19th Annual International Conference on Privacy, Security & Trust

22 - 25 August 2022

Fredericton, New Brunswick, Canada.

pstnet.ca

#PST2022

Dr. Ali Ghorbani
Tier 1 Canada Research Chair in Cybersecurity

Professor and Director
Canadian Institute for Cybersecurity

WELCOME

On behalf of the organizing and technical program committees, we warmly welcome all of you to the 19th International Conference on Privacy, Security, and Trust (PST2022). PST2022 continues the tradition of bringing together researchers around the three themes of privacy, security, and trust, together with a new blockchain special theme to present their latest findings and discuss their results and application in practice. It has undoubtedly been a challenge arranging a conference of this scale while dealing with the global response to the COVID pandemic and the resultant uncertainties. While a physical, in-person conference was much preferred, we have successfully managed to make arrangements to hold this as a combination of an in-person Cybersecurity Industry Summit on August 22, a virtual main conference on August 23-24, and hybrid workshops on August 25 while still covering the intended topics.

The annual Privacy, Security, and Trust research conference has established itself as a leading international forum for the presentation and discussion of the latest challenges and solutions covering a wide range of related topics. This conference is unique in its broad approach, including examining the issues from both the research and practice perspectives. The conference encourages multidisciplinary research and fosters collaboration between academia, the private sector, and the government. Accordingly, our keynote speakers this year are experts over the range of our topics of interest and cover the spectrum from industry to academia to the public sector.

The conference encompasses industry and academic discussions with a balanced program covering various cybersecurity topics. The speakers include representatives from the industrial, government, and academic sectors. Conference participants will have the opportunity to hear leading experts and researchers present their research results, participate in three hybrid workshops, and view twenty-one thesis research posters related to real-world cybersecurity issues. The posters will be exhibited at the Fredericton Convention Centre during the Industry Summit and made available on the conference website for virtual attendees.

Thirty-one high-quality papers (including twenty-five regular papers and six short papers) were accepted for presentation on August 23-24 (GMT-3). Researchers will present their research results, which cover the spectrum of Privacy, Security and Trust, examining topics as diverse as network security, software security, IoT security, authentication and protocol security, malware analysis, security analytics, privacy-preserving computing, user's trust, privacy model, protocol and assessment, online social network privacy, cryptography, crypto-mining, and blockchain security.

We would like to thank Atlantic Canada Opportunities Agency (ACOA), IEEE New Brunswick Section, and Ignite Fredericton for their sponsorship. We are especially grateful to IEEE Computer Society for their continued support and technical co-sponsorship.

Naturally, an endeavour such as this can only be accomplished with dedicated and professional help. Many people contributed to the success of this conference. The dedicated members of the program committee coordinated the refereeing of all submitted papers. The referees assessed the scientific contents of the submitted papers; their dedication and efforts were irreplaceable in ensuring the quality of the accepted papers. We are also grateful to our technical and organizing committee members.

A big thank you to all those who have submitted their research papers, those who will be presenting their papers, 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
PST2022 General Chair
Fredericton, New Brunswick, Canada, August 2022

Xiaodong Lin[1] *and* **Rongxing Lu**[2]
PST2022 Technical Program Chairs
[1]University of Guelph, Canada
[2]Canadian Institute for Cybersecurity, University of New Brunswick, Canada.

Canadian Institute for Cybersecurity

A hub of cybersecurity innovation and talent development in Canada

CIC is 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 has played an integral role in cybersecurity research and innovation in Canada. Today, the University has the largest network security research group in the country and is well positioned to lead this effort through the Canadian Institute for Cybersecurity. The Institute is working with industry and governments to solidify Canada's position as a world-class cybersecurity hub for innovation and talent development.

