Cyber Science 2024

Building Community of Good Practice in Cybersecurity

Edinburgh Napier University, Scotland, UK
JUNE 27 – 28, 2024

@cmricorg #Cyberscience2024

www.c-mric.org

C-MRiC.ORG Springer

Our Sponsors

Edinburgh Napier UNIVERSITY

Springer

SINTEF

C-MRiC CENTRE FOR MULTIDISCIPLINARY RESEARCH, INNOVATION AND COLLABORATION ®

DCU

dotLAB

UNIVERSITY OF OXFORD DEPARTMENT OF COMPUTER SCIENCE

CYBER SECURITY OXFORD

Cyber Science 2024

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.

Springer is the technical co-sponsor and publisher of this year's conference. The 2024 Cyber Science proceedings will be published in the Springer Proceedings in Complexity book series.

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

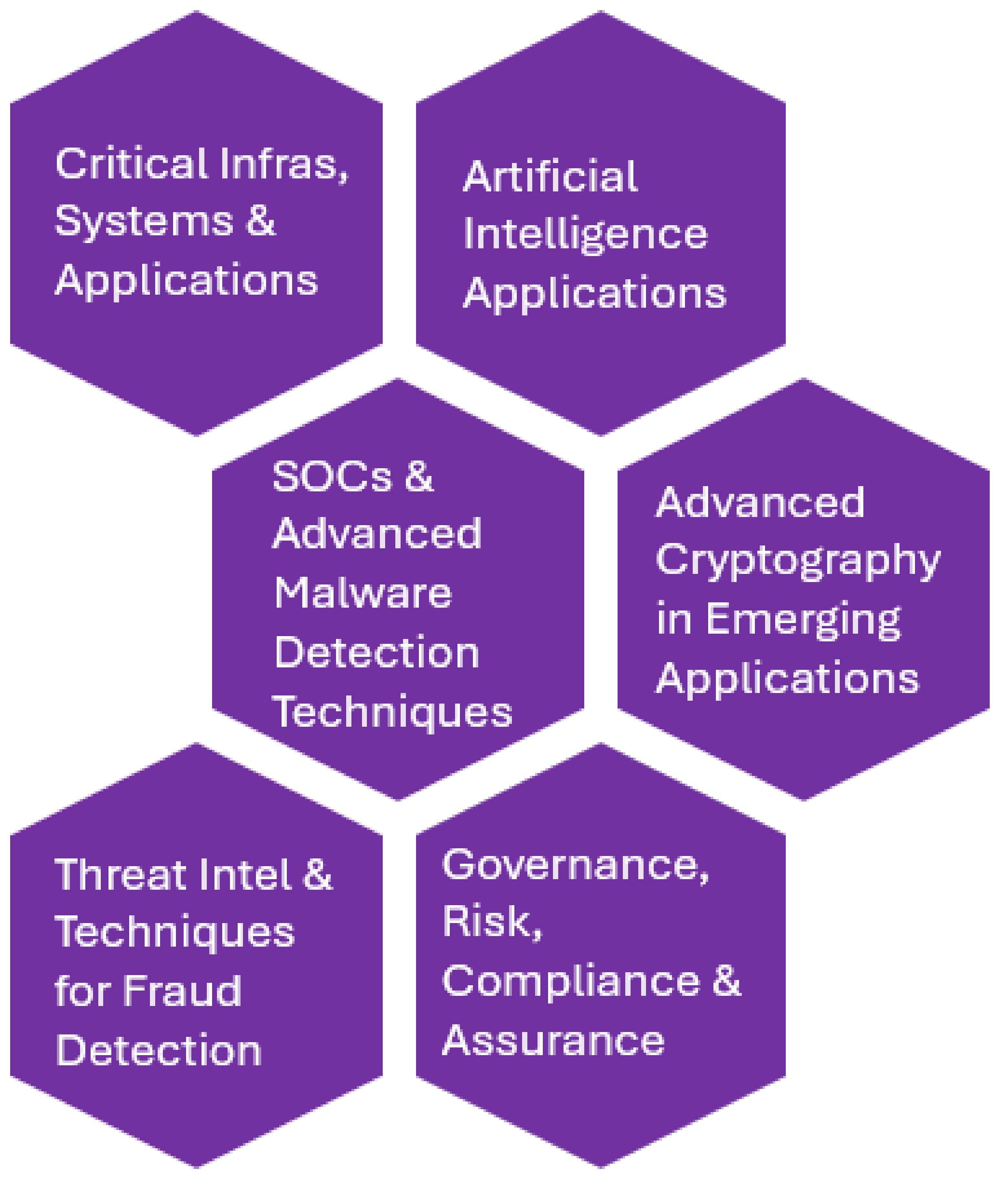
It is a yearly conference held at various cities; the first three meetings have been in London, followed by Glasgow, Scotland in 2018, University of Oxford, England in 2019, and Dublin City University, Dublin, Ireland in 2020, and again at Dublin City University, Ireland in 2021 (held virtually due to COVID-19). The 2022 conference was held at Cardiff Metropolitan University, Wales, UK. In 2023, the conference was held at the University of Aalborg, Copenhagen, Denmark.

THE THEME FOR CYBER SCIENCE 2024

IS

Building Community of Good Practice in Cybersecurity

CyberScience 2024 Themes



Critical Infras, Systems & Applications

Artificial Intelligence Applications

SOCs & Advanced Malware Detection Techniques

Advanced Cryptography in Emerging Applications

Threat Intel & Techniques for Fraud Detection

Governance, Risk, Compliance & Assurance

Contents

CYBER SCIENCE 2024 CONFERENCE PRESENTATION TIMETABLE
TIME IN UK (GMT +1)

CYBER SCIENCE 2024 CONFERENCE INFORMATION

Thursday, June 27th

Friday, June 28th

Conference Venue

Edinburgh Napier University, **Craiglockhart Campus**, Scotland, UK

Edinburgh Napier University

Edinburgh Napier University is a public university located in Edinburgh, Scotland. It was established in 1964 as Napier Technical College and gained university status in 1992. Named after John Napier, the 16th-century mathematician and philosopher known for inventing logarithms. The university offers a wide range of undergraduate and postgraduate programs.

