22nd Annual International Conference on Privacy, Security & Trust

26 – 28 August 2025
Industry Summit & Academic Conference
Fredericton, New Brunswick, Canada

pstnet.ca

#PST2025

WELCOME

Dr. Ali Ghorbani
Tier 1 Canada Research Chair in Cybersecurity

Professor and Director
Canadian Institute for Cybersecurity

On behalf of the Organizing Committee and the Technical Program Committee, we warmly welcome you to the 22nd International Conference on Privacy, Security, and Trust (PST 2025).

PST 2025 continues the tradition of bringing together researchers to explore the three core themes of privacy, security, and trust, along with an emerging technologies and trends track. Participants will present their latest findings and disc uss practical applications of their work. Organizing a conference of this scale has certainly been a challenge, but we are pleased to offer a dynamic program that includes an in-person Cybersecurity Industry Summit on August 26, 2025, and a hybrid main conference on August 27–28, 2025, covering all intended topics.

PST 2025 offers a balanced program that bridges industry and academic perspectives across a wide range of cybersecurity topics. The conference features keynote speakers from academia, government, and industry.

Keynote speakers at the Cybersecurity Industry Summit include:

Abhay Raman, Senior Vice President and Chief Security Officer, Sun Life

Dr. Ahmed Al-Rawi, Associate Professor, School of Communication, Simon Fraser University

Dr. Argyri Panezi, Canada Research Chair in Digital Information Law and Policy, University of New Brunswick

Chris Lynam, Director General, Royal Canadian Mounted Police

Colin MacSween, Director General of National Cyber Security, Public Safety Canada

Dan Doran, Vice President of Marketing and Business Development, ADGA Group

Elaine Hum, Director of Cybersecurity Partnerships, Scotiabank

Igor Opushnyev, Principal Software Engineer/Architect, Mastercard

Jennifer Sloan, SVP of Government Affairs and Stakeholder Engagement, Mastercard Canada

Kelly Anderson, Director of International Cyber and Critical Technology Policy, Global Affairs Canada

Kostia Nikolaiev, Product Manager, Mastercard

Dr. Kwasi Boakye-Boateng, Deputy Director of Research & Training, Cyber Attribution Data Centre

Paul Hanley, SVP Cyber Security, Rogers

Rajiv Gupta, Head, Canadian Centre for Cyber Security

Steve Sparkes, Chief Information Security Officer, TD Bank

Academic keynote speakers at the hybrid main conference include:

Dr. Lingyu Wang, University of British Columbia Okanagan

Dr. Sébastien Gambs, Université du Québec à Montréal

Dr. Roozbeh Razavi-Far, University of New Brunswick

Conference participants will have the opportunity to hear from these leading experts and researchers.

A total number of 69 papers (including 42 regular papers and 27 short papers) out of around 160 submissions were accepted for presentation on August 24–27, 2025 (GMT-3). Researchers will present their research results covering the spectrum of Privacy, Security, and Trust, examining topics as diverse as network intrusion detection, adversarial machine learning, IoT security, authentication and access control, malware classification, privacy-preserving computing, trust assessment models, online social network privacy, homomorphic encryption, blockchain security, and digital identity.

We would like to thank the Canadian Institute for Cybersecurity (CIC), University of New Brunswick, Knowledge Park, and Ignite Fredericton for their sponsorship. We are especially grateful to IEEE for their continued support and technical co-sponsorship.

A big thank you to all those of you who have submitted research and will be presenting, and to all the participants. We sincerely hope you will find the conference beneficial and are grateful to you for being a part of this conference.

Ali Ghorbani
PST 2025 General Co-Chair

Benoît Dupont, PHD
PST 2025 General Co-Chair

Canadian Institute for Cybersecurity

A hub of cybersecurity innovation and talent development in Canada

The Canadian Institute for Cybersecurity drives cutting-edge research and innovation, extending its impact well beyond the Maritimes to national and global stages.

Situated in Eastern Canada, the province of New Brunswick has emerged as a strategic leader in advancing cybersecurity technologies. Since 2000, the University of New Brunswick (UNB) has been a cornerstone in this effort, cultivating one of the country's largest and most respected network security research groups. UNB continues to build expertise in areas such as Operational Technologies, Critical Infrastructure protection, Artificial Intelligence, and the Industrial Internet of Things. At the forefront of this progress is the Canadian Institute for Cybersecurity, which partners with industry and government to position Canada as a global centre for cybersecurity innovation and talent development.

TABLE OF CONTENTS

INDUSTRY SUMMIT PROGRAM

TUESDAY, 26 AUGUST 2025

FREDERICTON CONVENTION CENTRE

OUR EMCEES

Dr. Samita Bai
Postdoctoral Fellow
Canadian Institute for Cybersecurity

Griffin Higgins
PhD Student & Cybersecurity
Software Developer
Canadian Institute for Cybersecurity

07:45	**Registration, Breakfast, & Networking**	
08:30	**Opening Remarks by** • Dr. Ali Ghorbani, Director of the Canadian Institute for Cybersecurity • Dr. Paul Mazerolle, President and Vice-Chancellor of the University of New Brunswick	
08:40	**Welcoming Remarks by** • Honourable Dominic LeBlanc, President of the King's Privy Council for Canada and Minister responsible for Canada-U.S. Trade, Intergovernmental Affairs and One Canadian Economy • Honourable Renée Legacy, Deputy Premier, Minister of Finance and Treasury Board, Minister of Energy, Government of New Brunswick • Tricia Geddes, Deputy Minister of Public Safety Canada	
09:00	**The Next Cyber Era** AI and quantum technologies are transforming the cyber threat landscape—AI enables hyper-realistic misinformation and automated attacks, while quantum computing threatens to break today's encryption. This talk will explore the current and future threats faced by Canadian critical infrastructure, and outline strategies to safeguard security, privacy, and trust in a rapidly evolving digital era.	**Rajiv Gupta,** *Head, Canadian Centre for Cybersecurity*
09:25	**From Risk to Reward: Strengthening Canada's Digital Trust with Threat Intelligence** Cyber threats today don't just erode economic confidence, they actively test the limits of our collective intelligence, agility, and trust. For Canada's leading organizations, digital trust is no longer a theoretical ideal, it's forged daily through real-time threat intelligence, robust information sharing, and public-private collaboration. This keynote explores how advanced threat intelligence, from global platforms like Recorded Future to Canadian-led innovation such as the Cyber Attribution Data Center at UNB, is transforming detection and response capabilities across our digital economy. It highlights the need for sustained collaboration—mirroring models like the Financial Services Information Sharing and Analysis Center (FS-ISAC)—and how intelligence-driven strategies are unlocking new opportunities for AI and cyber startups, positioning Canada as a leader in global resilience.	**Jennifer Sloan,** *SVP, Government Affairs and Stakeholder Engagement, Mastercard Canada*

09:40	**Becoming Cyber Girl: A Cybersecurity Superhero Origin Story** Join Elaine Hum, Director of Cybersecurity Partnerships at Scotiabank, in an inspiring session as she shares her transformation into "Cyber Girl." Recognized as one of IT World's Top Women in cybersecurity in 2023, Elaine's story is one of resilience and empowerment. She provides invaluable insights and practical advice on navigating the cybersecurity industry, particularly for women seeking to overcome challenges and thrive. Prepare to be inspired and informed by her journey of dedication, skill, and passion in this dynamic field. Don't miss this opportunity to be captivated by Elaine's transformation and leave equipped with the tools and mindset to forge your own superhero origin story in cybersecurity!	**Elaine Hum,** *Director, Cybersecurity Partnerships, Scotiabank*
10:10	**Nutrition Break & Research Poster Session**	
10:25	**Taking Public-Private Collaboration in combatting Cybercrime to the next level: Perspectives from the RCMP's National Cybercrime Coordination Centre (NC3)** Cybercrime continues to impact Canadians on an unprecedented scale. Innovative actions and a Whole of Society approach are the only ways Canada is going to effectively respond to cybercrime. Chris Lynam, who leads both the National Cybercrime Centre (NC3) and Canadian Anti-Fraud Centre (CAFC), will outline how these organizations have evolved their approaches in the last few years, and he will showcase some of its recent collaborative successes to reduce the impact of cybercrime on Canadians.	**Chris Lynam,** *Director General National Cybercrime Coordination Centre and Canadian Anti-Fraud Centre, RCMP*
10:50	**The New World of Cyber Risk** Cybersecurity is a critical concern for all organizations, regardless of size or industry. As cyber threats continue to evolve, businesses and individuals must be proactive in assessing both current and future risks. Understanding these threats is key to building strong defenses, ensuring that sensitive data and operations remain secure. Paul will bring this session to life by offering valuable insights into the ever-changing cybersecurity landscape. He will debunk common myths that often mislead organizations and individuals, providing clarity on what truly matters in cyber protection. Beyond dispelling misconceptions, Paul will also deliver practical strategies to safeguard yourself and your organization against cyber threats. His expert guidance will help participants prepare for the next wave of cybersecurity challenges, equipping them with the tools and knowledge needed to stay ahead. This session is designed to be both informative and actionable, ensuring that attendees leave with a clear understanding of how to protect their digital assets effectively.	**Paul Hanley,** *SVP Cyber Security, Rogers*

