vincent Blake, Vice President and ITSO at Pearson UK

Vincent Blake is Pearson's Vice President, Information Technology Security Officer (ITSO) and Governance, Risk, Compliance and Assurance, joining in September 2014.

Vincent is accountable for Pearson's Global Enterprise Platform and Cloud information security framework. This includes executing Pearson's Platform Security by Design strategy and in-market Product security assurance. Vincent is responsible for security governance and compliance across 100+ countries, ensuring it is deployed and managed to protect the business and the learner's information assets. Pearson is the world's leading learning company; we help people all over the world

make progress in their lives through learning. Smart and innovative uses of technology are vital to Pearson, especially as we become more global, more open and more closely connected with learners.

Prior to joining Pearson, **Vincent** worked for Raytheon Systems in the UK for five years, establishing the EMEA Cyber Security Practice, supporting customers within government, defence and intelligence, and spent two years as the Chief Security Officer for the e-Borders programme. **Vincent** is a Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP) and Information Systems Security Management Professional (ISSMP).

Dr Phillippa M. Spencer, Senior Principal Statistician at DSTL, UK

Dr Phillippa M. Spencer

Dr Phillippa M. Spencer is the 2019 winner of the ***Woman of the Year*** Women in Defence and ***Outstanding Contribution to Defence*** Awards. The annual awards, this year held at Guildhall in London, recognise exceptional women across UK defence. With more than 470 nominations received, the competition was high.

Phillippa was cited for her work as a polymath, applying mathematical and statistical thinking across a number of areas such as cyber, artificial intelligence, data fusion, chemistry and biology; She has worked at Defence Science and Technology Laboratory (Dstl) for 17 years.
Her analysis was used amongst healthcare workers in Sierra Leone during the Ebola outbreak and she was a key subject matter expert in bringing the F-35 fighter into service. More recently, **Phillippa** was involved in the clean-up of Salisbury following the Novichok incident, where she applied statistical modelling to determine whether locations or vehicles were safe to use.

This year **Phillippa** was awarded a patent for her method of interrogating mixtures of nuclear acids by short tandem repeat analysis. This complements her existing patents at Dstl including for the pre-symptomatic diagnosis of sepsis.

Dr Jason R.C. Nurse, Assistant Professor in Cyber Security at the University of Kent, UK


Dr Jason R.C. Nurse

Dr Jason R.C. Nurse is an Assistant Professor in Cyber Security at the University of Kent. He is also a Visiting Academic at the University of Oxford, a Visiting Fellow in Defence and Security at Cranfield University, and a professional member of various associations relating to cyber security research and practice.

Prior to joining Kent in 2018, **Dr Nurse** was a Research Fellow at the University of Oxford for 7 years. For his research into the interdisciplinary aspects of cyber, **Dr Nurse** was nominated as a Rising Star within the UK's EPSRC RISE Awards Campaign. Specifically, his research concentrates on investigating interdisciplinary approaches to enhance and maintain cyber security for organisations, individuals and governments. This considers the full spectrum of technologies in use today and encompasses topics such as security risk management in cyberspace, privacy and security in the internet-of-things, cyber insurance, and dimensions of cybercrime.

Dr Siôn Lloyd

Dr Siôn Lloyd, Lead Security, Stability & Resiliency Specialist; ICANN

Dr Siôn Lloyd is a member of the Internet Corporation for Assigned Names and Numbers (ICANN's) Internet identifiers Security, Stability and Resiliency Team.

Siôn's work is currently focused on understanding the ways in which bad actors are making use of the global COVID-19 pandemic to promote their campaigns; specifically, around the misuse of the Domain Name System (DNS). He has worked in the domain name industry for over 20 years and has been researching the use and misuse of DNS from a security point of view for much of that time. He has seen how the DNS can be used in attack and defence and how it can be made more secure; even for those people who have never heard of it and don't realise that they are using it.

James Chappell

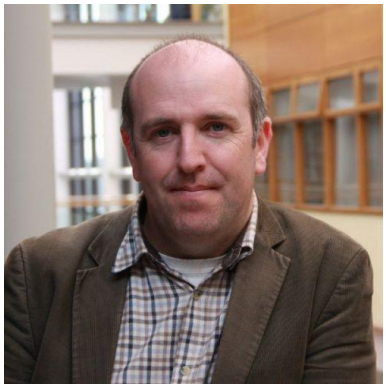
James Chappell, Founder & Chief Innovation Officer, Digital Shadows

James has led teams in InfoSec and Cybersecurity since 1997, working across the private sector and government organisations helping them to understand technical aspects of information security.
James spent over ten years of his career as a security architect and deputy head of Information Security professional at BAE Systems Detica; he previously worked at Nortel Networks in the United States.

James has always been fascinated by innovative ways of countering the growth of crime and fraud in computer networks and developing effective ways of measuring and managing the security big picture. In 2011 this journey led to an exploration of digital footprints, and their impact on the security of the modern business.

James is a regular speaker at technology events and cyber security conferences across the globe and is regularly quoted in the press.

Conference Chairs & Organisers



Professor Theo Lynn

Professor Theo Lynn – Full Professor of Digital Business, Dublin City University, Ireland

Theo Lynn is Professor of Digital Business at DCU Business School where specializes in the role of digital technologies in transforming business processes. He has been published widely in leading journals in both business and computer science. He is the Series Editor on the Palgrave Studies in Digital Business & Enabling Technologies. Previously, he was Principal Investigator of the Irish Centre for Cloud Computing and Commerce, an EI/IDA funded Cloud Computing Technology Centre (2011-2018), Associate Dean (Industry Engagement and Innovation) at DCU Business School (2015-2017), Business Innovation Platform Director for DCU (2015-2016) and Director of the Leadership, Innovation and Knowledge Research Centre at DCU (2009-2011). He has won over 200 grants representing over €20m in total project funding. He was a PI on the Horizon 2020 Cloud Lightning Project (2015-2017) and the Horizon 2020 RECAP Project (2017-2019). He is currently a PI on the Horizon 2020 RINNO Project.

Theo has founded a number of companies incl. Enki Information Systems, Educational Multimedia Group and Atomic Assets, the businesses of which have been acquired by Rochford Brady Group, Intuition and Cambridge University Press respectively. He advises a number of domestic and international companies.

Dr Pierangelo Rosati

Dr Pierangelo Rosati – Assistant Professor in Business Analytics at Dublin City University, Ireland.

Dr. Pierangelo Rosati is Assistant Professor in Business Analytics at DCU Business School, Co-Deputy Director of the Irish Institute of Digital Business (IIDB). He is also Deputy CEO at European Capital Markets CRC (ECMCRC) and Business Community Lead of the IEEE UK and Ireland Blockchain Group. He previously worked as Post-Doctoral Researcher of the Irish Centre for Cloud Computing and Commerce (IC4).

Dr. Rosati holds a PhD in Accounting and Finance from the University of Chieti-Pescara (Italy) and an MSc in Management and Business Administration from the Alma Mater Studiorum University of Bologna (Italy).

He was appointed Visiting Professor at Universidad de las Américas Puebla (Mexico), University of Edinburgh Business School (United Kingdom) and Católica Porto Business School (Portugal), and visiting Ph.D Student at the Capital Markets Cooperative Research Center (CMCRC) in Sydney (Australia).

His research interests include data analytics, business value of IT, FinTech, Blockchain, cloud computing, and cyber security.

Dr Patricia Endo

Dr Patricia Endo, Universidade de Pernambuco, Brazil

Dr Patricia Endo is an Adjunct Professor at the Universidade de Pernambuco and researcher with the the Networking and Telecommunications Research Group (GPRT/UFPE) at Universidade Federal de Pernambuco. Her primary focus in in using mathematical analysis for resource management, high availability, and edge, fog and cloud integration.

Patricia recent focus is on the use of ML/DL for a variety of cloud and network optimisation use cases with Ericsson, and tropical disease, with the Fundação de Medicina Tropical Doutor Heitor Vieira Dourado in Manaus, Brazil. Previously Patricia was a post-doctoral researcher at the Irish Centre for Cloud Computing and Commerce and was a researcher on the Horizon 2020 RECAP project.

Dr Grace Fox

Dr Grace Fox – Assistant Professor of Digital Business, of Digital Business, Dublin City University, Ireland

Dr Grace Fox is Assistant Professor in Digital Business at DCU Business School. She has previously worked as a postdoctoral researcher at the Irish Centre for Cloud Computing and Commerce (IC4) and the Health Information Systems Research Centre in University College Cork. Grace's research interests intersect the areas of information privacy, digital technology adoption and assimilation, digital inclusion, and digital literacy. Her research has been published in numerous national and international conferences, peer-reviewed journals and books.

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.

Dr Xavier Bellekens

Dr Xavier Bellekens – Lecturer, Chancellor's Fellow, University of Strathclyde, Glasgow, 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 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

Prof Frank Wang

Professor Frank Wang – Chair, Computer Society, IEEE UK & Ireland and Professor of Future Computing, School of Computing, University of Kent, UK

Frank Z. Wang is a Chair, Computer Society, IEEE UK & Ireland, and Professor in Future Computing, School of Computing, University of Kent, UK. The School of Computing was formally opened by Her Majesty the Queen. Professor Wang's research interests include cloud computing, big data, green computing, brain computing and future computing. He has been invited to deliver keynote speeches and invited talks to report his research worldwide, for example at Princeton University, Carnegie Mellon University, CERN, Hong Kong University of Sci. & Tech., Tsinghua University (Taiwan), Jawaharlal Nehru University, Aristotle University, and University of Johannesburg. In 2004, he was appointed as Chair & Professor, Director of Centre for Grid Computing at CCHPCF (Cambridge-Cranfield High Performance Computing Facility). CCHPCF is a collaborative research facility in the

Universities of Cambridge and Cranfield (with an investment size of £40 million). Prof Wang and his team have won an ACM/IEEE Super Computing finalist award. Prof Wang is Chairman (UK & Republic of Ireland Chapter) of the IEEE Computer Society and Fellow of British Computer Society. He has served the Irish Government High End Computing Panel for Science Foundation Ireland (SFI) and the UK Government EPSRC e-Science Panel.

Dr Cyril Onwubiko – IEEE Computer Society Distinguished Visitor Program (DVP) Speaker & Director, Enterprise Security Architecture, Pearson Plc

Dr Cyril Onwubiko

Dr Cyril Onwubiko is IEEE Computer Society DVP Speaker, and Director, Enterprise Security Architecture, Pearson Plc, where he is responsible for directing and shaping enterprise security architecture strategy within the Chief Information Security Office (CISO). Prior to Pearson Plc, 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".

The Organising Committee would like to thank our DCU Marketing and Support Team – **Niamh Byrne, Robert Walsh, Molly Brennan,** and **Caitlan Brownlow.**

Cyber Security 2020, SecSE 2020, & Cyber Incident 2020

Cyber Threat Intelligence and the Cyber Meta-Reality and Cyber Microbiome

Joshua Sipper
Air Force Cyber College, *United States Air Force, USA*

Abstract: In a cyber meta-reality filled with zero-day exploits, autonomous code, Worms modeled from Stuxnet, and the coming onslaught of AI enabled malware, the need for actionable, virtually prescient threat intelligence is paramount. It is almost uniformly recognized that the current reactionary paradigm concerning cyber threats is severely lacking. Cyber threat analysts desperately need a systematic approach to cyber threat characterization and how cyber threats evolve within a greater construct defined here as the cyber microbiome. This paper will first define the concept of the cyber microbiome and its place in what has become the cyber meta-reality. Cyber threats will then be examined in relation to this paradigm and recommendations will be made regarding how threat characterization and genetic mutation can be examined in light of this new, techno-biological understanding.

Acoustic Emanation of Haptics as a Side-Channel for Gesture-Typing Attacks

Jonathan Francis Roscoe and Max Smith-Creasey
Future Security and Cyber Defence, BT Applied Research, Adastral Park, UK

Abstract: Abstract—In this paper, we show that analysis of acoustic emanations recorded from haptic feedback during gesture-typing sessions is a viable side-channel for carrying out eavesdropping attacks against mobile devices. The proposed approach relies on acoustic emanation resulting from haptic events, namely the buzz of a small vibration motor as the finger initiates the gesture typing of a work in a sentence. By analysing time between haptic feedback events, it is possible to identify the text that a user enters via the soft keyboard on their device. The attack requires no prior interaction or need to install software on the target device (unlike similar works); only the ability to record audio within the vicinity. We present an experimental framework to illustrate the feasibility of the attack. In the experiments we show that sentences can be detected with an accuracy of 70% with some sentences identified with up to 95% accuracy. The attack can be conducted with minimal computation and on non-specialist consumer equipment. The paper concludes by proposing a number of countermeasures that mitigate the ability of an attacker to successfully intercept keyboard input.

A Security Perspective on Unikernels

Joshua Talbot[1], Przemek Pikula[1], Craig Sweetmore[1], Samuel Rowe[1], Hanan Hindy[1], Christos Tachtatzis[2], Robert Atkinson[2] and Xavier Bellekens[12]
[1]Division of Cyber-Security, Abertay University, Dundee, Scotland
[2]EEE Department, University of Strathclyde, Glasgow, Scotland

Abstract: Cloud-based infrastructures have grown in popularity over the last decade leveraging virtualisation, server, storage, compute power and network components to develop flexible applications. The requirements for instantaneous deployment and reduced costs have led the shift from virtual machine deployment to containerisation, increasing the overall flexibility of applications and increasing performances. However, containers require a fully fleshed operating system to execute, increasing the attack surface of an application. Unikernels, on the other hand, provide a lightweight memory footprint, ease of application packaging and reduced start-up times. Moreover, Unikernels reduce the attack surface due to the self-contained environment only enabling low-level features. In this work, we provide an exhaustive description of the unikernel ecosystem; we demonstrate unikernel vulnerabilities and further discuss the security implications of Unikernel-enabled environments through different use-cases.