TABLE OF CONTENTS

INDUSTRY SUMMIT PROGRAM

Monday 22 August 2022

07:45 - 08:30	**Registration, Networking, & Breakfast**	
08:30 - 08:45	**Welcoming Remarks by** • Dr. Ali Ghorbani, Conference General Chair • The Honourable Bill Hogan, Minister of Public Safety • Dr. Paul Mazerolle, University of New Brunswick President, and Vice Chancellor	
08:45 - 09:10	**Addressing Cybercrime in Canada through Law Enforcement collaboration, innovation, and partnerships.** Combatting cybercrime in 2022 and beyond requires unprecedented levels of law enforcement collaboration and pursuing innovative ways to reduce the impact on Canadian individuals, businesses, and organizations. Chris Lynam, who leads both the National Cybercrime Centre (NC3), and Canadian Anti-Fraud Centre (CAFC) will outline how these organizations are working with a range of partners and developing innovative approaches to enable Canadian law enforcement to tackle this ubiquitous threat.	**Chris Lynam,** *Director General National Cybercrime Coordination Unit, RCMP*
09:10 - 09:35	**Critical Infrastructure Security** Complex systems can be self-healing or so vulnerable as to be self-defeating. Critical infrastructure risk is a balance of security, emergency management, and business continuity, with very complex business and regulatory frameworks. Who gets the balance between economic output, risk, and societal interests right? And on the bad day, who can respond and recover best?	**Andrew Easton,** *Assistant Deputy Minister of Justice & Public Safety, Province of New Brunswick*
09:35 - 10:00	**The Road to 5G – Partnership & Collaboration** 5G is here. Enabling faster connectivity speeds, lower latency, and greater bandwidth, it's sparked the evolution of smart cities, e-sports, and augmented reality. With that comes rapid increases in complexity, scalability, and a new generation of cyber security threats. Leading the forefront of 5G in Canada requires a robust 5G ecosystem that brings research, academia, government, and the world's leading technology partners together from coast to coast.	**Greg Murray,** *SVP Information Security & CISO, Rogers Communications*
10:00 - 10:25	**From Sea to Sea: Mobilizing to Address Canada's Cybersecurity Needs** The Mastercard network handles billions in commerce every day, making it a vital part of the global economy. As such, cybersecurity is paramount, and failure is not an option. Canada is key to these efforts; Mastercard has established a global Intelligence and Cyber Centre of Excellence in Vancouver and is forging partnerships throughout the country to address labour force needs and improve cyber awareness in the digital economy, across Canada and around the world.	**Jennifer Sloan,** *Vice President Public Policy, Mastercard Canada*

10:25 - 10:35	**Nutrition Break**	
10:35 - 11:00	**Thinking Broadly About Privacy, Security and Trust in a Connected World** Privacy, security, and trust continues to play a critical role in traditional industry use cases such as banking but as our communities, our world and our universe become more connected bigger and broader thinking is needed. An expanded conversation about challenges and solutions in non-traditional use cases will provide insight to opportunities for new and existing technologies, applications, and collaborations in an increasingly connected world.	**Dr. Joel Martin,** *Chief Digital Research Officer, National Research Council*
11:00 - 11:25	**Confidence in AI systems — Can we trust AI-based systems?** AI-based systems have demonstrated impressive levels of effectiveness across a variety of application domains. As more and more applications come to rely on AI, we face the question of how to assess and improve the trustworthiness of AI-based systems in the presence of possible adversarial behaviour by some entities in those systems. In this talk, I will first give an overview of security and privacy considerations in AI-based systems, then give an overview of one such concern, ML model extraction, and finally, time permitting, discuss the challenges in simultaneously protecting against multiple ML security and privacy threats.	**Dr. N. Asokan,** *David R. Cheriton Chair in Software Systems, University of Waterloo*
11:25 - 11:50	**Supply Chain Risk – The weakest link** As the threat landscape continues to evolve, defending your networks may not be sufficient, as bad actors turn attention to our less-visible partners. Having a robust approach to managing supply chain risk is crucial for companies and organizations in today's interconnected and outsourced economy. Learn how Bell, Canada's largest communications company, frames the problem and manages supply chain risk.	**Rod Hynes,** *Director Information Security, Bell Canada Enterprise*
11:50 - 12:15	**Enabling a Secure and Digital Canada** The cyber threat landscape is rapidly evolving and over the past few years we have seen the rise in cyber threat activity from cybercriminals and state-sponsored actors. Please join Rajiv Gupta, Associate Head of the Canadian Centre for Cyber Security where he will discuss the threat landscape in Canada, and what we can do together to enhance cyber resilience to enable a secure digital Canada.	**Rajiv Gupta,** *Associate Head, Canadian Centre for Cyber Security*
12:25 - 13:00	**Lunch & Poster Session**	
13:00 - 13:25	**Prioritizing Risk to Mitigate Attacks on Public Cloud Deployed Workloads** Discussion around mitigation of attack paths have changed in cloud deployed workloads. Examples to show evaluating risk by potential data exposure, not just by vulnerability using identity and lateral movement as the primary defensive control.	**Sandy Bird,** *Co-founder & Chief Technology Officer, Sonrai Security*