11:15	**AI's Impact on Cybersecurity** As artificial intelligence continues to transform industries, it is simultaneously reshaping the cybersecurity landscape, introducing unprecedented opportunities and complex risks. In this presentation, Steve Sparkes, Chief Information Security Officer, TD Bank will explore the implications of AI on cybersecurity strategy, defense, and threat evolution. His presentation will focus on how AI-driven tools can enhance threat detection, automate incident response, and strengthen predictive analytics. The conversation will address the growing use of AI by malicious actors to craft more sophisticated cyberattacks, including automated phishing and AI-assisted malware. Attendees will gain insight into the critical need for adaptive security frameworks, ethical AI governance, and resilient infrastructure to keep pace with evolving threats. The conversation aims to equip security leaders with actionable guidance on integrating AI responsibly while mitigating emerging risks in an increasingly intelligent threat environment.	**Steve Sparkes,** *Chief Information Security Officer, TD Bank* **Pamela Simpson,** *AI Business Information Security Officer, TD Bank*
11:40	**The legal dilemmas of cyber-attribution** This talk explores the complex legal challenges surrounding cyber-attribution research, with a particular focus on domestic privacy laws and international laws. Cyber-attribution — the process of assigning responsibility for (malicious) cyber activities to specific actors — relies on a combination of intelligence gathering, forensic analysis, and contextual interpretation. It is an inherently interdisciplinary and complex process that intersects with multiple legal domains, including domestic law (particularly criminal and privacy laws), international law, and political attribution. The talk seeks to clarify these legal complexities and provoke discussion on how legal frameworks can evolve to support responsible and effective cyber-attribution research.	**Argyri Panezi,** *Canada Research Chair in Digital Information Law and Policy, University of New Brunswick*
12:00	**Fellowship Presentations**	
12:10	**Lunch & Research Poster Session**	
13:05	**Panel — Cyber Attribution — Beyond the Breach: Challenges, Techniques, and Policy Implications** This panel's primary aim is to promote dialogue across technical, academic, and policy domains to enhance cyber defence, resilience, and accountability mechanisms. The panel members will discuss the evolving landscape of cyber attribution in response to increasingly complex and persistent cyber threats. Moving beyond the initial breach, the panellists will address the technical, operational, and legal challenges of identifying threat profiles and actors, attributing attacks with confidence, and navigating geopolitical sensitivities. The discussion will illuminate the critical needs for cyber attribution across various contexts, including national security and the protection and resilience of critical infrastructure, where the stakes are high and the consequences far-reaching. Another focus of the panel is the emerging methodologies, such as AI-assisted forensics and behavioural analytics, for policy development and deterring future threats. Panelists: • Kelly Anderson, Director, International Cyber and Critical Technology Policy, Global Affairs Canada • Ahmed Al-Rawi, Associate Professor, Simon Fraser University • Argyri Panezi, Canada Research Chair in Digital Information Law and Policy, University of New Brunswick • Kostia Nikolaiev, Product Manager, Mastercard	Moderator: **Colin MacSween,** *Director General, National Cybersecurity, Public Safety Canada*

14:30	**Nutrition Break & Research Poster Session**	
14:50	**Security in a Volatile World** In today's rapidly evolving global landscape, information security faces unprecedented challenges shaped by mounting geopolitical tensions and the shifting sands of data and technology sovereignty. This talk delves into the complex interplay between nation-state interests, cross-border data flows, and the fragmented regulatory environments that organizations must navigate. As geo-political tensions rise, and international regulations intensify, security becomes both a technical and strategic imperative. Meanwhile, the emergence of transformative technologies—most notably AI and quantum computing—threatens to upend established cryptographic standards, demanding urgent adaptation and forward-thinking risk management. Compounding these challenges is a pervasive lack of information sharing between public and private sectors, leaving gaps that adversaries can exploit. This session will explore the multifaceted risks arising from these trends, offering insights into developing resilient security strategies in a volatile world. Participants will gain a nuanced understanding of how to safeguard critical assets and foster collaboration amid uncertainty and rapid technological advancement.	**Abhay Raman,** *Senior Vice President and Chief Security Officer, Sun Life*
15:15	**Emerging Cybersecurity Threats** In an era defined by rapid digital transformation, the cybersecurity landscape is evolving at an unprecedented pace. This talk explores the most pressing and sophisticated emerging threats facing organizations and individuals today. From AI-driven cyberattacks and novel approaches utilizing sophisticated computational techniques, we will examine how threat actors are leveraging cutting-edge technologies to outpace traditional defenses such as perimeter security, antivirus software, bot detectors and other. Attendees will gain insights into real-world case studies, the shifting tactics of cyber adversaries, and proactive strategies for resilience. This session will equip you with the knowledge to anticipate and counter the next wave of cyber threats.	**Igor Opushnyev,** *Principal Software Engineer/Architect, Mastercard* **Kostiantyn Nikolaiev,** *Product Manager, Mastercard*
15:40	**Cyber Attribution Data Centre (CADC): The Future of Identifying Cyber Threat Actors** The Cyber Attribution Data Centre (CADC) marks a bold step into the future of cybersecurity in Canada. Supported by a $10 million federal investment from Public Safety Canada via the Atlantic Canada Opportunities Agency, CADC's five-year plan combines advanced analytics, secure infrastructure, and top-tier expertise to combat malicious cyber actors directly. The Centre is committed to developing AI-powered tools to identify threat actors with unmatched accuracy, while training the next generation of cybersecurity professionals to sustain this mission. CADC's primary goals are (1) to create a state-of-the-art, highly secure research facility and data centre, (2) to generate intelligence that is verifiable, reproducible, and reliable, and (3) to develop innovative tools and datasets to share with the community, grounded in strict ethics and a firm commitment to privacy and national security.	**Ali Ghorbani,** *Director, Canadian Institute for Cybersecurity* **Kwasi Boakye-Boateng,** *Interim Deputy Director of Research and Training, CADC*
16:05	**Closing Remarks & Best Research Poster Awards** Dr. Ali Ghorbani, Director of the Canadian Institute for Cybersecurity	
16:30-18:00	**Reception & Networking**	

SPEAKERS & PANELISTS

Dr. Ahmed Al-Rawi

Associate Professor, Simon Fraser University

Dr. Ahmed Al-Rawi is an Associate Professor of News, Social Media, and Public Communication at the School of Communication at Simon Fraser University. He is also the founder and director of the Disinformation Project, and his research interests are related to news, global communication, misinformation, and social media with emphasis on Canada and the Middle East.

Kelly Anderson

Director, International Cyber and Critical Technology Policy, Global Affairs Canada

Kelly Anderson currently serves as Director for International Cyber and Critical Technology Policy at Global Affairs Canada. She joined the Department of Foreign Affairs and International Trade in 1997.

