21st Annual International Conference on Privacy, Security & Trust

---

28 – 30 August 2024
Academic Conference & Industry Summit
Sydney, Australia

17 – 18 October 2024
Industry Summit
Fredericton, New Brunswick, Canada

pstnet.ca   #PST2024

Dr. Ali Ghorbani
Tier 1 Canada Research Chair in Cybersecurity

Professor and Director
Canadian Institute for Cybersecurity

WELCOME

On behalf of the organizing committee of the 21st International Conference on Privacy, Security, and Trust (PST), I extend a warm welcome to all of you. The conference aims to bring together researchers specialized in privacy, security, and trust with new emerging technologies and trends track to present their latest findings, discuss their results, and explore their practical applications. We would have preferred an in-person conference, but due to the circumstances, we have combined a hybrid main conference, including an industry day (August 28–30 at the University of New South Wales (UNSW), Sydney, Australia) and an in-person Cybersecurity Industry Summit (October 18 in Fredericton, New Brunswick, Canada).

The annual PST research conference has established itself as a leading international forum for presenting and discussing the latest challenges and solutions covering a wide range of related topics. The conference offers a balanced program that covers various cybersecurity topics, comprising industry and academic discussions. It uniquely approaches the examination of issues from both research and practical perspectives, encouraging multidisciplinary research and fostering collaboration between the academic, private sector, and government sectors.

The annual Cybersecurity Industry Summit is a gathering of cybersecurity leaders, researchers, and practitioners. The Summit has gained significant recognition in Canada. This year's Summit will feature two panels, and keynote talks from leading Cybersecurity and AI experts and leaders in Canada. The first panel will focus on the impact of Generative AI in Cybersecurity and will feature the CIO/CISO of major carriers and financial institutions. The second panel will include some of the top women in Canadian Cybersecurity, who will discuss ways to empower women in Cybersecurity and build an inclusive and diverse cybersecurity workforce. Additionally, twenty-eight research posters related to real-world cybersecurity issues will be exhibited at the Fredericton Convention Centre during the Industry Summit.

A total of thirty-eight high-quality papers were accepted for presentation on August 28–30. The papers include twenty-nine regular papers and nine short papers covering various topics related to privacy, security, and trust. The researchers presented their results in different areas such as network security, software security, IoT security, authentication and protocol security, malware analysis, security analytics, privacy-preserving computing, user trust, privacy model, protocol and assessment, online social network privacy, cryptography, crypto-mining, and blockchain security.

We express our gratitude to UNSW, TPG Telecom, UNSW School for Engineering, TCS TATA Consultancy Services, the Canadian Institute for Cybersecurity (CIC), the Atlantic Canada Opportunities Agency (ACOA), Opportunities New Brunswick (ONB), MOBIA, Interac, YubiCo, and Ignite Fredericton for sponsoring the conference. We particularly appreciate the continuous support and technical co-sponsorship provided by the IEEE Computer Society.

The success of this conference is the result of the hard work and contributions of many people. The technical program committee members played a crucial role in coordinating the review process for all submitted papers. The referees, whose dedication and efforts were invaluable, assessed the scientific content of the papers to ensure the quality of those accepted. We are grateful to our organizing committee members of the main conference in Sydney and the Industry Summit in Fredericton for their support and assistance.

We are grateful to all the participants who have submitted research papers and posters and will present and give keynote talks at the conference and the Summit. Thank you for being an invaluable part of this event. We hope you will find the conference informative, engaging, and rewarding.

Ali Ghorbani
2024 Industry Summit Chair

Canadian Institute for Cybersecurity

A hub of cybersecurity innovation and talent development in Canada

The Canadian Institute for Cybersecurity provides trailblazing cybersecurity research and innovation – not just for the Maritimes, but for Canada and the world.

The province of New Brunswick, located in Eastern Canada, is strategically focusing on technological innovation in cybersecurity. Since 2000, the University of New Brunswick (UNB) has played an integral role in cybersecurity research and innovation. Today, the University has one of the largest network security research groups in the country and continues to expand its cybersecurity expertise in areas including Operational Technologies, Critical Infrastructure protection, Artificial Intelligence, and Industrial Internet of Things. UNB leads this effort through the Canadian Institute for Cybersecurity. The Institute works with industry and governments to solidify Canada's position as a world-class cybersecurity hub for innovation and talent development.

TABLE OF CONTENTS

CYBERSECURITY IN THE QUANTUM ERA WORKSHOPS

THURSDAY, 17 OCTOBER 2024
CYBER CENTRE, KNOWLEDGE PARK DRIVE

An engaging afternoon of workshops hosted by CIC that focus on cutting-edge developments in cybersecurity, with a special emphasis on Quantum-Resistant Technologies, post-quantum cryptography, post-attack mitigation, and risk management in critical infrastructure. The sessions will cover advancing cryptographic agility in Quantum-Resistant Technologies and exploring the future of post-quantum solutions. Whether you work in cybersecurity, critical infrastructure, or operational technology, these presentations will provide a valuable opportunity to connect with industry leaders, expand your expertise, and discover innovative strategies for securing critical systems.

Time	Session	Speaker
13:00–13:35	**Government views on the quantum threat and transition to post quantum cryptography** Have you ever wondered what the government's role is in cryptography and the nexus with quantum computing and cyber security? In this presentation, you will: • Learn about the Canadian Centre for Cyber Security at the Communications Security Establishment and their role as the technical authority in cryptography for the federal government; • Hear about the work that they are doing to support the post quantum cryptography transition in Canada including evaluation of the NIST quantum-safe cryptography standards and providing advice and guidance on cryptographic algorithms and protocols; and • Receive an overview of cryptographic agility and why it is important to consider as part of the quantum safe transition, timelines for the transition to post quantum cryptography and helpful resources available to support Canadians with this important initiative.	**Melanie Anderson,** *Director General, Information Assurance at the Canadian Centre for Cyber Security*
13:40–14:15	**Adapting cybersecurity workforce to prepare for quantum risk mitigation** Given the looming threat of quantum computing technology rendering current cryptographic algorithms obsolete, enterprises must proactively prepare for a post-quantum era. To understand preparation requirements, we explore potential impacts of quantum computing on professional cybersecurity disciplines within enterprises from a socio-technical perspective. Based on an in-depth case study of a large financial institution, we identify impacts and preparation and migration roles for five major disciplines within the cybersecurity group. We also identify four common challenges across cybersecurity disciplines, along with recommendations for addressing them.	**Dr. Atty Mashatan,** *Canada Research Chair in Quality of Security Framework for Internet-of-Things*
14:15	**Nutrition Break & Research Poster Session**	

14:30–15:15	**Advancing Cryptographic Agility in Emerging Quantum-Resistant Technologies** As quantum computing advances, the security of current cryptographic systems faces significant threats, making the development of quantum-resistant technologies imperative. Advancing Cryptographic Agility in Emerging Quantum-Resistant Technologies addresses this need by focusing on cryptographic agility, which is the capability to swiftly adapt and switch between cryptographic algorithms in response to emerging threats. This discussion will assess the readiness of current cryptographic standards against quantum attacks, explore progress in standardizing quantum-resistant algorithms, and examine hybrid cryptographic implementations that combine classical and post-quantum methods. Additionally, we will discuss practical use cases where these technologies can be applied, providing insights into their impact on various industries and sectors.	**Dr. Vikas Chouhan,** *Postdoctoral Fellow at the Canadian Institute for Cybersecurity*
15:15	**Nutrition Break & Research Poster Session**	
15:30–16:30	**Post-Attack Mitigation and Risk Management in Critical Infrastructure** Critical Infrastructure (CI) plays an essential role in our daily lives. In Operational Technology (OT)-based CI such as energy and manufacturing, while extensive research has focused on preventing and detecting attacks, there is a significant gap in strategies for mitigating damage once an attack has been fully executed. This workshop addresses this gap by proposing a mitigation framework designed to address attacks that have occurred, with the aim of tackling scenarios involving zero-day exploits. Additionally, the workshop will explore the role of Internet of Things (IoT) devices in health-based CI, discussing their profiling, vulnerabilities, and the datasets available for research on related attacks. Finally, we will examine business-process-oriented risk management in mission-critical CI within the context of military operations. This section will focus on integrating risk management strategies that consider the specific military processes affected by cyber-attacks. Through these discussions, the workshop aims to advance understanding and preparedness in mitigating the impacts of cyber threats on critical infrastructure.	**Dr. Kwasi Boakye-Boateng,** *Research Associate at the Canadian Institute for Cybersecurity*

INDUSTRY SUMMIT PROGRAM
FRIDAY, 18 OCTOBER 2024
FREDERICTON CONVENTION CENTRE

OUR EMCEES

Dr. Sajjad Dadkhah
R&D Team Lead and Assistant Professor
Canadian Institute for Cybersecurity

