#SECREV2024 DETAILED PROGRAM

1. SUNGKYUNKWAN UNIVERSITY- SOUTH KOREA

- UTC 0 :00~UTC 2 :00 : Cybercrime Investigation and Digital Forensics for Cyber Security

- Hosted by Dr. Gibum Kim

- Approach for Prioritization of Digital Evidence Screening Based on Metadata Similarity - Seoyeon Lee
- A Study on Institutionalization and Advancement of Digital Forensic Proficiency Test Provider - Na Bomi
- An Inquiry into the Integration of eXtended Reality (XR) Technologies in Digital Forensics: Exploring Efficacy, Challenges, and Opportunities - Jeong Jaehyun
- Analysis of Cyber Gambling Organized Crime Networks - Investigative Strategies through Centrality and Structural Holes - Moon Bunghun
- Ransomware Attack Criminal Law Revision: Comparative Analysis of Ransomware Criminal Law in Korea and the United States. - Lee Gyung Ju

---

2. DEAKIN UNIVERSITY – AUSTRALIA

- UTC 2 :00~UTC 4 :00 : Cybercrime in the Indo-Pacific region: Trends and Challenges

- Hosted by: Dr Lennon Chang, Sr Chad Whelan
- Speakers include : Dr Duc Huy Phan, Ms Andi Brown, Mr Souvik Mukherjee, Ms Irnasya Shafira

---

3. THE HAGUE UNIVERSITY OF APPLIED SCIENCES – THE NETHERLANDS

- UTC 4 :00~UTC 5 :00 : Cybercrime: Mules, Markets, Minors and Money.

- Willingness to pay among entrepreneurs after Ransomware Victimization – Sifra Matthijsse
- Recruiting money mules in a digital age: the online and offline involvement mechanisms of cybercrime – Luuk Bekkers
- Exploring the Operational Mechanisms and Trust Signlas in a Cybercrime-as-a-Service Marketplaces Training Remote Access Tools – Hannah Kool
- Origin and growth of, and crimes committed by cybercriminal youth networks – Joeri Loggen

---

4. SECREV PRESENTS

- UTC 5:00~UTC 6:00 : CyberFrontiers: The Next Generation of Researchers

This session will present a series of interviews with up-and-coming researchers who are fascinated by cybercrime and cybersecurity. this diverse group are studying current issues in the world of cybersecurity from the different perspectives afforded by different disciplines. From the realms of computer science, sociology, business and more we present some bright minds talking about what is to be a researcher in the modern dynamic world of research.

---

5. THE INTERNATIONAL INSTITUTE OF JUSTICE AND POLICE SCIENCES (IIJPS) & CENTRE FOR CYBER VICTIM COUNSELLING- INDIA

- UTC 6:00~UTC 8:00 : Cyber Criminology and Cyber Security in South Asia: Issues and Introspection

This session will delve into the intricate world of cybercrime and cybersecurity, focusing specifically on the South Asian region. From examining emerging threats to discussing strategies for resilience, this session promises insightful discussions and

introspection into the challenges and opportunities facing this dynamic field. Participants are invited to embark on a journey of exploration and collaboration to better understand and address the pressing issues in cyber criminology and cybersecurity in South Asia.

- Introduction and Moderation by Dr K. Jaishankar
- Cybersecurity for Space Sector in India - Sagar Singamsetty,
- Cyber Violence against Women in Bangladesh - Rukhsana Siddiqua
- Panel Discussion on Cyber Crime and Cyber Security in South Asia with special reference to India - K. Jaishankar, Prasanna Guntur, Raj Pagariya, Yashwanth A S.

---

6. THE UNIVERSITY OF PORTSMITH- UK

- UTC 8:00~UTC 10:00 : Cybercrime, Cybersecurity and Society

- Hosting Introduction - Iain Reid
- Cyber Geostrategy Incident response - Soraya Harding
- Exploring The Human Reaction to Prompts and Commands from Computer Vision Enabled Machines - Martin Lynch
- Countering Online Social Propaganda using Online Visual Narratives - Brandon May
- Title Forthcoming - Lauren Stevens

---

7. LIVEGIG LTD. - NIGERIA

- UTC 10:00~UTC 12:00 : Navigating the Evolving Cybersecurity Landscape in AFRICA: Compliance and Beyond

- Hosted by Frank Bazuaye and Kobina Adomadzi Longdon

  This topic will focus on the challenges and opportunities in harmonizing cybersecurity regulations across different African countries. The discussion will explore the benefits of having consistent cybersecurity laws and the challenges posed by diverse

legal frameworks. It will also address strategies for promoting collaboration among African nations to create a unified approach to cybersecurity regulation.