At Headquarters, Anderson has worked in a variety of assignments including Deputy Director for NATO, OSCE and European Defence Cooperation; Deputy Director for Conventional, Chemical and Biological Weapons; and, as Deputy Director for Space Policy and Regulation. She has served overseas at the Canadian Embassies in Belgrade, Serbia and Washington, DC. She was Deputy Permanent Representative of Canada to the Conference on Disarmament in Geneva from 2011-2014 and, most recently, served as Counsellor and Head of the Foreign Policy and Diplomacy section of the Canadian Embassy to Austria.

Dr. Kwasi Boakye-Boateng

Deputy Director of Research and Training, Cyber Attribution Data Centre

Dr. Kwasi Boakye-Boateng is the Interim Deputy Director of Research and Training for the Cyber Attribution Data Centre at the Canadian Institute for Cybersecurity. He also serves as a Research Associate and Cybersecurity R&D Team Lead, focusing cyber attribution, and operational technology and mission-critical infrastructure-related cybersecurity. He has worked with various industry and military-based on intrusion detection systems, attack methodologies, risk models, and impact assessments. With over a decade of experience in telecommunications, he brings expertise in securing communication networks. Boakye-Boateng holds a Ph.D. in Computer Science from the University of New Brunswick.

Dan Doran

Vice President, Business Development and Marketing, ADGA Group Consultants Inc.

Dan Doran, Vice President of Business Development and Marketing at ADGA Group Consulting, joined the Canadian Forces in 1998 and served in Afghanistan, Sudan, and the Democratic Republic of Congo. He currently advises the Office of the Chief Military Engineer in the Army Reserve. Doran's civilian career spans leadership roles at McGill, WSP, and KPMG, where he led defence and security initiatives. He also serves as Climate Security and Defence Lead for King Charles III's Sustainable Markets Initiative.

Doran holds a bachelor's in civil engineering and two master's degrees in Human Security and Peacebuilding, and Business Administration. He's a licensed engineer, PMP, and CRHA, and actively contributes to the Vimy Foundation, Canadian Military Engineers Association, and IFPSP.

Tricia Geddes

Deputy Minister, Public Safety Canada

Tricia Geddes was appointed Deputy Minister of Public Safety Canada in October 2024. Prior to her appointment, Geddes held the role of Associate Deputy Minister of Public Safety as of June 2022.

Before joining the department, Geddes was the Deputy Director, Policy and Strategic Partnerships (DDP) at CSIS since April 2020. As DDP, she was responsible for key partnerships in the areas of strategic policy development, foreign relations, external review and compliance, communications, academic outreach and stakeholder engagement, as well as litigation and disclosure. She also supported the Director and the Minister of Public Safety in their accountability for the overall operational activities of the Service, and ensured CSIS was accountable, transparent, and attuned to the strategic interests of the Government of Canada.

Dr. Ali Ghorbani

Director, Canadian Institute for Cybersecurity

Dr. Ali Ghorbani is a Professor of Computer Science at the University of New Brunswick and the Tier 1 Canada Research Chair in Cybersecurity. He founded the Canadian Institute for Cybersecurity in 2016 and served as Dean of the Faculty of Computer Science from 2008 to 2017. With over 44 years in academia, Ghorbani has supervised more than 250 researchers and published over 300 peer-reviewed articles. He holds four awarded patents in network security and web intelligence and co-founded three startups: Sentrant Security, EyesOver Technologies, and Cydarien Security. Dr. Ghorbani is a co-founder of the UNB-NRC Cybersecurity Collaboration Consortium, established in 2019, and the National Cybersecurity Consortium (NCC), founded in 2020. He also co-founded the Privacy, Security, and Trust (PST) Network in Canada, which hosts an annual international conference. In 2017, Dr. Ghorbani received the Startup Canada Senior Entrepreneur Award. In 2019, he was recognized by Canadian Immigrant Magazine as one of the RBC Top 25 Canadian Immigrants. In 2022, he was featured in Mark Bulgutch's book, "Forty Brilliant Canadians and Their Vision for the Nation," highlighting inspiring Canadians. In 2024, he was honoured with the Lifetime Achievement Award from CAIAC — the Canadian Artificial Intelligence Association.

Rajiv Gupta

Director, Canada Cyber Centre

Rajiv Gupta is the Head of the Canadian Centre for Cyber Security (the Cyber Centre), a part of the Communications Security Establishment Canada (CSE). As Head, Gupta leads the Cyber Centre in providing expert advice, guidance and services to the Canadian government, the private sector including Canada's critical infrastructure sectors and the Canadian public.

Prior to this role, Gupta served as the Associate Head of the Cyber Centre for three years, where he was responsible for achieving national level cyber security outcomes for Canada through collaborative efforts with industry partners. Previously a software engineer in the telecommunications sector, Gupta joined CSE in 2007 and has held a number of leadership roles in the cyber security domain, including Director General of Cyber Defence Capabilities.

Paul Hanley

SVP Cyber Security, Rogers

Paul Hanley is the Senior Vice President for Cybersecurity at Rogers Communications. He is a recognized global expert in Cybersecurity, with over 25 years experience in the field, during which time he has successfully played both CISO and ex-Big-4 Senior Partner roles.

While strongly versed in all areas of Cyber Risk and Security, Hanley has particular experience in aligning security functions to the needs of the business and providing Cyber Security direction for Board level Executives. Hanley 's key subject matter expertise includes forming and running global security functions, business transformation, and leading large-scale Cybersecurity programs in Financial Services.

Elaine Hum

Director, Cybersecurity Partnerships, Scotiabank

Elaine Hum is a recognized leader with over 20 years of experience in strategy, partnerships, and cross-sector collaboration. Her work spans finance, government, academia, and nonprofits, where she has collaborated with leaders to provide strategic guidance and shape effective cybersecurity policies.

In 2023, Hum was honoured as one of IT World Canada's Top Women in Cybersecurity, highlighting her significant contributions to the field. Currently, as the Director of Cybersecurity Partnerships at Scotiabank, she is the chief architect of the Bank's Cybersecurity Partnership Program—a strategic initiative focused on attracting diverse talent from equity-deserving groups and fostering innovation through leading-edge R&D collaborations.

Honourable Dominic LeBlanc

President of the King's Privy Council for Canada and Minister responsible for Canada-U.S. Trade, Intergovernmental Affairs and One Canadian Economy

First elected in 2000 and re-elected eight times since, the Honourable Dominic LeBlanc has represented the riding of Beauséjour for 25 years.

A senior member of Cabinet, Minister LeBlanc has held a number of portfolios over the years, including Finance, Intergovernmental Affairs, Public Safety and Democratic Institutions, and Infrastructure and Communities. He has also served as President of the King's Privy Council for Canada, as Minister of Northern Affairs and Internal Trade, as Minister of Fisheries, Oceans and the Canadian Coast Guard, and as Leader of the Government in the House of Commons. Additionally, he has served as Deputy Government Whip and Parliamentary Secretary to the Minister of National Defence.

Honourable Renée Legacy

Deputy Premier, Minister of Finance and Treasury Board, Minister of Energy, Government of New Brunswick

René Legacy was first elected as MLA in 2020, in his riding of Bathurst West-Beresford and was re-elected in 2024 in the redrawn riding of Bathurst. In November 2024, he was sworn in as the Deputy Premier, Minister of Finance and Treasury Board, Minister of Energy and Minister responsible of the Right to Information and Protection of Privacy Act.

Born and raised in the City of Bathurst, Legacy built a successful career in the financial industry spanning a period of over 25 years, mostly comprised of executive roles with the Caisse populaires acadiènnes, then later named UNI Coopération Financière.

Chris Lynam

Director General, National Cybercrime Coordination Centre and Canadian Anti-Fraud Centre, RCMP

Chris Lynam is currently the Director General of the National Cybercrime Coordination Centre and the Canadian Anti-Fraud Centre within the RCMP. He led extensive work and consultations with other government departments, law enforcement partners across Canada and the private sector to conceptualize and design a national cybercrime coordination mechanism for Canada. Lynam previously worked for Public Safety Canada and within the Security and Intelligence Secretariat of the Privy Council Office where he was part of the team that supported the National Security Advisor to the Prime Minister. Outside the RCMP, he is a member of the Primary Reserve and served as the Lieutenant-Colonel Commanding of the Governor General's Foot Guards, an Infantry Regiment based in Ottawa.