Dr. Windhya Rankothge
Research Associate
Canadian Institute for Cybersecurity

Time	Session	Speaker
07:45	**Registration, Breakfast, & Networking**	
08:30	**Opening Remarks by** • Dr. Ali Ghorbani, Conference General Chair • Dr. Paul Mazerolle, President and Vice-Chancellor, University of New Brunswick	
08:40	**Welcoming Remarks by** • The Honourable Anita Anand, President of the Treasury Board of Canada • The Honourable Frank McKenna, Deputy Chair, Wholesale Banking, TD Bank Group	
09:00	**Shared Services Canada – Delivering Digital Solutions Together for Canada** When Shared Services Canada (SSC) was created in 2011, its goal was to provide modern, reliable and secure technology services to the Government of Canada. Since then, SSC has advanced digital government in a variety of ways, from improving network infrastructure and equipping public servants with modern tools, to providing the sort of efficient hosting and client-centric digital services that proved critical to government services and programs during the pandemic. Thirteen years later, the global IT landscape has changed dramatically, but SSC's goal remains the same: to equip the Government of Canada with the technology it needs to effectively deliver services to Canadians. But technology moves fast, and with it, the cyber threats faced by organizations globally. As an integrated service delivery organization, SSC is working as one, powering digital services for the Government of Canada to make	**Patrice Nadeau,** *Senior Assistant Deputy Minister, Networks and Security Services*
09:25	**Elevating Cyber Security** This session will focus on the need to change how cyber security should be a core business strategy, not just a compliance checkbox. We'll explore the need to incentivise cyber security as a key value that enhances operations and mitigates risks and examine how operational practices and policies influence the digital threat landscape.	**Bridget Walshe,** *Associate Head of the Canadian Centre for Cyber Security*

09:50	**Grounding socioeconomic aspects of AI in their context** In this talk, Ebrahim will address the complex interplay between artificial intelligence (#AI) and socioeconomic dynamics, drawing parallels from historical technological advancements. Through a series of examples, he will point to both the promise and peril of AI, examining how past innovations have shaped societies, economies, and individual lives. From the transformative power of industrialization to the ethical dilemmas of technology, he hopes to explore lessons learned and insights gained, offering a nuanced perspective on navigating the evolving landscape of AI's impact on our world.	**Dr. Ebrahim Bagheri,** *Canada Research Chair in Social Information Retrieval*
10:15	**Nutrition Break & Research Poster Session**	
10:35	**Teaching AI: Why an inclusive and diverse workforce is key in avoiding biases in AI** AI has the power to transform entire facets of our economy and how we approach cybersecurity. To fully harness AI's power, we must eliminate blind spots in this technology, and this requires a diverse workforce and ensuring people from all backgrounds are involved in the design and implementation of AI. In this keynote address, Jennifer Sloan will unpack key themes including technology and prosperity, security as a top concern and inclusive growth.	**Jennifer Sloan,** *Senior Vice President, Mastercard Canada*
11:00	**Panel Discussion: Empowering Women in Cybersecurity: Towards a More Inclusive and Dive** Panelists: • Ireen Birungi, Head of Information Security and CISO at Interac Corp. • Melanie Anderson, Director General, Information Assurance at the Canadian Centre for Cyber Security • Dr. Atty Mashatan, Canada Research Chair in Quality of Security Framework for Internet-of-Things • Sundeep Sandhu, Vice President of Cyber Security and CISO Rogers Bank, Rogers Communications	*Chair* **Elaine Hum,** *Director of Cybersecurity Partnerships with Scotiabank*
12:00	**Lunch & Research Poster Session**	
13:00	**Canadian Institute for Cybersecurity Video Debut**	
13:05	**Preserving Dataset Integrity for Earth Observation and Spaceborne Reconnaissance** Putting satellites in orbit or accessing spaceborne imagery used to be very expensive propositions which only government agencies or industrialized counties could afford. This has changed over the last decade with the appearance of micro-satellites and commercial LEO constellations which have tremendously reduced the cost of data, and opened new opportunities for scientific applications. For example, soil moisture can now be measured from space in near real time allowing for better crop and wildfire management. But data integrity has not been a priority for many commercial operators, there is little consistency when it comes to storage or encryption, and entire databases are at risk. This talk will illustrate these concerns with practical cases and suggest priorities for future work.	**Rick Fawcett,** *Vice President Strategy and Business Development, ADGA Group*

Time	Session	Speaker
13:30	**Panel Discussion: GenAI and Cybersecurity** Panelists: • Steve Sparkes, Exec VP/Chief Information Security Officer at Scotiabank • Mansur Mirani, Vice President and Lead, Vancouver Tech Hub at Mastercard • Ireen Birungi, CISO at Interac Corp. • Carey Frey, Chief Security Officer at Telus	*Chair* **Greg Murray,** *SVP Cyber Security, Networks & Technology Risk Loblaw Companies Limited*
14:30	**Nutrition Break & Research Poster Session**	
14:50	**Security Challenges Arising from AI Advancements** With the rapid advances in AI, there is a real risk of these technologies being used for cyber-attacks. In particular, we'll examine the misuse of AI technology as a means of impersonating individuals. It's clear how this irresponsible use could enhance a social engineering attack and make it more believable. We encourage participants to consider how they use AI technology and how a hacker could exploit that.	**Vio Onut,** *Head, IBM Center for Advanced Studies and Co-Director uOttawa-IBM Cyber Range*
15:15	**Defending Democracy: Combatting Information Disorder** Information disorders can be broadly categorized into three types: misinformation, disinformation, and malinformation. Each represents different challenges and impacts, especially now that information can travel and spread rapidly. They are among the most significant challenges today, impacting cybersecurity, public trust, democratic processes, and societal cohesion. In this presentation, we will discuss these challenges and their impact. We will also demonstrate our AI-powered deep defender system that can help protect the integrity of information and maintain public trust.	**Dr. Sajjad Dadkhah,** *R&D Team Lead, Canadian Institute for Cybersecurity*
15:40	**AI in Defence** Artificial Intelligence plays a vital role within the Armed Forces in collecting and operationalizing data on the battlefield. This presentation offers an overview of its uses and challenges within this domain.	**Dennis Garcia,** *Cyber Solution Engineer GDMS–Canada*
16:05	**Data Privacy and Security Research at the National Research Council** The National Research Council's Digital Technologies Research Centre (DTRC) is a global leader in research and development in artificial intelligence (#AI), helping to drive the adoption of digital technologies across academia, government and private sector. At the intersection of AI with other technologies, DTRC has developed profound expertise in #cybersecurity, #cryptography, and privacy-enhancing technologies. While DTRC operates from many locations across Canada, a significant degree of work is conducted in Fredericton, in close collaboration with the Canadian Institute for Cybersecurity. In this talk, we will present an overview of our research, citing specific examples of success stories, and also discussing how academia, industry and other government departments can collaborate with us.	**Dr. Scott Buffett,** *Research Officer at the National Research Council Canada*
16:30	**CIC Report & Deep Defender**	**Dr. Ali Ghorbani**
16:30–18:00	**Closing Remarks, Reception, & Networking**	

SPEAKERS & PANELISTS

Hon. Anita Anand
President, Treasury Board of Canada

The Honourable Anita Anand is the President of the Treasury Board of Canada Secretariat. Minister Anand was first elected as the Member of Parliament for Oakville in 2019. From 2019 to 2021, she served as Canada's Minister of Public Services and Procurement. From 2021 to 2023, Anand served as Canada's Minister of National Defence, spearheading initiatives to tackle sexual misconduct and bring about cultural change in the Canadian Armed Forces. During this time, she led Canada's efforts to provide comprehensive military aid and personnel to train Ukrainian soldiers following Russia's illegal invasion. Anand has worked as a scholar, lawyer, researcher, and legal academic, including as a Professor of Law at the University of Toronto.

Melanie Anderson
Director General, Information Assurance , Canadian Centre for Cyber Security

Melanie Anderson is the Director General, Information Assurance at the Canadian Centre for Cyber Security. She is responsible for applied cryptographic research, architecture, engineering and development of secure cryptographic solutions, and advice and guidance on the transition to quantum safe cryptography. Anderson is passionate about mentoring and supporting women to pursue STEM careers. She has worked as a software developer, technical trainer, IT Project Manager, technical liaison and led teams in Cyber Defence. She holds a BCS from the University of New Brunswick and completed the Senior Executive Fellows Program through the Harvard Kennedy School. In 2023, Melanie was named one of Canada's Top 20 Women in Cyber Security by IT World Canada.

Dr. Ebrahim Bagheri
Canada Research Chair in Social Information Retrieval

Ebrahim Bagheri is an interdisciplinary researcher with focus on Efficient and Responsible Information Retrieval methods who has impacted industry, government and civil society through community engagement and knowledge translation. He currently holds a Canada Research Chair in Social Information Retrieval and an NSERC Industrial Research Chair on Social Media Analytics. His NSERC CREATE on Responsible AI initiative is unique in that it highlights the need to balance economic development with social good. More recently, he is the Scientific Co-Director of the Bridging Divides program, a CFREF funded program that examines the intersection of advanced digital technologies and the future of immigration and migrant integration.

Ireen Birungi
Head of Information Security & CISO, Interac Corp.