13:25 - 13:50	**The cyber-resilience imperative: recent trends and future needs** This presentation will discuss why the current threat landscape calls for a rethinking of conventional cybersecurity paradigms to build more cyber-resilient systems and organizations. After having reviewed the fundamental differences between cybersecurity and cyber-resilience, I will examine the current state of adversarial innovation, the fragile posture of Canadian businesses, emerging cyber-resilience standards and regulations, platforms that enable the operationalization of cyber-resilience, and organizational biases that hinder cyber-resilience.	**Dr. Benoît Dupont,** *Canada Research Chair in Cybersecurity, Université de Montréal*
13:50 - 14:50	**Panel Discussion: Delivering on the Cybersecurity Talent Challenge** Almost all industries are struggling with a shortage of talent to meet demand; one of the larger gaps is in Cybersecurity. We are experiencing growing threats and breaches. Not surprisingly, boards and executives consider Cyber to be a #1 risk to their respective firms. Recent studies have estimated the current gap to be approximately 60,000 unfilled open positions in the United States and 2,200 in Ontario. Solving this gap will take coordinated efforts from all participants in the ecosystem: industry, government, education, and everything in between. This panel will bring to life the challenges, some success stories where progress is being made, remaining gaps in our future, and what more needs to be done collectively to meet these challenges.	**Jeff Henderson** *(Chair), CTO, Interac Corp.* **Adrienne O'Pray,** *Executive Director The McKenna Institute* **Elaine Hum,** *Cybersecurity Partnerships Director, Scotiabank* **Greg Murray,** *SVP Information Security & CISO, Rogers Communications* **Hugh Hicks,** *Talent and Partnership Development Manager, Canadian Institute for Cybersecurity* **Jane Rooney,** *Director Cyber Certification, Technology & Talent, Innovation, Science & Economic Development Canada*
14:50 - 15:00	**Nutrition Break**	
15:00 - 15:25	**Ahead of the Curve: Building on Canada's Trust Advantage** For many years, Canada has cemented it s position on the global stage as a leader in governance, privacy, and trust. With the onset of the COVID pandemic, Canada has emerged as one of few jurisdictions with the provenance to combine its governance, rule of law, diversity, and technology to create a foundation for technologically consistent trust platforms that allow for the effective linking, connecting, analysis and securitization of data ecosystems.	**Bill Tam,** *Co-founder & Chief Operating Officer, Digital Technology Supercluster.*

15:25 - 15:50	**Practical lessons from Zero Trust adoption** Zero trust is no longer a buzzword but a reality for many organizations modernizing Security as cyber threats continue to rise with increasing attack surface and evolving threat landscape. Zero trust is not just a product but a set of principles that require a holistic approach for adoption. In this session, we will discuss zero-trust client adoption patterns and share blueprints and best practices based on several deployments.	**Dr. Sridhar Muppidi,** IBM Fellow & Chief Technology Officer, IBM Security
15:50 - 16:15	**Recent Evolutions in Open Security** Since PST 2021, a number of high-impact changes have occurred in the landscape of Open Security. Join us as we explore recent innovations from entitles such as Splunk, AWS, the Open Cybersecurity Alliance, and the Open Network User Group, and more, as we explore how the "power of the crowd" is helping shift the balance of power back to the cybersecurity defender.	**Jason Keirstead,** Chief Technology Officer, IBM Security Threat Management
16:15 - 16:50	**Confidence in AI systems — Can we trust AI-based systems? CyberSecure Canada Certification Program by Jane Rooney** The Government has made significant investments in helping Canadian small and medium-sized enterprises (SMEs) enhance their cyber posture including through Innovation, Science and Economic Development Canada's (ISED) CyberSecure Canada certification program and its complementary e-learning series. CyberSecure Canada aims to raise the cyber security baseline among SMEs, increase consumer confidence in the digital economy, promote international standardization and better position SMEs to compete globally. This session will discuss the importance of adopting cyber security measures and potential impacts of weak cyber security posture and provide details about the CyberSecure Canada program that can help SMEs protect themselves from cyber threats. **Cyber Security Innovation Network Program by Hamza Khan** Demands on the digital economy continue to rapidly grow, and cyber security is an ever-increasing concern for Canadians and Canadian businesses. ISED's Cyber Security Innovation Network (CSIN) program is investing in a national collaborative cyber security network of academic and industry partners that will enhance cyber security R&D, increase commercialization, and develop skilled talent. This session will discuss the CSIN program's objectives to position Canada as a global leader in cyber security.	**Jane Rooney,** Director Cyber Certification, Technology & Talent, Innovation, Science & Economic Development Canada **& Hamza Khan,** Manager, Innovation, Science & Economic Development Canada
16:50 - 17:05	Master of Applied Cybersecurity, University of New Brunswick Capstone Project Presentations	Griffin Higgins & Michal Widomski
17:05 - 18:00	**Closing Remarks & Reception**	