Colin MacSween

Director General, National Cyber Security, Public Safety Canada

Colin MacSween is the Director General, National Cyber Security within the National and Cybersecurity Branch at Public Safety Canada. He has previously worked with the Department of National Defence, the Canada Border Services Agency and, most recently, the Canadian Security Intelligence Service. MacSween holds a Master of Public Administration from Dalhousie University.

Dr. Paul Mazerolle

President and Vice Chancellor, University of New Brunswick

Dr. Paul Mazerolle is UNB's 19th president and vice chancellor. An internationally recognized criminologist with degrees from the University of New Brunswick, Northeastern University and the University of Maryland, Paul is also a professor in the department of sociology at UNB.

Dr. Mazerolle is a member of the New Brunswick Business Council, the Universities Canada Board of Directors, Chair of the Association of Atlantic Universities Executive Committee and Board of Directors, the Atlantic University Sport (AUS) Executive Committee and Board of Directors and Chair of the AUS Governance Committee.

Kostiantyn Nikolaiev

Product Manager, Mastercard

Kostiantyn (Kostia) Nikolaiev is a seasoned Product Manager with over 15 years of cross-functional experience in technology and software development. Currently at Mastercard, he leads initiatives in identity verification and fraud detection. Nikolaiev has held leadership roles across diverse sectors including gaming, fintech, and B2B SaaS, and has a strong track record of building and scaling product teams, launching innovative solutions, and driving business growth. He holds a Master's degree in Mathematics and Computer Science and is a Certified Scrum Product Owner.

Igor Opushnyev

Principal Software Engineer/Architect, Mastercard

Igor Opushnyev is a Principal Software Engineer/Architect at Mastercard since 2018. He has almost 30 years of experience in software engineering, with a strong focus on cybersecurity and secure systems design. Along the way, he's been named as the principal inventor or co-inventor on 11 patents in cybersecurity. Opushnyev enjoys sharing what he has learned and connecting with others who are just as excited about tech and innovation.

Dr. Argyri Panezi

Canada Research Chair in Digital Information Law and Policy, University of New Brunswick

Dr. Argyri Panezi is the Tier 2 Canadian Research Chair in Digital Information Law and Policy at the University of New Brunswick (UNB), an affiliated member of the Canadian Institute for Cybersecurity. In her role as the director of UNB's Legal Innovation Laboratory she is also involved in policymaking in New Brunswick, working in collaboration with the judiciary, government, and civil society actors. Panezi's research explores the effects that disruptive technologies have on citizens, institutions, and the law.

Abhay Raman

Senior Vice President and Chief Security Officer, Sun Life

Abhay Raman is Senior Vice President and Chief Security Officer at Sun Life. In this role, he is accountable globally for all aspects of Cyber & Physical security, Crisis, and Technology Risk Management. Raman is committed to continually improving Sun Life's security posture as the organization advances its digital transformation, artificial intelligence, and innovation agenda.

He is the Chair of the Board at the Canadian Cyber Threat Exchange (CCTX), and a board director at Victims Services Toronto. Raman is also an Executive-in-Residence with the TMU Cybersecurity Accelerator, an active advisor to the 'Cyber Right Now' Campaign and the Canadian Forum for Digital Infrastructure Resilience (CFDIR).

Pamela Simpson

AI Business Information Security Officer, TD Bank

Pam Simpson is an AI Business Information Security Officer at TD, where she leads security governance for generative AI initiatives and contributes to multiple industry working groups exploring AI's impact on the financial sector. She previously supported insider investigations and strategic cyber threat intelligence at TD and focused on state-sponsored threats and ransomware while at BMO. Simpson is the Engagements Lead for TD's Platforms and Technology Indigenous Peoples Committee, facilitating partnerships with Indigenous-led organizations in the tech space. She serves on the steering committees and is an active member of the NIST AI Working Groups, the Cyber Risk Institute, Cloud Security Alliance, and the Canadian Bankers Association.

Jennifer Sloan

Senior Vice President Public and 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 government affairs and stakeholder engagement for Mastercard Canada.

A passionate advocate for social impact, Jennifer 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. She's a Vital Voices Global Ambassador and serves on numerous corporate and association boards including Immediate past Chair of the Canadian American Business Council; Immediate past Chair of Music Canada; Director Indigenous Prosperity Foundation; Director Women's College Hospital; and Director of the Board of Trust of the Grady College of Journalism and Communication at the University of Georgia.

Steve Sparkes

Chief Information Security Officer, TD Bank

Steve Sparkes joined TD Bank in 2025 as Chief Information Security Officer and has more than 35 years of experience in leadership roles in technology infrastructure, application development, IT Operational Risk, and Cybersecurity.

Previously, Sparkes joined Scotiabank in 2021 as Chief Information Security Officer and SVP Information Security and Control. In November 2023 he added responsibility for Enterprise Infrastructure, as well as IT and Cyber Risk strategies, systems and procedures. Prior to Scotiabank, he spent 6 years at Bank of America as a Managing Director, being COO for Cybersecurity and then Head of Cybersecurity Technology. His early career included extensive software development for financial systems.

ORGANIZING COMMITTEES

Conference General Chairs

Benoît Dupont, Université de Montréal, Canada

Ali Ghorbani, University of New Brunswick, Canada

Technical Committee Chairs

Florian Kerschbaum, University of Waterloo, Canada

Rongxing Lu, Queen's University, Canada

Track Chairs

Kalikinkar Mandal, University of New Brunswick, Canada

Jianbing Ni, Queen's University, Canada

Sajjad Dadkhah, University of New Brunswick, Canada

Suryadipta Majumdar, Concordia University, Canada

Pooria Madani, Ontario Tech University, Canada

Yunguo Guan, Eastern Michigan University, USA

Qiang Ye, Dalhousie University, Canada

Kwasi Boakye-Boateng, University of New Brunswick, Canada

Publication Chairs

Saqib Hakak, University of New Brunswick, Canada

Xichen Zhang, Saint Mary's University, Canada

Local Organizing and Web Chairs

Ruth M. Murgatroyd, University of New Brunswick, Canada

Windhya Rankothge, University of New Brunswick, Canada

Industry Summit Organizing Committee, Canadian Institute for Cybersecurity

Ali Ghorbani, Chair, University of New Brunswick

Windhya Rankothge, Local Organizing Chair and Poster Presentation Coordinator

Pamela Kitchen, Operations Coordinator

Morakinyo Omolaja Oke, Industry Liaison

Sumit Kundu, Communications and Sponsorship Coordinator

Mohamed Badawy, Technical Coordinator

Michael Odartei Mills, Web Chair

Ruth M. Murgatroyd, Administration and Logistics

Plus, numerous others.

ACADEMIC PROGRAM

RECEPTION & EARLY REGISTRATION
4:30PM TUESDAY, 26 AUGUST 2025

FREDERICTON CONVENTION CENTRE, 670 QUEEN STREET

DAY 1: ACADEMIC PRESENTATIONS

WEDNESDAY, 27 AUGUST 2025

WU CONFERENCE CENTRE, 6 DUFFIE DRIVE

08:00	**Conference On-Site Registration**	
08:30	**Welcoming Remarks by** • Dr. Ali Ghorbani, Director of the Canadian Institute for Cybersecurity • Dr. Rongxing Lu, Professor, School of Computing, Queen's University	
08:45	**Understanding and Addressing Fairwashing in Machine Learning** Fairwashing refers to the risk that an unfair black-box model can be explained by a fairer model through post-hoc explanation manipulation. In this talk, I will first discuss how fairwashing attacks can transfer across black-box models, meaning that other black-box models can perform fairwashing without explicitly using their predictions. This generalization and transferability of fairwashing attacks imply that their detection will be difficult in practice. Finally, I will nonetheless review some possible avenues of research on how to limit the potential for fairwashing.	**Dr. Sébastien Gambs,** *Canada Research Chair in Privacy-Preserving & Ethical Analysis of Big Data, UQAM*
09:45	**Nutrition Break & Research Poster Session**	