Vulnerability-Based Impact Criticality Estimation for Industrial Control Systems

Uchenna Daniel Ani[1], Hongmei He[2] and Ashutosh Tiwari[3]
[1]Department of Science, Technology Engineering and Public Policy, University College London, UK
[2]School of Aerospace, Transport, and Manufacturing, Cranfield University, UK
[3]Department of Automatic Control and Systems Engineering, The University of Sheffield, UK

Abstract: Cyber threats directly affect the critical reliability and availability of modern Industry Control Systems (ICS) in respects of operations and processes. Where there are a variety of vulnerabilities and cyber threats, it is necessary to effectively evaluate cyber security risks, and control uncertainties of cyber environments, and quantitative evaluation can be helpful. To effectively and timely control the spread and impact produced by attacks on ICS networks, a probabilistic Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model for impact estimation and prioritised remediation is presented. This offer a new approach for combining three major attributes: vulnerability severities influenced by environmental factors, the attack probabilities relative to the vulnerabilities, and functional dependencies attributed to vulnerability host components. A miniature ICS testbed evaluation illustrates the usability of the model for determining the weakest link and setting security priority in the ICS. This work can help create speedy and proactive security response. The metrics derived in this work can serve as sub-metrics inputs to a larger quantitative security metrics taxonomy; and can be integrated into the security risk assessment scheme of a larger distributed system.

An Empirical Study of CERT Capacity in the North Sea

Martin Gilje Jaatun[1], Lars Bodsberg[1], Tor Olav Grøtan[1] and Marie Moe[2]
[1]Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway
[2]IIK, NTNU, Gjøvik, Norway

Abstract: This paper documents the results of an empirical study of cyber incident response readiness in the Norwegian petroleum industry. The study addressed the Computer Emergency Response Team (CERT) capacity among various actors in the industry in handling critical cybersecurity incidents in industrial control and safety systems, with a focus on Operational Technology (OT) systems. The paper presents results from interviews with personnel in petroleum companies as well as interviews with national and international CERT actors. The informants in the petroleum industry are relatively satisfied with their own CERT capacity today, but it is acknowledged that one can always improve. Oil and gas companies and drilling companies share information and experience in various (virtual) meeting places and forums organized by external actors, but there is little focus, especially among the smaller companies, on systematic sharing of information and experiences of cyber incidents. There is a strong need for coordinating and harmonizing cybersecurity in IT and OT systems, as there are significant differences in terminology, maturity of technical solutions and culture today. CERT actors pointed out a need for better communication and contact between CERT actors and key persons within the companies, something that could be accomplished with the establishment of a petroleum sector Information Sharing and Analysis Centre (ISAC).

Automated Vulnerability Testing via Executable Attack Graphs

Drew Malzahn, Zachary Birnbaum, and Cimone Wright-Hamor
The Johns Hopkins University Applied Physics Laboratory, USA

Abstract: Cyber risk assessments are an essential process for analyzing and prioritizing security issues. Unfortunately, many risk assessment methodologies are marred by human subjectivity, resulting in non-repeatable, inconsistent findings. The absence of repeatable and consistent results can lead to suboptimal decision making with respect to cyber risk reduction. There is a pressing need to reduce cyber risk assessment uncertainty by using tools that use well defined inputs, producing well defined results. This paper presents Automated Vulnerability and Risk Analysis (AVRA), an end-to-end process and tool for identifying and exploiting vulnerabilities, designed for use in cyber risk assessments. The approach presented is more comprehensive than traditional vulnerability scans due to its analysis of an entire network, integrating both host and network information. AVRA automatically generates a detailed model of the network and its individual components, which is used to create an attack graph. Then, AVRA follows individual attack paths, automatically launching exploits to reach a particular objective. AVRA was successfully tested within a virtual environment to demonstrate practicality and usability. The presented approach and resulting system enhance the cyber risk assessment process through rigor, repeatability, and objectivity.

Towards a Framework for Measuring the Performance of a Security Operations Center Analyst

Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke and Pete Burnap
School of Computer Science and Informatics Cardiff University Cardiff, UK

Abstract: The past few years have seen several studies reporting on the role of a Security Operations Center (SOC) analyst and metrics for assessing the performance of analysts. However, research suggests that analysts are dissatisfied with existing metrics as they fail to take into consideration several aspects of their tasks. Existing works advocate for research into this area. A major challenge to devising adequate metrics is that the real work of analysts that needs to be taken into consideration to assess their holistic performance has not been fully discussed. Furthermore, at present, there is no agreement on what constitutes core analysts' functions. Analysts' overall performance in a SOC could be obtained if there is a common agreement on the core functions upon which their performance can be evaluated. In this paper, we propose a framework depicting the core functions of analysts and KPIs that can be used to measure the performance of analysts. To do this, we conducted a thorough analysis of the functions of a SOC described in multiple sources of literature and engaged with several analysts and SOC managers from different industries using qualitative semi-structured interviews. Our research results identify the following: quality of analysts' analysis, quality of analysts' report, time-based measures and the absolute numbers derived from an analyst's tasks as the key performance indicators (KPIs) for assessing analysts' performance. We hope that our findings will stimulate more interest among cybersecurity researchers on assessment methods for analysts.

Privacy Protection Behaviours: a diversity of individual strategies

Bertrand Venard[1,2]
[1]Audencia, Nantes, France
[2]Oxford Internet Institute, University of Oxford, Oxford, UK

Abstract: The aim of the article is to study the determinants of privacy protection behaviours, using a qualitative approach with face-to-face interviews of students in France (N=49). Based on our interviews, we are able to find 2 main behaviours regarding privacy: surrender and defender. We found some empirical evidences for the privacy paradox. More than a static position, we show a dynamic positioning of our respondents between surrender and defender of their Online privacy that depends on: perceived personal susceptibility to digital threat, self-efficacy, catalytic information, social vs institutional space, type of shared information and age. Our research also shows that the privacy protection behaviour is highly related to the cybersecurity behaviour.

Developing a security behavioural assessment approach for cyber rating U.K. MSBs

Andrew Rae and Asma Patel
School of Computing and Communications, Lancaster University, Lancaster, UK
School of Computing and Digital Technologies, Staffordshire University, Staffordshire, UK

Abstract: Micro and small businesses in the U.K. account for over 99% of all U.K. businesses. Still, a growing perception gap is how these businesses perceive the relevance and value of cyber security and the potential impacts concerning them. The recent U.K. government studies have shown a significant increase in the average cost to these smaller businesses after suffering a disruptive attack. Yet, their engagement with recognised standards and best practices is still relatively low. This paper aims to ascertain the influences behind this situation and understand whether the implementation of a new security behavioural assessment methods is linked to an overall cyber rating scheme. This assessment will also provide a way to engage better and reduce the perception gap amongst smaller U.K. businesses while helping to drive better security behaviours overall.

Using Amazon Alexa APIs as a Source of Digital Evidence

Clemens Krueger and Sean McKeown
School of Computing, Edinburgh Napier University, Edinburgh, Scotland

Abstract: With the release of Amazon Alexa and the first Amazon Echo device, the company revolutionised the smart home. It allowed their users to communicate with, and control, their smart home ecosystem purely using voice commands. However, this also means that Amazon processes and store a large amount of personal data about their users, as these devices are always present and always listening in peoples' private homes. That makes this data a valuable source of evidence for investigators performing digital forensics. The Alexa Voice Service uses a series of APIs for communication between clients and the Amazon cloud. These APIs return a wide range of data related to the functionality of the device used. The first goal of this research was to clarify exactly what kind of

information about the user is stored and accessible through these APIs. To do this, a combination of literature review and exploratory analysis was used to establish a list of all relevant APIs. Then, possible artefacts and conclusions to be drawn from their responses were identified and presented. Lastly, the perspective of the users was taken, and options for improving their privacy were reviewed. Specifically, the history of interaction between the user and Alexa is available through multiple APIs, and there are several options to delete it. It was determined that these options have different behaviours and that most of them do not remove all data related to user interaction.

A Taxonomy of Approaches for Integrating Attack Awareness in Applications

Tolga Ünlü, Lynsay Shepherd, Natalie Coull and Colin McLean
Division of Cyber Security, School of Design and Informatics, Abertay University, Dundee, Scotland, UK

Abstract: Software applications are subject to an increasing number of attacks, resulting in data breaches and financial damage. Many solutions have been considered to help mitigate these attacks such as the integration of attack-awareness techniques. In this paper, we propose a taxonomy illustrating how existing attack awareness techniques can be integrated into applications. This work provides a guide for security researchers and developers, aiding them when choosing the approach which best fits the needs of their application.

Cyber-security research by ISPs: A NetFlow and DNS Anonymization Policy

Martin Fejrskov Andersen[1], Jens Myrup Pedersen[2] and Emmanouil Vasilomanolakis[3]
[1]Technology, IP Network and Core, Telenor A/S, Aalborg, Denmark
[2]Cyber Security Network, Aalborg University, Aalborg, Denmark
[3]Cyber Security Network, Aalborg University, Copenhagen, Denmark

Abstract: Internet Service Providers (ISPs) have an economic and operational interest in detecting malicious network activity relating to their subscribers. However, it is unclear what kind of traffic data an ISP has available for cyber-security research, and under which legal conditions it can be used. This paper gives an overview of the challenges posed by legislation and of the data sources available to a European ISP. DNS and NetFlow logs are identified as relevant data sources and the state of the art in anonymization and fingerprinting techniques is discussed. Based on legislation, data availability and privacy considerations, a practically applicable anonymization policy is presented.

Towards Security Attack and Risk Assessment during Early System Design

Lukas Gressl[1], Michael Krisper[1], Christian Steger[2] and Ulrich Neffe[3]
[1]ITI TU Graz, Austria
[2]Austria TU GRaz, Austria
[3]Austria NXP Semiconductors Austria GmbH

Abstract: The advent of the Internet of Things (IoT) and Cyber-Physical Systems (CPS) enabled a new class of connected, smart, and interactive devices. With their continuous connectivity and their access to valuable information in both the digital and physical world, they are highly attractive targets for security attackers. Hence, with their integration into both the industry and devices used in our daily lives, they added a new surface for cybersecurity attacks. These potential threats call for special care of security vulnerabilities during the design of novel IoT devices and CPS. The design of secure systems is a complex task, especially if they must adhere to various other constraints, such as performance, power consumption, and others. A range of design space exploration tools have been proposed in academics, which aim to support system designers in their task of finding the optimal selection of hardware components and task mappings. Said tools offer a limited way of modeling attack scenarios as constraints for a system under design. The framework proposed in this paper aims at closing this gap, offering system designers a way to consider security attacks and security risks during the early phase of system design. It offers designers the possibility to model security constraints from the view of potential attackers, assessing the probability of successful security attacks and security risk. The framework's feasibility and performance is demonstrated by revisiting a potential system design of an industry partner.

Technical codes' potentialies in cyber security. A contextual approach on the ethics of small digital organizations in France

Theo Simon[1] and Bertrand Venard[2]
[1]Management department Audencia Nantes, France
[2]Audencia, Oxford Internet Institute University of Oxford Oxford, UK

Abstract: With the proliferation of malware, viruses and phishing attacks, information security has become a major challenge for companies. Organizations of all sizes have had to develop efficient cybersecurity strategies. Part of the literature has explained the growing cyber risks by the human factor such as the mistakes of users. Our aim is to analyse the user's ethics in relation to the security of information technology system. We used the Feenberg's concepts of technical codes' potentialities to interpret the technical codes of users about information security (IS). We found three technical codes representing a variety of dimensions and combined a diversity of point of view about IS: interest, values and priorities. These technical codes allow us to uncover alternative representations of user's ethics and to think critically on the way researchers, practitioners and information security specialists' views and imagine the future of information security among tiny structures. Our empirical findings are based on a qualitative research among tiny organizations with similar information and communication technology security in France.

Examining the Impact of Implementing Cyber Security Articulation Agreements Between Public and Private Higher Educational Institutions in 9-12 High Schools

Thomas Rzemyk
Mount Michael Benedictine School, Columbia Southern University, USA

Abstract: Abstract— Over the past decade, the term cyber security has become quite the buzzword in the public and private sectors in the United States and abroad. Further, there has been explosive growth and interest in cyber security majors at colleges and universities globally. In addition to added growth in higher education, many high school students (grades 9-12) are now seeking out programs that offer science, engineering, technology, mathematics (STEM) and cyber security-based curriculum at the high school level. Educating young men and women in cyber security curriculum prior to college will address the work sector shortage of STEM based professionals for both males and females that exists today. It is imperative that both 9-12 high schools and higher educational institutions take notice to the growing trends in cyber security curriculum today. This work in progress paper will outline proven best practices that public and private 9-12 high schools can use to establish relationships with colleges and universities to secure valuable cyber security and STEM education articulation agreements. Over the past four years, a private high school in the state of Nebraska (lead by the author of this paper) has utilized several strategies to formulate a collaborative relationship and articulation agreement with the University of Nebraska-Omaha to offer college credits to grades 9-12 for those that take a dual-enrollment course entitled Cyber Security. The outcomes of this research will focus on strategies to: collaborative course syllabus development with host universities, course credit and semester hour allocations, training students, professional development for cyber security faculty, integrating field trips to data centers, bringing in professional cyber security speakers from the private sector and government agencies, establishing networking and internship opportunities, offering hands-on and virtual computer networking labs, and much more.. This work in progress will present data results, graduation records, course majors, job placement results, internship results, and much more from those students who have taken Cyber Security over the 48 months.