Ireen Birungi has over 20 years of experience in cybersecurity in a variety of industries across the public, private, and consulting sectors with a focus on risk management, compliance, identity and access management and incident response. Birungi is currently the Head of Information Security and CISO at Interac Corp., where she leads the charge in safeguarding digital assets and information systems from cyber threats. Birungi has a passion for mentorship as well as building and leading resilient and high performing teams that together are focused on maturing the security posture for organizations. Birungi is a Women in Payments nominee, an active member of various cyber-member lead communities and forums and an advisory board member.

Dr. Kwasi Boakye-Boateng
Research Associate, Canadian Institute for Cybersecurity

Kwasi Boakye-Boateng received his BSc. and MPhil degrees in Computer Engineering from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana. Boakye-Boateng received his Ph.D. degree in Computer Science from the University of New Brunswick, specializing in smart grid security. During his time as a PHD student and Postdoctoral Fellow, he participated in various industrial-related cybersecurity projects with renowned industry giants such as Siemens, General Dynamics Missions Systems-Canada, and IBM. His roles included Research Team Lead and Research Assistant. Boakye-Boateng's research interests include trust in smart grid, threat intelligence sharing, security of military-based mission-critical systems and smart grid security.

Dr. Scott Buffett
Research Officer, National Research Council Canada

Scott Buffett is a Senior Research Officer in the Digital Technologies research centre at the National Research Council, leading the centre's Cybersecurity research team. Buffett holds a PhD in computer science from the University of New Brunswick, where he continues to serve as an Adjunct Professor. His research interests lie in artificial intelligence and machine learning, specifically in the area of pattern analysis for behavioural analytics.

Dr. Vikas Chouhan
Postdoctoral Fellow, Canadian Institute for Cybersecurity

Vikas Chouhan presently serves as a Postdoctoral Fellow and Team Lead at the Canadian Institute for Cybersecurity. His academic journey includes the attainment of M.Tech and Ph.D. degrees in Computer Science and Engineering from the Indian Institute of Technology in India. Chouhan actively participates in the academic community as a program committee member for international conferences and as a reviewer for conferences and journals. His research interests encompass areas such as Cloud Computing, Cloud Security & Privacy, Information Security & Reliability, Blockchain Technology, and Post-Quantum Security. Chouhan is committed to applying state-of-the-art cryptographic techniques in practical, real-world scenarios.

Dr. Sajjad Dadkhah
R&D Team Lead and Assistant Professor, Canadian Institute for Cybersecurity

Sajjad Dadkhah is an R&D Team Lead and Assistant Professor at the Canadian Institute of Cybersecurity. He has over ten years of experience in cybersecurity, IoT security, digital multimedia security, AI-based detection systems, Intrusion detection systems, and natural language processing. Dadkhah has established himself as a leading authority in the field of cybersecurity and security in IoT by involving in several security projects as a team leader and researcher, and security consultant in different organizations such as CIC-NRC, Kyushu University (Japan), Universiti Malaya (UM), IRIS Smart Technology Complex, and Kyushu Institute of Technology (Japan).

Rick Fawcett
Vice President Strategy and Business Development, ADGA Group, Inc.

Rick Fawcett served for thirty-four years as a Signal Officer in the Canadian Armed Forces, serving in Canada and Europe as well as participating in six expeditionary operations. Since joining Canada's defence industry, Fawcett has focused on the design and integration of Command and Control and Communications systems, including the cyber protection of these systems. He now serves as Strategic Advisor at ADGA. Fawcett was awarded the NATO Meritorious Service Medal and was inducted into the Order of Military Merit. In his spare time, he enjoys spending time at his cottage and playing hockey and golf.

Carey Frey
Chief Security Officer, TELUS

Carey Frey is a Canadian technology executive working to advance the cybersecurity industry, driven by a passion for creating a more secure digital world for everyone. As Chief Security Officer for TELUS, he is responsible for delivering corporate programs securing the company's global assets and delivering managed cybersecurity services to TELUS customers. Prior to TELUS, Frey served in the Government of Canada at the Communications Security Establishment in a variety of technology, intelligence and cybersecurity leadership roles bringing security innovation to federal departments and building collaborative relationships with global information and communications technology companies.

Dennis Garcia
Cyber Solution Engineer, General Dynamics Mission Systems–Canada

With over twenty years at General Dynamics Mission Systems Canada, Dennis Garcia is an experienced system engineer with extensive expertise in military communications. His work has included collaborations with the United Kingdom and Canadian military, focusing on ad hoc networking for tactical environments. Recently, Garcia's focus has shifted towards the integration of cloud-based platforms and the enhancement of cybersecurity and cyber defense capabilities for military enterprise systems.

Dr. Ali Ghorbani
Director, Canadian Institute for Cybersecurity

Ali Ghorbani has dedicated 42 years to academia, currently serving as a Professor of Computer Science, a Tier 1 Canada Research Chair in Cybersecurity, and Director of the Canadian Institute for Cybersecurity. During this time, he also published a book, co-invented four awarded patents and co-founded the National Cybersecurity Consortium. Ghorbani's research spans machine learning, cybersecurity, and Critical Infrastructure Protection, with over three hundred peer-reviewed articles. A co-founder of several startups, he has received multiple accolades, including the Startup Canada Senior Entrepreneur Award and recognition as one of the RBC Top 25 Canadian Immigrants. Ghorbani was honored with the 2024 Lifetime Achievement Award from CAIAC last summer.

Elaine Hum
Director, Cybersecurity Partnerships, Scotiabank

Elaine Hum has been a leader and an active voice in the cybersecurity field for over two decades. She has worked with government, not-for-profit, academic, and industry leaders to advise, govern, and strategically steer cybersecurity policy. In her current position as Director, Cybersecurity Partnerships, Scotiabank, she was instrumental in creating the Cybersecurity Partnership Program – a unique strategy centred on developing a cybersecurity talent pipeline to attract diverse talent from a variety of equity deserving groups. In 2023, Hum was recognized by IT World Canada's list of Top Women in Cybersecurity, which celebrates the achievements of twenty women who are surpassing expectations in the field of cybersecurity.

Dr. Atty Mashatan
Canada Research Chair in Quality of Security Framework for Internet-of-Things

Atty Mashatan holds a Canada Research Chair in cybersecurity and is an Associate Professor of Information Technology Management and the founder and director of the Cybersecurity Research Lab at Toronto Metropolitan University. Her research is focused on the development of novel cybersecurity designs based on emerging technologies such as IoT, Blockchain, and Quantum Computing. She investigates challenges and opportunities brought forward by these new technologies and how they change the threat landscape of cybersecurity. Mashatan studies industry relevant research problems and proposes solutions that can be developed as part of the industry-academic collaborations.

Dr. Paul Mazerolle
President and Vice-Chancellor, University of New Brunswick

Paul Mazerolle is the University of New Brunswick's 19th president and vice-chancellor. An internationally recognized criminologist with degrees from the University of New Brunswick (UNB), Northeastern University and the University of Maryland. Paul is a member of the New Brunswick Business Council, the New Brunswick Ministerial Economic Advisory Board, Universities Canada Board of Directors and the Association of Atlantic Universities. Among the many initiatives Mazerolle is currently driving at UNB, is an aspirational vision for the future – UNB Toward 2030 – which is focused on the growth and impact of the university locally, nationally, and globally.

Hon. Frank McKenna
Deputy Chair, Wholesale Banking, TD Bank Group

Frank McKenna has been an executive with TD Bank Group since 2006 and joined TD Securities in 2020. As Deputy Chair, he is focused on supporting the continued expansion of TD Securities' global footprint. McKenna was elected Premier of New Brunswick in 1987 and since leaving public life, he has been in demand as a Corporate Director and acted as Counsel to two national law firms. Prime Minister Jean Chrétien named him to the Security Intelligence Review Committee, and in 2005, he accepted an invitation to become Canadian Ambassador to the United States of America. Afterwards, McKenna resumed his corporate career and in 2021, he established The McKenna Institute at UNB.

Mansur Mirani
Vice President and Lead, Vancouver Tech Hub, Mastercard Canada

riven by a passion for technology, design, human interaction, and security, Mansur Mirani is a technology professional with over twenty-five years of experience across a diverse range of roles. Holding a Bachelor of Technology in Human-Computer Interaction, Mirani has excelled in roles such as business owner, web designer & developer, UX manager, and director of architecture and analytics. Currently, as Vice President and Lead for Mastercard's Global Intelligence and Cyber Centre of Excellence in Vancouver, he supports teams driving technology and intelligence initiatives, focusing on cybersecurity, decisioning, and AI-driven solutions. His career is marked by a commitment to innovation and team leadership in advancing cutting-edge technology with a user-focused approach.