10:15	**In-Person Session PS1**	**In-Person Session PS2**	**Online Session OS1**	
11:55	**Lunch & Research Poster Session**			
13:00	**Attack Detection, Investigation, and Mitigation for Network Functions Virtualization (NFV)** By decoupling network functions from proprietary physical boxes, Network Functions Virtualization (NFV) allows tenants to host their network services on top of existing clouds managed by third-party providers. NFV may also lead to novel security challenges at different abstraction levels. In this talk, I will present three of our recent works on securing NFV through attack detection (USENIX Security'24), attack investigation (S&P'25), and attack mitigation (NDSS'24). First, NFV tenants typically cannot directly inspect the underlying cloud infrastructure to detect cloud-level attacks on their network function deployment. Existing solutions add a cryptographic trailer to every packet, which may incur significant performance overhead. We propose ChainPatrol, a lightweight solution for tenants to perform continuous detection and classification of cloud-level attacks on SFCs. Our main idea is to "virtualize" cryptographic trailers by encoding them as side-channel watermarks, such that those trailers can be transmitted without adding any extra bit to packets. Second, while provenance analysis is one of the go-to solutions for investigating security incidents, existing solutions share the limitation of merely regarding the incident as an abstract starting point. We observe that doing so may lead to missed opportunities for pruning the provenance graph, since the incident is typically associated with rich external information about the corresponding vulnerability or exploit. Based on such an observation, we propose CONTEXTS, a solution that complements existing pruning approaches by leveraging such external information about the incident. Third, unpatched vulnerabilities in containers represent a major challenge to mitigating attacks in NFV environments. The average time-to-patch of zero-day vulnerabilities has stayed above 100 days in recent years, which leaves a wide attack window. We propose Phoenix, a solution for blocking exploits of unpatched vulnerabilities by accurately and efficiently filtering sequences of system calls identified through provenance analysis. To achieve this, Phoenix cleverly combines the efficiency of Seccomp filters with the accuracy of Ptrace-based deep argument inspection, and it provides the novel capability of filtering sequences of system calls through a dynamic Seccomp design.			**Dr. Lingyu Wang,** *Professor of Computer Engineering,* *School of Engineering,* *UBC Okanagan*
14:00	**In-Person Session PS3**	**In-Person Session PS4**	**Online Session OS2**	
15:40	**Nutrition Break & Research Poster Session**			
16:10	**In-Person Session PS5**	**In-Person CIC Cybersecurity 4MT Competition**	**Online Session OS3**	
18:30	**Academic Banquet & Best Paper Awards** Beaverbrook Art Gallery 703 Queen Street			

10:15 – 11:55

In-Person Session PS1
Malware Detection with Machine Learning

Room: Chancellor's Room
Chair: Dr. Mahdi Rabbani, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 7: Using Counterfactuals for Explainable Android Malware Detection
Authors: Maryam Tanha, Winston Zhao, Aaron Hunter, Ashkan Jangodaz

Paper ID 107: TOM-Net: Few-Shot IoT Malware Classification via Open-Set Aware Transductive Meta-Learning
Authors: Man-Ying Chen, Tao Ban, Shin-Ming Cheng, Takeshi Takahashi

Paper ID 109: Evaluating Efficient Patch-Based Backdoor Attacks in Satellite Image Classification Systems
Authors: Ghazal Rahmanian, Pooria Madani

Paper ID 130: A Per-Bag Suspicion-Based Bagging Strategy for Fighting Poisoning Attacks in Classification
Authors: Aghoghomena Akasukpe, Tomi Adeyemi, Pooria Madani, Li Yang, Miguel Vargas Martin

Paper ID 133: Harnessing Language Models to Analyze Android App Permission Fidelity
Authors: Yunik Tamrakar, Ritwik Banerjee, Ethan Myers, Lorenzo De Carli, Indrakshi Ray

In-Person Session PS2
Privacy-Preserving Data and Image Processing

Room: J. Harper Kent Auditorium
Chair: Sara Miller, Senior Privacy Consultant, Mariner Innovations

Paper ID 40: Context-Aware Location De-identification Using Denoising Diffusion
Authors: Md Shopon, Marina Gavrilova

Paper ID 99: Private Function Evaluation using CKKS-based Homomorphic Encrypted LookUp Tables
Authors: Haoyun Zhu, Takuya Suzuki, Hayato Yamana

Paper ID 151: Privacy-Preserving Image Learning Across Trust Boundaries
Authors: Atsuko Miyaji, Tomoshi Yagishita, Yuki Hyohdoh

Online Session OS1
Anomaly Detection and Vulnerability Analysis

Room: Aitken Room
Chair: Dr. Mohammad Jafari Dehkordi, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 75: Exploring Clustering Algorithms for Anomaly Detection in Electric Vehicle Charging Stations Infrastructure using OCPP
Authors: Chris Tchassem, Yendoubé Kombate, Pierre-Martin Tardif

Paper ID 93: Legal Retrieval Augmented Generation with Structured Retrieval and Iterative Refinement
Authors: Chaitanya Dhananjay Jadhav, Chang Liu, Jun Zhao

Paper ID 136: Characterizing Event-themed Malicious Web Campaigns: A Case Study on War-Themed Websites
Authors: Maraz Mia, Mir Mehedi Ahsan Pritom, Tariqul Islam, Shouhuai Xu

Paper ID 149: TFVDFuzzer: Transformer-based Fuzzing Framework for Vulnerability Detection in Modbus Protocol
Authors: Ahmed Reda Aldysty, Nour Moustafa, Erandi Lakshika

Paper ID 154: Database Systems Examination and Digital Forensics Tool: the Progress and Limitations
Authors: Oluwasola Mary Adedayo

14:00 – 15:40

In-Person Session PS3
Cryptographic Techniques and Secure Systems

Room: Chancellor's Room
Chair: Dr. Vikas Chouhan, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 2: A Static Analysis of Popular C Packages in Linux
Authors: Jukka Ruohonen, Krzysztof Sierszecki, Mubashrah Saddiqa

Paper ID 50: CHOO-PIR: Hint-Based Private Information Retrieval with Commodity Servers
Authors: Kittiphop Phalakarn, Ryuya Hayashi

Paper ID 114: Empirical Evaluation and Reclassification of Cryptographic Algorithms for Energy-Efficient Secure Communication in Medical IoT Devices
Authors: Sidra Anwar, Jonathan Anderson

Paper ID 116: Comparing Client- & Server-Side AEAD Encryption in Software-Defined Storage Systems
Authors: David Mohren, Minh Tien Truong, Brett Kelly, Kenneth Kent

Paper ID 158: Securing Android Inter-Process Communication (IPC) Using NGAC
Authors: Jason Simental, Elmaddin Azizli, Mahmoud Abdelgawad, Indrakshi Ray

In-Person Session PS4
Intrusion Detection and Threat Mitigation

Room: J. Harper Kent Auditorium
Chair: Dr. Hossein Shokouhinejad, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 74: Cyber Threat Mitigation with Knowledge-Infused Reinforcement Learning and LLM-Guided Policies
Authors: Md. Shamim Towhid, Shahrear Iqbal, Euclides Neto, Nashid Shahriar, Scott Buffett, Madeena Sultana, Adrian Taylor

Paper ID 78: On Feature Selection for Botnet Detection using Adaptive Exploration in Binary Particle Swarm Optimization Algorithm
Authors: Syed Tehjeebuzzaman, Mustafa Siam-Ur-Rafique, Ashikur Rahman, Abderrahmane Leshob, Raqeebir Rab

Paper ID 111: Exploring the Impact of Feature Selection on Non-Stationary Intrusion Detection Models in IoT Networks
Authors: Muaan Ur Rehman, Hayretdin Bahsi, Rajesh Kalakoti

Paper ID 140: A Longitudinal Look at GDPR Compliance
Authors: Brian Kim, Yang Cao, K. Suzanne Barber