Edinburgh Napier is known for its applied research that addresses real-world issues. Research areas include health, environment, technology, and creative industries. The university has a diverse student body, with students from over 100 countries. It maintains partnerships with institutions worldwide, enhancing its global reach and opportunities for students.

Location

Craiglockhart Campus, 219 Colinton Road, Edinburgh, EH14 1DJ

Conference Structure/ Organisation

- The conference is in-person only starting from Thursday June 27 to June 28, 2024.
- There are a total of three keynote speakers and a panel discussion.
- The Conference proceedings will be opened by Professor Profession William (Bill) Buchanan OBE on Thursday 27th June 2024 at 10:00 GMT+1.
- The first keynote session will take place on 27th June 2024 at 10:40 GMT+1 and will be presented by Dr Lynsay Shepherd, a Reader in Cybersecurity and Human-Computer Interaction at Abertay University.
- The second keynote session to be delivered by Dr. R.V. Gunder, a Criminologist and Lecturer at the University of the West of Scotland, Scotland, UK at 15:15 GMT+1 on 27th June 2024
- The third keynote session will be delivered by Dr Uchenna Daniel Ani on Friday June 28th, 2024. Dr Ani is a Lecturer in Cybersecurity and Programme Lead MSc in Cyber Security Keele University, UK.
- A panel discussion entitled "AI for Cybersecurity: How do we use Artificial Intelligence (AI) to secure Applications and Systems" will be held on Friday 28th June 2024. The discussion is led by Professor Rajendra K. Raj, Dr Sara Vecchini and Dr Cyril Onwubiko.
- There are two parallel sessions each day. Please use the conference timetable to make a choice of the sessions you plan to attend. 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.
- Furthermore, all talks, presentations and keynote speeches will be recorded to give people the opportunity to watch them on-demand.
- The Conference proceedings will be closed by Dr Cyril Onwubiko, the founder of the Centre for Multidisciplinary Research, Innovation and Collaboration and Conference Co-Chair.

CYBER SCIENCE 2024 KEYNOTE SPEAKERS

Keynote Speakers

Professor Bill Buchanan OBE

William (Bill) J Buchanan OBE is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS and Principal Fellow of the HEA. He was appointed an Officer of the Order of the British Empire (OBE) in the 2017 Birthday Honours for services to cybersecurity.

Bill currently leads the Blockpass ID Lab and the Centre for Cybersecurity and Cryptography. He works in the areas of blockchain, cryptography, trust and digital identity. He has one of the most extensive cryptography sites in the World (asecuritysite.com), and is involved in many areas of novel research and teaching. He has published over 30 academic books, and over 350 academic research papers. Along with this, Bill's work has led to many areas of impact, including three highly successful spin-out companies (Zonefox, Symphonic Software and Cyan Forensics), along with awards for excellence in knowledge transfer, and for teaching.

Bill recently received an "Outstanding Contribution to Knowledge Exchange" award, and was included in the FutureScot "Top 50 Scottish Tech People Who Are Changing The World".

Dr Lynsay Shepherd

Dr Lynsay Shepherd is a Reader in Cybersecurity and Human-Computer Interaction at Abertay University and works within the School of Design and Informatics. Lynsay holds a Ph.D. in Usable Security (a combination of HCI and security research), an M.Sc. in Internet Computing, and a B.Sc. (Hons) in Computing.

Lynsay focuses on applied research in the human aspects of cybersecurity, investigating how people interact with emerging technologies, and their behaviour in the context of secure interactions.

Lynsay is particularly interested in the use of eye-tracking measures, serious games, embodied agents, extended reality (XR), safety and accessibility in the metaverse, and romance fraud detection and prevention techniques using machine learning.

Dr R. V. Gundur

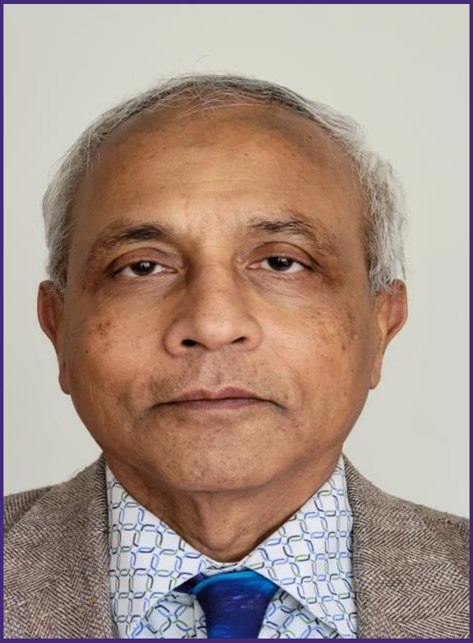
Dr. R. V. Gundur is a Senior Lecturer in Criminology at Flinders University in Australia. He holds a PhD in criminology from Cardiff University, where he was an ESRC scholar; an MSc in Criminology Research Methods from the University of Oxford; an MA in International Relations from The Australian National University, where he was a Hedley Bull Scholar; and a BA in Spanish and Latin American Studies from Tulane University.

His areas of expertise include illicit enterprise, gangs, and cybercrime. His work has appeared in reports published by the European Union and the City of London Corporation, and he has been published in several academic journals including Urban Affairs Review; Deviant Behavior; Crime, Law and Social Change; Trends in Organized Crime; Global Crime, and International Criminal Justice Review. He is the author of Trying to Make It: The Enterprises, Gangs, and People of the American Drug Trade, on Cornell University Press.

Dr Uchenna Daniel Ani

Dr Ani obtained his first degree in Computer Science and his Masters Degree in Computer Security and Forensics from the University of Bedfordshire, UK, and took up the role of Lecturer in Computer Science at Federal University Lokoja, Nigeria. Dr Ani later went on to complete a PhD in Industrial Control System Cybersecurity at Cranfield University, UK.

Prior to joining Keele University, Dr Ani was a Senior Research Fellow in Cybersecurity at the PETRAS National Centre of Excellence for IoT Systems Cybersecurity at the Department of Science Technology Engineering and Public Policy (STEaPP), University College London (UCL). He was involved in leading and guiding the direction of some of the IoT-enabled critical infrastructure security projects in the PETRAS Centre Consortium, as well as supporting teaching in Cybersecurity Risk Assessment and Governance Module for Masters Students. His work is deeply ingrained in multidisciplinary research – exploring and understanding how technical cybersecurity solutions interact with social elements including human, standards, and policy attributes to create safe, secure, practical, and future-proof cyber security and resilient outcomes.