Industry Day Keynote
SPEAKERS & PANELISTS

Dr. N. Asokan
David R. Cheriton Chair in Software Systems
University of Waterloo

Dr. N. Asokan has been a Professor of Computer Science at the University of Waterloo since 2019 where he holds a David R. Cheriton Chair and serves as the Executive Director of the Waterloo Cybersecurity and Privacy Institute. He is also an adjunct professor at Aalto University where he was the founding director of the Helsinki-Aalto Institute for Cybersecurity.

Sandy Bird
Co-founder & Chief Technology Officer
Sonrai Security

Sandy Bird is the co-founder and CTO of Sonrai Security, helping enterprises secure their data in the cloud. Sandy was the co-founder and CTO of Q1 Labs, which was acquired by IBM in 2011. At IBM, Sandy became the CTO for the global security business and worked closely with research, development, marketing, and sales to develop new and innovative solutions to help the IBM Security business grow to ~$2B in annual revenue.

Dr. Benoît Dupont
Canada Research Chair in Cybersecurity
Université de Montréal

Dr. Benoît Dupont is a Professor of Criminology at the Université de Montréal as well as the Canada Research Chair for Cybersecurity and the Research Chair for the Prevention of Cybercrime. Benoît serves as a Board Director of the Canadian Cyber Thread Exchange and as a member of CATAAlliance's Cybercrime Advisory Council. He researches the interactions between organizational and technological aspects of cybersecurity, including identity theft, bank fraud, information pirating, telecommunications fraud, and emerging cyber-security practices such as cyber-resilience.

Andrew Easton
Assistant Deputy
Minister of Justice & Public Safety
Province of New Brunswick

Andrew Easton is the Provincial Security Advisor for the Province of New Brunswick and the Assistant Deputy Minister of the Security and Emergencies Division of the Department of Justice and Public Safety. He leads the Office of the Provincial Security Advisor, along with the Emergency Measures, Community Capacity and Resiliency, and NB911 portfolios. Andrew holds a degree from Dalhousie University and Certificates in Executive Management from Queens University and National and International Security from Harvard Kennedy School.

Rajiv Gupta
Associate Head
Canadian Centre for Cyber Security

Rajiv Gupta is the Associate Head of the Canadian Centre for Cyber Security (the Cyber Centre). In this role, Rajiv is responsible for advancing the Cyber Centre's strategic vision to enable a secure digital Canada. Prior to this role, he was the Director General of Cyber Defence Capabilities. Rajiv holds a Bachelor of Arts degree and a Master's degree in Engineering. He is a Professional Engineer in the Province of Ontario.

Jeff Henderson
CTO
Interac Corp.

Jeff was recently appointed CTO at Interac Corp. Interac is one of the most trusted financial service brands in Canada, rooted in a deep history of innovation. Prior to this role, Jeff was a technology executive for 28 years at TD Bank, where he was EVP and Group CIO. With 3 active children under 20, Jeff's free time is primarily spent being integrated into their lives and volunteering.

Hugh Hicks
Talent and Partnership
Development Manager
Canadian Institute for Cybersecurity

Hugh Hicks holds a Master's in Business Administration from the University of New Brunswick. He has worked with Atlantic Canada Opportunities Agency. At the Agency, he has held various positions including Director in units such as Enterprise Development (working with private sector), Community Development (communities and not-for-profits), and on strategic initiatives through the Policy, Advocacy & Coordination unit. Most recently he managed a team focused on innovation and commercialization on key files that included smart grid, oceans, and cybersecurity.

Elaine Hum
Cybersecurity Partnerships Director
Scotiabank

Elaine Hum is Director, Cybersecurity Partnerships at Scotiabank, where she develops partnerships with academic and non-academic institutions for cybersecurity talent and innovation. Currently, she is also the Chair of the Talent Management Working Group for the Canadian Financial Services Cybersecurity Governance Council. She is also a coach for the Scotiabank Ignition Program, a STEM recent graduate rotation program for Technology.

Rod Hynes

Director Information Security
Bell Canada Enterprise

Rod has provided strategic and thought leadership at Bell Canada for 20+ years, specializing in IT, Network, and Information Security. Prior to Rod's current role leading the Cyber strategy, architecture, Governance, and compliance functions across BCE Inc., he was responsible for the evolution, operations and security of Bell Canada's Corporate network and telecom infrastructure.