- Harmonizing Cybersecurity Regulations Across African Jurisdictions - Victor Ikenna Mgboji, Esq

  This topic will delve into the complexities of data privacy regulations in Africa and the challenges associated with cross-border data transfers. The discussion will explore the current landscape of data protection laws across different African countries, including key provisions and enforcement mechanisms. It will also address the implications of international data transfer regulations such as GDPR and the strategies organizations can employ to ensure compliance while facilitating the flow of data across borders.

- Data Privacy and Cross-Border Data Transfers in Africa - Iheanyi Nwankwo

  This topic will focus on the legal considerations surrounding incident response and cyber insurance in Africa. The panel will discuss the legal requirements for reporting data breaches, coordinating with law enforcement agencies, and managing liabilities in the aftermath of a cybersecurity incident. Additionally, the discussion will explore the role of cyber insurance in mitigating financial risks associated with cyber threats and the legal implications of insurance policies in the event of a claim.

- Legal Implications of Incident Response and Cyber Insurance - Josephine Sam

  This topic will focus on the legal considerations surrounding incident response and cyber insurance in Africa. The panel will discuss the legal requirements for reporting data breaches, coordinating with law enforcement agencies, and managing liabilities in the aftermath of a cybersecurity incident. Additionally, the discussion will explore the role of cyber insurance in mitigating financial risks associated with cyber threats and the legal implications of insurance policies in the event of a claim.

- Regulatory Compliance and Third-Party Risk Management - Onyinyechi Nwachukwu

  This topic will examine the legal obligations of organizations in managing third-party cybersecurity risks and ensuring regulatory compliance. The panel will discuss the legal frameworks governing third-party relationships, including vendor contracts, service level agreements, and data processing agreements. It will also address the legal considerations for conducting due diligence on third-party vendors, assessing their cybersecurity posture, and implementing contractual safeguards to mitigate risks associated with outsourcing IT services and data processing operations.

- Implementing Secure Infrastructure in African Organizations - Herber Muhirwa

  This topic will cover the practical aspects of implementing secure IT infrastructure within African organizations. The discussion will explore strategies for building robust cybersecurity systems, including network security, endpoint protection, and secure cloud services. It will also address the unique challenges faced by African organizations in adopting and maintaining secure IT infrastructure, such as limited resources and infrastructure gaps.

- Emerging Threats and Mitigation Strategies in African Cybersecurity - Jema Ndibwile

  This topic will focus on identifying and mitigating emerging cybersecurity threats in the African context. The discussion will cover trends such as ransomware attacks, social engineering, and supply chain vulnerabilities, and explore effective strategies for detecting, preventing, and responding to these threats. Additionally, the panelist will discuss the role of threat intelligence sharing and collaboration in enhancing cybersecurity resilience across African organizations.

---

8. THE CANADIAN INSTITUTE FOR CYBERSECURITY, THE UNIVERSITY OF NEW BRUNSWICK - CANADA

o UTC 12:00~UTC 14:00 : The 5W's of Cybersecurity Dataset Creation at CIC (Canada)

- Hosted by Sumit Kundu
- From Profiling to Protection: Leveraging Datasets for Enhanced IoT Security - Dr. Sajjad Dadkhah

  Securing these interconnected environments has become paramount in the era of ubiquitous Internet of Things (IoT) devices. This talk concentrates on the complexities and challenges of IoT security, underscored by the exponential growth of devices and their diverse applications across sectors such as smart homes, healthcare, and transportation. We illuminate the cutting-edge methodologies employed in IoT device profiling, fingerprinting, and behavioral analysis through a detailed examination of four recently published datasets. These datasets offer a foundation for understanding device behaviors under various scenarios, including attack simulations, and enhance our ability to conduct vulnerability assessments and develop robust security frameworks. This presentation aims to equip researchers, developers,

and cybersecurity professionals with the knowledge and tools needed to strengthen IoT ecosystems against emerging threats by exploring the convergence of machine-learning approaches, real-time data analysis, and comprehensive attack documentation.