Professor Rajendra K Raj

Professor of Computer Science, Rochester Institute of Technology, USA

Professor Raj earned a B.Tech. in Electrical Engineering, IIT Madras, India; MS in Computer Science, University of Tennessee, Knoxville; Ph.D. in Computer Science, University of Washington, Seattle. He co-created the Computer Science 2023 curriculum, a joint task with IEEE CS, ACM and AAAI. He was also a member of the committee for Computer Science 2013 curriculum development efforts. He's an award winner of various foundations including the National Science Foundation to develop a hands-on data science course for non-computing majors.

You can reach him at https://www.rit.edu/directory/rkrics-rajendra-raj

Dr Sara Vecchini

Dr Sara Vecchini is a highly accomplished security operations and data science expert with a strong background in cyber and fraud data analytics. She holds a PhD in Physics from the University of Modena, Italy. She combines her rigorous scientific training with cutting-edge data science techniques and is interested in the threats and benefits of emerging technologies, LLMs and AI.

Dr Vecchini has held significant roles in organisations such as the Department for Work and Pensions (DWP) and Pearson. She is the Security Operations and Data Science Leader for 2T Security and has been instrumental in developing a specialised SOC for CNI. She is a passionate advocate for women in technology, committed to inspiring future generations of female tech leaders.

Organisers & Chairs

Professor Aunshul Rege

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

Dr Pierangelo Rosati

Dr Pierangelo Rosati is Associate Professor in Digital Business and Society at University of Galway and the Business Community Lead of the IEEE UK & Ireland Blockchain Group. Dr Rosati specialises in measuring the business value of digital technologies and his research has been published widely including European Accounting Review, Computers and Human Behaviour, New Media & Society, European Journal of Finance, International Review of Financial Analysis, Information Technology & People, JASIST and others. He is also a Series Editor on the Palgrave Studies in Digital Business & Enabling Technologies. Dr Rosati previously worked as an Assistant Professor in Business Analytics at DCU Business School where he was Co-Deputy Director of the Irish Institute of Digital Business (IIDB). Dr. Rosati holds a PhD in Accounting and Finance from the University of Chieti-Pescara (Italy), and an MSc and a BSc in Management and Business Administration from the University of Bologna. He has been a visiting professor to ESCP Europe (Italy), Universidad de Las Americas Puebla (Mexico), University of Bologna (Italy), University of Edinburgh Business School (United Kingdom), Católica Porto Business School (Portugal), FGV-EAESP (Brazil) and a visiting Ph.D. student to the Capital Markets Cooperative Research Centre (Australia).

Dr Hanan Hindy

Hanan Hindy, Ph.D. is currently a Lecturer (Assistant Professor) at the Computer Science Department, Faculty of Computer and Information Sciences, Ain Shams University in Egypt. Hanan received her doctorate from the Division of Cyber-Security at Abertay University, Dundee, Scotland. She received her bachelor’s degree with honours (2012) and masters (2016) degrees in Computer Science from the Faculty of Computer and Information Sciences at Ain Shams University, Cairo, Egypt. Her research interests include Intrusion Detection Systems, Computer and Network Security, Artificial Intelligence, and Deep Learning.

Hanan won the IEEE Women in Engineering “Excellence in Engineering" Award in 2021.

You can reach Hanan at https://hananhindy.com

Dr Arnau Erola

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 is the CEO of Lupovis.io, a spinout company of the University of Strathclyde focusing on dynamic cyber-deception, a non-resident senior fellow with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security and a Chancellor's Fellow, Lecturer with the Department of Electronic and Electrical Engineering at the University of Strathclyde. He is also the Chair of the blockchain group and the Vice-Chair of the cyber-security group for IEEE UK and Ireland. He also has over 10 years of experience in consulting across public and private sector. His experience spans from cyber-defence, deception, deterrence and attribution of cyber-threats in critical infrastructures to cyber-situational awareness and cyber-diplomacy and frequently appears in the media to provide commentary to international press – on radio, tv and newspapers on major cyber-events

Professor Martin Gilje Jaatun

Professor Martin Gilje Jaatun is a Senior Scientist at SINTEF Digital in Trondheim, Norway and adjunct professor at the University of Stavanger. Formerly, he 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. Dr. Jaatun graduated with a sivilingeniør degree in telematics from the Norwegian Institute of Technology, and received the Dr.Philos degree from University of Stavanger. He is Vice Chairman of the Cloud Computing Association, an IEEE Cybersecurity Ambassador, an IEEE Computer Society Distinguished Visitor, and a senior member of IEEE.

Dr Cyril Onwubiko

Dr Cyril Onwubiko is the Chief Information Security Officer (CISO), Research Series Limited, London, UK. Also, he is the Vice President, Professional and Educational Activities, a Board of Governor (BoG) and a Distinguished Speaker (DVP) of the IEEE Computer Society. And a Member of the European Public Policy Committee for ICT and Artificial Intelligence. He was a Senior Director, Enterprise Security Architecture at Pearson, and Director, Artificial Intelligence, Blockchain and Cyber Security at Research Series Limited, where he was responsible for directing AI, Blockchain and cyber security strategies and governance. Prior to Pearson, he had worked in the Financial, Telecommunication, Government & Public Services Sectors.

Cyril is a leading scholar in Cyber Situational Awareness (Cyber SA), Cyber Security, and Cyber Science. He is knowledgeable in Information Assurance, HMG Security Policy Framework and Risk Assessment & Management, Cyber-Threat Analysis, Graph Theory, Intrusion Detection Systems and Data Fusion. And interested in the mathematical analysis of security and the application of mathematics in solving real-life problems. His current focus includes Artificial Intelligence, Machine Learning for Cyber Security, and Blockchain Technologies.