16:10 – 17:30

In-Person Session PS5
Security and Privacy in Machine Learning and Systems

Room: Chancellor's Room
Chair: Dr. Vikas Chouhan, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 120: Probing AlphaFold's Input Attack Surface via Red-Teaming
Authors: Tia Pope, Ahmad Patooghy

Paper ID 122: Detecting Ransomware Before It Bites: A Hybrid Model Approach for Early Ransomware Detection
Authors: Sk Mahtab Uddin, Saqib Hakak, Miguel Garzón

Online Session OS3

Room: Aitken Room
Chair: Dr. Mahdi Rabbani, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 94: Beyond SSO: Mobile Money Authentication for Inclusive e-Government in Sub-Saharan Africa
Authors: Oluwole Adewusi, Wallace Msagusa, Jean Pierre Imanirumva, Okemawo Obadofin, Jema Ndibwile

Paper ID 155: Assessing Privacy Practices on Ontario Municipal Websites
Authors: Adegboola David Adelabu, Yan Yan, Wenjing Zhang, Sampa Rauti, Ville Leppänen, Zuhaibuddin Bhutto, Wenthorpe

Paper ID 57: Per-Attribute Privacy in Large Language Models Using Matrix-Variate Gaussian Mechanism
Authors: Islam Monir, Gabriel Ghinita

Paper ID 61: Trust-Aware Federated Defense Against Data Poisoning in ML-Driven IDS For CAVs
Authors: Mahsa Tavasoli, Abdolhossein Sarrafzadeh penalizing, Ali Karimoddini, Milad Khaleghi, Tienake Phuapaiboon, Amauri Goines, Aiden Harris, Jason Griffith

KNOWLEDGE PARK
STRATEGICALLY LOCATED | EXCEPTIONALLY CONNECTED
THE PLACE FOR SECURE INNOVATION
THE CYBER CENTRE IS YOUR SOLUTION TO DEDICATED CRITICAL INFRASTRUCTURE PROTECTION
LEVEL II SECURITY ENABLED
365 OPERATIONS
REDUNDANT & DIVERSIFIED
ADVANCED FIBER FACILITY
KnowledgePark.ca
THE FASTEST GROWING HIGH-TECH CLUSTER IN EASTERN CANADA

DAY 2: ACADEMIC PRESENTATIONS

THURSDAY, 28 AUGUST 2025

WU CONFERENCE CENTRE, 6 DUFFIE DRIVE

08:00	**Conference On-Site Registration**			
08:00	**Networking**			
08:45	**Toward Secure Federated Learning** Federated learning has emerged as a privacy-preserving solution enabling collaborative model training across distributed and sensitive data sources without direct data sharing. However, the decentralized and opaque nature of federated learning introduces new vulnerabilities to both model integrity and data privacy. In this keynote, I will explore the evolving threat landscape in federated learning, including poisoning, backdoors, inference, and model manipulation. I will walk through emerging threat models and cutting-edge defense techniques highlighting their promise and limitations. In this talk, I will present one of our recent works on securing federated learning systems. This talk will be of interest to researchers and practitioners working at the intersection of machine learning, cybersecurity, and distributed systems.			**Dr. Roozbeh Razavi-Far,** *Associate Professor, Canadian Institute for Cybersecurity, Faculty of Computer Science, University of New Brunswick*
09:45	**Nutrition Break & Research Poster Session**			
10:15	**In-Person Session PS6**	**In-Person Session PS7**	**Online Session OS4**	
11:55	**Lunch & Research Poster Session**			
13:00	**In-Person Session PS8**	**In-Person Session PS9**	**Online Session OS5**	
14:40	**Nutrition Break & Research Poster Session**			
15:10	**In-Person Session PS10**		**Online Session OS6**	
16:30	**Closing Remarks**			

10:15 – 11:55

In-Person Session PS6
Authentication and Trust Mechanisms

Room: Chancellor's Room
Chair: Dr. Vikas Chouhan, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 79: A Dynamic, Context-Aware Trust Model for Distributed Computing Environments
Authors: Divya Bansal, Sabrina Dhalla, Jaspal Kaur Saini

Paper ID 129: Stateless Decentralized Authentication Using Segmented ZKPs for Microservices Architectures
Authors: Vinh Quach, Ram Dantu, Sirisha Talapuru, Apurba Pokharel, Shakila Zaman

Paper ID 46: Dynamic Decentralized Social Trust for Financial Inclusion with Regulatory Compliance
Authors: Suzana Moreno, Alessandro Aldini, Seigneur Jean-Marc, Paul-Antoine Bisgambiglia

Paper ID 139: Verify All: Establish Bidirectional and Provable Trustworthiness in Microservices Architecture
Authors: Vinh Quach, Ram Dantu, Sirisha Talapuru, Indravadan Patel, Alexis Blackwell

Paper ID 157: Formal Specification and Verification of Protection in Transit (PIT) Protocol Using UPPAAL
Authors: Takwa Rhaimi, Hamed Aghayarzadeh, Rakesh Podder, Indrakshi Ray

In-Person Session PS7
Federated Learning and Privacy Techniques

Room: J. Harper Kent Auditorium
Chair: Dr. Mahdi Rabbani, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 10: Multilingual Phishing Email Detection Using Lightweight Federated Learning
Authors: Dakota Staples, Hung Cao, Saqib Hakak, Paul Cook

Paper ID 24: Privacy Preservation with Noise in Explainable AI
Authors: Sonal Allana, Rozita Dara

Paper ID 45: An Efficient and Privacy-Preserving AdaBoost Federated Learning Framework for AiP System
Authors: Zhuliang Jia, Rongxing Lu, Mohammad Mamun, Suprio Ray

Paper ID 65: SynQP: A Framework and Metrics for Evaluating the Quality and Privacy Risk of Synthetic Data
Authors: Bing Hu, Yixin Li, Asma Bahamyirou, Helen Chen

Online Session OS3
Authentication and Access Control

Room: Aitken Room
Chair: Dr. Mohammad Jafari Dehkordi, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 125: Short Training Techniques to Enhance Usability of System-Assigned PINs
Authors: Israt Jui, Amirali Salehi-Abari, Julie Thorpe

Paper ID 148: Securing Multi-Domain Systems: Intelligent ABAC Policy Learning for Cross-Domain Access Control
Authors: Asmita Biswas, Barsha Mitra, Iqbal Gondal, Qiang Fu

Paper ID 153: Enhancing Visual Speaker Authentication using Dynamic Lip Movement and Meta-Learning
Authors: Pooja Pathare, Garima Bajwa

Paper ID 144: Detecting Deepfakes using Temporal Consistency of Facial Expression Transitions
Authors: Renjith Eettickal Chacko, Garima Bajwa

Paper ID 53: Toward a Lexicon for Privacy, Security, and Trust: Analysing Digital Identity in Media using NLP
Authors: Matthew Comb, Andrew Martin

13:00 – 14:40

In-Person Session PS8

Deception Detection and Fact-Checking

Room: Chancellor's Room
Chair: Dr. Hossein Shokouhinejad, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 37: FactCellar: An Evidence-based Dataset for Automated Fact-Checking
Authors: Arbaaz Dharmavaram, Farrukh Bin Rashid, Saqib Hakak

Paper ID 38: An Intelligent Framework for Deceptive Review Detection Using Advanced Trust Vector Modeling
Authors: Lily Dey, Md Shopon, Marina L Gavrilova

Paper ID 88: From Birthday Cheers to Privacy Fears: Unraveling the Paradox of Social Media Celebrations in Nigeria
Authors: Victor Yisa, Rita Orji

Paper ID 124: LAID: Lightweight AI-Generated Image Detection in Spatial and Spectral Domains
Authors: Nicholas Chivaran, Jianbing Ni

Paper ID 132: Comparing Macro and Micro Approaches for Detecting Phishing Where It Spreads
Authors: Mina Erfan, Paula Branco, Guy-Vincent Jourdan

In-Person Session PS9

Secure Infrastructure and Access Control

Room: J. Harper Kent Auditorium
Chair: Dr. Mohammad Jafari Dehkordi, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 64: RF-RADS: A Robust Framework for Risk Assessment in Digital Substations
Authors: Mahdi Abrishami, Kwasi Boakye-Boateng, Hossein Shokouhinejad, Emmanuel Dana Buedi, Kishore Sreedharan, Shabnam Saderi Oskouei