Testing and Hardening IoT Devices Against the Mirai Botnet

Christopher Kelly[1], Nikolaos Pitropakis[1], Sean Mckeown[1] and Costas Lambrinoudakis[2]
[1]School of Computing, Edinburgh Napier University, Edinburgh, Scotland, UK
[2]Department of Digital Systems, University of Piraeus, Greece

Abstract: A large majority of cheap Internet of Things (IoT) devices that arrive brand new, and are configured with out-of-the-box settings, are not being properly secured by the manufactures, and are vulnerable to existing malware lurking on the Internet. Among them is the Mirai botnet which has had its source code leaked to the world, allowing any malicious actor to configure and unleash it. A combination of software assets not being utilised safely and effectively are exposing consumers to a full compromise. We configured and attacked 4 different IoT devices using the Mirai libraries. Our experiments concluded that three out of the four devices were vulnerable to the Mirai malware and became infected when deployed using their default configuration. This demonstrates that the original security configurations are not sufficient to provide acceptable levels of protection for consumers, leaving their devices exposed and vulnerable. By analysing the Mirai libraries and its attack vectors, we were able to determine

appropriate device configuration countermeasures to harden the devices against this botnet, which were successfully validated through experimentation.

Sociotechnical Approaches to Cyber Security in Emerging Nations: A Case Study in Risk Management for Rwandan Health Care

Joseph Kaberuka and Christopher Johnson
School of Computing Science, The University of Glasgow, Glasgow, Scotland, UK

Abstract: Healthcare is increasingly dependent on digital systems. In emerging nations, it can be particularly hard for hospital administrators to maximize the benefits of these advances and at the same time mitigate the potential cyber security risks associated with healthcare information systems. This paper argues that limited resources, rising demand and rapidly evolving organizational structures create a pressing need for holistic approaches to address sociotechnical security challenges in healthcare. We do not underestimate the technological challenges of cyber security in these countries; equally technical solutions are unlikely to be effective unless supported by holistic risk assessment. We address these problems by the use of STAMP (Systems Theoretic Accident Model and Processes) for cyber security analysis, STPA-sec. Our results show that this open-ended analytical technique requires additional methodological structure in countries where there are significant shortages of trained analysts; to guide the application of STPA-sec and also to provide common reference when individual analysts must justify their findings. It is for this reason that we explicitly integrate the US National Institute of Science and Technology (NIST) controls into STPA-sec. This provided our stakeholders with a starting point for the application of socio-technical analysis; further studies are required to determine whether such support becomes superfluous as analysts become familiar with socio-technical methods. Our arguments have been validated through extensive observation, interviews and document reviews with healthcare providers in Rwanda. In particular, we focus on an initiative to improve the cyber security of a hospital Picture Archiving and Communication System (PACS). It is our hope that the lessons learned in one country might inform cyber security risk management for healthcare across other emerging nations who face limited resources, significant public demand and an increasing range of threats.

Restricting Data Flows to Secure Against Remote Attack

John Oraw[1] and David Laverty[2]
[1]Department of Computing Letterkenny Institute of Technology Donegal, Ireland
[2]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast

Abstract: Fully securing networks from remote attacks is recognized by the IT industry as a critical and imposing challenge. Even highly secure systems remain vulnerable to attacks and advanced persistent threats. One-way flows are a novel approach to improving the security of telemetry for critical infrastructure, retaining some of the benefits of inter-connectivity whilst maintaining a level of network security analogous to that of unconnected devices. Simple and inexpensive techniques can be used to provide this unidirectional security, removing the risk of remote attack from a range of potential targets and subnets. The application of one-way networks is demonstrated using IEEE compliant PMU data streams as a case study. Scalability is demonstrated using SDN techniques. Finally, these techniques are combined, demonstrating a node which can be secured from remote attack, within defined limitations.

Deep Down the Rabbit Hole: On References in Networks of Decoy Elements

Daniel Reti, Daniel Fraunholz, Janis Zemitis, Daniel Schneider and Hans Dieter Schotten
Intelligent Networks Research Group, German Research Center for Artificial Intelligence, Kaiserslautern, Germany

Abstract: Deception technology has proven to be a sound approach against threats to information systems. Aside from well-established honeypots, decoy elements, also known as honeytokens, are an excellent method to address various types of threats. Decoy elements are causing distraction and uncertainty to an attacker and help detecting malicious activity. Deception is meant to be complementing firewalls and intrusion detection systems. Particularly insider threats may be mitigated with deception methods. While current approaches consider the use of multiple decoy elements as well as context-sensitivity, they do not sufficiently describe a relationship between individual elements. In this work, inter-referencing decoy elements are introduced as a plausible extension to existing deception frameworks, leading attackers along a path of decoy elements. A theoretical foundation is introduced, as well as a stochastic model and a reference implementation. It was found that the proposed system is suitable to enhance current decoy frameworks by adding a further dimension of inter-connectivity and therefore improve intrusion detection and prevention.

An Empirical Study of Key Generation in Cryptographic Ransomware

Pranshu Bajpai and Richard Enbody
Department of Computer Science and Engineering, College of Engineering, Michigan State University, USA

Abstract: Ransomware implement a denial-of-access attack on a user's irreplaceable data achieved by encrypting user files. Successful encryption requires secure key generation and therefore understanding ransomware's key generation procedures is critical for developing effective solutions. This paper presents a study of key generation strategies observed in modern ransomware. We explain the weak strategies that we have discovered to be in use that can be circumvented and strong strategies that cannot be circumvented. We provide empirical evidence in the form of code snippets and disassembly of real-world ransomware. Finally, we provide guidance on swiftly identifying the differences between effective and weak key generation strategies in novel ransomware.

Forensic Considerations for the High Efficiency Image File Format (HEIF)

Sean Mckeown and Gordon Russell
School of Computing, Edinburgh Napier University, Edinburgh, Scotland

Abstract: The High Efficiency File Format (HEIF) was adopted by Apple in 2017 as their favoured means of capturing images from their camera application, with Android devices such as the Galaxy S10 providing support more recently. The format is positioned to replace JPEG as the de facto image compression file type, touting many modern features and better compression ratios over the aging standard. However, while millions of devices across the world are already able to produce HEIF files, digital forensics research has not given the format much attention. As HEIF is a complex container format, much different from traditional still picture formats, this leaves forensics practitioners exposed to risks of potentially mishandling evidence. This paper describes the forensically relevant features of the HEIF format, including those which could be used to hide data, or cause issues in an investigation, while also providing commentary on the state of software support for the format. Finally, suggestions for current best-practice are provided, before discussing the requirements of a forensically robust HEIF analysis tool.

Secure Framework for Anti-Money-Laundering using Machine Learning and Secret Sharing

Arman Zand, James Orwell and Eckhard Pfluegel
Faculty of Science, Engineering & Computing, Kingston University, London, UK

Abstract: Nowadays, the scale of Money Laundering is difficult to estimate in the UK and elsewhere. Proceeds of crimes might be transferred using the available business infrastructure offered by banks, and this is a considerable problem. This paper makes three contributions to the development of transaction analysis systems to detect money laundering activity. The first contribution is a novel framework given in an Anti-Money Laundering (AML) context that encompasses collaboration, analysis and cryptography. Such a system that must respect confidentiality constraints is a primary requirement, given that both banks and their clients have commercial and legal motivations for maintaining the privacy of transaction information. An innovative system is proposed that satisfies these constraints, using cryptographically secure signals generated by the banks, and then a secret sharing protocol to give feedback to co-operating banks. This allows banks to participate in the collective analysis of transactions, without compromising client confidentiality. The second contribution is to the detection process that operates on the set of cryptographic signals. A suitable real-time detection architecture is proposed, with detailed consideration of data-set characteristics, and engineering of input features. The output, defined as the probability that any given transaction is associated with money laundering activity, can be used in isolation or else integrated alongside estimates derived from other approaches, outside the domain of transaction analysis, as part of an overall process for accurate and timely detection of money laundering activity. Finally, the third contribution is the application of secret sharing in order for banks to recover the probability of money laundering in a secure collaborative fashion. To our knowledge, this is the first proposal to AML combining both machine learning and secret sharing.

What Could Possibly Go Wrong? Smart Grid Misuse Case Scenarios

Inger Anne Tøndel[1], Ravishankar Borgaonkar[1], Martin Gilje Jaatun[1] and Christian Frøystad[2]
[1]Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway
[2]Secure Practice, Trondheim, Norway

Abstract: In this paper we present misuse cases related to Smart Grid security in three overall areas: Managing flexibility in the TSO-DSO relation, Smart distribution grids and Microgrids. The misuse cases represent potential security challenges to be considered when working on modernising the grid, however they are not exhaustive. Future

work can include improving the misuse case scenarios as more details on the future solutions become available. More important is however to take such scenarios into account when working on future solutions, so that the risks associated with these and other misuse case scenarios can be reduced.

ethVote: Towards Secure Voting with Distributed Ledgers

Johannes Mols and Emmanouil Vasilomanolakis
Cyber Security Network, Aalborg University, Copenhagen, Denmark

Abstract: The topic of performing safe and secure elections is a long-standing debate. Regardless, of the various attempts for electronic or Internet-based voting, the majority of countries still use paper ballots. Nevertheless, with major advancements occurring over the last years in both cryptography and distributed ledgers we believe that there is space now for re-investigating this area. In this paper, we propose ethVote an Internet voting system that makes use of the Ethereum blockchain, state of the art cryptographic mechanisms and a P2P-based front-end to ensure a secure voting process. In addition, we provide an open-source proof of concept implementation that features the majority of the needed components for securely using ethVote. Our proposal is tested both in terms of unity testing, requirement verification, and with regard to the feasibility to perform such an operation in a public distributed ledger.

A DLT-based Trust Framework for IoT Ecosystems

Tharindu Ranathunga[1], Ramona Marfievici[2], Alan McGibney[1] and Susan Rea[1]
[1]Cork Institute of Technology, Ireland
[2]Digital Catapult, UK

Abstract: An IoT eco-system includes IoT network components, network services and network participants such as organizations, consumers, governments, and businesses. Due to its diversity and scale, trustworthiness is a critical concern to be considered during architectural design and the operational phase of these eco-systems. To do this, security, privacy, reliability, resilience and safety must be assured. However, existing solutions partially address these requirements using centralized approaches that come with challenges such as a single point of failure, scalability, and dependence on a third party. In this context, Distributed Ledger Technology (DLT) and Smart Contracts, due to its intrinsic properties of transparency, immutability, and underlying secure-by-design architecture allows distributed, decentralized, automated workflows which can be incorporated to automate the management of the next generation IoT networks. In this paper, we propose a framework for IoT eco-systems providing seamless integration between IoT and DLT to create a decentralized trusted architecture which ensures trustworthiness of IoT eco-systems at design time and a trust reputation model based on the architecture to protect it during the run-time. Furthermore, we have presented the initial steps towards the implementation of this framework.

Memory Forensics Against Ransomware

Pranshu Bajpai and Richard Enbody
Department of Computer Science and Engineering, College of Engineering, Michigan State University, USA

Abstract: Ransomware leverages the unique knowledge of cryptographic secrets, such as the encryption key, against the victim. Obtaining the decryption key removes that leverage and hence eliminates the requirement of paying the ransom. In this paper, we examine the effectiveness of physical memory forensics against ransomware to recover raw symmetric and asymmetric keys and demonstrate file decryption against several real-world ransomware. We also use our own virulent ransomware that are equipped with an effective hybrid cryptosystem to explore the limits of such memory-based side-channel attacks on ransomware. Our results indicate that cryptographic keys can be discovered during encryption in the ransomware process memory for durations long enough to facilitate complete data recovery.

Slave Clock Responses to Precision Time Protocol Attacks: A Case Study

Waleed Alghamdi and Michael Schukat
School of Computer Science National University of Ireland, Galway Galway, Ireland

Abstract: The IEEE 1588 Precision Time Protocol (PTP) is especially important for many financial and industrial applications, as it can provide highly accurate time synchronisation down to microsecond level. However, any PTP infrastructure is vulnerable to cyber-attacks that can de-synchronise some or all network devices, causing potentially destructive consequences. This paper will focus on how two of these attacks, the asymmetric delay and the byzantine

attack, can be implemented in a PTP network, analyses their impact on slave clocks, and investigates how these attacks can be detected.

"What did you say?": Extracting unintentional secrets from predictive text learning systems

Gwyn Wilkinson and Phil Legg
Department of Computer Science and Creative Technologies, The University of the West of England, Bristol, UK

Abstract: As a primary form of communication, text is used widely for online communications, including e-mail conversations, mobile text messaging, chatroom and forum discussions. Modern systems include facilities such as predictive text, recently implemented using deep learning algorithms, to estimate the next word to be written based on previous historical entries. However, we often enter sensitive information such as passwords using the same input devices - namely, smartphone soft keyboards. In this paper, we explore the problem of deep learning models which memorize sensitive training data, and how secrets can be extracted from predictive text models. We propose a general black-box attack algorithm to accomplish this for all kinds of memorised sequences, discuss mitigations and countermeasures, and explore how this attack vector could be deployed on an Android or iOS mobile device platforms as part of target reconnaissance.