- IoTProMo: Securing IoT Networks using Device Profiling and Monitoring - Alireza Zohourian

  IoT networks are attracting increasing attention and are becoming more complex with each passing day. The IoT environment is characterized by its dynamic, heterogeneous nature, while IoT devices often face limitations in terms of resources, hindering their ability to implement sophisticated security measures. Consequently, the attack surface within IoT networks is extensive. This presentation delves into the concept of IoT device profiling and monitoring through behavioral fingerprinting as a potential solution to address the complexities of IoT networks. By adopting this approach, the aim is to mitigate the challenges posed by the diverse nature of IoT environments, thereby enhancing their overall security posture.

- CICEVSE2024: Creation of a dataset to advance cybersecurity research in Electric Vehicle Charging Stations - Emmanuel Dana Buedi

  The rapid adoption of electric vehicles (EVs) is fundamentally transforming the automotive industry, prompting a surge in the installation of charging stations to accommodate the growing number of EVs and enhance overall mobility and user experience. Efforts to conduct machine learning-based cybersecurity research and developing solutions to address the growing threats and vulnerabilities in EV charging station infrastructure face challenges stemming from the unavailability of suitable datasets. The primary contribution of this study is addressing these challenges by publishing a multi-dimensional dataset that comprises power consumption data, network traffic and host activities of the EVSE in both benign and attack conditions. The experimental testbed utilizes a real EVSE, Raspberry Pi and standard industry communication protocols for EV charging infrastructure, with the scenarios observing the EVSE in both idle and charging states. The results of statistical analysis and machine learning classification tasks demonstrate the suitability of this dataset for baseline behavioral profiling, classification and anomaly detection tasks.

- Securing Substations with Trust, Risk Posture, and Multi-Agent Systems: A Comprehensive Approach - Dr. Kwasi Boakye-Boateng

  The Smart Grid is an IT-integrated power grid that generates, transmits, and distributes electricity to households and businesses. The substation is a crucial element of the Smart Grid's operation, which adjusts voltages during the entire process. The integration of IT has increased in the substation's attack surfaces.

Sophisticated attacks such as the Pipeline APT contain multi-protocol modules for various devices. Performance constraints make substations a unique case; hence it is challenging to implement encryption and intrusion detection systems. We believe trust can tackle this problem. We present an improved trust model that detects protocol-based attacks toward an IED/SCADA HMI. This model is included within a multi-agent-based trust management system that computes the substation's risk posture. Our proposed design was implemented in a Docker-based testbed environment with a SOC-influenced dashboard to provide real-time updates. The implementation was subjected to three attack scenarios: external attack, internal attack from compromised SCADA HMI, and internal attack from a compromised non-trusted IED. We observed that our model was robust against all attacks except for the baseline replay and delay response attacks. Detecting these attacks will be considered for future work as well as trust transferability. Our institute's website provides a publicly available dataset containing captures of our MAS testbed.

---

9. ROGERS CYBERSECURE CATALYST - TORONTO METROPOLITAN UNIVERSITY- CANADA

- UTC 14:00~UTC 16:00 Transforming Cyber Threats into Opportunities with GenAI & Algorithmic security challenges of machine learning models

- Introducing Host – Dr. Randy Purse

- Navigating the Shift: Transforming Cyber Threats into Opportunities with GenAI - Dr. Jeff Schwartzentruber,

  In this talk, Dr. Schwartzentruber explores the impact of Generative AI (GenAI) on cybersecurity, emphasizing its dual role in expanding the threat landscape and providing new defensive tools. It begins with an overview of GenAI's adoption across industries, highlighting the growth of potential threats and the need for advanced security measures. The discussion covers GenAI's applications for both attackers and defenders, presenting three novel GenAI-enabled attacks and practical defense strategies. Additionally, the talk showcases how GenAI is used internally to improve security operations and support for customers, concluding with future predictions for the GenAI market and cybersecurity trends.