CYBER SCIENCE 2024
ACCEPTED PAPERS

A Case Study of a Ransomware and Social Engineering Competition

Aunshul Rege and Rachel Bleiman

Abstract: The average cost of a ransomware attack in 2022 was $4.49 million and the recovery time rose from 7.8 days in 2021 to 14.9 days in 2022. Organizations often bring in professional negotiators to represent them during these attacks to lower ransom demands, buy time for incident response, get evidence of decryptors, and determine who is behind the attack; these research and negotiation skills fall under the area of social engineering. This paper shares a case study of a real-time virtual Ransomware and Social Engineering Competition (RSEC), which occurred in summer 2022 and hosted 8 high school and 6 undergraduate teams. The paper demonstrates how students learned about using psychological persuasion in ransomware negotiations, leveraging OSINT and the ATT&CK framework for attack attribution, and interfacing with the clients to best represent their needs. The paper discusses how the skills and knowledge stemming from RSEC are mapped to the NICE framework.

Malware Detection using Machine Learning Algorithms

Nureni Ayofe Azeez, Ogechukwu Juliet Nzeribe, Charles Van der Vyver and Ademola Philip Abidoye

Abstract: Recent years have seen a surge in malware attacks, which have caused considerable financial and operational damage to individuals and businesses alike. As malware techniques continue to evolve, it is essential to be proactive and adaptive in order to detect and reduce the risk of such attacks. To address this issue, this research is focused on creating a sophisticated malware detection system that utilizes machine learning algorithms to detect Malware attacks. With this technique, a comparative assessment of the algorithms used was carried out. The models were trained using four datasets. The machine learning algorithms used are Decision Trees, Xgboost, Logistic Regression, Naïve Bayes and Random Forest, and are tested for their ability to detect Malware behaviors. A comparison of the results was carried out using four evaluation metrics namely: Accuracy, Precision, Recall and F1-score. At the end of the experiments - For Dataset 1, XGBoost had the highest accuracy of 0.982456. For Dataset 2, Random Forest had the highest accuracy of 0.990432. For Dataset 3, XGBoost, Random Forest and Decision Tree had the highest accuracy of 1.0 meaning they achieved a perfect accuracy of 100%. For Dataset 4, both Random Forest and XGBoost had the highest accuracy with values respectively 0.628474 and 0.628135. A bar chart was used to graphically represent our results for each evaluation metrics. Boxplot used to represent results showing the minimum, maximum, and quartile ranges.

An Exemplar Incident Response Plan for Security Operations Center Analysts

Enoch Agyepong and Cyril Onwubiko

Abstract: The significance of a cyber security incident response plan cannot be overemphasised, especially at a time when cyberattacks are becoming increasingly prevalent and sophisticated. The average cost of a singular cyber incident response in 2023 was ~USD 4.45 million. This figure represents a notable increase over the past few years, showing a rising trend in the costs associated with cyber breaches. Therefore, it is imperative that organisations must have a focused and coordinated approach when responding to cyber incidents. Security Operations Centres (SOCs) need a well-defined incident response plan to facilitate the detection and response activities in the event of a cyberattack. While there are several well-known incident response plans, these plans typically have a broad scope and are designed to assist teams and organisations develop their own incident handling processes. Previous studies propose a tailored incident response plan for the Computer Security Incident Response Team (CSIRT). This paper presents an example incident response plan for SOC analysts. The proposed approach leverages the United States National Institute of Standards and Technology (NIST) incident response framework. The proposed approach will be beneficial to analysts with varying levels of experience/expertise, especially junior and early-career analysts, since research indicates that these categories of analysts are burdened by the complexity of security incident analysis.

RingGuard: A privacy protected Peer-to-Peer Federated Learning Framework

Narasimhan Kovalai, Ramsundar Tanikella, Rojalini Tripathy and Padmalochan Bera

Abstract: Recently, collaborative learning-based training is being used to develop accurate ML models. However, due to privacy and regulatory compliance, data owners are constrained to share their data. To address this, Federated Learning (FL) has emerged as a solution, enabling collaborative model training without the need to share raw data. Instead, only model parameters are exchanged among participating parties. However, FL faces many challenges, particularly its reliance on a central server, managing data heterogeneity and security challenges of parameter sharing. In this paper, we propose a peer-to-peer federated learning framework that leverages secure multiparty computation (SMC) to overcome these challenges. Our framework eliminates the dependency on a central server, ensuring enhanced security in parameter sharing. We implement our proposed framework for both Independent and Identically Distributed (IID) and non-Independent and Identically Distributed (non-IID) data distributions, using FedProx for non-IID data and FedAvg for IID data. We evaluated the performance of our framework using MNIST and FEMNIST datasets, incorporating varying numbers of clients, and conducted a comprehensive analysis. Experimental results demonstrate that our framework performs better in terms of test accuracy and smooth learning than existing centralized FL frameworks.

TIPS: Threat Sharing Information Platform for Enhanced Security

Lakshmi Rama Kiran Pasumarthy, Hisham Ali, William Buchanan, Jawad Ahmad,
Audun Josang, Vasileios Mavroeidis and Mouad Lemoudden

Abstract: There is an increasing need to share threat information for the prevention of widespread cyber-attacks. While threat-related information sharing can be conducted through traditional information exchange methods, such as email communications etc., these methods are often weak in terms of their trustworthiness and privacy. Additionally, the absence of a trust infrastructure between different information-sharing domains also poses significant challenges. These challenges include redaction of information, the Right-to-be-forgotten, and access control to the information-sharing elements. These access issues could be related to time bounds, the trusted deletion of data, and the location of accesses. This paper presents an abstraction of a trusted information-sharing process which integrates Attribute-Based Encryption (ABE), Homomorphic Encryption (HE) and Zero Knowledge Proof (ZKP) integrated into a permissioned ledger, specifically Hyperledger Fabric (HLF). It then provides a protocol exchange between two threat-sharing agents that share encrypted messages through a trusted channel. This trusted channel can only be accessed by those trusted in the sharing and could be enabled for each data-sharing element or set up for long-term sharing.

Workshop Insights: Navigating Cybersecurity Regulations for Device
Manufacturers and Healthcare Operators

Andrea Skytterholm, Lars Halvdan Flå and Martin Gilje Jaatun

Abstract: Both the manufacture and use of medical devices are heavily regulated, but stakeholders have a varying level of maturity, and often struggle to comply with rules and regulations. This paper reports on an empirical elicitation activity that sought to enumerate the challenges faced by (particularly smaller) device manufacturers and device operators (typically: hospitals, with a goal to informing the creation of tools that these stakeholders can use to address the challenges.