Introducing a forensics data type taxonomy of acquirable artefacts from programmable logic controllers

Marco Cook, Ioannis Stavrou, Sarah Dimmock and Christopher Johnson
School of Computing Science, University of Glasgow, Glasgow, Scotland

Abstract: The understanding of available data artefacts is fundamental to performing digital forensics. There is good understanding of what data artefacts are acquirable from common information technology (IT) systems such as a Windows operating system and what their potential forensic value could be. As a result, IT forensic investigators can make clear predictions about what information the acquired data would yield. The same level of understanding for programmable logic controllers (PLCs) found within industrial control systems (ICS) is limited. Previous research has restricted the discussion of PLC data to generic and common data formats. This makes it challenging to prepare for incidents proactively, develop new forensic capabilities and prioritise the collection of data should an incident occur. Examples of previous cyber incidents such as Stuxnet and Triton have employed ad-hoc methods for forensic the investigation, highlighting the lack of a systematic approach. This paper examines the specific data types stored on a PLC and describes a forensic artefact taxonomy based on the acquirable data. Data acquisition tests were performed primarily using third-party communication libraries that utilise the PLC's proprietary industrial communications protocol to leverage data stored within memory structures of each of the tested PLCs. Three PLCs, from two different manufacturers were examined. Potential PLC attack scenarios, identified from the literature, were used to guide the evaluation of the acquirable data, categorised into high-level data types, to highlight the potential benefits of acquiring each form of data.

Moving Targets: Addressing Concept Drift in Supervised Models for Hacker Communication Detection

Andrei Queiroz[1], Brian Keegan[2] and Susan Mckeever[2]
[1]Informatics Centre - CPD, University of Bras´ılia - UnB, Bras´ılia, Brazil
[2]Applied Intelligence Research Centre, Technological University (TU) Dublin, Dublin, Ireland

Abstract: In this paper, we are investigating the presence of concept drift in machine learning models for detection of hacker communications posted in social media and hacker forums. The supervised models in this experiment are analysed in terms of performance over time by different sources of data (Surface web and Deep web). Additionally, to simulate real-world situations, these models are evaluated using time-stamped messages from our datasets, posted over time on social media platforms. We have found that models applied to hacker forums (deep web) presents an accuracy deterioration in less than a 1-year period, whereas models applied to Twitter (surface web) have not shown a decrease in accuracy for the same period of time. The problem is alleviated by retraining the model with new instances (and applying weights) in order to reduce the effects of concept drift. While our results indicated that performance degradation due to concept drift is avoided by 50% relabelling, which is challenging in real-world scenarios, our work paves the way to more targeted concept drift solutions to reduce the re-training tasks.

Smarter Password Guessing Techniques Leveraging Contextual Information and OSINT

Aikaterini Kanta[1, 2], Iwen Coisel[2] and Mark Scanlon[2]
[1]Forensics and Security Research Group, School of Computer Science, University College Dublin, Ireland
[2]Cyber and Digital Citizen Security, European Commission Joint Research Centre, Ispra, Italy

Abstract: In recent decades, criminals have increasingly used the web to research, assist and perpetrate criminal behaviour. One of the most important ways in which law enforcement can battle this growing trend is through accessing pertinent information about suspects in a timely manner. A significant hindrance to this is the difficulty of accessing any system a suspect uses that requires authentication via password. Password guessing techniques generally consider common user behaviour while generating their passwords, as well as the password policy in place. Such techniques can offer a modest success rate considering a large/average population. However, they tend to fail when focusing on a single target -- especially when the latter is an educated user taking precautions as a savvy criminal would be expected to do. Open Source Intelligence is being increasingly leveraged by Law Enforcement in order to gain useful information about a suspect, but very little is currently being done to integrate this knowledge in an automated way within password cracking. The purpose of this research is to delve into the techniques that enable the gathering of the necessary context about a suspect and find ways to leverage this information within password guessing techniques.

Epistemological Questions for Cybersecurity

Timothy D. Williams
School of Construction Management and Engineering, University of Reading, Reading, UK

Abstract: The purpose of this theoretical paper is to facilitate interdisciplinary dialogue regarding the roots of knowledge be- tween cybersecurity researchers and those from other disciplines. The approach taken is to articulate questions based on personal reflections on the common ground and differences between cybersecurity knowledge and selected epistemological sources. Although no independent evidence is presented for the validity or utility of these questions, the author hopes to refine these questions and the underlying assumptions on which they are based both through feedback on this paper and empirical data capture.

Privacy Policy – “I agree”?! – Do alternatives to text-based policies increase the awareness of the users?

Pascal Faurie, Arghir-Nicolae Moldovan and Irina Tal
School of Computing National College of Ireland Dublin, Ireland

Abstract: Since GDPR was introduced, there is a reinforcement of the fact that users must give their consent before their personal data can be managed by any website. However, many studies demonstrated that users often skip these policies and click the ”I agree” button to continue browsing, being unaware of what the consent they gave was about, hence defeating the purpose of GDPR. This paper aims to investigate if different ways of presenting users the privacy policy can change this behaviour and can lead to an increased awareness of the user in relation to what the use agrees with. Three different types of policies were used in the study: a full-text policy, a ‘so called’ usable policy and a video-based policy. Results demonstrated that the type of policy have a direct influence on the user awareness and user satisfaction. The two alternatives to the text-based policy lead to a significance increase of user awareness in relation to the content of the policy and to a significant increase in the user satisfaction in relation to the usability of the policy.

Platform for monitoring and clinical diagnosis of arboviruses using computational models

Sebastião Rogério da Silva Neto[1], Thomás Tabosa de Oliveira[1], Vanderson Sampaio[2,3], Theo Lynn[4] and Patricia Endo[1,4]
[1]Universidade de Pernambuco, Brazil
[2]Fundac¸˜ao de Medicina Tropical, Brazil
[3]Fundac¸˜ao de Vigilˆancia em Sa´ude do Amazonas, Brazil
[4]Irish Institute of Digital Business, Ireland

Abstract: As part of SDG, the members of the UN aim to end epidemics of neglected tropical diseases by 2030. These include wide range communicable diseases that prevail in tropical and subtropical conditions. These diseases are present in over 149 countries worldwide and are a significant burden on health systems and economies. One major category of neglected tropical disease are arthropod-borne viruses or arboviruses including West Nile virus,

yellow fever, dengue, chikungunya and Zika. Arboviruses spread rapidly and as they present very similar symptoms, it is hard to diagnose and select the best treatment. The use of machine learning for the diagnosis and prognosis of these diseases has become increasingly common however there is a paucity of research on deep learning and associated decision support platforms for frontline staff. This work-in-progress proposes a platform for arbovirus monitoring and clinical diagnosis using deep learning models.

Evaluation of Machine Learning Algorithms for Anomaly Detection

Nebrase Elmrabit[1], Feixiang Zhou[2], Fengyin Li[3] and Huiyu Zhou[2]
[1]Department of Cyber Security Glasgow Caledonian University Glasgow, UK
[2]School of Informatics University of Leicester Leicester, UK
[3]School of Information Science Qufu Normal University Rizhao 276826, China

Abstract: Malicious attack detection is one of the critical cyber-security challenges in the peer-to-peer smart grid platforms due to the fact that attackers' behaviours change continuously over time. In this paper, we evaluate twelve Machine Learning (ML) algorithms in terms of their ability to detect anomalous behaviours over the networking practice. The evaluation is performed on three publicly available datasets: CICIDS-2017, UNSW-NB15 and the Industrial Control System (ICS) cyber-attack datasets. The experimental work is performed through the ALICE high-performance computing facility at the University of Leicester. Based on these experiments, a comprehensive analysis of the ML algorithms is presented. The evaluation results verify that the Random Forest (RF) algorithm achieves the best performance in terms of accuracy, precision, Recall, F1-Score and Receiver Operating Characteristic (ROC) curves on all these datasets. It is worth pointing out that other algorithms perform closely to RF and that the decision regarding which ML algorithm to select depends on the data produced by the application system.

An Overview of Web Robots Detection Techniques

Hanlin Chen, Hongmei He and Andrew Starr
School of Aerospace, Transport and Manufacturing, Cranfield University, UK

Abstract: Web robots or web crawlers have become the major source of web traffic. While some robots are well-behaving such as search engines, others can perform DDoS attacks, which put great threats on websites. Effectively detecting web robots will benefit not only for network traffic cleaning, but also for improving the cybersecurity of IoT enabled systems and services. To get the state of the arts in web robot detection, this paper reviews recent decade research on web robot or web robot/crawler detection techniques and compares their performances and identify the challenges of different techniques, thus providing researchers a reference for the development of web robots detection in real applications. To protect web content from malicious web robots, researchers have investigated various approaches, but they can be classified into three themes: offline web log analysis, honeypots and online robot detection. We conclude that off-line web log analysis methods have quite high accuracy, but they are time-consuming compared to online detection methods. Honeypots, as a computer security mechanism, can be used to engage and deceive hackers and identify malicious activities performed over the Internet, but they may block legitimate robots. The review shows that a hybrid method is better than an individual classifier, and the performance of online web robot detection needs to be improved. Also, different types of features could play different roles in different machine learning models. Therefore, feature selection is important for web robot/crawler detection.

Cost-Effective OCR Implementation to Prevent Phishing on Mobile Platforms

Yunjia Wang[1], Yang Liu[2], Tiejun Wu[3] and Ishbel Duncan[1]
[1]University of St Andrews, UK
[2]Independent Scholar, China
[3]NSFocus IT Co Ltd, China

Abstract: Phishing is currently defined as a criminal mechanism employing both social engineering and technical subterfuge to gather any useful information such as: user personal data or financial account credentials. Many users are sensible about this kind of attack from suspicious URL addresses or obvious warning information from browsers, but phishing still accounts for a larger proportion of all of malicious attacks. Moreover, these warning features will be eliminated if the victim is under a DNS hijacking attack. There is much research about the prevention and evaluation of phishing, in both PC platforms and mobile platforms, but there are still technical challenges to reducing the risk from phishing, especially in mobile platforms. We presented a novel method to prevent phishing attacks by using an Optical Character Recognition (OCR) technology in a previous paper. This method not only overcomes the limitation of current preventions, but also provides a high detection accuracy rate. However, whether this method can be implemented ideally in mobile devices needed to be further examined, especially in relation to the challenges of

limited resources (power and bandwidth). In this paper, we apply the OCR method in a mobile platform and provide a prototype implementation scheme to determine applicability. Experiments are performed to test the technique under DNS hijacking attacks.

Automated Artefact Relevancy Determination from Artefact Metadata and Associated Timeline Events

Xiaoyu Du, Quan Le and Mark Scanlon
University College Dublin, Ireland

Abstract: Case-hindering, multi-year digital forensic evidence backlogs have become commonplace in law enforcement agencies throughout the world. This is due to an ever-growing number of cases requiring digital forensic investigation coupled with the growing volume of data to be processed per case. Leveraging previously processed digital forensic cases and their component artefact relevancy classifications facilitates the opportunity for training automated artificial intelligence based evidence processing systems to aid investigators in the discovery and prioritisation of evidence. This paper presents one approach for file artefact relevancy determination based on the growing move towards a centralised, Digital Forensics as a Service (DFaaS) paradigm. This approach enables the use of previously encountered illegal files to detect pertinent files in an investigation. Trained models can aid in the detection of these files during the acquisition stage, i.e., during their upload to a DFaaS system. The technique used is based on a relevancy score determined from file similarity using each artefact's filesystem metadata and associated timeline events. The approach presented is validated against three experimental usage scenarios.

Think Smart, Play Dumb: A Game-Theoretic Approach to Study Deception in Hardware Trojan Testing

Tapadhir Das, Abdelrahman Eldosouky and Shamik Sengupta
Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA

Abstract: In recent years, integrated circuits (ICs) have become significant for various industries and their security has been given greater priority, specifically in the supply chain. Budgetary constraints have compelled IC designers to offshore manufacturing to third-party companies. When the designer gets the manufactured ICs back, it is imperative to test for potential threats like hardware trojans (HT). In this paper, a novel multi-level game-theoretic framework is introduced to analyze the interactions between a malicious IC manufacturer and the tester for the IC designer. In particular, the game is formulated as a non-cooperative, zero-sum, repeated game using prospect theory (PT) that captures different players' rationalities under uncertainty. The repeated game is separated into a learning stage, in which the defender learns about the attacker's tendencies, and an actual game stage, where this learning is used. Experiments show great incentive for the attacker to deceive the defender about their actual rationality by "playing dumb" in the learning stage (deception). This scenario is captured using hypergame theory to model the attacker's view of the game. The optimal deception rationality of the attacker is analytically derived to maximize utility gain. For the defender, a first-step deception mitigation process is proposed to thwart the effects of deception. Simulation results show that the attacker can profit from the deception as it can successfully insert HTs in the manufactured ICs without being detected.

Towards Detecting Human Actions, Intent, and Severity of APT Attacks by Applying Deception Techniques

Joel Chacon, Sean McKeown and Richard Macfarlane
Eigen Ltd, Surrey, England, UK
School of Computing, Edinburgh Napier University Edinburgh, Scotland

Abstract: Deception techniques and decoy objects, often called honey items, can be useful in intrusion detection, and attack analysis. Attacks by Advanced Persistent Threats (APTs) have been shown to be difficult to detect due to the stealthy and sophisticated nature of the attack techniques. Structured attacks carried out over a period of time are difficult for traditional defences to detect. Using deception techniques and honey items may be a way of highlighting these APT actor type interactions as they progress through a structured attack. This work explores the use of honey items to classify intrusion interactions, differentiating automated attacks from those which need some human reasoning and interaction towards APT detection. Multiple decoy items are deployed on honeypots in a virtual honey network, some as breadcrumbs to detect indications of a structured manual attack. Monitoring functionality was created around Elastic Stack with a Kibana dashboard created to display interactions with various honey items. APT type manual intrusions are simulated by an experienced pen testing practitioner carrying out simulated attacks.