Greg Murray
SVP Cyber Security, Networks & Technology Risk, Loblaw Companies Limited

With over twenty-five years of international executive experience, Greg Murray is a recognized expert in business-focused technology and cybersecurity. He has a proven record of establishing public-private partnerships and delivering transformational technological solutions through high-performing, people-centric teams. Murray is committed to community engagement, serving as the Technology & Cyber Security Director-in-Residence for Rotman's National ICD Directors Education Program. He has instructed over 3,300 board members, co-found the Toronto Metropolitan University's Rogers Cybersecure Catalyst, and developed inclusive cybersecurity programs that have trained over 800 students. He serves as a Board Director for the National Cyber Consortium, advancing cybersecurity innovation and talent development in Canada.

Patrice Nadeau
Senior Assistant Deputy Minister, Networks & Security Services

Patrice Nadeau is the Senior Assistant Deputy Minister of Networks and Security Services, Shared Services Canada (SSC) / Government of Canada. Before this, Nadeau was the Director General responsible for Data Networks in the Networks and End Users Branch. He joined SSC from Public Works and Government Services Canada (PWGSC) as a Delivery Executive for the Telecommunications and the Information Technology Security lines of business. Nadeau began his career in the private sector with Matrox in Dorval, and subsequently joined the federal Public Service in 1996 with PWGSC as an Account Manager for the Government Telecommunications and Informatics Services.

Dr. Iosif Viorel (Vio) Onut
Head, IBM Center for Advanced Studies and Co-Director uOttawa-IBM Cyber Range

Iosif Viorel (Vio) Onut is passionate about curriculum and product innovation acceleration through R&D. In the past decade, he has managed more than 150 research projects involving thirty-five universities, led by over ninety professors, over 360 students and over 330 IBM staff. On a technical level, he specializes in cybersecurity and cybercrime. He has been in this space for 20+ years in various technical, academic and management roles. He is co-Director of the University of Ottawa and IBM Cyber Range; Adjunct Professor at the University of Ottawa; Head of Centre for Advanced Studies, IBM Canada Lab and IBM Master Inventor at IBM Security.

Sundeep Sandhu
VP Cyber Security and CISO, Rogers Bank at Rogers Communications

Sundeep Sandhu, the Vice President of Cyber Security and CISO at Rogers Bank for Rogers Communications, spearheads transformative cybersecurity initiatives while safeguarding Canadian interests. Her accolades include receiving the 2023 Women in Communications & Technology Woman of the Year Award for her notable contributions to cybersecurity and the community. Renowned for assembling high-impact teams and promoting diversity in cyber leadership, Sandhu actively fosters cross-sector collaboration, championing strategic partnerships that drive innovation and shared success. Her dedication to STEM initiatives has left an indelible mark on the cybersecurity landscape, earning her a reputation as a trailblazer.

Jennifer Sloan
Senior Vice President, Public Policy & Stakeholder Engagement, Mastercard Canada

A former public servant and political-staffer-turned-diplomat, Jennifer Sloan made her foray into the private sector and currently leads public policy and stakeholder engagement for Mastercard Canada. Earlier in her career, she was the Director of Communications for one of the longest serving Industry Ministers in Canada and continued in this role as he moved to Foreign Affairs, then Deputy Prime Minister and Minister of Finance. She continued this work when she was appointed to the Consulate General of Canada in New York City. Sloan developed The Mastercard Changeworks™ program, a grassroots initiative that partners with the not-for-profit sector in Canada to improve their technology and data capabilities.

Steve Sparkes
EVP, CISO and Head of Enterprise Platforms, Scotiabank

Steve Sparkes was appointed Executive Vice President, Chief Information Security Officer and Enterprise Platforms in 2023. In this role, he is responsible for the development of enterprise infrastructure, IT and cyber risk strategies, systems, and procedures, as well as applications in support of HR, Operations and Compliance, and fraud technologies. Sparkes joined Scotiabank in 2021 as Chief Information Security Officer and SVP, Information Security and Control. He has over thirty years of experience in leadership roles in technology infrastructure, application development, IT and operational risk, and cybersecurity. Prior to Scotiabank, Sparkes was the Managing Director and Head of Cybersecurity Technology at Bank of America and Managing Director at Morgan Stanley.

Bridget Walshe
Associate Head, Canadian Centre for Cyber Security

Bridget Walshe is the Associate Head of the Canadian Centre for Cyber Security. Prior to this role, Walshe served the Director General of Operations, Security and Intelligence at the Privy Council Office for two years, where she was responsible for providing advice on key operational and policy issues in the Canadian Security and Intelligence community. Walshe began her career at CSE in 2003 and has held various positions including Director General for the Secure Solutions and Services Directorate where she was responsible for applied research, architecture, engineering and development of secure cryptographic solutions.

ORGANIZING
COMMITTEES

PC Chairs

Shabnam Kasra Kermanshahi, University of New South Wales, Australia

Veronika Kuchta, Florida Atlantic University, USA

Industry Chairs

Sanjay Jha, University of New South Wales, Australia

Lee Barney, GM Tech Security, TPG Telecom

Local Chairs

Nadeem Ahmed, University of New South Wales, Australia

Abuadbba, Sharif, CSIRO's Data61, Australia

Privacy Track

Xingliang Yuan, University of Melbourne, Australia

Jianbing Ni, Queen's University, Canada

Security Track

Qianhong Wu, Beihang University, China

Tanmoy Chakraborty, IIT Delhi, India

Xiaojie Zhu, KAUST (King Abdullah University of Science and Technology), Saudi Arabia

Trust Track

Arash Shaghaghi, University of New South Wales, Australia

Carol Fung, Concordia University, Canada

Emerging Technologies and Trends Track

Rongxing Lu, University of New Brunswick, Canada

Xiaohui Liang, University of Massachusetts Boston, USA

Publicity Chairs

Xichen Zhang, Saint Mary's University, Canada

Sajjad Dadkhah, Canadian Institute for Cybersecurity, Canada

Min Wang, University of Canberra, Australia

Finance Chair

Golnoush Abaei, RMIT University, Australia

Steering Committee

Ali Ghorbani (Chair), University of New Brunswick, Canada

Josep Domingo-Ferrer, Universitat Rovira i Virgili, Catalonia, Spain

Stephen Marsh, University of Ontario Institute of Technology, Canada

Hossein Sarrafzadeh, North Carolina Agricultural and Technical State University

Ali Miri, Ryerson University, Canada

Weizhi Meng, Denmark Technical University, Denmark

Sydney Industry Summit Organizing Committee, University of New South Wales

Sanjay Jha, General Chair

Lee Barney, General Chair

Jeremy Ginger, Program Co-Chair

Praveen Gauravaram, General Chair

Jawad Ahmed, General Chair

Rahat Masood, Publicity Chair

Nancy Cordina, Event Management and Marketing

Susan Manjikian, Event Management and Marketing

Hunter Xu, Website Manager

Plus 26 members of the Program Committee

Fredericton Industry Summit Organizing Committee, Canadian Institute for Cybersecurity

Ali Ghorbani, Chair, University of New Brunswick

Windhya Hansinie Rankothge, Local Organizing Chair

Pamela Kitchen, Industry Liaison

Sumit Kundu, Communications and Sponsorship Coordinator

Mohamed Badawy, Technical Coordinator

Sajjad Dadkhah, Poster Presentation Coordinator

Rashmi N. Muralinath, Web Chair

Ruth M. Murgatroyd, Publicity and Logistics

Plus, numerous others.

SYDNEY INDUSTRY DAY PROGRAM
MONDAY, 28 AUGUST 2024
UNSW SYDNEY, AUSTRALIA

Time	Session
08:00	**Registration**
08:45	**PST Conference & Industry Day Opening Remarks** **Prof. Sanjay Jha,** Director of Research and Innovation at School of Computer Science and Engineering UNSW Australia, **Dr. Shabnam Kasra,** Program Committee Chair, **Prof. Attila Brungs,** Vice-Chancellor and President at UNSW Australia, **Prof. Stephen Rodda,** Pro Vice-Chancellor Industry and Innovation at UNSW Australia, **Lee Barney,** General Manager Technology Security at TPG Telecom
09:15	Keynote I: **Lieutenant General Michelle McGuinness,** National Cyber Security Coordinator at Department of Home Affairs Australia.
09:45	Keynote 2: **Giovanni Chiarelli,** Group Chief Technology Officer at TPG Telecom.
10:00	**Morning Coffee Break**
10:30	**Panel 1: Post-Quantum Cryptography (PQC) Adoption for Communications** • Moderator: **Lee Barney,** General Manager Technology Security at TPG Telecom, • Panellists: **Dr. Surya Nepal,** Senior Principal Research Scientist at CSIRO Data61 Australia, **Kiranmai Akidi,** Business Relationship Manager at Tata Consultancy Services Australia, **Rizwan Mahmood,** Chief Technology Officer & Founder at GuardWare Australia, **Vikas Dahiya,** Cybersecurity Global Sales Leader- Cloud and Network Services at Nokia
11:15	**Panel 2: Weaponization of AI and the Digital Arms Race** • Moderator: **Prof. Sanjay Jha,** Director of Research and Innovation at School of Computer Science and Engineering UNSW Australia, • Panellists: **Richard Searle,** Chief AI Officer at Fortanix United Kingdom, **Stuart Peck,** Head of Attack & Respond at TPG Telecom, **Prof. Toby Walsh,** ARC Laureate Fellow and Scientia Professor of AI at UNSW and CSIRO Data61 Australia, **Prof. Ganna Pogrebna,** Executive Director – Artificial Intelligence and Cyber Futures Institute at Charles Sturt University Australia