Jason Keirstead

Chief Technology Officer
IBM Security Threat Management

Jason Keirstead is an IBM Distinguished Engineer and the CTO of Threat Management for IBM Security, where he is responsible for the design and development of products that span the threat management lifecycle from threat detection and investigation through to response. Jason has been involved in open technology for decades, contributing to and serving as maintainer of several major open-source projects over the years.

Hamza Khan

Manager
Innovation, Science & Economic Development Canada

Hamza Khan is a Manager in the Science Research Sector at Innovation, Science and Economic Development Canada responsible for the development and implementation of the Cyber Security Innovation Network. Hamza previously worked as Financial Manager in the Science Research Sector and prior to that held various finance roles in the federal government. Hamza has an undergraduate degree from the University of Ottawa and is a Chartered Professional Accountant (CPA, CMA).

Chris Lynam

Director General National Cybercrime
Coordination Unit, RCMP

Chris Lynam is currently the Director General of the National Cybercrime Coordination Unit and Canadian Anti-Fraud Centre within the Royal Canadian Mounted Police. He previously worked for Public Safety Canada and within the Security and Intelligence Secretariat of the Privy Council Office. Outside the RCMP, he is a member of the Army Reserve and previously served as the Lieutenant-Colonel Commanding of the Governor General's Foot Guards, an Infantry Regiment based in Ottawa.

Dr. Joel Martin

Chief Digital Research Officer
National Research Council

Dr. Joel Martin is the NRC's Chief Digital Research Officer and Chief Science Officer. He holds a Ph.D. in Computer Science, Machine Learning, from the Georgia Institute of Technology and completed postdoctoral studies at the University of Pittsburgh. Since joining the NRC in 1994, he has been a researcher and served in multiple leadership roles in the Digital Technologies Research Centre.

Dr. Sridhar Muppidi

IBM Fellow & Chief Technology Officer
IBM Security

Dr. Sridhar Muppidi is an IBM Fellow and CTO for IBM Security. He has a Ph.D. in Computer Science from Texas A&M University and serves on TAMU's board of directors. He is responsible for driving the technical strategy, architecture, and research for IBM Security's portfolio of products and services to help clients manage defenses against threats and protect digital assets. Sridhar is an IBM Master inventor with 60+ issued patents.

Greg Murray
SVP Information Security & CISO
Rogers Communications

Greg Murray is an Internationally experienced executive with more than 25 years in technology across various industries. Greg has a proven track record of successfully delivering transformational, business oriented, and risk reducing technological business solutions. Greg also leads the Rogers technology organization's Inclusion and Diversity Program and Committee at Rogers Technology. Greg is a graduate of University of Toronto and Athabasca University, as well as the ICD.D designations from the Institute of Corporate Directors.

Adrienne O'Pray
Executive Director
The McKenna Institute

Adrienne brings deep leadership experience and a passion for economic and social development in New Brunswick to her role at the helm of the McKenna Institute. She holds an MBA from the University of New Brunswick and a BSc from Dalhousie University. Adrienne has more than 25 years in senior management positions in the public and private sectors and has served as president and CEO of the New Brunswick Business Council and COO of Atlantic Lottery Corp.

Jane Rooney
Director Cyber Certification,
Technology & Talent
Innovation, Science & Economic
Development Canada

Jane oversees four digital inclusion programs aimed at providing Canadians the necessary access, tools, and skills to participate in the digital economy, as well as the CyberSecure Canada program that supports small and medium sized organizations better understand cyber security and improve their cyber posture. Prior to this role, Jane gained more than 25 years experience in the financial services regulatory environment, including almost 20 years at the Financial Consumer Agency of Canada.

Jennifer M. Sloan
Vice President of Public Policy
Mastercard Canada

Jennifer Sloan leads the development and management of the company's public affairs and government relations programs. She is also the North America Region Lead for Mastercard's Women's Leadership Network. In 2019, Jennifer was recognized with Mastercard's North America President's Award and the Mastercard CEO Force for Good Award. Jennifer has a Bachelor of Arts degree in journalism from the University of Georgia in Athens, Georgia.

Bill Tam
Co-founder & Chief Operating Officer
Digital Technology Supercluster

Bill Tam is recognized as one of the pre-eminent leaders of the British Columbia tech sector. He is the co-founder and COO of the Digital Technology Supercluster, a $950-million initiative by the Government of Canada, to develop and scale high-potential technologies in Canada. He earned his MBA from Western University and his Bachelor of Electrical Engineering (Summa Cum Laude) from McGill University.