The results show that it is possible to differentiate automatic attacks from manual structured attacks; from the nature of the interactions with the honey items. The use of honey items found in the honeypot, such as in later parts of a structured attack, have been shown to be successful in classification of manual attacks, as well as towards providing an indication of severity of the attacks.

Assessing the Influencing Factors on the Accuracy of Underage Facial Age Estimation

Felix Anda, Brett Becker, David Lillis, Nhien-An Le-Khac and Mark Scanlon
University College Dublin, Ireland

Abstract: Swift response to the detection of endangered minors is an ongoing concern for law enforcement with the rapid growth of disk capacities and data being stored in the cloud. Automated tools are needed to aid in CSEM investigation -- both to expedite the evidence discovery process, while lessening the investigator's exposure to traumatic material. In these investigations, age estimation techniques show great promise in helping decrease the overflowing backlog of evidence obtained from the vast array of devices and online services. A lack of sufficient training data combined with natural human variance has been hindering accurate automated age estimation, especially for underage subjects. A comprehensive evaluation of the performance achieved on over 21,800 underage subjects with two cloud age estimation services is presented, namely Amazon Web Service's Recognition service and Microsoft Azure's Face API. The objective of this work is to evaluate the influence that certain human biometric factors, facial expressions, and image quality, i.e., blur, noise, exposure and resolution, have on the outcome of automated age estimation services. The thorough evaluation of the correlation and effects of such factors aids the understanding of the performance and allows us to identify the most influencing factors to be overcome in future age estimation modelling.

Insider Threat Detection: A Solution in Search of a Problem

Jordan Schoenherr[1,2] and Robert Thomson[2]
[1]Institute of Data Science, Department of Psychology, Carleton University, Canada
[2]ACI, US Military Academy, Canada

Abstract: Insider threats (IT) reflects a growing concern in the security communities. Despite a rapid increase in the number of papers examining IT, definitions, research methods, and models, critical evaluations are rare. The present paper provides a critical review of these issues. Definitions of insider threat have varied from general, focusing on all forms of organizational deviant behavior to specific, focusing on individual difference and social context variables. Research methods include models based on deductive principles and based on intuitions of subject matter experts, computational models based on social media activity, and empirical observations based on synthetic or inaccessible data sets, i.e., black data. Following a review of these considerations, we demonstrate that many existing approaches within the behavioral and social sciences can provide more solid foundations to the IT literature. Using insight from research on organizational deviant behavior and workplace incivility, we conclude by proposing a multidimensional classification system for insider threat SIEVE: severity (S), intentionality (I), type of employee norm violation (EV), and ethicality (E).

Introducing & Evaluating ‘Nutrition Facts’ for Online Content

Matthew Spradling[1], Jeremy Straub[2] and Jay Strong[1]
[1]Computer Science, Engineering, and Physics Department, University of Michigan, USA
[2]Institute for Cyber Security Education and Research North Dakota State University, USA

Abstract: So-called ‘fake news’ – deceptive online content that attempts to manipulate readers – is a growing problem. It has been blamed for election interference, public confusion and other issues, both in the United States and beyond. A tool of state intelligence agencies, scammers and marketers alike, deceptive online content is poised to have growing consequences. This problem is made particularly pronounced as younger generations choose social media sources over journalistic ones for their information. This paper considers a prospective solution in the form of providing consumers with ‘nutrition facts’ style information for online content. To this end, it reviews prior work in product labeling and disclaimers, considers several possible approaches to the challenge and the tradeoffs between them.

AI Crimes: A Classification

Fadi Sibai
College of Computer Engineering and Science, Prince Mohammad Bin Fahd University, Al-Khobar, Saudi Arabia

Abstract: Intelligent and machine learning systems have infiltrated cyber-physical systems and smart cities with technologies such as IOT, image processing, robotics, speech recognition, self-driving, and predictive maintenance. To gain user trust, such systems must be transparent and explicable. Regulations are required to control crimes associated with these technologies. Such regulations and legislations depend on the severity of the AI crimes subject to these regulations, and on whether humans and/or intelligent systems are responsible for committing such crimes, and therefore can benefit from a classification tree of AI crimes. The aim of this paper to review prior work in ethics for AI, and classify AI crimes by producing a classification tree to assist in AI crime investigation and regulation.

Social big data: A Twitter text mining approach to the communication of universities during the Lebanese protests

Katia Raya[1], Nicole D'almeida[2] and Maroun Chamoun[3]
[1]CELSA - ESIB Sorbonne University – Saint Joseph University of Beirut Beirut, Lebanon
[2]CELSA Sorbonne University Paris, France
[3]ESIB Saint Joseph University of Beirut Beirut, Lebanon

Abstract: Since October 17, 2019, Lebanon has experienced unprecedented popular protests, demanding the departure of the entire political class, accused of being gangrened by corruption. Country paralyzed, institutions closed for more than two weeks, the eyes are turned to universities that have closed their doors but whose community (teachers and students) actively participate in the national jump. This study explores the use of social media by universities in Lebanon during the national revolution using social big data technology on Twitter in comparison to the national usage of twitter. Important information was collected, analyzed and visualized using the R language.

Blurring lines between fiction and reality: Perspectives of experts on marketing effectiveness of virtual influencers

Evangelos Moustakas[1], Nishtha Lamba[1], Dina Mahmoud[3] and C Ranganathan[2]
[1]Marketing, Branding and Tourism, Middlesex University Dubai Dubai, UAE
[2]Information and Decision Sciences University of Illinois at Chicago, Chicago, USA
[3]MPN Social, Dubai, UAE

Abstract: Virtual influencers are computer generated human avatars with a wide following on social media. Luxury brands such as Louis Vuitton and Prada are increasingly partnering with them to promote their new line of products. Lil Miquela, the most popular virtual influencer, has 1.7 million followers on Instagram. She is fictional, recognizes herself as a robot, but displays human emotions through her posts and interactions with her followers. Generally, research suggests that virtual influencers offer novelty but may lack authenticity and reliability like human social influencers. Despite increased recent media attention on the topic, to our knowledge, there is no empirical research on the effectiveness of using virtual influencers as a marketing gimmick. Due to lack of literature in the field, we chose an exploratory qualitative design to explore the advantages and disadvantages of using fictional characters as a marketing strategy. We administered semi-structured interviews with six experts in the field of digital media. Thematic analysis was utilized to explore repetitive patterns in their opinions and suggestions. The respondents primarily highlighted potential challenges of using virtual influencers, identified factors which may make them successful as a marketing strategy, and compared the appeal of humanized versus animated virtual influencers.

Shouting Through Letterboxes: A study on attack susceptibility to voice assistants

Andrew McCarthy, Benedict Gaster and Phil Legg
Department of Computer Science and Creative Technologies, University of the West of England

Abstract: Voice assistants such as Amazon Echo and Google Home have become increasingly popular for many home users, for home automation, entertainment, and convenience. These devices will process speech commands from a user to execute some action, such as playing music, making online purchases, or triggering home automation such as lights or security locks. The process of mapping speech input to a text command is performed using a machine learning model. In this study, we explore the concept of how voice assistants could potentially be exploited, where genuine audio commands are manipulated such that an attacker could trigger an alternative responses from the voice assistant. We present a small-scale study to examine mis- interpretations made by voice assistants. We also study user perception of how secure their voice devices are, and their approach to security and privacy.

Cyber SA 2020, CIRC 2020, & Social Media 2020

Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks

Suleiman Yerima[1] and Mohammed Alzaylaee[2]
[1]Cyber Technology Institute, Faculty of Computing, Engineering and Media, De Montfort University, Leicester, UK
[2]Al-Qunfudah College of Computing, Umm Al-Qura University, Saudi Arabia

Abstract: Android, being the most widespread mobile operating systems is increasingly¬ becoming a target for malware. Malicious apps de-signed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus making them a serious threat. This calls for more effective methods for the detection of Android botnets. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). The models we implemented utilize CNN trained on 342 static features to distinguish between botnet apps and normal apps. The trained botnet detection models were evaluated on a set of 6,802 real applications containing 1,929 botnets from the ISCX botnet dataset. The results show that our CNN-based approach had the highest overall prediction accuracy compared to other popular machine learning classifiers. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning based Android Botnet detection.

The Data that Drives Cyber Insurance: A Study into the Policy Underwriting and Claims Processes

Jason Nurse[1], Louise Axon[2], Arnau Erola[2], Ioannis Agrafiotis[2], Michael Goldsmith[2] and Sadie Creese[2]
[1]School of Computing, University of Kent, UK
[2]Department of Computer Science, University of Oxford, UK

Abstract: Cyber insurance is a key component in risk management, intended to transfer risks and support business recovery in the event of a cyber incident. As cyber insurance is still new in practice and research, there are many unanswered questions regarding the data and economic models that drive it, the coverage options and pricing of premiums, and its more procedural policy-related aspects. This paper aims to address some of these questions by focusing on the key types of data involved in cyber insurance, particularly within decision-making in cyber-risk underwriting and claims processes. We further explore practitioners' perceptions of the challenges they face in gathering and using data, and identify gaps where further data gathering is required. We draw our conclusions from a qualitative study by conducting a focus group with a range of cyber-insurance professionals (including underwriters, actuaries, claims specialists, breach responders, cyber operations specialists) and provide new contributions to research. These contributions include providing examples of key data types which contribute to the calculation of premiums and decisions on claims, the identification of challenges and gaps at various stages of data gathering, and initial perspectives on the development of a pre-competitive dataset for the cyber insurance industry. We believe an improved understanding of data gathering and usage by cyber insurers, and of current challenges faced, can be invaluable for informing future research and practice in cyber insurance.

Naval Cyber-Physical Anomaly Propagation Analysis Based on a Quality Assessed Graph

Nicolas Pelissero[1], Pedro Merino Laso[2] and John Puentes[3]
[1]Chair of Naval Cyber Defense, E´cole Navale, Brest, France
[2]French Maritime Academy - ENSM, Nantes, France
[3]IMT Atlantique, Lab-STICC, UMR CNRS 6285, Brest, France

Abstract: As any other infrastructure relying on cyber-physical systems (CPS), naval CPS are highly interconnected and collect considerable data streams, on which depend multiple command and navigation decisions. Being a data-driven decision system requiring optimized supervisory control on a permanent basis, it is critical to examine the CPS vulnerability to anomalies and their propagation. This paper presents an approach to detect CPS anomalies and estimate their propagation applying a quality assessed graph, which represents the CPS physical and digital subsystems, combined with system variables dependencies and a set of data and information quality measures vectors. Following the identification of variables dependencies and high-risk nodes in the CPS, data and information quality measures reveal how system variables are modified when an anomaly is detected, also indicating its propagation path. Taking as reference the normal state of a naval propulsion management system, four anomalies in the form of cyber-attacks – port scan, programmable logical controller stop, and man in the middle to change the motor speed and operation of a tank valve – were produced. Three anomalies were properly detected, and their

propagation path identified. These results suggest the feasibility of anomaly detection and estimation of propagation estimation in CPS, applying data and information quality analysis to a system graph.

Smart Security Audit: Reinforcement Learning with a Deep Neural Network Approximator

Konstantin Pozdniakov[1], Eduardo Alonso[1], Vladimir Stankovic[1], Kimberly Tam[2] and Kevin Jones[2]
[1]City, University of London, UK
[2]University of Plymouth, Plymouth, UK

Abstract: A significant challenge in modern computer security is the growing skill gap as intruder capabilities increase, making it necessary to begin automating elements of penetration testing so analysts can contend with the growing number of cyber threats. In this paper, we attempt to assist human analysts by automating a single host penetration attack. To do so, a smart agent performs different attack sequences to find vulnerabilities in a target system. As it does so, it accumulates knowledge, learns new attack sequences and improves its own internal penetration testing logic. As a result, this agent (AgentPen for simplicity) is able to successfully penetrate hosts it has never interacted with before. A computer security administrator using this tool would receive a comprehensive, automated sequence of actions leading to a security breach, highlighting potential vulnerabilities, and reducing the amount of menial tasks a typical penetration tester would need to execute. To achieve autonomy, we apply an unsupervised machine learning algorithm, Q-learning, with an approximator that incorporates a deep neural network architecture. The security audit itself is modelled as a Markov Decision Process in order to test a number of decision making strategies and compare their convergence to optimality. A series of experimental results is presented to show how this approach can be effectively used to automate penetration testing using a scalable, i.e. not exhaustive, and adaptive approach.

Pattern Extraction for Behaviours of Multi-Stage Threats via Unsupervised Learning

Ahmed Alghamdi and Giles Reger
Department of Computer Science, The University of Manchester, UK

Abstract: Detection of multi-stage threats such as Advanced Persistent Threats (APT) is extremely challenging due to their deceptive approaches. Sequential events of threats might look benign when performed individually or from different addresses. We propose a new unsupervised framework to identify patterns and correlations of malicious behaviours by analysing heterogeneous log-files. The framework consists of two main phases of data analysis to extract inner-behaviours of log-files and then the patterns of those behaviours over analysed files. To evaluate the framework we have produced a (publicly available) labelled version of the SotM43 dataset. Our results demonstrate that the framework can (i) efficiently cluster inner-behaviours of log-files with high accuracy and (ii) extract patterns of malicious behaviour and correlations between those patterns from real-world data.