12:00	**Initiative Presentations (10 Mins Per initiative, Hybrid)** • Gowri Ramachandran - Towards a Portability Scheme for Decentralized Identifiers in Self-Sovereign Identities • Arash Shaghaghi - Lack of Systematic Approach to Security of IoT Context Sharing Platforms • Emma Romanous - AI Efficiency in Cybersecurity: Estimating Token Consumption for Optimal Operations • Mohammad Reza Nosouhi - The Value of Strong Identity and Access Management for ICS/OT Security • Jason Ford - Insource vs Outsourcing Offensive Security Operations
13:00	**Networking Lunch**
14:00	**Initiative Presentations (10 Mins Per initiative, Hybrid)** • Rishabh Kumar - Privacy Preservation in Service Operations by Minimizing Sensitive Data Exposure • Bruno Santos - Cybersecurity in Industry 5.0: Open Challenges and Future Directions
14:30	**Panel 3: Security of Critical Infrastructure (SOCI)** • Moderator: **Dr. Amit Chaubey,** National Cyber Security Advisor at Australia India Business Council (AIBC), • Panellists: **Prof. Helge Janicke,** Deputy CEO and Research Director at Cyber Security Cooperative Research Centre (CSCRC) Australia, **Dr. Susanne Lloyd-Jones,** CSCRC Post Doctoral Fellow at UNSW Faculty of Law and Justice Australia, **Nick Ellsmore,** Partner – Cyber at Mantel Group Australia, **Amanda Sutton,** Acting Director Communication and Coordination, CISG at Department of Home Affairs Australia, **William Coote,** Managing Associate at Allens
15:15	**Afternoon Coffee Break**
15:45	**Panel 4: Lessons from General Data Protection Regulation (GDPR) and Avoiding Mistakes in Data Privacy Regulation** • Moderator: **Kate Carruthers,** Chief Data & Insights Officer at UNSW Australia, • Panellists: **Dr. Tatiana Bokareva,** Principal Data Scientist at Teradata Australia, **Michael Loewy,** Co-Founder / CEO at Tide Foundation, **Kate Monckton,** Cyber Partner at Deloitte, **Vineet Kumar,** Founder and Global President at CyberPeace)
16:30	**Closing Remarks**
16:45	**Networking Drinks/ Demo (Sponsored by School of Computer Science and Engineering (CSE) - UNSW Sydney)** Opening Remarks - **Prof. Julien Epps,** Dean at UNSW Australia and **Prof. Arcot Sowmya,** Head of School at School of Computer Science and Engineering UNSW Australia

SYDNEY INDUSTRY DAY SPEAKERS

Lieutenant General Michelle McGuinness
National Cyber Security Coordinator, Department of Home Affairs Australia

Lieutenant General Michelle McGuinness, CSC was appointed as Australia's National Cyber Security Coordinator (the Coordinator) on 26 February 2024. As the Coordinator, LTGEN McGuinness leads national cyber security policy, the coordination of responses to major cyber incidents, whole of government cyber incident preparedness efforts, and the strengthening of Commonwealth cyber security capability. LTGEN McGuinness has served in the Australian Defence Force for 30 years in a range of tactical, operational, and strategic roles in Australia and internationally.

Giovanni Chiarelli
Group Chief Technology Officer, TPG Telecom

Giovanni joined TPG Telecom as Chief Technology Officer in January 2022. He has responsibility for mobile and fixed networks, information technology and digital. His previous experience includes Chief Technology & Information Officer at MTN South Africa, Chief Technology Officer at Vodafone Romania and Chief Information Officer at Telecom Italia. Giovanni holds a Master of Engineering and Master of Business Administration.

Prof. Attila Brungs
Vice-Chancellor and President, UNSW Australia

Professor Brungs commenced his appointment on 31 January 2022, joining UNSW from his position as Vice-Chancellor and President of University of Technology Sydney (UTS) (2014 – 2021). He was Deputy Vice-Chancellor and Vice-President (Research), UTS (2009 – 2014). In November 2021, Professor Brungs was appointed Emeritus Professor and Emeritus Vice-Chancellor, UTS. He is a distinguished academic and higher education leader with extensive experience in the government and corporate sectors.

Prof. Stephen Rodda
Pro Vice-Chancellor Industry and Innovation, UNSW Australia

Professor Stephen is responsible for providing strategic leadership across all facets of UNSW's industry engagement, knowledge transfer, business development and commercialisation, and oversight of the Entrepreneurial Campus. Stephen's professional career has focused on technology commercialisation, corporate governance, executive leadership and investment portfolio management. He's played an active role in supporting hundreds of technology licensing deals, the formation and financing of dozens of companies and securing well in excess of $500 million in investments, grants and other funding.

Prof. Julien Epps
Dean, UNSW Australia

Prof. Julien Epps holds a BE (Hons I) and PhD in Electrical Engineering from UNSW. He worked at Motorola Labs, National ICT Australia, and UNSW, becoming Professor and Head of School in 2019. In 2023, he was appointed Dean of UNSW Faculty of Engineering. He is also Co-Director of NSW Smart Sensing Network and held roles at Data61, CSIRO, and Sonde Health. He has delivered invited tutorials and keynotes at international conferences and serves as Associate Editor for IEEE Transactions on Affective Computing. He has held various leadership roles in academic conferences and associations.

Prof. Arcot Sowmya
Head of School – CSE, UNSW Australia

Prof. Arcot Sowmya holds a PhD in Computer Science from IIT Bombay and is a Professor and Head of School at School of Computer Science and Engineering, UNSW. Her research focuses on machine learning for computer vision, including object models, feature extraction, and recognition. She applies this expertise to medical image analysis, diagnostics, and remote sensing. Recently, she has expanded into biomedical informatics and rapid diagnostics. Her work is supported by competitive funding. Additionally, she has applied machine learning techniques to social sciences, developing a forecasting model for genocide and politicide that informs policy makers. Her research has far-reaching impacts across various domains.

Prof. Sanjay Jha
Director of Research and Innovation, UNSW Australia

Sanjay K. Jha is a Professor and Director of Research and Innovation at the School of Computer Science and Engineering, UNSW Australia, and leads UNSW in the Cybersecurity Cooperative Research Centre. His research focuses on using cutting-edge AI techniques to combat cyber threats. His areas of interest include Combining AI and network security for improved defenses, Generative AI for voice cloning, Applying AI to identify phishing scams and malware and leveraging wireless signals for activity detection. Prof Jha has s successful track record in building and mentoring high-performing teams of researchers who can work closely and integrate with industry partners.

Lee Barney
General Manager Technology Security, TPG Telecom

Lee Barney is the General Manager Technology Security at TPG Telecom, bringing nearly two decades of cyber security expertise to the forefront of telecommunications security. With a distinguished career that spans across military service, consulting with the Big Four, entrepreneurship, and pivotal roles within the government and retail sectors, Lee has demonstrated a relentless dedication to advancing cyber security practices and leading teams to excellence. His ability to translate complex security concepts into engaging and impactful practices has made him a sought-after speaker and thought leader in the industry.

Dr. Surya Nepal
Senior Principal Research Scientist , CSIRO Data61 Australia

Dr Surya has been with CSIRO since 2000 and currently leads the cybersecurity and quantum systems research group comprising 70 staff and 50 PhD students. His primary area of research focuses on the development and implementation of technologies in distributed systems, with a specific emphasis on security, privacy, and trust. He currently serves as the Interim Editor-in-Chief of IEEE Transactions on Service Computing and is a member of the editorial board of ACM Transactions on Internet Technology. Additionally, Dr. Nepal holds the position of Deputy Research Director at the Cybersecurity Cooperative Research Centre and is also a Conjoint Professor at UNSW.

Kiranmai Akidi
Business Relationship Manager, Tata Consultancy Services Australia

Kiranmai joined Tata Consultancy Services in 2005. She led multiple domains Telecom, Retail, Transport and Public Services in ANZ geography. Heading Cybersecurity, Marketing, Digital Transformation and Sustainability portfolios for Telecom customers. Past experience includes management of IT Service Delivery, Cyber Security, Quality Assurance, Service Operations and Largescale Cloud Transformation initiatives. Kiranmai has served in TCS for 20 years managing tactical and strategic initiatives across Australia and India.

Rizwan Mahmood
Chief Technology Officer & Founder, GuardWare Australia

Rizwan is the Founder and CTO of GuardWare, a company dedicated to eliminating data theft using unique encryption techniques and post-quantum cryptography. With 21 years of experience managing R&D units, Rizwan has designed, developed, and commercialized off-the-shelf software in security, encryption, and compliance. He holds a Master's degree in Information Technology Management from Staffordshire University, UK, and is a certified Information Systems Security Professional and Project Management Professional. In his previous roles at cybersecurity firms, Rizwan has held various strategic and leadership positions, playing a key role in business growth. His efforts have contributed to protecting over a million users worldwide.