TRIST: Towards a container-based ICS testbed for cyber threat simulation and anomaly detection

Carol Lo, Jack Christie, Thu Yein Win, Zeinab Rezaeifar, Zaheer Khan and Phil Legg

Abstract: Cyber-attacks on Industrial Control Systems (ICS), as exemplified by the incidents at the Maroochy water treatment plant and the Ukraine's electric power grid, have demonstrated that cyber threats can inflict significant physical impacts. These incidents caused widespread service disruptions and substantial economic losses, underscoring the urgent need for an in-depth understanding of cyber threats in industrial environments. Industrial security research is usually conducted on physical testbeds to avoid safety issues, production interruptions and other operational constraints in industrial processes. Nevertheless, security defenders often encounter obstacles in developing or accessing physical testbeds due to associated costs and complexities. These factors hinder research progress to devise early detection mechanisms for cyber threats – essential for effective incident response. To overcome these obstacles, this paper presents a container-based virtual testbed. Its lightweight architecture enables replicable and efficient deployment of testbeds at low cost for simulating cyber threats on Cyber-Physical Systems (CPS) – the cornerstone of industrial automation and control systems. Also, the container-based virtual testbed provides a cost-effective option for producing datasets for training, testing and optimization of unsupervised anomaly detection models. Besides, an evaluation on resource consumption is conducted. The paper also discusses the benefits and limitations of proposed container-based ICS testbeds and suggests future research areas.

Exploring DTrace as an Incident Response Tool for Unix Systems

Joe Duin, Sean McKeown and Mwrwan Abubakar

Abstract: Critical National Infrastructure (CNI) is often the target of sophisticated and sustained cyber-attacks perpetrated by advanced threat actors with considerable resources. These attacks can lead to interruptions in core services such as energy and water supplies, transportation, healthcare, and telecommunications. The effective and swift remediation of such attacks is contingent on the respective Digital Forensics and Incident Response (DFIR) professionals possessing the appropriate tooling and resources for the target environments. However, the Unix systems which often run critical infrastructure are poorly accommodated in comparison to their Windows and Linux counterparts. This paper seeks to expand the options available to DFIR analysts on Unix systems by exploring the potential for DTrace as a potential Incident Response utility. DTrace is included in many Unix operating systems by default, while also having support for Linux, Windows and macOS, making it a useful pre-packaged solution. We explore the utility of DTrace, and the visibility it provides into the OS and kernel, through a variety of proof-of-concept case studies based on tactics and techniques in the MITRE ATT\&CK framework. We find that DTrace's functionality lends itself well to a real-time monitoring and probing solution for Unix systems, which could potentially form the basis of an EDR solution to revolutionise Incident Response on such platforms.

Fuzzing the ARM Cortex-M: A Survey

Silje Marie Sørlien, Åse Marie Solnør, Karin Bernsmed and Martin Gilje Jaatun

Abstract: Security testing is challenging with low-level connected devices such as Internet of Things (IoT) devices, with limitations in memory, communication bandwidth, and processing power. As a result, traditional testing processes become difficult and time-consuming in such cases. In this paper, we survey recent fuzz testing platforms suitable for security testing of embedded firmware, and assess how suitable they are for a specific use case.

Cybersecurity Upskilling for Criminal Justice Professionals

Yan Bai and Juan Li

Abstract: A diverse and interdisciplinary cybersecurity workforce plays a crucial role in enhancing cybersecurity worldwide. Criminal justice (CJ) professionals are at the forefront of investigating cybercrimes and bringing cyber-criminals to justice. Their expertise and efforts in cybersecurity are essential to maintaining the integrity of our digital ecosystem and ensuring the safety and security of individuals, organizations, and society. However, many CJ professionals have not received comprehensive cybersecurity education and training. This knowledge gap poses significant challenges and limitations to effectively combating cybercrime. With the sponsorship of National Science Foundation, The University of Washington Tacoma and North Dakota State University are developing scenario-based offensive security and Web-based showcase labs with interactive simulations and case studies in three progressive courses, revolutionizing cybersecurity education for future CJ professionals. This project integrates artificial intelligence into the curriculum to enhance CJ professionals'

capabilities. Our ultimate goal is to develop a skilled workforce of CJ professionals with cybersecurity and privacy knowledge, addressing the critical need for such expertise in the field. Our poster will explain the motivations behind our project, the course framework used, and preliminary implementation results.

vSPACE: Voting in a Scalable, Privacy-Aware and Confidential Election

Se Elnour, William Buchanan, Paul Keating, Mwrwan Abubaka and Sirag Elnour

Abstract: The vSPACE experimental proof-of-concept (PoC) on a TrueElect extended protocol presents a novel approach to secure, private, and scalable elections, extending the TrueElect and other related protocols with the integration of Self-Sovereign Identity (SSI) enabled Privacy-Enhancing Technologies (PETs). Zero-Trust Architecture (ZTA) principles and practices were used for a split-trust design to minimize human errors or attacks, along with using a trustworthy Infrastructure as Code (IaC) automation for staging a perfectly democratized e-governance polling; while also leveraging confidential computing, continuous authentication, multi-party computation (MPC), and Well-Architected Framework principles to address cybersecurity and privacy protection challenges. Moreover, vSPACE integrates Distributed Ledger Technology (DLT) for immutable and certifiable audit trails, and employs Kubernetes confidential clusters as ZTA spokes for hosting decentralized applications (dapps) with a connectivity hub of an nTier-based Enterprise-Scale Landing Zone (ESLZ). The IaC model ensures rapid deployment, consistent management, and adherence to security standards, making vSPACE a future-proof solution for digital voting systems. Our poster and concept note include motivations behind low-level design choices, ZTA specifications with a threat modeling assurance review, quantitative metrics on efficiency performance, and preliminary implementation IaC tooling.