The Visual Design of Network Data to Enhance the Cyber Security Awareness of the Everyday Internet User

Fiona Carroll[1], Phil Legg[2] and Bastian Bønkel[1]
[1]School of Technologies, Cardiff Metropolitan University
[2]Department of Computer Science and Creative Technologies, University of the West of England

Abstract: Technology and the use of online services are very much prevalent across much of our everyday lives. As our digital interactions continue to grow, there is a need to improve public awareness of the risks to our personal online privacy and security. Designing for privacy and security online has never been so important, so that users can make better judgements about the information that they share and how they interact online. Typically, users are interacting with systems for some given purpose, and so are not primarily focused on the personal security and privacy implications of how they perform these actions. For example, when shopping online users will give attention to the item that they wish to purchase, but may not necessary pay attention to additional activity on the page, such as URL requests that are being made to third-party advertisements at the same time.This work provides further exploration in to how personal network activity data can be visually conveyed using simple yet informative representation, with a view of helping users to learn more about their online interactions, and how this may inform their decisions to better manage the security and privacy of their online interactions.

Application of the Benford's law to Social bots and Information Operations activities

Lale Madahali and Margeret Hall
University of Nebraska at Omaha Omaha, USA

Abstract: Benford's Law shows the pattern of behavior in normal systems. It states that in natural systems digits' frequency have a certain pattern such that the frequency of numbers' first digits is not evenly distributed. In systems with natural behavior, numbers begin with a "1" are more common than numbers beginning with "9". It implies that if the distribution of first digits is outside of the expected distribution it can be indicative of fraud. It has many applications in forensic accounting, stock markets, finding abnormal data in survey data, and natural science. We investigate whether social media bots and Information Operations activities are conformant to the Benford's law. Our results showed that bots' behavior adhere to Benford's Law, suggesting that using this law helps in detecting malicious online automated accounts and their activities on social media. However, activities related to Information Operations did not show consistency in regards to Benford's Law. Our findings shed light on the importance of examining regular and anomalous online behavior to avoid malicious and contaminated content on social media.

Explainable AI in Smart Healthcare

Urja Pawar and Ruairi O'Reilly
Cork Institute of Technology, Ireland

Abstract: In recent years, technology is shifting the healthcare paradigm from being disease centered to preventive and proactive. Big tech companies like Google, Apple, Amazon are actively getting involved in making healthcare services accessible and affordable to as many with the help of devices like Fitbit and Apple watch. This has led to the evolution of smart healthcare ecosystem in which participants are encouraged to be in control of their well-being using real-time health information on a fitness app or device which can be shared with clinicians for further diagnosis. We propose an idea of involving explainable AI as an intermediate in the analysis and diagnosis so that users can better understand issues in their lifestyle. It will also help clinicians to determine whether the alerts generated require immediate attention or are just caused by some external trivial factors.

5Es -> 4Cs 21st-century skills learning

Jasmina Maric
The Swedish School of Library and Information Science, University of Borås, Borås, Sweden

Abstract: This paper proposes a model which suggests that learning can be relevant and effective, while at the same time delivering 21st-century skills to those who learn. The motivation behind this research lies in the fact that we need new teaching approaches to successfully prepare our youngest for the 21st-century. Through a quantitative and qualitative mixed-methods approach, we looked at the effects of specifically tailored UX design course on acquisitions of missing 21st-century skills with our students. Drawing from the different scientific research experiences this paper calls for Bruner's 5Es for the acquisition of 4Cs, or 5Es → 4Cs model, for contemporary learning.

A Design Exploration Framework for Secure IoT-Systems

Lukas Gressl[1], Alexander Rech[1], Christian Steger[1], Andreas Sinnhofer[2] and Ralph Weissnegger[3]
[1]ITI TU GRaz, Austria
[2]Austria NXP Semiconductors Austria GmbH, Austria
[3]Austria CISC Semiconductor GmbH, Austria

Abstract: Cybersecurity is vital for embedded systems, especially for Internet of Things (IoT) systems. IoT systems have become essential in our daily lives, as they are usable for various application areas. They are usually small, connected with other systems, and perform a wide range of tasks. They are subject to multiple constraints in terms of performance, power consumption, chip area, etc. Attackers often target such devices as they are in constant interaction with each other or connected to the internet during private data processing. Cybersecurity, thus, plays a vital role in the design of IoT systems. Hence, designing secure IoT systems is a complex task, particularly for designers with limited security know-how. Security measures increase both computation time and power consumption, creating a conflict between these constraints, which must be solved by the designers. Balancing these constraints is a highly complex task. In this paper, we propose a new approach for considering security constraints in design space exploration, including possible security attacks on embedded systems. The method simplifies the consideration of security requirements at the start of the system design. We introduce a security attack based design

space exploration framework, capable of finding the optimal design for an IoT system, based on its architectural, behavioral, and security attack description. The paper shows the feasibility and benefits of the framework, employing a secure sensor use case.

A Data Extraction Method for Anomaly Detection in Naval Systems

Clet Boudehenn[1], Jean-Christophe Cexus[2] and Abdel Boudra[3]
[1]Chair of Naval Cyber Defense, E´cole Navale, Brest, France
[2]French Maritime Academy - ENSM, Nantes, France
[3]Art et Métiers ParisTech - Ecole Navale

Abstract: With the exponential growth of Cyber-Physical Systems (CPS), new security challenges have emerged. Over the past few years, Naval Systems have seen an increase of the deployment of Intrusion Detection Systems (IDS) to ensure the security of Programmable Logic Controller (PLC) and Industrial Control System (ICS) due to a plenty of vulnerabilities. In this context, several methods have been developed to effectively detect anomalies and intrusions such as cyber and physical alerts. Those methods need to be managed powerfully in order to increase anomaly detection in the cybernetic flows within naval systems. In this paper, we present a new strategy to generate meta data of naval cybernetics flows to illustrate vulnerabilities of naval systems. An anomaly detection method based on Teager-Kaiser operator is developed to show such vulnerabilities by analysing the collected time series. Simulations of three scenarios are provided to validate the new approach in Naval systems. The obtained results show the interest of the proposed naval anomaly detection strategy.

Focusing on the Recovery Aspects of Cyber Resilience

Cyril Onwubiko
Research Series Limited, London, UK

Abstract: Advances in technology and emerging cyber security tactics, techniques, and procedures (TTPs) are pillars for the 'social good' on the one hand. On the other hand, they have advanced the landscape for adversarial purposes, for example, the increasing number of cyber incidents and data breaches. This realisation that cyber incidents cannot be completely avoidable has made cyber resilience an extremely important preposition of any comprehensive and reliable cyber security strategy. Despite the importance, little contributions exist on cyber recovery – a core aspect of the cyber resilience, and cyber security standard. In this paper, we develop and present a comprehensive cyber recovery operational framework. An adaptive, robust framework that can be used as it is, or adapted by an organisation to create its own cyber recovery manual or operative. Each aspects of the framework are discussed thoroughly. Further, we showed how a cutdown version of the framework is implemented, mindful that not all organisations are of the same size.

Analysis of the RPL Version Number Attack with Multiple Attackers

Ahmet Aris and Sema F. Oktug
Faculty of Computer and Informatics Engineering, ˙Istanbul Technical University, Turkey

Abstract: In this study, we aim to understand the effect of multiple Version Number Attackers (VNA) in RPL (IPv6 Routing Protocol for Low Power and Lossy Networks)-based Internet of Things (IoT) networks. VNA is one of the most detrimental Denial of Service (DoS) attack that targets the availability of IoT networks. Almost all of the studies targeting the VNA considered a single attacker. However, once an attacker has a chance to compromise a node in the network, it may easily compromise more devices, thus 1) affect the performance of the network more and misuse the resources quicker, 2) circumvent the existing security mechanisms and 3) perform other attacks which require more than one malicious node (e.g., wormhole, etc.). Therefore, we have to take multiple attackers into account when designing security systems. In this work, we analyze the effect of multiple attackers from various points of view. Based on extensive simulations and analysis, we conclude that increasing the number of attackers affects only the packet delivery ratio and does not affect average network delay and average power consumption. Our results also show that, attacking positions closer to the root cause longer delays and higher power consumption results while central attacking positions are more effective on packet delivery ratio. Lastly, we evaluate the performance of a recently proposed mitigation technique against multiple attackers.

Self-Attention for Cyberbullying Detection

Ankit Pradhan, Venu Madhav Yatam and Padmalochan Bera
IIT Bhubaneswar, Odisha, India

Abstract: In recent years, cyberbullying has grown out of proportion due to the increasing usage of social media platforms along with the benefit of user anonymization over the Internet. Affecting people across all demographics, the effect of cyberbullying has been more pronounced over adolescents and insecure individuals. Victims suffer from societal isolation, depression, degrading self-confidence and suicidal thoughts. Thus, prevention of cyberbullying becomes a necessity and requires timely detection. Recent advances in Deep learning and Natural Language Processing have provided suitable models to predict whether a text sample is an example of cyberbullying. In this context, we explore the adaptivity and efficiency of self-attention models in detecting cyberbullying. Though a few of the recent works in this context have employed models like deep neural networks, SVM, CNN, LSTM and other hybrid models, to the best of our knowledge, this is the first work exploring self-attention models which have achieved state-of-the-art accuracies in Machine Translation tasks since 2017. We experiment with the Wikipedia, Formspring and Twitter cyberbullying datasets and achieve more efficient results over existing cyberbullying detection models. We also propose new research directions within cyberbullying detection over recent forms of media like Internet memes which pose a variety of new and hybrid problems.

Towards an Aggregate Signature-based Authentication for Opportunistic Networks

Blaise Cossi Avoussoukpo[1], Chunxiang Xu[2], Marius Tchenagnon[2] and Eltayieb Nabeil[2]
[1]College of International Education, Southwest University of Finance and Economics, P.R. China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, P.R. China

Abstract: Opportunistic Networks are particular networks where independent nodes come together under the supervision of a Seed OppNet to achieve a precise goal. For only certified nodes are allowed to help an extended or expanded Seed OppNet achieve its goal; making sure that unauthorized users do not disrupt the smooth completion of the Seed OppNet's mission, Helpers' authentication is critical. However, despite the significant contributions tackling the issue of authentication within an OppNet's environment, so far, in literature, most OppNets authentication proposed schemes just focused on (Helper-Helper) authentication; there is no scheme intended to (Helpers-Seed OppNet) authentication in an extended OppNet's environment. Resorting to the properties of Digital Signature, BLS Signature, and aggregate BLS signatures, this paper proposes an authentication mechanism that allows a Seed OppNet to process pieces of information effectively and efficiently. The proposed scheme is secure against the rogue pubic key, tapping, forgery, replay, and man-in-the-middle attacks.

Graphical analysis of captured network packets for detection of suspicious network nodes

Felix Larbi Aryeh[1], Boniface Kayode Alese[2] and Olayemi Olasehinde[3]
[1]Computer Sci. and Eng. Department University of Mines and Technology Tarkwa, Ghana
[2]Department of Cybersecurity, Federal University of Technology, Akure, Nigeria
[3]Department of Computer Science Federal Polytechnic, Ile Oluji Ondo State, Nigeria

Abstract: The advent of the Internet has yielded the rapid development of Information Technology related applications over the past two decades. Most organizations have adopted the use of a computer network to make accessibility and sharing of network applications and devices possible. However, currently, network security has been one of the critical things most organization and corporation has to handle. Each day, attacks are continually being executed into professional secured corporate or organization networks and sometimes into private networks. Wireshark is a tool generally used for network packet capture however, it is very tedious sometimes to filter and follow TCP streams. This problem exacerbates in a situation where huge network data or traffic needs to be analyzed for suspicious traffic. This paper leverages the use of Python libraries and Data Science techniques to ease the packet capturing and analysis process. By using these techniques will enhance the gleaning out more interesting attributes of network packet and fish out the suspicious IP address, network ports or malicious data readily within the shortest possible time. The research conducted showed how a broadcast IP address 255.255.255.255 might be suspicious within the internal network of UMaT. The suspicion was based on the payload data sent to this address and a possible error or misconfiguration on the Ubiquiti UniFi access point.

Decentralized Identifier Distribution for Moving Target Defense and Beyond

Daniel Krohmer and Hans D. Schotten
German Research Center for Artificial Intelligence (DFKI), Kaiserslautern, Germany

Abstract: In this work, we propose a novel approach for decentralized identifier distribution and synchronization in networks. The protocol generates network entity identifiers composed of timestamps and cryptographically secure random values with a significant reduction of collision probability. The distribution is inspired by Unique Universal Identifiers and Timestamp-based Concurrency Control algorithms originating from database applications. We defined fundamental requirements for the distribution, including: uniqueness, accuracy of distribution, optimal timing behavior, scalability, small impact on network load for different operation modes and overall compliance to common network security objectives. An implementation of the proposed approach is evaluated and the results are presented. Originally designed for a domain of proactive defense strategies known as Moving Target Defense, the general architecture of the protocol enables arbitrary applications where identifier distributions in networks have to be decentralized, rapid and secure.

Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence

Abdulmajeed Alahmari[1] and Robert Duncan[2]
[1]Department of Accounting and Finance University of Aberdeen Aberdeen, UK
[2]Department of Computing science University of Aberdeen Aberdeen, UK

Abstract: Even though small and medium-sized enterprises (SMEs) have been encouraged to take advantage of any possible business opportunities by utilizing and adopting new technologies such as cloud computing services, there is a huge misunderstanding of their cyber threats from the management perspective. Underestimation of cybersecurity threats by SMEs leads to an increase in their vulnerabilities and risks, which unfortunately can become actual challenges to them and other related parties. The purpose of this paper is to provide a systematic literature review based on recently available evidence on cybersecurity risk management in SMEs in order to understand the current situation. The authors aim to reveal the role the SMEs' management is playing in addressing cybersecurity risks in recent years, as found in the literature, and to suggest avenues for further research. The paper follows a well-known method by [1] for conducting a systematic literature review. Starting with a keyword search and an assessment of fitness for this review, 15 papers out of 50 have been analysed by NVivo software according to bibliographical information, research design and findings. The review identified 5 major perspectives that play a key role in SMEs' cybersecurity risk management, which are threats, behaviours, practices, awareness, and decision-making respectively. Importantly, empirical research on cybersecurity risk management in SMEs would be appreciated.