Vikas Dahiya
Cybersecurity Global Sales Leader- Cloud and Network Services, Nokia

Vikas Dahiya drives strategy and revenues for security business line across CSPs and enterprises globally. He has held various leadership roles with many global players like HP, Capgemini, Microsoft, Oracle and Mastercard. He is an accomplished business leader with extensive experience in successfully managing large teams to deliver solutions in cyber risk management, digital identity and authentication, AI/ML financial crime and transaction fraud models, network services, Billing and OSS. He holds an Electronics and Telecommunications Engineering degree from NIT, a Management degree from IMT Ghaziabad and has completed Cybersecurity Graduate Certificate Program from Harvard.

Richard Searle
Chief AI Officer, Fortanix United Kingdom

As the Chief AI Officer at Fortanix, a pioneer of Confidential Computing technology for data and AI security, Dr Richard Searle leads the development and deployment of artificial intelligence (AI) systems that are secured within Trusted Execution Environments (TEEs). Richard is conducting innovative research on quantum information security, AI security, and the use of artificial intelligence (AI) systems within the context of national security. He holds a Doctor of Business Administration degree from Henley Business School at the University of Reading and is the Principal Investigator for Fortanix within the NIST AI Safety Institute Consortium (AISIC).

Stuart Peck
Head of Attack & Respond, TPG Telecom

Stuart Peck is the Head of Attack and Respond at TPG Telecom, bringing a wealth of experience from his previous roles as the Global Head of Threat Intelligence and Hunt at Vodafone Group and the Director of Cyber Security Strategy at ZeroDayLab. A recognised expert in the field including tracking state-sponsored attackers and cyber-criminal groups and responding to high-profile incidents. With a distinguished career marked by significant achievements, Stuart is a four-time black badge winner for TraceLabs Missing Person event and has the unique accolade of being the first person to train US District Attorneys on Open-Source Intelligence investigation techniques and ethics.

Prof. Toby Walsh
ARC Laureate Fellow and Scientia Professor of AI, UNSW and CSIRO Data61 Australia

Prof. Toby Walsh is an ARC Laureate Fellow and Scientia Professor of AI at UNSW and CSIRO Data61. He is Chief Scientist of UNSW.AI, UNSW's new AI Institute. He is a strong advocate for limits to ensure AI is used to improve our lives, having spoken at the UN, and to heads of state, parliamentary bodies, company boards and many others on this topic. This advocacy has led to him being 'banned indefinitely' from Russia. He is a Fellow of the Australia Academy of Science and was named on the international 'Who's Who in AI' list of influencers. He has written four books on AI for a general audience, the most recent is 'Faking It! Artificial Intelligence in A Human World'.

Prof. Ganna Pogrebna
Executive Director – Artificial Intelligence and Cyber Futures Institute, Charles Sturt University Australia

Prof. Ganna is a pioneer in behavioural data science. She serves as the Executive Director of the AI and Cyber Futures Institute at Charles Sturt University, Honorary Professor at the University of Sydney, and Lead for Behavioural Data Science at the Alan Turing Institute. Her expertise blends behavioural science, AI, computer science, data analytics, and business innovation. Ganna's work aids diverse groups, including businesses, governments, and individuals, in understanding decision-making processes and optimizing behaviour for enhanced outcomes. Her recent projects span smart technologies, cybersecurity, human-computer interactions, and innovative business models.

Dr. Amit Chaubey
National Cyber Security Advisor, Australia India Business Council (AIBC)

A seasoned Technology and cybersecurity risk professional spanning a career of over 22+ years across the Asia Pacific, with extensive experience in managing IT & cyber risk in the Financial Industry, Technology services and Critical Infrastructure. A member of multiple Executive Advisory Boards, Chair of the AISA (Australian Information Security Association) New South Wales, Australia, National Cybersecurity Advisor for Australia India Business Council, and Cyber Ambassador for Investment NSW. Amit has been awarded an Honorary PhD in Information Technology Specialisation Cybersecurity from a French University.

Prof. Helge Janicke
Deputy CEO and Research Director, Cyber Security Cooperative Research Centre (CSCRC) Australia

Prof. Helge is affiliated with Edith Cowan University and holds a visiting Professorship in Cyber Security at De Montfort University, UK. His current research investigates the application of Agile Techniques to Cyber Incident Response in Critical Infrastructure, Managing Human Errors that Lead to Cyber Incidents, and Cyber warfare and Cyber peacekeeping. Prof. Janicke established DMU's Cyber Technology Institute and its Airbus Centre of Excellence in SCADA Cyber Security and Forensics Research. He founded the International Symposium on Industrial Control System Cyber Security Research and has contributed over 150 peer-reviewed papers from his collaborative research with industry partners such as Airbus, BT, Deloitte, Rolls-Royce, and QinetiQ.

Dr. Susanne Lloyd-Jones
CSCRC Post Doctoral Fellow, UNSW Faculty of Law and Justice Australia

Dr. Susanne Lloyd-Jones is a Cyber Security CRC Post Doctoral Fellow based in the UNSW Faculty of Law and Justice. Her professional background spans academia, government, industry, and private practice. Susanne's research focuses on cyber security law and policy, emerging technology, critical infrastructure regulation, law and technological change, and national security regulation in complex industry sectors, such as telecommunications, broadcasting, news media, digital platforms, and cloud services. She has presented her research at domestic and international conferences, including recently at the 11th Annual Governance of Emerging Technology and Science Conference held at Arizona State University.

Nick Ellsmore
Partner – Cyber, Mantel Group Australia

Nick Ellsmore leads the cybersecurity domain at Mantel Group. Nick founded, built & sold two of Australia's leading cybersecurity professional services firms: Hivint, acquired by Trustwave in 2018; and SIFT/Stratsec, acquired by BAE Systems Australia in 2010. Both companies were Telstra Business Awards Winners and members of various 'fast growth' lists. He is a Graduate of the AICD Company Directors Course and has served on boards and forums including the Internet Industry Association, the NATA AAC for Software Testing, UNSW Advisory Boards, and as an Australian delegate to the APEC TEL Security & Prosperity Steering Group.

Amanda Sutton
Acting Director Communication and Coordination, CISG, Department of Home Affairs Australia

Amanda Sutton is Acting Director, Communication and Coordination, within the Cyber and Infrastructure Security Group (CISG), Department of Home Affairs. Amanda leads the coordination of stakeholder engagement with owners and operators of critical infrastructure, leveraging partnerships across sectors and between agencies, to assist stakeholders to understand their obligations and mitigate risk through the provision of timely and relevant information. Amanda has previously worked across several Commonwealth departments in compliance policy and regulatory reform programs and initiatives.

William Coote
Managing Associate, Allens

William is a Managing Associate in Allens' market leading Technology Media and Telecommunications team. Will specialises in technology and digital infrastructure transactions and his regulatory practice spans telecommunications, radiocommunications, cyber security, and, most relevantly, security of critical infrastructure compliance. Over the past 24 months Will and his colleagues have worked with clients who operate in 9 of the 11 critical infrastructure sectors and have advised relevant entities in respect of 19 of the 22 classes of critical infrastructure assets.

Kate Carruthers
Chief Data & Insights Officer, UNSW Australia

Kate Carruthers is working at the intersection of data, AI, privacy, data protection, cyber and information security. She is Chief Data & Insights Officer for UNSW Sydney and is the Head of Business Intelligence for the UNSW AI Institute. Kate has extensive experience in senior roles in ICT across the finance sector, in the public sector, in retail and wholesale distribution, and in marketing, with expertise in data and digital. She has completed postgraduate studies in business; terrorism and security; and tertiary education. Kate also co-founded several technology startups and currently advises a number of startups.

Dr. Tatiana Bokareva
Principal Data Scientist, Teradata Australia

Dr. Tatiana leads a team of technology experts and leaders in data science. Her mission is to help businesses realise real value from ML and AI projects, given the rapid change and evolution in the analytics landscape. Tatiana has extensive experience helping clients with analytical vision, roadmap, architecture through to the delivery of analytical projects. She works with clients ranging from federal and state government agencies to enterprises in FSI, telco and retail. Her leadership, management, communication and people skills have been shaped by over 20 years of in-depth industry experience, working for Fortune 500 companies and hands-on data science expertise.