Paper ID 76: Houdini: Benchmarking Container Security Confinement
Authors: Huzaifa Patel, David Barrera, Anil Somayaji

Paper ID 104: No Safety in Numbers: Traffic Analysis of Sealed-Sender Groups in Signal
Authors: Eric Brigham, Nicholas Hopper

Paper ID 131: An Integer Programming Formulation for Access Control Optimization Problems
Authors: Padmavathi Iyer

Online Session OS5

Cryptographic Methods and Security

Room: Aitken Room
Chair: Dr. Vikas Chouhan, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 68: Quantum Computing Threats to Management and Operational Safeguards of IEC 62351
Authors: Brian Goncalves, Arash Mahari, Atefeh Mashatan, Reza Arani, Marthe Kassouf

Paper ID 82: A Machine Learning-Based Framework for Assessing Cryptographic Indistinguishability of Lightweight Block Ciphers
Authors: Jimmy Dani, Kalyan Nakka, Nitesh Saxena

Paper ID 87: Encryption Struggles Persist: When Tech-Savvy Students Face Challenges with PGP in Thunderbird
Authors: Md Imanul Huq, Ahmed Tanvir Mahdad, Nitesh Saxena

Paper ID 119: GPU-Optimized Piecewise Linear Activations for Efficient and Secure Neural Networks
Authors: Hiba Guerrouache, Menat Allah Fadoua Slama, Yacine Challal, Karima Benatchba

Paper ID 145: Secret Sharing in 5G-MEC: Applicability for joint Security and Dependability
Authors: Thilina Pathirana, Ruxandra F. Olimid

15:10 – 16:30

In-Person Session PS10

Network Security and Adversarial Attacks

Room: Chancellor's Room
Chair: Dr. Hossein Shokouhinejad, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 36: RefPentester: A Knowledge-Informed Self-Reflective Penetration Testing Framework based on Large Language Models
Authors: Hanzheng Dai, Yuanliang Li, Jun Yan, Zhibo Zhang

Paper ID 86: DNS Profiler: Quantifying User Browsing Risk from DNS Traffic Patterns
Authors: Mahdi Firoozjaei, Yaser Baseri, Qing Tan

Paper ID 48: FragmentFool: Fragment-based Adversarial Perturbation for Graph Neural Network-based Vulnerability Detection
Authors: Muhammad Fakhrur Rozi, Tao Ban, Seiichi Ozawa, Hiroaki Inoue, Takeshi Takahashi, Sajaad Dadkah

Paper ID 156: Identifying and Addressing User-level Security Concerns in Smart Homes Using "Smaller" LLMs
Authors: Hafijul Hoque Chowdhury, Riad Ahmed Anonto, Sourov Jajodia, Suryadipta Majumdar, Md. Shohrab Hossain

Online Session OS6

Trust and Verification

Room: Aitken Room
Chair: Dr. Mahdi Rabbani, Research Scientist, Canadian Institute for Cybersecurity

Paper ID 16: TrollSleuth: Behavioral and Linguistic Fingerprinting of State-Sponsored Trolls
Authors: Havva Alizadeh Noughabi, Fattane Zarrinkalam, Abbas Yazdinejad, Ali Dehghantanha

Paper ID 71: Temporal-Spatial Feature Modification Attacks Against Machine Learning-Based Network Intrusion Detection Systems
Authors: Eeshan Walia, Sohini Pillay, Christopher Yoeurng, Dongfeng Fang, Shengjie Xu

Paper ID 80: G-STAR: A Threat Modeling Framework for General-Purpose AI Systems
Authors: Pulei Xiong, Saeedeh Lohrasbi, Prini Kotian, Scott Buffett

Paper ID 103: A Modeling and Static Analysis Approach for the Verification of Privacy and Safety Properties in Kotlin Android Apps
Authors: Bara Nazzal, James Cordy, Manar Alalfi

ACADEMIC KEYNOTE PRESENTERS

Dr. Sébastien Gambs

Canada Research Chair in Privacy-Preserving & Ethical Analysis of Big Data, UQAM

Sébastien Gambs has held the Canada Research Chair in Privacy and Ethical Analysis of Massive Data since December 2017 and has been a professor in the Department of Computer Science at the Université du Québec à Montréal since January 2016. His main research theme is privacy in the digital world. He is also interested in solving long-term scientific questions such as the existing tensions between massive data analysis and privacy as well as ethical issues such as fairness, transparency and algorithmic accountability raised by personalized systems.

Dr. Roozbeh Razavi-Far

Associate Professor, Canadian Institute for Cybersecurity, University of New Brunswick

Dr. Roozbeh Razavi-Far is an Associate Professor with the Canadian Institute for Cybersecurity, Faculty of Computer Science, University of New Brunswick. His research focuses on machine learning, adversarial machine learning, secure AI, big data analytics, computational intelligence, and cybersecurity of cyber-physical systems. He has authored or co-authored more than 170 papers in scholarly journals and international conferences. In 2024, Stanford listed him among the top two percent of most-cited researchers for the third consecutive year. He is the recipient of several awards and grants including NSERC-DG, NSERC-ECR, NBIF, USRG, MITACS, NCC R&D, and NSERC-PDF. He is an associate editor at several journals, including the Neurocomputing, Machine Learning and Knowledge Extraction, Machine Learning with Applications, Discover Artificial Intelligence, IEEE Transactions on Industrial Cyber-Physical Systems, and IEEE Access. He served as a guest editor and chair for several journals and peer-reviewed conferences, and the chapter chair of IEEE Computational Intelligence, and Systems, Man and Cybernetics Societies at Windsor Section.

Dr. Lingyu Wang

Professor of Computer Engineering, School of Engineering, UBC Okanagan

Dr. Lingyu Wang is a Professor of Computer Engineering in the School of Engineering at UBC Okanagan. Prior to joining UBC, he was a Professor in the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University. He held the NSERC/Ericsson Industrial Research Chair (IRC) in SDN/NFV Security between 2019 and 2024. He received his Ph.D. degree in Information Technology in 2006 from George Mason University, USA. His research interests include cloud computing security, SDN/NFV security, network security metrics, software security, and privacy. He has been the principal investigator of over four million dollars of research grants. He has co-authored seven books, six patents, and over 150 conference and journal articles, including many published at top security conferences/journals such as S&P, CCS, USENIX Security, NDSS, TOPS, TIFS, TDSC, JCS, etc. He was the recipient of several best (student) paper awards. He has (co-)supervised 50 graduate students, among whom 10 former Ph.D. students are currently holding academic positions. He has served on the editorial boards of IEEE Transactions on Dependable and Secure Computing (TDSC), Computers & Security, and Annals of Telecommunications (ANTE). He has also served as the program (co)-chair of seven international conferences and the technical program committee member of over 150 international conferences.