- Algorithmic security challenges of machine learning models - Dr. Reza Samavi

  Recent advances in Artificial Intelligence (AI) and Machine Learning (ML) have ushered in transformative changes in technology, from generative models (GM) and large language models (LLM) that mimic human conversation to health diagnostics. Yet, their integration raises significant security issues, highlighted by their susceptibility to adversarial attacks, memorization of private information, uncertainty in decision-making, and ethical concerns. Dr. Samavi's research targets the enhancement of ML trustworthiness, focusing on model robustness against varied inputs and the improvement of uncertainty quantification.

  In this talk, Dr. Samavi will outline our approach to developing robust, reliable, and ethically sound ML models, crucial for safe AI applications in sensitive domains like autonomous driving and healthcare. Our efforts highlight the importance of addressing the new generation of cybersecurity concerns that include algorithmic security challenges of AI systems and go beyond traditional security threats.

- Q&A with discussion – Pragmatic issues integrating AI into cybersecurity

---

10. CYBERSEA - CARLETON UNIVERSITY - CANADA

- UTC 16:00~UTC 18:00 : Securing AI-Based Systems: From Design to Operations to Assurance

- Dr. Jason Jaskolka, Marwa Zeroual, and Xinrui Zhang

---

11. HUMAN-CENTRIC CYBERSECURITY PARTNERSHIP - CANADA

- UTC 18:00~UTC 19:00 : The Gamified Canadian Cybersecurity Education Training and Awareness Panel Championship

- Hosted by Michael Joyce this session will see the cybersecurity awareness space represented by teams of Solutions Providers, Researching Academics and Practitioners who will compete and collaborate to answer important questions for cybersecurity education training and awareness
- The Panel will include Kjadkida Baig (MediaSmarts), Marie-Claude Belanger (CCCS), Kara Brisson-Boivin (MediaSmarts), Kimberly Duthie (Get Cybersafe), Laura Fifield (CCCS), Sandy Gillis (Bell), Anthony Hope (CCCS), Sana Maqsood (York University), Claudiu Popa (KnowledgeFlow), David Shipley (Beaceron), Elizabeth Stobert (Carleton University), Scott Wright (ClickArmor).

---

12. THE CENTRE FOR CYBERCRIME INVESTIGATION AND CYBERSECURITY & THE ESCUELA LATINOAMERICANA DE CIBERCRIMINOLOGÍA

- UTC 20:00~UTC 22:00: Amenazas digitales e impunidad en el ciberespacio *Digital threats and impunity in cyberspace*

- Introducción y Moderación - Andrés Aguilera - Mike Toro | LATAM
- Delitos informáticos en el metaverso - Carla Bertoni
- Guacamayas y sus responsables - Walter Huaman
- Amenazas digitales y planes de ataque en las escuelas - Quésia Pereira Cabral | Brasil
- Ciberdelincuencia en el canal - Damaris Cardoso | Panama
- Big Telco Ransomware Centroamerica - Yuri Coello | Honduras

13. THE CENTRE FOR CYBERCRIME INVESTIGATION AND CYBERSECURITY & THE ESCUELA LATINOAMERICANA DE CIBERCRIMINOLOGÍA

- UTC 22:00~UTC 24:00 Impunidad en el ciberespacio *Impunity in cyberspace and capabilities to counteract it*

  - Introducción y Moderación - Guadalupe Atilano - Mike Toro
  - La impunidad en la investigación del cibercrimen - Tomas Moreno | Mexico
  - Las sombras de Wannacry - Ximena Cuscano | Peru
  - Recorrido historíco de ciberamenazas - Leslie Marin / José Miguel Brenes | Costa Rica
  - Ciberarmas y capacidades de daño - Ana Castañeda Escuela LATAM
  - Retos en el manejo de Evidencia Digital con Café Forense - Hernán Peña | Colombia
  - Ciberespionaje corporativo. Análizar y extraer evidencia desde dispositivos móviles - Oscar Mendoza | Mexico