Michael Loewy
Co-Founder / CEO, Tide Foundation

Michael is a Co-founder/CEO of Tide Foundation, a deep tech start-up reimagining trust in the digital world. He's a seasoned entrepreneur with a rich C-Level history leading the productisation and commercialisation of transformational software for organisations like Dell, Yahoo!, News Limited, NetRegistry, Telstra, Motorola through to greenfield startups. Michael was an academic professional at the University of Illinois, and is a research partner with RMIT, Deakin and UoW in the field of cryptography. He currently serves on the advisory board of the Children's Medical Research Institute.
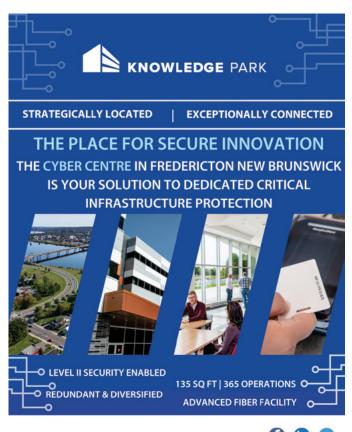
Kate Monckton
Cyber Partner, Deloitte

Kate leads Deloitte's Cyber Strategy and Transformation practice. Prior to this, she spent ten years in multiple leadership roles as part of the National Broadband Network's (nbn) Security Group Senior Leadership Team, including Chief Privacy Officer. Kate has also held security and privacy leadership roles at Symantec (UK) and Microsoft (Australia). Kate spent five years on the Board of the International Association of Privacy Professionals (IAPP ANZ), including two as President. In 2024 she won the Cyber Security award at the B&T Women Leading Tech Awards and in 2021, recognized as 'Australia's Most Outstanding Women in IT Security' at the Australian Women in Security Awards.

Vineet Kumar
Founder and Global President, CyberPeace

Vineet Kumar, Founder and Global President of CyberPeace, is an expert in CyberPeace, Internet Governance, and Cybersecurity. He previously served as Founder CTO and Chief of Cyber Defence Research Center for the Jharkhand government. Educated at Cranfield and Cambridge Universities, he has contributed to UN and Commonwealth cyber initiatives. Kumar establishes Centers of Excellence with universities and organizes the Global CyberPeace Challenge. A frequent speaker at global events, he has received 26 awards, including the IVLP, Chevening Fellowship, and British Council Future Leaders. Kumar is dedicated to improving global cyber resilience and safety.

ACADEMIC PROGRAM
THURSDAY, 29 AUGUST 2024
UNSW SYDNEY, AUSTRALIA

09:10–10:10	**Session 1: INVITED TALK: Albert Zomaya** Location: Colombo Theatre A
10:30–12:10	**Session 2A: Security Track** Location: Colombo Theatre A • 10:30: William Aiken, Paula Branco and Guy-Vincent Jourdan • DevilDiffusion: Embedding Hidden Noise Backdoors into Diffusion Models • 10:50: Mohammed-El-Amin Tebib, Oum-El-Kheir Aktouf, Pascal André and Mariem Graa • PrivBench: A Benchmark Capturing Privilege Escalation Vulnerabilities in Android (ONLINE TALK) • 11:10: Kevin Saric, Gowri Sankar Ramachandran, Raja Jurdak and Surya Nepal • Efficient Data Security Using Predictions of File Availability on the Web • 11:30: Saurabh Anand, Shubham Malaviya, Manish Shukla and Sachin Lodha • CompFreeze: Combining Compacters and Layer Freezing for Enhanced Pre-Trained Language Model (ONLINE TALK) • 11:50: Ross Porter, Morteza Biglari-Abhari, Duleepa Thrimawithana and Benjamin Tan • Extending ISO 15118-20 EV Charging: Preventing Downgrade Attacks and Enabling New Security Capabilities

10:30–11:50	**Session 2B: Privacy Track** Location: Session Room LG01 • 10:30: Huanyi Ye, Ziyao Liu, Yu Jiang, Jiale Guo and Kwok-Yan Lam • Malicious Unlearning in Ensemble Models • 10:50: Atthapan Daramas, Vimal Kumar and Marinho Barcellos • Quantifying Privacy in Cooperative Awareness Services Through Trajectory Reconstruction • 11:10: Masaya Kobayashi, Atsushi Fujioka, Koji Chida, Akira Nagai and Kan Yasuda • Pk-Anonymization Meets Differential Privacy • 11:30: Mst Mahamuda Sarkar Mithila, Fangyi Yu, Miguel Vargas Martin and Shengqian Wang • Visualizing Differential Privacy: Assessing Infographics' Impact on Layperson Data-sharing Decisions and Comprehension
13:30–14:30	**Session 3: INVITED TALK: Willy Susilo** Location: Colombo Theatre A
14:50–16:30	**Session 4A: Security Track** Location: Colombo Theatre A • 14:50: Abdelfattah Amamra, Rym Khettab and Raissa Mezine • Enhancing Network Intrusion Detection Systems: A Review of Feature Selection Algorithms for Streaming Data Processing • 15:10: Arthur Drichel and Ulrike Meyer • A Comprehensive Study on Multi-Task Learning for Domain Generation Algorithm (DGA) Detection • 15:30: Juliet Samandari and Clémentine Gritti • Post-Quantum Authentication and Integrity in 3-Layer IoT Architectures • 15:50: Ahmed Tanvir Mahdad and Nitesh Saxena • Mobile Login Bridge: Subverting 2FA and Passwordless Authentication via Android Debug Bridge. (ONLINE TALK) • 16:10: Duc-Thuan Dam, Trong-Hung Nguyen, Thai-Ha Tran, Binh Kieu-Do-Nguyen, Trong-Thuc Hoang and Cong-Kha Pham • An Efficient Method for Accelerating Kyber and Dilithium Post-Quantum Cryptography
14:50–15:50	**Session 4B: Privacy track** Location: Session Room LG01 • 14:50: Jinglin Sun, Basem Suleiman and Imdad Ullah • Effectiveness of Privacy-Preserving Algorithms for Large Language Models: A Benchmark Analysis • 15:10: Costanza Alfieri, Suriya Ganesh Ayyamperumal, Limin Ge, Jingxin Shi and Norman Sadeh • "I was diagnosed with...": sensitivity detection and rephrasing of Amazon reviews with ChatGPT (ONLINE TALK) • 15:30: Hiroaki Anada, Masayuki Fukumitsu and Shingo Hasegawa • Group Signatures with Designated Traceability over Openers' Attributes from Symmetric-Key Primitives

15:50–16:20	**Session 5: Trust Track** Location: Session Room LG01 • 15:50: Huong Nguyen, Hong-Tri Nguyen, Lauri Loven and Susanna Pirttikangas • Stake-Driven Rewards and Log-Based Free Rider Detection in Federated Learning (ONLINE TALK)

FRIDAY, 30 AUGUST 2024

09:00–10:00	**Session 6A: Privacy Track** Location: Session Room LG02 • 09:00: Jesse Merhi, Erik Buchholz and Salil S. Kanhere • Synthetic Trajectory Generation Through Convolutional Neural Networks • 09:20: Mahmuda Akter, Nour Moustafa and Benjamin Turnbull • PEL: Privacy Embedded Learning in Smart Healthcare Systems (ONLINE TALK) • 09:40: Malte Breuer, Ulrike Meyer and Susanne Wetzel • Efficient Integration of Exchange Chains in Privacy-Preserving Kidney Exchange
09:00–10:00	**Session 6B: Security Track** Location: Session Room LG01 • 09:00: Zehui Tang, Shengke Zeng, Song Han, Qi Yu, Shihai Jiang and Peng Chen • DEFD: Dual-Entity Fuzzy Deduplication for Untrusted Environments • 09:20: Mohamed Abdelsalam, Isaac Mpidi Bita, Simon Greiner, Oum-El-Kheir Aktouf and Annabelle Mercier • Model-Based Security Analysis of Interconnected Subsystems: A Methodology for Security Compatibility Evaluation • 09:40: Brooke Kidmose and Weizhi Meng • can-fp: An attack-aware analysis of false alarms in automotive intrusion detection models
10:20–11:20	**Session 7A: Emerging Technologies and Trends Track** Location: Session Room LG02 • 10:20: Raymond K. Zhao, Nazatul H. Sultan, Phillip Yialeloglou, Dongxi Liu, David Liebowitz and Josef Pieprzyk • MIKA: A Minimalist Approach to Hybrid Key Exchange • 10:40: Qi Li and Xiaodong Lin • Proactive Audio Authentication using Speaker Identity Watermarking (ONLINE TALK) • 11:00: Guibin Zhao, Pengfei Li, Zhibo Zhang, Fusen Guo, Xueting Huang, Wei Xu, Jinyin Wang and Jianlong Chen • Towards SAR Automatic Target Recognition Multi- Category SAR Image Classification Based on Light Weight Vision Transformer. (ONLINE TALK)

10:20–11:40	**Session 7B: Security Track** Location: Session Room LG01 • 10:20: Sandro Rodriguez Garzon, Dennis Natusch, Artur Philipp, Axel Küpper, Hans Joachim Einsiedler and Daniela Schneider • DID Link: Authentication in TLS with Decentralized Identifiers and Verifiable Credentials • 10:40: Thai-Ha Tran, Duc-Thuan Dam, Binh Kieu-Do-Nguyen, Van-Phuc Hoang, Trong-Thuc Hoang and Cong-Kha Pham • Hardware Implementation of a Hybrid Dynamic Gold Code-Based Countermeasure Against Side-Channel Attacks • 11:00: Hesamodin Mohammadian, Arash Habibi Lashkari and Ali Ghorbani • Poisoning and Evasion: Deep Learning-Based NIDS under Adversarial Attacks • 11:20: Anuradha Mandal and Nitesh Saxena • Disease Detector: A Disease Inference Attack Using Brainwave Signals Associated with Body Postures (ONLINE TALK)

FREDERICTON INDUSTRY DAY SUMMIT RESEARCH
POSTERS

- **Towards Efficient Machine learning Method for IoT DDoS attack detection** by Pavitra Modi.