RESEARCH POSTERS

- **Toward Behavior-Based Detection of Impersonators in Virtual Metaverse Environments** *by Yoonjib Kim, Saqib Hakak, and Ali A. Ghorbani.*

- **Towards Enhanced Graph Neural Network Based Explanations for Malware Detection** *by Hossein Shokouhinejad, Griffin Higgins, Roozbeh Razavi-Far, Hesamodin Mohammadian and Ali A. Ghorbani.*

- **Evaluating Generative Reasoning Models for Credential Tweaking and Lightweight Client-Side Defense in IoT Ecosystems** *by Erika Thea Hernandez Ajes, Mahdi Rabbani, Zeynab Anbiaee, Rongxing Lu, Sajjad Dadkhah, and Ali Ghorbani.*

- **Toward Quantum-Safe Cryptography: Algorithmic Risk Assessment and Solutions** *by Vikas Chouhan, Vahid Maleki Raee, Amir Hassanpour Zarghani, Michael Odartei Mills, Arun Kaniyamattam, and Ali Ghorbani.*

- **AI-Driven Post-Quantum Malware Detection** *by Michael Odartei Mills, Vahid Maleki Raee, Amir Hassanpour Zarghani, Arun Kaniyamattam, Vikas Chouhan and Ali Ghorbani.*

- **DataSense: A Real-Time Sensor-Based Benchmark Dataset for Attack Analysis in IIoT with Multi-Objective Feature Selection** *by Amir Firouzi, Sajjad Dadkhah, Sebin Abraham Maret, Ali A. Ghorbani.*

- **An Advanced Source Code Dataset for LLM Pre-training & Fine-tuning** *by Hamed Jelodar, Mohammad Meymani, Samita Bai, Parisa Hamedi, Tochukwu Emmanuel Nwankwo, and Roozbeh Razavi-Far.*

- **Enhancing Anonymity for Electric Vehicles in the ISO 15118 Plug-and-Charge** *by Nethmi Hettiarachchi, Kalikinkar Mandal, and Saqib Hakak.*

- **A Knowledge-Based Learning Framework for Phishing Email Detection Using Attention-Augmented BiLSTM** *by Morteza Eskandarain, Mahdi Rabbani, Arun Kaniyamattam, Fatemeh Nejati, Mansur Mirani, Gunjan Piya, Igor Opushnyev, Ali A. Ghorbani, and Sajjad Dadkhah.*

- **SAFEGrid: Secure Authenticated Framework for Energy Grid Automation** *by Shabnam Saderi Oskouei, Kalikinkar Mandal, and Ali. A Ghorbani.*

- **Privacy-Preserving Aggregation for Ethical ML: Splitting Data to Protect and Learn** *by Abhijat Sharma, and Kalikinkar Mandal.*

- **FactCellar — An AI-Driven Approach to Automated Fact-Checking** *by Arbaaz Dharmavaram, Farrukh Bin Rashid, and Saqib Hakak.*

- **LLM and MITRE framework** *by Kwasi Boakye-Boateng, Aviposh Bhan, and Htet Ko Naing.*

- **Adaptive Fingerprint-Based Intrusion and Device Recognition System for IoT via Optimized Multi-Task Learning** *by Ogobuchi Daniel Okey, Sajjad Dadkhah, Demõstenes Z. Rodriguez, and João H. Kleinschmidt.*

- **Cost of Confidentiality: Analyze Query Performance in Secure Enclave (Intel SGX)** *by Ankon Ghosh Argho, Suprio Ray, and Kalikinkar Mandal.*

- **Resilient by Design: Cybersecurity Challenges and Architecture for DER-Enabled Smart Grids** *by Nethmi Hettiarachchi, Shabnam Saderi Oskouei, Abhijat Sharma, Aymen Basli, and Kalikinkar Mandal.*

- **A Priority-Aware Task Scheduling Model for Efficient Network Utilization** *by Vahid Maleki Raee, Windhya Rankothge, Kwasi Boakye-Boateng, Mohammad Jafari Dehkordi, Aviposh Bhan, and Htet Ko Naing.*

- **Cybersecurity Compliance for Cloud-Based Collaborative Environments in Canadian Organizations** *by Windhya Rankothge, Hessam Mohammadian, Farrukh Bin Rashid, Erfan Ghiasvand, and Ali Ghorbani.*

CALL FOR PAPERS

www.pstnet.ca

23rd Annual International Conference on Privacy, Security & Trust

PST2026

August 26–28, 2026, Ottawa, Canada

(Hybrid) Technically co-sponsored by IEEE (TBD)

The 23rd Annual International Conference on Privacy, Security & Trust (PST2026) provides a premier forum for sharing advances in cybersecurity research and security applications. PST2026 will be held in Ottawa, Canada, and will offer one industry day followed by two days of keynotes and technical presentations focused on Privacy, Security, and Trust, along with a special track on Emerging Technologies and Trends. The hybrid format of PST2026 will allow authors who are unable travel to Canada to present their work remotely.

PST TECHNICAL SCOPE

Papers are invited which address new and previously unpublished results in Privacy, Security & Trust, as well as in the special theme and related topics.

- Access Control and Capability Delegation
- Anonymity and Privacy vs. Accountability
- Biometrics, National ID Cards, Identity Theft
- Cloud Security, Web Security and Privacy
- Critical Infrastructure Protection
- Cryptographic Technologies
- Digital Forensics
- Digital Rights Management
- Generative AI security, privacy, and trust
- Human Computer Interaction and PST
- Identity and Trust Management
- Implications of, and Technologies for, Lawful Surveillance
- Internet of Things (IoT) Security and Privacy
- Intrusion Detection / Prevention Technologies
- Network and Wireless Security
- Observations of PST in Practice, Society, Policy and Legislation
- Operating Systems Security
- Post-quantum cryptography
- Privacy Preserving / Enhancing Technologies
- Privacy, Traceability, and Anonymity
- PST Challenges in e-Services, e.g. e- Government, e-Commerce, e-Health
- Quantum Cryptography beyond QKD
- Quantum Key Distribution (QKD) Protocols
- Recommendation, Reputation and Delivery Technologies
- Secure Software Development and Architecture
- Security Analytics and Data Mining
- Security and Privacy Challenges in Blockchain and its Applications
- Trust and Reputation in Self-Organizing Environments
- Trust Technologies, Technologies for Building Trust in e-Business Strategy
- Zero-Day Vulnerabilities, Continuous Authentication

SUBMISSION GUIDELINES

High-quality submissions in all PST-related areas are solicited. Papers must not be under review or previously published or accepted elsewhere at the time of submission. Accepted papers will be published as either 'regular full' papers up to 10 pages, or 'short' papers of up to 6 pages including references and appendix. Authors MUST ensure to select the track (Privacy, Security, or Trust) or the special track most relevant to their research when submitting their paper. All submissions will be handled via EasyChair.

IMPORTANT DATES

Paper submission deadline: May 1, 2026

Final camera-ready paper due: July 3, 2026

Early-bird Registration ends: August 2, 2026

Notification of acceptance: June 1, 2026

Author Registration: July 3, 2026

Conference date: Aug 26–28, 2026

ORGANIZING COMMITTEE

- Conference General Chairs
  - Paria Shirani, University of Ottawa, Canada
  - Ali Ghorbani, University of New Brunswick, Canada
- Technical Program Chairs
  - Rongxing Lu, Queen's University, Canada
  - Suryadipta Majumdar, Concordia University, Canada
- Track Chairs
  - Privacy: Carlisle Adams, University of Ottawa, Canada; Alessandro Brighente, University of Padova, Italy
  - Security: Furkan Alaca, Queen's University, Canada; Paria Shirani, University of Ottawa, Canada
  - Trust: Lianying Zhao, Carleton University, Canada; Savio Sciancalepore, Eindhoven University of Technology, Netherlands
  - Special Track: Jun Yan, Concordia University, Canada; Yuhong Liu, Santa Clara University, USA
- Industry Day Chairs
  - Vio Onut, IBM, University of Ottawa, Canada;
  - Guy-Vincent Jourdan, University of Ottawa, Canada

JOURNAL SPECIAL ISSUES

Selected papers presented at PST2026 will be recommended (after a significant extension of 40% new material) for some special issues of SCI-indexed journals based on the topic suitability. Final acceptance will be subject to additional rounds of review conducted by the respective journal editors.

For registration and the most up-to-date conference information, please visit the PST2026 website or contact the conference office at **pst2026@easychair.org**.

FREDERICTON INDUSTRY DAY SUMMIT SPONSORS & SUPPORTERS

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

UNB EST. 1785 UNIVERSITY OF NEW BRUNSWICK | Canadian Institute for Cybersecurity

IEEE | IEEE COMPUTER SOCIETY

MIXER

KNOWLEDGE PARK

Canadian Institute for Cybersecurity
PRIVACY, SECURITY AND TRUST
INDUSTRY SUMMIT
RESEARCH POSTERS
1
1ST PLACE
Prize Value
$1,000 CAD
UNB | Canadian Institute for Cybersecurit
Privacy Security Trust

22nd Annual International Conference
on Privacy, Security & Trust

pstnet.ca

#PST2025