Examining the Cyber Security of a Real World Access Control Implementation

Julian J. Teule, Marius F. Hensel, Victor Büttner, Jonathan V. Sørensen, Magnus Melgaard and Rasmus L. Olsen
Department of Electronic Systems, Aalborg University, Aalborg, Denmark

Abstract: As smart cards have become increasingly prevalent in electronic access control systems, this paper investigates an implementation at a national institution, which uses a smart card with publicly known weaknesses. The main outcome is a set of recommendations which can be used for securing electronic access control systems against the discovered flaws of this work: The implementation did not follow guidelines from the manufacturer of the cards, the content of the restricted sector was printed onto each card, and in-house services with inherent security flaws were built around the cards, but not maintained. These flaws meant that the civil registration number of any employee at the institution could be revealed. Additionally, the flaws allowed for changing the PIN code of any card in the system.

Educating multidisciplinary undergraduates on security and privacy

Katorah Williams, Mollie Ducoste and Aunshul Rege
Department of Criminal Justice Temple University Philadelphia, USA

Abstract: As digital services have become more prevalent; the accompanying terms and conditions documents have been increasingly criticized for being too long and shrouded in legal terms that are difficult for the average person to understand. Past research has shown that it would take the average user 201 hours a year, an equivalent of $3,534 dollars' worth of time, to read privacy statements word-for-word. Inspired by this line of research and its findings, a

professor at a U.S. university developed a creative experiential learning course project aimed at educating undergraduate students across multiple STEM disciplines on security and privacy. This paper will discuss the ways in which the students implemented the hands-on project, including their experiences with completing ethics training, developing effective social engineering pretexts and strategies, conducting field research and interviews, and analyzing data. Additionally, this paper will discuss student successes and failures, adaptations to challenges, and key reasons why their fellow students did or did not read the terms and/or conditions. Lastly, this paper will include an overview of the lessons learned by the educator, which include ethical considerations, takeaways about assignment construction, development, and grading, and recommendations for future assignment modifications.

Big Fish, Little Fish, Critical Infrastructure: An Analysis of Phineas Fisher and the `Hacktivist' Threat to Critical Infrastructure

Peter Maynard and Kieran Mclaughlin
Centre for Secure IT, Queen's University Belfast

Abstract: The hacktivist threat actor is listed in many risk decision documents. Yet their tactics and techniques often remain a mystery. We create a MITRE ATT&CK (ATT&CK) model of a well-known hacktivist who goes under the pseudonym of Phineas Fisher, and map that threat to critical infrastructure. The analysis is derived from hacker manifestos, journalist reporting, and official government documentation. This analysis fills a gap in current threat models, to better define what skills and methods a determined hacker might employ. This paper also identifies seven essential mitigations which can be deployed by critical infrastructure operations and asset owners, in order to prevent such intrusions by hacktivists. We in the process of contributing this threat actor into the MITRE ATT&CK knowledge base.

Beyond the Prisoner’s Dilemma: the Social Dilemmas of Cybersecurity

Jordan Schoenherr[1, 2] and Robert Thomson[2]
[1]Institute of Data Science, Department of Psychology, Carleton University, Canada
[2]ACI, US Military Academy, Canada

Abstract: The Prisoner’s Dilemma represents a ubiquitous approach to security modeling that emphasizes adversarial relationships between actors. Adopting this approach helps understand ambiguous relationships in information domains. Despite the fact that some actors might adopt these frames, the Prisoner’s Dilemma reflects only one of many possible social dilemmas. In this paper, we outline a computational approach to cybersecurity based on Interdependence Theory. Interdependence Theory provides a means to decompose pay-off matrices into social influence components based on the amount of control actors and partners have in a situation. It additionally accounts for joint control that develops from the mutual decisions of both players. By focusing on two-person, two-option games, this approach can model many different social situations that reflect nor-mal and anomalous network activity.

Implementing the NIS Directive, driving cybersecurity improvements for Essential Services

Tania Wallis and Christopher Johnson
School of Computing Science, University of Glasgow, Glasgow, UK

Abstract: A review by the National Audit Office of the National Cyber Security Programme recommended a more robust performance framework, to understand the impact of the Programme and to focus activities going forward. The Directive on security of network and information systems (the NIS Directive) has placed responsibility for essential aspects of supply chains on Operators of Essential Services (OES). Our dependence on international supply chains also requires a performance framework to assist cybersecurity improvements in this area. The following sections describe work to investigate the implementation of the NIS Directive by Competent Authorities (CA) and OES and proposes a framework to monitor performance across interdependencies. This is to enable development of a more effective set of performance metrics to guide interventions and improvements in cybersecurity for critical infrastructure.

High-Performance Monitoring Sensors for Home Computer Users Security Profiling

Farhad Foroughi[1], Hossein Hadipour[2] and Ahmad M. Shafiee[3]
[1]Institute of Computer Science Universoty of Rostock, Germany
[2]Institute of Computer Science IA University of Najafabad, Iran
[3]Institute of Computer Science IA University of Najafabad, Iran

Abstract: Recognising user behaviour in real-time is crucial to provide user critical information about their risky behaviour to keep them safe and secure against cyber threats. User's behaviours or actions are usually erratic, evolve with time, and occasionally computer users behave differently due to a change in goals or purposes. Therefore, it is essential to create a user profile which is personalised application and tailored to cover user requirements. This research tries to identify the monitoring factors and extract features to provide an observation solution to create high-performance sensors to generate user security profile from home computers to analyse user behaviours.

Smart Grid Data Security using Practical CP-ABE with Obfuscated Policy and Outsourcing Decryption

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

Abstract: Smart grid consists of multiple different entities related to various energy management systems which share fine-grained energy measurements among themselves in an optimal and reliable manner. Such delivery is achieved through intelligent transmission and distribution networks composed of various stakeholders like Phasor Measurement Units (PMUs), Master and Remote Terminal Units (MTU and RTU), Storage Centers and users in power utility departments subject to volatile changes in requirements. Hence, secure accessibility of data becomes vital in the context of efficient functioning of the smart grid. In this paper, we propose a practical attribute-based encryption scheme for securing data sharing and data access in Smart Grid architectures with the added advantage of obfuscating the access policy. This is aimed at preserving data privacy in the context of competing smart grid operators. We build our scheme on Linear Secret Sharing (LSS) Schemes for supporting any monotone access structures and thus enhancing the expressiveness of access policies. Lastly, we analyze the security, access policy privacy and collusion resistance properties of our cryptosystem and provide an efficiency comparison as well as experimental analysis using the Charm-Crypto framework to validate the proficiency of our proposed solution.

Application and analysis of record linkage techniques to integrate Brazilian health databases

Maicon Herverton Lino Ferreira da Silva Barros[1], Morgana Thalita da Silva Leite, Vanderson Sampaio[2,3], Patricia Takako Endo[1,4] and Theo Lynn[4]
[1]Universidade de Pernambuco, Brazil
[2]Fundacao de Medicina Tropical Doutor Heitor Vieira Dourado, Brazil
[3]Portal da Fundacao de Vigilancia em Saude do Amazonas, Brazil
[4]Dublin City University, Dublin, Ireland

Abstract: The amount of data generated by health institutions is abundant and obtaining knowledge and insights from such data is a major challenge in the process of digital transformation in the area of healthcare, due to the fact that such data are complex, high-dimensional and heterogeneous. This work-in-progress has as main goal to integrate two Brazilian health database in order to improve the data quality regarding tuberculosis death information. For that, we applied a phonetic encoding technique (Soundex) and a pattern matching recognition (Jaro), and compare the results.

A survey of cyber security in the Swedish manufacturing industry

Ulrik Franke[1] and Joakim Wernberg[2]
[1]RISE Research Institutes of Sweden and KTH Royal Institute of Technology Kista, Sweden
[2]Swedish Entrepreneurship Forum Stockholm, Sweden

Abstract: Manufacturing is being transformed by new technologies. While these technologies are not all digital, they are mostly digitally enabled, i.e., their use is made possible only by dependable electronic sensors, actuators, and other digital devices. Thus, without cyber security, no smart industry. It is against this background that we investigate cyber security practices in Swedish manufacturing. Through a sector-wide survey performed in collaboration the with Association of Swedish Engineering Industries, cyber risk perception, existing risk controls, and scope for

improvements are mapped. The results are based on 649 questionnaire responses received (a response rate of 17%.). Overall, risk perception is relatively low, with only some 15--20% responding that risks are high or very high. About 80% have incurred no incidents in the past year. Business interruption is a much bigger worry than data breach, in line with previous findings. Furthermore, the use of cyber risk controls in Swedish manufacturing industry is still in its infancy, with less than half of respondents having cyber security strategies or continuity plans, and even fewer training their employees or conducting incident management exercises. The paper is concluded with the identification of a few interesting follow-up questions for future work.

Cyber Insurance Market in Israel - What is the Official Policy?

Tal Pavel
Head of Cyber Studies, The Academic College of Tel Aviv Yaffo, Israel

Abstract: Since 1997, with the first Internet security liability policy (Granato and Polacek, 2019, the cyber insurance market has evolved. But despite the importance of cyber insurance as one of the tools for organizations to manage their cyber risks, there are still problems relating to this market which have persisted over the years, mainly in aspects of the lack of information and knowledge that affect market maturity and the willingness to use it. These problems have been addressed by academic research. This study seeks to examine Israel's policy on cyber insurance based upon official policy documents and academic papers on Israeli cyberspace, while emphasizing that in Israel, as in other countries, cyber insurance is still in the process of implementation. The conclusion of the study is that action must be taken to make the relevant information accessible and to create activities of guidance and regulation by relevant government agencies.

Cyber Science 2020 Conference Presentation Timetable

Monday June 15, 2020

Theme: Advancing a multidisciplinary approach to Cyber Security		
11:00 – 11:30	**Conference Opening, Introduction and Announcements** **Dr Cyril Onwubiko – Conference Chair | Prof Theo Lynn – Conference Chair** **Dr Xavier Bellekens – Conference Chair | Dr Pierangelo Rosati – Conference Chair** **Dr Arnau Erola – Conference Chair | Dr Grace Fox – Conference Chair** **Dr Martin Gilje Jaatun – Conference Chair | Dr Patricia Endo – Conference Chair**	
	Track 1: Critical National Infrastructures & CERTs	**Track 2: Cyber Attacks, SOCs & Deception**
11:30 - 12:00	**An Empirical Study of CERT Capacity in the North Sea** *Martin Gilje Jaatun, Lars Bodsberg, Tor Olav Grøtan and Marie Elisabeth Gaup Moe*	**Naval cyber-physical anomaly propagation analysis based on a quality assessed graph** *Nicolas Pelissero, Pedro Merino Laso and John Puentes*
12:00 – 13:00	**Coffee Break & Social Networking**	
13:00 – 13:30	**Smart Grid Data Security using Practical CP-ABE with Obfuscated Policy and Outsourcing Decryption** *Ankit Pradhan, Punith. R, Kamalakanta Sethi and Padmalochan Bera*	**Towards a Framework for Measuring the Performance of a Security Operations Center Analyst** *Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke and Pete Burnap*
13:30 – 14:00	**Developing a security behavioural assessment approach for cyber rating U.K. MSBs** *Andrew Rae and Asma Patel*	**Slave Clock Responses to Precision Time Protocol Attacks: A Case Study** *Waleed Alghamdi and Michael Schukat*
14:00 – 15:00	**Coffee Break & Social Networking**	
15:00 – 16:00	**Keynote | Dr. Ruoyi Zhou, Director of IBM Research**	
16:00 – 16:30	**Coffee Break & Social Networking**	
16:30 – 17:00	**Examining the Cyber Security of a Real World Access Control Implementation** *Julian J. Teule, Marius F. Hensel, Victor Büttner, Jonathan V. Sørensen, Magnus Melgaard and Rasmus L. Olsen*	**Deep Down the Rabbit Hole: On References in Networks of Decoy Elements** *Daniel Reti, Daniel Fraunholz, Janis Zemitis, Daniel Schneider and Hans Dieter Schotten*
17:00 – 17:30	**Vulnerability-Based Impact Criticality Estimation for Industrial Control Systems** *Uchenna Daniel Ani, Hongmei He and Ashutosh Tiwari*	**A Data Extraction Method for Anomaly Detection in Naval Systems** *Clet Boudehenn, Jean-Christophe Cexus and Abdel Boudra*
17:30 – 18:00	**Coffee Break & Social Networking**	
18:00 – 18:30	**What Could Possibly Go Wrong? Smart Grid Misuse Case Scenarios** *Inger Anne Tøndel, Ravishankar Borgaonkar, Martin Gilje Jaatun and Christian Frøystad*	**Restricting Data Flows to Secure Against Remote Attack** *John O'Raw and David Laverty*
18:30 – 19:00	**Big Fish, Little Fish, Critical Infrastructure: An Analysis of Phineas Fisher and the `Hacktivist' Threat to Critical Infrastructure** *Peter Maynard and Kieran Mclaughlin*	**An Overview of Web Robots Detection Techniques** *Hanlin Chen, Hongmei He and Andrew Star*

19:00 – 19:30	**Automated Artefact Relevancy Determination from Artefact Metadata and Associated Timeline Events** *Xiaoyu Du, Quan Le and Mark Scanlon*	**Towards Detecting Human Actions, Intent, and Severity of APT Attacks by Applying Deception Techniques** *Joel Chacon, Sean McKeown and Richard Macfarlan*