- **IoT-LiteLine: Lightweight Pipeline for IoT Device Identification, Profiling and Monitoring** by Alireza Zohourian, Dr. Sajjad Dadkhah and Dr. Ali Ghorbani.

- **Towards Efficient and Privacy-Preserving High-Dimensional Range Query in Cloud** by Lili Sun, Yonggang Zhang, Yandong Zheng, Weiyu Song, and Rongxing Lu.

- **An Efficient Edge-based Privacy-preserving Range Aggregation Scheme for Aging in Place System** by Zhuliang Jia, Jinkun Gui, Rongxing Lu, and Mohammad Mamun.

- **A Review of Hybrid KEM Combiners with a Focus on Performance and Efficiency** by Amir Hassanpour Zarghani, Vikas Chouhan, Arun Kaniyamattam, and Somayeh Sadeghi.

- **Threshold Authenticated Encryption Scheme for Secure Communications in Aging-in-Place Systems** by Jinkun Gui, Zeming Zhou, Rongxing Lu, and Mohammad Mamun.

- **Automated IDS/IPS System for Data Exfiltration Protection in AWS Cloud** by Mustafa Kamal Taqi and Windhya Hansinie Rankothge.

- **Vulnerabilities in Autonomous Vehicle V2X Communication: Safety at Risk** by Ishan Randeniya and Saqib Hakak.

- **Post-Attack Mitigation in Digital Substations: A Practical Approach** by Mahdi Abrishami, Kwasi Boakye-Boateng, Hossein Shokouhinejad, Kishore Sreedharan, Shabnam Saderi Oskouei, Rongxing Lu, and Ali Ghorbani.

- **A Comprehensive Survey on Chaos Based Satellite Image Encryption: Background, Methodologies, Challenges and Future Directions** by Farrukh Bin Rashid, Windhya Rankothge, Somayeh Sadeghi, Hesamodin Mohammadian, and Ali Ghorbani.

- **DeepFakes** by Muhammad Zubair, and Saqib Hakak.

- **Assessing the impact of cyber threat in substations: A Practical approach** by Kishore Sreedharan, Kwasi Boakye-Boateng, Hossein Shokouhinejad, Mahdi Abrishami, Shabnam Saderi Oskouei, Rongxing Lu, and Ali Ghorbani.

- **RuleSense: Efficient and Lightweight Rapid Rule-Based Anomaly Detection for IIoT Streaming Data** by Amir Firouzi, Sajjad Dadkhah, Heather Molyneaux, and Ali A. Ghorbani.

- **FIGS: A Lightweight Intrusion Detection Framework For Highly Imbalanced IoT Environments** by Zeynab Anbiaee, Sajjad Dadkhah, and Ali A. Ghorbani.

- **Protecting Ciphertext Integrity in Software-Defined-Storage Systems** by David Mohren, Minh Truong, Brett Kelly, and Kenneth Kent.

- **A Communication-efficient Conjunctive Query Scheme under Local Differential Privacy** by Ellen Z. Zhang, Yunguo Guan, Rongxing Lu, and Harry Zhang.

- **Graph Neural Network Based Malware Detection System** by Hesamodin Mohammadian, Griffin Higgins, Samuel Ansong, Hossein Shokouhinejad, Mahdi Rabbani, Roozbeh Razavi-Far.

- **Mitigating Contextual Weaknesses in OpenAIs Beta Assistants API** by Griffin Higgins, Sajjad Dadkhah, and Alireza Zohourian.

- **Large Language Models (LLMs) and Pretrained Transformers for Combating Healthcare Misinformation: A Comprehensive NLP framework** by Hamed Jelodar, Sajjad Dadkhah, and Amir Firouzi.

- **A Lightweight IoT Device Identification Using Enhanced Behavioral-Based Features** by Mahdi Rabbani, Jinkun Gui, Zeming Zhou, Fatemeh Nejati, Rongxing Lu, and Ali A. Ghorbani.

- **Analyzing the Dynamics of the Spread of True and False News on Twitter** by Arbaaz D. Mohammed, and Saqib Hakak.

- **Detecting Distributed Denial-of-Service (DDoS) attacks that generate false authentications on Electric Vehicle (EV) charging infrastructure** by Yoonjib Kim, Saqib Hakak, Ali Ghorbani.

- **Robust Visual Anomaly Detection in Autonomous Vehicles: A Deep Learning Approach** by Samuel Ansong, and Ali Ghorbani.

- **Large-Scale Feature Selection via Graph Learning** by Alireza Fathalizadeh, Parisa Hamedi, and Roozbeh Razavi-Far.

- **Privacy Preserving Advanced Metering Infrastructure** by Arash Kariznovi and Kalikinkar Mandal.

- **Enhancing Privacy in EV Authentication** by Nethmi Hettiarachchi, Kalikinkar Mandal, and Saqib Hakak.

- **Fortifying Publish-Subscribe Communication: Advanced Security Solutions** by Shabnam Saderi, Kalikinkar Mandal and Ali Ghorbani.

- **GridLock: Defending the Digital Frontiers in Energy Security** by Nethmi Hettiarachchi, Shabnam Saderi, Arash Kariznovi, and Kalikinkar Mandal.

CALL FOR PAPERS

www.pstnet.ca

22ⁿᵈ Annual International Conference on Privacy, Security & Trust

PST2025

August 25–27, Fredericton NB

Innovation in ubiquitous interconnected technologies, together with the growth of interconnected computing and storage, defines the foundation to a vast landscape of unforeseen digital services and social networks. Instant access to services, real-time data, and the ability to share content down to detailed social and very personal information. Developing sustainable communities and optimizing the utilization of resources, such as energy, led to the development of new technologies for smart cities, smart transport, and the evolution of autonomous technologies for manufacturing and transportation. Significant commercial opportunities promised by these technologies and services inevitably attract cybercrime and the need for research and innovation in Privacy, Security and Trust. The Annual International Conference on Privacy, Security & Trust (PST) provides a premier forum for sharing advances in cybersecurity research and security applications.

TOPIC LIST

- Privacy Preserving/ Enhancing Technologies
- Critical Infrastructure Protection
- Network and Wireless Security
- Cloud Security, Web Security and Privacy
- Internet of Things (IoT) Security and Privacy
- Operating Systems Security
- Intrusion Detection/ Prevention Technologies
- Secure Software Development and Architecture
- PST Challenges in e-Services, e.g., e-Health, e-Government, e-Commerce
- Digital Forensics
- Security Analytics and Data mining
- Cryptographic Technologies
- Recommendation, Reputation and Delivery Technologies
- Continuous Authentication
- Security and Privacy Challenges in Blockchain and its Applications
- Trust Technologies, Technologies for Building Trust in e-Business Strategy
- Observations of PST in Practice, Society, Policy, and Legislation
- Digital Rights Management
- Identity and Trust Management
- Human Computer Interaction and PST
- Biometrics, National ID Cards, Identity Theft
- Implications of, and Technologies for, Lawful Surveillance
- Privacy, Traceability, and Anonymity
- Trust and Reputation in Self-Organizing Environments
- Anonymity and Privacy vs. Accountability
- Access Control and Capability Delegation
- Representations and Formalizations of Trust in Electronic and Physical Social Systems
- Security and Privacy Challenges in Fog Computing-Enhanced IoT

SUBMISSION GUIDELINES

All papers must be original and not simultaneously submitted to another journal or conference.

Full & Short papers: High-quality papers in all PST-related areas that, at the time of submission, are not under review and have not already been published or accepted for publication elsewhere are solicited. Accepted papers will be accepted as 'regular' papers up to ten pages, or 'short' papers of up to six pages. Up to two additional pages will be allowed in each category with over-length charges. Every additional page has a cost of $100.00 (CND). Authors MUST ensure to select the track (Privacy, Security, or Trust) or special session (to be determined) most relevant to their research when submitting their paper.

Check the Privacy, Security & Trust conference website for updates.

FREDERICTON INDUSTRY DAY
SUMMIT SPONSORS & SUPPORTERS

Atlantic Canada Opportunities Agency / Agence de promotion économique du Canada atlantique — Canada

UNB University of New Brunswick | Canadian Institute for Cybersecurity

IEEE | IEEE Computer Society

GOLD

MOBIA | SentinelOne

SILVER

Interac

BRONZE

ONB Opportunities | Opportunités NB

yubico

MIXER & WORKSHOPS

KNOWLEDGE PARK

UNIVERSITY OF NEW SOUTH WALES EVENT SPONSORS

21st Annual International Conference
on Privacy, Security & Trust

pstnet.ca

#PST2024