Perception of cyber risk for assisted living technologies in the Norwegian healthcare sector – key stakeholders perceptions

Alvhild Skjelvik and Bian Yang

Abstract: Facing a demographic shift and healthcare personnel shortage, Norway and other European nations anticipate increased healthcare demands. Assisted living technologies are seen as potential solutions to manage demands, yet they carry inherent cybersecurity risks. While the majority of prior research within cybersecurity for assisted living technology has focused on tech-nical risks, this study examines cybersecurity risk perception among key stakeholders in the Norwegian healthcare sector. Utilizing the BCISQ-questionnaire and incorporating a behavioral simulation, we analyzed risk perception patterns among 185 survey respondents and 33 interviewees. Despite observable differences in risk perception among stakeholders, attributed to factors like human error, organizational affiliation, and technology familiarity, the sample size limits generalizability. Key findings highlight the risk perception related to assisted living technology amongst five stakeholder groups, where their perception of risk is formed by likelihood and consequence in light of confidentiality, integrity and availability. This study not only capture stakeholders' cybersecurity perception but also identify the differences between the groups, and factors influencing their perceptions.

Attention based Image Steganography Using CNNs in Integration with Quantization

Sravan Kumar Gatram, Kamalakanta Sethi, Piyush Joshi and Rakesh Kumar Sanodiya

Abstract: Steganography is a security mechanism that is primarily used to hide secret information in various forms of digital media. This is useful for transmitting sensitive information without disclosing its existence. In this paper, we present a novel deep learning based steganographic approach that integrates Convolutional Neural Networks (CNNs) with Quantization and Convolutional Block Attention Module (CBAM). Our steganography approach overcomes various shortcomings of existing methods, including low embedding capacity and visual distortions in images. The integration of CNNs in our proposed approach enables efficient feature extraction, while Quantization refines and enhances the extracted features which helps to preserve the image quality after embedding. In addition, the CBAM attention mechanism captures useful features while filtering out noise and irrelevant information. This helps us to reduce the feature distortions and improve the feature representations. We have implemented and tested the effectiveness of our steganographic approach with various evaluation metrics. The experimental results show that our model outperforms the state-of-the-art approaches.

Improving Credit Card Fraud Detection with Combined Feature Extraction and Class Balance Optimisation Techniques

Boluwatife Ajibade-Ajibosin, Uchenna Daniel Ani, Theocharis Kyriacou and Mark Turner

Abstract: Credit card fraud is a persistent and evolving challenge that poses significant financial harm to cardholders, financial institutions, national, and global economies. The use of Machine Learning (ML) methods has heavily enhanced the detection of credit card fraud, offering improvements to other traditional credit card fraud detection approaches such as manual checks and rule-based methods. However, there are limitations that impact the performance and efficiency of the credit card detection using ML. This work addresses some of the current challenges associated with employing ML for credit card fraud by developing a robust credit card fraud detection model. The proposed model employs Syn-thetic Minority Oversampling Technique (SMOTE) to address the class im-balance issue typically akin to credit card fraud datasets. A Recursive Feature Elimination with Cross-Validation (RFECV) scheme was utilized as a feature selection technique to select the optimal subset of features that can improve the accuracy of the credit card fraud detection model. Following rigorous evaluation, the proposed credit card fraud detection system demonstrates exceptional performance above other known existing systems across critical metrics including accuracy, recall, precision, F1 score, and ROC-AUC. Thus, is considered a better solution for more accurate detection of credit card fraud instances.

Digital Evidence from the Legal Practitioners' Perspective

Ibeabuchi Egbu, Jacques Ophoff and Annelize McKay

Abstract: Cybersecurity, much like traditional security, requires the collaborative effort of various stakeholders, including government, regulators, tech professionals, and legal practitioners. Each party must play their part effectively to achieve the objective of a cyber environment free from danger or threat. Ironically, legal practitioners who are responsible for prosecuting cybercrimes and administering justice face significant challenges in interpreting and applying the technical aspects of digital investigations. Existing research indicates that this difficulty largely stems from their predominantly non-technical background, which hinders their ability to fully grasp the implications of digital evidence. This research study aimed to investigate how employing analogies to traditional forms of evidence could aid legal practitioners in better understanding and applying the technical terms encountered in digital investigations. Building on existing literature on legal practitioners' digital awareness, this research study adopted a five-step methodological approach. First, a digital forensics report was analysed to identify technical terms. These technical terms were simplified and analogies to traditional evidence were constructed. These analogies were published via a website, and made accessible through a custom-built Microsoft Word add-in. A survey involving 16 participants was carried out to assess the value of the simplification provided by the analogies, and the impact was evaluated against Bloom's taxonomy of cognitive learning. Results show that the analogies improved understanding of the digital forensics report and the way practitioners interpreted and applied technical terms found in the report.

Attack Resilient Federated Learning Framework

Sushant Kumar, Kasturi Routray and Padmalochan Bera

Abstract: Federated learning stands out as a promising paradigm for collaborative training of machine learning models where a server supervises the learning process while keeping sensitive data on the user devices. Here, training is decentralized and conducted on edge devices beyond the control of a server. This increases the potential for malicious clients to tamper with the learning process and compromise the global model, resulting in a significant security risk. The majority of existing solutions are tailored to scenarios where data exhibits independent and identically distributed (IID) characteristics across devices. A notable performance degradation is observed when the data distribution deviates from the independent and identically distributed (nonIID) scenario. In this paper, we first evaluate the performance of existing byzantine robust aggregation schemes in non-IID settings within an adversarial scenario. Then, we introduce a novel attack resilient aggregation scheme named FedResil with the objective of enhancing performance in the same adversarial environment. It leverages non-private data, which is collectively agreed upon by the participating clients before the training process begins, to delineate clusters of clients. Subsequently, the server applies existing byzantine robust aggregation rules to each cluster independently, generating model updates within each cluster. The model update from each cluster is then aggregated to construct the final global model. Through extensive experimentation, we demonstrate that FedResil in malicious settings achieves performance similar to those in scenarios where there is no malicious client.

Design of Pairing Free Attribute-based Encryption for Smart Grid Applications

Anjali Kumari, Sreevallabh Karanam, Swejan Annabathini and Kamalakanta Sethi

Abstract: Smart grids are light-weight, intelligent and reliable devices used daily for power supply. Smart grids continuously measure the incoming and outgoing flow of electricity and other connected smart grids. This data is shared with many stakeholders like the users (the actual user of electricity), phasor units etc. The data security here plays a crucial role. Initially pairing CP-ABE was used in order to provide fine grain access control and data integrity and confidentiality. But the computationally complexity of the cryptographic technique add overhead to the system reducing its performance. In order to improve the performance matrix of smart grids we propose the Pairing Free CP-ABE (PF CP-ABE) which uses replaces the complex bilinear pairing with simpler scaler multiplication. At last, we have analyzed the security, access policy and collusion resistance properties along with the performance analysis of our system.