Tuesday June 16, 2020

Themes: Focusing on Cyber Insurance and Risk Controls & Machine Learning for insight in Cyber Security and Situational Awareness		
	Track 3: Exploiting Deep Learning for Cyber Security	**Track 4: Human Factors & Visual Analytics**
11:00 - 11:30	**Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks** *Suleiman Y. Yerima and Mohammed K. Alzaylaee*	**Towards an Aggregate Signature-based Authentication for Opportunistic Networks** *Cossi Blaise Avoussoukpo, Chunxiang Xu, Marius Tchenagnon and Nabeil Eltayieb*
11:30 - 12:00	**"What did you say?": Extracting unintentional secrets from predictive text learning systems** *Gwyn Wilkinson and Phil Legg*	**The Visual Design of Network Data to Enhance the Cyber Security Awareness of the Everyday Internet User** *Fiona Carroll, Phil Legg and Bastian Bønkel*
12:00 – 13:00	**Coffee Break & Social Networking**	
13:00 – 13:30	**Smart Security Audit: Reinforcement Learning with a Deep Neural Network Approximator** *Konstantin Pozdniakov, Eduardo Alonso, Vladimir Stankovic, Kimberly Tam and Kevin Jones*	**Privacy Policy – "I agree"?! – Do alternatives to text-based policies increase the awareness of the users?** *Pascal Faurie, Arghir-Nicolae Moldovan and Irina Tal*
13:30 – 14:00	**Focusing on the Recovery Aspects of Cyber Resilience** *Cyril Onwubiko*	**Beyond the Prisoner's Dilemma: the Social Dilemmas of Cybersecurity** *Jordan Schoenherr and Robert Thomson*
14:00 – 15:00	**Coffee Break & Social Networking**	
15:00 – 16:00	**Keynote | Dr Phillippa M. Spencer, DSTL**	
16:00 – 16:30	**Coffee Break & Social Networking**	
	Track 5: Workshop on Cyber Insurance & Risk Controls	**Track 6: Cyber Threat Intelligence, OSINT & Cyber Microbiome**
16:30 – 17:00	**The Data that Drives Cyber Insurance: A Study into the Policy Underwriting and Claims Processes** *Jason Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith and Sadie Creese*	**Smarter Password Guessing Techniques Leveraging Contextual Information and OSINT** *Aikaterini Kanta, Iwen Coisel and Mark Scanlon*

17:00 – 17:30	**A survey of cyber security in the Swedish manufacturing industry** *Ulrik Franke and Joakim Wernberg*	**High-Performance Monitoring Sensors for Home Computer Users Security Profiling** *Farhad Foroughi, Hossein Hadipour and Ahmad M. Shafiee*
18:00 – 18:30	**Cyber Insurance Market in Israel - What is the Official Policy?** *Tal Pavel*	**Cyber Threat Intelligence and the Cyber Meta-Reality and Cyber Microbiome** *Joshua Sipper*
18:30 – 19:30	**Keynote | Dr Jason R.C. Nurse, Assistance Professor, University of Kent**	

Wednesday June 17, 2020

Theme: Tactics, Techniques and Procedures (TTPs) for Cyber Incident Response in a fast paced Digital World		
	Track 7: Digital Evidence & Forensics	**Track 8: Cyber Security Detection**
11:00 - 11:30	**Shouting Through Letterboxes: A study on attack susceptibility to voice assistants** *Andrew McCarthy, Benedict R. Gaster and Phil Legg*	**Self-Attention for Cyberbullying Detection** *Ankit Pradhan, Venu Madhav Yatam and Padmalochan Bera*
11:30 - 12:00	**Forensic Considerations for the High Efficiency Image File Format (HEIF)** *Sean Mckeown and Gordon Russell*	**A Security Perspective on Unikernels** *Joshua Talbot, Przemek Pikula, Craig Sweetmore, Samuel Rowe, Hanan Hindy, Christos Tachtatzis, Robert Atkinson and Xavier Bellekens*
12:00 – 13:00	**Coffee Break & Social Networking**	
13:00 – 13:30	**Using Amazon Alexa APIs as a Source of Digital Evidence** *Clemens Krueger and Sean McKeown*	**A Taxonomy of Approaches for Integrating Attack Awareness in Applications** *Tolga Ünlü, Lynsay Shepherd, Natalie Coull and Colin McLean*
13:30 – 14:00	**Introducing a forensics data type taxonomy of acquirable artefacts from programmable logic controllers** *Marco Cook, Ioannis Stavrou, Sarah Dimmock and Christopher Johnson*	**Cyber-security research by ISPs: A NetFlow and DNS Anonymization Policy** *Martin Fejrskov, Jens Myrup Pedersen and* Emmanouil Vasilomanolakis
14:00 – 15:00	**Coffee Break & Social Networking**	
15:00 – 16:00	**Keynote | Paul C. Dwyer, CEO, Cyber Risk International**	
16:00 – 16:30	**Coffee Break & Social Networking**	
	Track 9: Mobile Security & Ransomware	**Track 10: Applications of Artificial Intelligence to Cyber Security**
16:30 – 17:00	**Moving Targets: Addressing Concept Drift in Supervised Models for Hacker**	**Acoustic Emanation of Haptics as a Side-Channel for Gesture-Typing Attacks**

	Communication Detection *Andrei Lima Queiroz, Brian Keegan and Susan Mckeever*	*Jonathan Francis Roscoe and Max Smith-Creasey*
17:00 – 17:30	**Memory Forensics Against Ransomware** *Pranshu Bajpai and Richard Enbody*	**AI Crimes: A Classification** *Fadi Sibai*
17:30 – 18:00	**Coffee Break & Social Networking**	
18:00 – 18:30	**An Empirical Study of Key Generation in Cryptographic Ransomware** *Pranshu Bajpai and Richard Enbody*	**Cost-Effective OCR Implementation to Prevent Phishing on Mobile Platforms** *Yunjia Wang, Yang Liu, Tiejun Wu and Ishbel Duncan*
18:30 – 19:00	**Assessing the Influencing Factors on the Accuracy of Underage Facial Age Estimation** *Felix Anda, Brett Becker, David Lillis, Nhien-An Le-Khac and Mark Scanlon*	**Pattern Extraction for Behaviours of Multi-Stage Threats via Unsupervised Learning** *Ahmed Alghamdi and Giles Reger*
19:00 – 19:30		**Evaluation of Machine Learning Algorithms for Anomaly Detection** *Nebrase Elmrabit, Feixiang Zhou, Fengyin Li and Huiyu Zhou*

Thursday June 18, 2020

Theme: Advancing Social Media Innovation and Convergence in a Digital Economy		
	Track 11: Emerging Nations & Risk Management	**Track 12: Social Media Analytics, Communities & Learning**
11:00 - 11:30	**Sociotechnical Approaches to Cyber Security in Emerging Nations: A Case Study in Risk Management for Rwandan Health Care** *Joseph Kaberuka and Christopher Johnson*	**5Es -> 4Cs 21st-century skills learning** *Jasmina Maric*
11:30 - 12:00	**Implementing the NIS Directive, driving cybersecurity improvements for Essential Services** *Tania Wallis and Christopher Johnson*	**Blurring lines between fiction and reality: Perspectives of experts on marketing effectiveness of virtual influencers** *Evangelos Moustakas, Nishtha Lamba, Dina Mahmoud and C Ranganathan*
12:00 – 13:00	**Coffee Break & Social Networking**	
13:00 – 13:30	**Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence** *Abdulmajeed Abdullah Alahmari and Robert Anderson Duncan*	**Social big data: A Twitter text mining approach to the communication of universities during the Lebanese protests** *Katia Raya, Nicole D'almeida and Maroun Chamoun*
13:30 – 14:00	**Towards Security Attack and Risk Assessment during Early System Design** *Lukas Gressl, Michael Krisper, Christian Steger and Ulrich Neffe*	**Introducing & Evaluating 'Nutrition Facts' for Online Content** *Matthew Spradling, Jeremy Straub and Jay Strong*
14:00 – 14:30	**Coffee Break & Social Networking**	

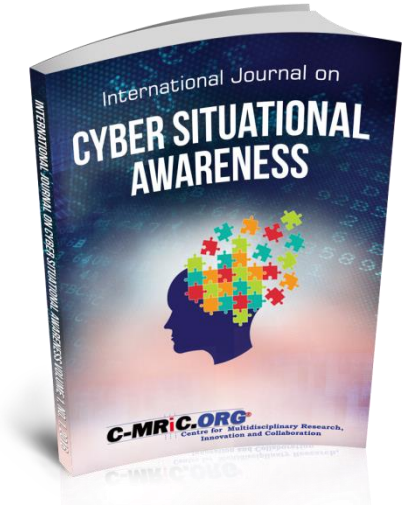
	Track 13: Cyber Security Education	Track 14: Cyber Security Privacy & Ethics
14:30 – 15:00	**Examining the Impact of Implementing Cyber Security Articulation Agreements Between Public and Private Higher Educational Institutions in 9-12 High Schools** *Thomas J. Rzemyk*	**Technical codes' potentialies in cyber security: A contextual approach on the ethics of small digital organizations in France** *Theo Simon and Bertrand Venard*
15:00 – 15:30	**Educating multidisciplinary undergraduates on security and privacy** *Katorah Williams, Mollie Rose Ducoste and Aunshul Rege*	**Privacy Protection Behaviours: a diversity of individual strategies** *Bertrand Venard*
15:30 – 16:00	**Coffee Break & Social Networking**	
16:00 – 17:00	**Keynote | Prof Steven B. Lipner, Executive Director, SAFECode**	
17:00 – 17:30	**Coffee Break & Social Networking**	
17:30 – 18:00	**Think Smart, Play Dumb: A Game-Theoretic Approach to Study Deception in Hardware Trojan Testing** *Tapadhir Das, Abdelrahman Eldosouky and Shamik Sengupta*	**Insider Threat Detection: A Solution in Search of a Problem** *Jordan Schoenherr and Robert Thomson*
18:00 – 18:30	**Epistemological Questions for Cybersecurity** *Timothy D. Williams*	**Platform for monitoring and clinical diagnosis of arboviruses using computational models** *Sebastião Neto, Thomás Oliveira, Vanderson Sampaio, Theo Lynn and Patricia Endo*
18:30 – 18:40	**Coffee Break & Social Networking**	
18:40 – 19:40	**Industry Panel Discussion** **Digital Shadows [TBC]** **Wayne Bursey**, Industrial Cyber Security Lead, Siemens Ltd	

Friday June 19, 2020

Theme: Data Science and Emerging Technologies		
11:00 – 12:00	**Industry Panel Discussion - IT Security & Governance, Risk & Assurance in the Enterprise post COVID-19** **Vincent Blake**, VP, IT Security & GRCA, Pearson Plc **Valerie Lyons**, COO, BH Consulting	
12:00 – 12:30	**Coffee Break & Social Networking**	
	Track 15: Data Science & Machine Learning for Cyber Security	**Track 16: Security Testing & Continuous Vulnerability Assessment**
12:30 - 13:00	**Graphical analysis of captured network packets for detection of suspicious network nodes** *Felix Larbi Aryeh, Boniface Kayode Alese and Olayemi Olasehinde*	**Analysis of the RPL Version Number Attack with Multiple Attackers** *Ahmet Aris and Sema F. Oktug*
13:00 - 13:30	**Secure Framework for Anti-Money-Laundering using Machine Learning and Secret Sharing** *Arman Zand, James Orwell and Eckhard Pfluegel*	**Decentralized Identifier Distribution for Moving Target Defense and Beyond** *Daniel Krohmer and Hans D. Schotten*
13:30 - 14:00	**Explainable AI in Smart Healthcare** *Urja Pawar and Ruairi O'Reilly*	**Automated Vulnerability Testing via Executable Attack Graphs** *Drew Malzahn, Zachary Birnbaum, and Cimone Wright-Hamor*
14:00 – 15:00	**Coffee Break & Social Networking**	
15:00 – 16:00	**Keynote Speech** | **Dr Siôn Lloyd**, Lead Security, Stability & Resiliency Specialist, ICANN	
16:00 – 17:00	**Coffee Break & Social Networking**	
	Track 17: Emerging Technologies, IoT & Bots	**Track 18: Blockchain & Crypto**
17:00 – 17:30	**A Design Exploration Framework for Secure IoT-Systems** *Lukas Gressl, Alexander Rech, Christian Steger, Andreas Sinnhofer and Ralph Weissnegger*	**ethVote: Towards secure voting with distributed ledgers** *Johannes Mols and Emmanouil Vasilomanolakis*
17:30 – 18:00	**Testing and Hardening IoT Devices Against the Mirai Botnet** *Christopher Kelly, Nikolaos Pitropakis, Sean Mckeown and Costas Lambrinoudakis*	**A DLT-based Trust Framework for IoT Ecosystems** *Tharindu Ranathunga, Ramona Marfievici, Alan McGibney and Susan Rea*
18:00 – 18:30	**Coffee Break & Social Networking**	
18:30 – 19:00	**Application and analysis of record linkage techniques to integrate Brazilian health databases** *Maicon Herverton Lino Ferreira da Silva Barros, Morgana Thalita da Silva Leite, Vanderson Sampaio and Patricia Takako Endo*	**Application of the Benford's law to Social bots and Information Operations activities** *Lale Madahali and Margeret Hall*
19:00 – 19:30	**Conference Closure - Plenary Q&A**	

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

Notes

Organiser / Contact Us

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

The 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