Critical Infrastructures in the Cloud

Martin Gilje Jaatun and Geir Kjetil Hanssen

Abstract: Cloud computing is increasingly being used not only to support critical infrastructure applications, but actually forms a vital part of them. This paper discusses challenges faced by custodians of critical infrastructures when moving to the cloud, and outlines some security requirements that are relevant to apply to critical infrastructure cloud applications

Radio Frequency (RF) Cyber Threats and a novel RF Cyber Kill Chain

Carolyn Swinney and Woods John

Abstract: Cyber threats are defined as those that target a system's availability, integrity, or confidentiality. As the threat landscape increases with 5G and IoT connectivity, so does the potential to directly affect or access connected 'system of systems' using Radio Frequency (RF) connections. The open architecture and low cost nature of today's Software Defined Radio (SDR) technology present opportunities to easily exploit RF access points with cyber threats in a growing connected cyber terrain. SDRs can provide low-cost, simple discrete attacks on a system's confidentiality, integrity, and availability, without a requirement for physical access. The Cyber Kill Chain, which focuses on external complex and persistent threats, is not fit for purpose for an RF-based threat. While traditional cyber threats may be increasing in complexity and time to render, it is suggested in this paper that RF enabled cyber-attacks are becoming less complex and easier to implement due to the availability of low-cost SDR technology and associated high-power amplifiers and antennas. In this paper, a new RF Cyber Kill Chain is proposed to aid penetration testers and improve the cyber-security of connected systems. The RF Cyber Kill Chain is shown through a case study to accurately map three stages of attack: Reconnaissance, Preparation, and Execution. SDR technology is also shown in this paper to have enormous potential when combined with machine learning (ML) to provide early warning of cyber-attacks utilising the RF spectrum.

Implementation of Zones and Conduits in Industrial Control and Automation Systems

Lars Halvdan Flå, Mary Ann Lundteigen, Fredrik Gratte and Martin Gilje Jaatun

Abstract: Despite being established concepts in standards we argue that zones and particularly conduits can benefit from more detailed discussions of their architecture and implementation. In this paper we make three contributions towards this. Firstly, we describe detailed principles for implementing conduits. Secondly, we outline a process for connecting zones with potentially different Security Levels (SLs), expressed in the form of a flow chart. Thirdly, we discuss a few highlighted challenges related to the application of zones and conduits in practice.

Towards a Secure Manufacturing Framework for Single Malt Whisky in Industry 4.0

Jacob Connell, Dimitrios Kasimatis, Pavlos Papadopoulos, William J. Buchanan, Panagiotis Sarigiannidis and Nikolaos Pitropakis

Abstract: Recent instances have brought to light the inherent vulnerability of the manufacturing sector to cyber security threats, particularly within the food and beverage industries. With the rapid adoption of Industry 4.0, supply chains are exposed to an expanding surface area of potential attacks. This paper delves into the paramount issue of supply chain security and explores the utilisation of distributed ledger technology to enhance the reliability and security of the whisky manufacturing process. We introduce an experimental framework that is focused on performance enhancements and security optimisations. Furthermore, a review of the implemented testbed evaluates the robustness of the business logic, emphasising additional benefits derived from implemented features. This analysis serves to showcase the advancements made in response to recent disruptions within similar supply chains.

Utilizing YARA: An Effective Method for Phishing Attack Response

Ferenc Leitold

Abstract: Phishing attacks continue to be a major threat to cybersecurity, leveraging deception to extract sensitive information from unsuspecting victims. This paper explores the use of YARA (Yet Another Recursive Acronym), a powerful tool for malware identification and classification, in enhancing the detection and response to phishing attacks. We delve into several phishing techniques such as spear phishing, whaling, and clone phishing, outlining their evolution and the increasing sophistication of these threats. The paper discusses the creation and application of YARA rules to identify phishing indicators within emails, including suspicious language, generic greetings, and malicious links or attachments. By integrating YARA into cybersecurity operations, organizations can create customizable and efficient detection frameworks that adapt to emerging threats. Through practical examples and case studies, we demonstrate the effectiveness of YARA in identifying both traditional and obfuscated phishing attacks, thereby

improving incident response and mitigating the impact of these pervasive threats to individuals and businesses alike. This research highlights YARA's versatility and its significant role in bolstering cybersecurity defenses against phishing.

Cyber Science 2024 Conference

Timetable

CYBER SCIENCE 2024 TIMETABLE

Thursday, June 27th – Friday 28th June | UK Time zone: **GMT+1**

Theme- Building Community of Good Practice in Cybersecurity

Thursday June 27, 2024 | UK Time zone: GMT+1

Time	Description
09:00 –09:45	**Registration and Breakfast**
09:45 –10:00	**Conference Announcements**

10:00-10:30	**Conference Proceedings Opening** **Professor William (Bill) Buchanan** OBE, PhD, FBCS, PFHEA, CEng, BSc (Hons)	
10:40 –11:40	**Keynote Session By** **Dr. Lynsay Shepherd** Reader in Cybersecurity and HCI School of Design and Informatics | Division of Cyber Security	
11:40 –11:50	**Coffee & Tea Break**	
11:50 -12:20	Day 1 / Session 1: Host & Moderator: Sean / Belinda	Day 1 / Session 2: Host & Moderator: Sana
	Towards a Secure Manufacturing Framework for Single Malt Whisky in Industry 4.0 *Jacob Connell, Dimitrios Kasimatis, Pavlos Papadopoulos, William J. Buchanan, Panagiotis Sarigiannidis and Nikolaos Pitropakis*	**Critical Infrastructures in the Cloud** *Martin Gilje Jaatun and Geir Kjetil Hanssen*
12:20 -12:50	**TIPS: Threat Sharing Information Platform for Enhanced Security** *Lakshmi Rama Kiran Pasumarthy, Hisham Ali, William Buchanan, Jawad Ahmad, Audun Josang, Vasileios Mavroeidis and Mouad Lemoudden*	**Design of Pairing Free Attribute-based Encryption for Smart Grid Applications** *AnjaliKumari,Sreevallabh Karanam, Swejan Annabathini and Kamalakanta Sethi*

12:50 -13:50	**Group Photography & Lunch Break**	

14:00 -14:30	**Utilizing YARA: An Effective Method for Phishing Attack Response** *Ferenc Leitold*	**Malware Detection using Machine Learning Algorithms** *Nureni Ayofe Azeez, Ogechukwu Juliet Nzeribe, Charles Van der Vyver and Ademola Philip Abidoye*
14:30 –15:00	**A Case Study of a Ransomware and Social Engineering Competition** *Aunshul Rege and Rachel Bleiman*	
15:00 –15:15	**Coffee & Tea Break**	
15:15 –16:15	**Keynote Session By** **R.V. Gundur, PhD** Criminologist & Lecturer University of the West of Scotland, Scotland, UK	
16:15 – 16:30	**Coffee & Tea Break**	
16:30 – 17:00	**Digital Evidence from the Legal Practitioners' Perspective** *Ibeabuchi Egbu, Jacques Ophoff and Annelize McKay*	**Attack Resilient Federated Learning Framework** *SushantKumar,KasturiRoutrayand Padmalochan Bera*
17:00 – 17:30	**Improving Credit Card Fraud Detection with Combined Feature Extraction and Class Balance Optimisation Techniques** *Boluwatife Ajibade-Ajibosin, Uchenna Daniel Ani, Theocharis Kyriacou and Mark Turner*	**Attention based Image Steganography Using CNNs in Integration with Quantization** *Sravan Kumar Gatram, Kamalakanta Sethi, Piyush Joshi and Rakesh Kumar Sanodiya*
18:00 – 21:00	Evening Dinner & Drinks	

Friday June 28, 2024
Theme – Building Community of Good Practice in Cybersecurity
UK Time zone: GMT+1

Cyber Science 2024 Conference		
09:00 – 09:30	**Coffee & Tea**	
09:30 – 10:30	**Keynote Session By** **Dr. Uchenna Daniel Ani** Lecturer in Cybersecurity, & Programme Lead MSc in Cyber Security Keele University, UK	
10:30 – 10:45	**Coffee & Tea Break**	
	Day 2 / Session 3: Host & Moderator: Naghmeh	Day 2 / Session 4: Host & Moderator: Matthew
10:45 – 11:15	**An Exemplar Incident Response Plan for Security Operations Center Analysts** *Enoch Agyepong and Cyril Onwubiko*	**Cybersecurity Upskilling for Criminal Justice Professionals** *Yan Bai and Juan Li*
11:15 – 11:45	**RingGuard: A privacy protected Peer- to-Peer Federated Learning Framework** *Narasimhan Kovalai, Ramsundar Tanikella, Rojalini Tripathy and Padmalochan Bera*	**Fuzzing the ARM Cortex-M: A Survey** *Silje Marie Sørlien, Åse Marie Solnør, Karin Bernsmed and Martin Gilje Jaatun*
11:45 – 12:00	**Coffee & Tea Break**	
	Industry Talk	
12:00 – 12:15	**Cystel – Building Resilience & Agility through Cybersecurity Quantum Innovation** by Dr Thomas Matheus, CTO Cystel	
12:15 – 12:30	**Smart Net Zero – Building Transformative network of Building Management System, Operational and Information Technology (OT/IT) Cybersecurity** by Andrew Rae, Security Director, Smart Net Zero	
12:30 – 13:30	**Perception of cyber risk for assisted living technologies in the Norwegian healthcare sector – key stakeholders perceptions** *Alvhild Skjelvik and Bian Yang*	**vSPACE: Voting in a Scalable, Privacy-Aware and Confidential Election** *Se Elnour, William Buchanan, Paul Keating, Mwrwan Abubaka and Sirag Elnour*
13:30 – 13:45	**Group Photography & Lunch Break**	

13:45 – 14:15	**Exploring DTrace as an Incident Response Tool for Unix Systems** *Joe Duin, Sean McKeown and Mwrwan Abubakar*

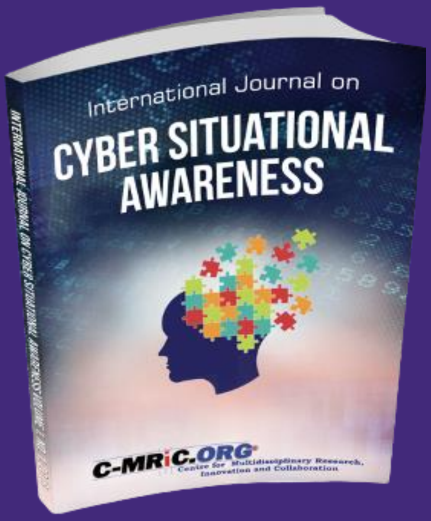
14:15 –14:45	**TRIST: Towards a container-based ICS testbed for cyber threat simulation and anomaly detection** *Carol Lo, Jack Christie, Thu Yein Win, Zeinab Rezaeifar, Zaheer Khan and Phil Legg*	**Workshop Insights: Navigating Cybersecurity Regulations for Device Manufacturers and Healthcare Operators** *Andrea Skytterholm, Lars Halvdan Flå and Martin Gilje Jaatun*
14:45 –15:00	**Coffee & Tea Break**	
15:00 –15:30	**Implementation of Zones and Conduits in Industrial Control and Automation Systems** *Lars Halvdan Flå, Mary Ann Lundteigen, Fredrik Gratte and Martin Gilje Jaatun*	**Radio Frequency (RF) Cyber Threats and a novel RF Cyber Kill Chain** *Carolyn Swinney and Woods John*
15:30 –16:30	**Panel Discussion** **AI for Cybersecurity:** **How do we use Artificial Intelligence (AI) to secure Applications and Systems** **Speakers: Professor Rajendra K. Raj, Dr Sara Vecchini and Dr Cyril Onwubiko**	
16:35	Closing of the Proceedings by Dr Cyril Onwubiko	

Legend

Conference Talks	**Conference Talks**	**Panel Session**	**Keynote Session**	**Lunch & Dinner / Drinks**

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

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

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

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

C-MRiC.ORG Springer