ORGANIZING Committees

Steering Committee:

Ali Ghorbani (Conference General Chair),
CIC, University of New Brunswick, Canada

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

Mourad Debbabi,
Concordia University, Canada

Nora Cuppens,
Télécom Bretagne, France

Patrick McDaniel,
Penn. State University, USA

Stephen Marsh,
University of Ontario Institute of Technology, Canada

Hossein Sarrafzadeh,
North Carolina Agricultural and Technical State University, USA

Ken Barker,
University of Calgary, Canada

Ali Miri,
Ryerson University, Canada

Sakir Zincir,
Queen's University, UK

Technical Committee:

Xiaodong Lin (Co-Chair),
University of Guelph, Canada

Rongxing Lu (Co-Chair),
CIC, University of New Brunswick, Canada

Atefeh Mashatan (Privacy Track),
Toronto Metropolitan University, Canada

Yuanxiong Guo (Privacy Track),
University of Texas at San Antonio, USA

Suryadipta Majumdar (Security Track),
Concordia University, Canada

Beibei Li (Security Track),
Sichuan University, China

Abdulrahman Alamer (Trust Track),
Jazan University, SA

Weizhi Meng (Trust Track),
Technical University of Denmark, Denmark

Vojislav Misic (Special Session, Blockchain),
Toronto Metropolitan University, Canada

Zongyang Zhang (Special Session, Blockchain),
Beihang University, China

Local Organizing Committee:

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

Windhya Hansinie Rankothge (Local Organizing Chair),
CIC, University of New Brunswick, Canada

Rongxing Lu (Academic Program),
CIC, University of New Brunswick, Canada

Asma Sormeily (Web Chair),
CIC, University of New Brunswick, Canada

Awele Oguejiofor (Marketing & Publicity),
CIC, University of New Brunswick, Canada

Haruna Isah (Publication Chair),
CIC, University of New Brunswick, Canada

Mohamed Badawy (Technical),
CIC, University of New Brunswick, Canada

Pamela Kitchen (Industry Liaison),
CIC, University of New Brunswick, Canada

Ruth M. Murgatroyd (Secretary),
CIC, University of New Brunswick, Canada

Xichen Zhang (Workshop),
CIC, University of New Brunswick, Canada

Plus, the 98 members of the Technical Program Committee.

ACADEMIC DAY PROGRAM - DAY 1

Tuesday, 23 August 2022

08:50 - 09:00	**Welcome Remarks**	
09:00 09:50 ~~08:45~~ - ~~09:10~~	**Keynote: Extraction of Complex DNN Models: Real Threat or Boogeyman** The success of deep learning in many application domains has been nothing short of dramatic. The success has brought the spotlight onto security and privacy concerns with deep learning. One of them is the threat of "model extraction": when a machine learning model is made available to customers via an inference interface, a malicious customer can use repeated queries to this interface and use the information gained to construct a surrogate model. In this talk, I will describe our work in exploring whether model extraction constitutes a realistic threat. I will also discuss possible countermeasures, focussing on deterrence mechanisms that allow for the verification of ownership of ML models. Finally, I will touch on the issue of conflicts that arise when protection mechanisms for multiple different threats need to be applied simultaneously to a given ML model, using ownership verification techniques as a case study.	**Dr. N. Asokan,** *David R. Cheriton Chair in Software Systems, University of Waterloo* *Chair:* **Xiaodong Lin**
09:50 - 10:00	**Break**	
10:00 - 11:20	1. *Efficient Homomorphic E-Voting Based on Batch Proof Techniques* , Kun Peng 2. *A Secure and Privacy-Preserving Dynamic Aggregation Mechanism for V2G System* Xiaodong Qu, Qinglei Kong, Feng Yin, and Lexi Xu 3. *A Vulnerability in Face Anonymization – Privacy Disclosure from Face-obfuscated video* Hiroaki Kikuchi, Shun Miyoshi, Takafumi Mori, and Andres Hernandez-Matamoros 4. *LOG-OFF: A Novel Behavior Based Authentication Compromise Detection Approach* Mingchang Liu, Vinay Sachidananda, Hongyi Peng, Rajendra Patil, Sivaanandh Muneeswaran, and Mohan Gurusamy	*Chair:* **Xichen Zhang**

11:20 - 11:30	**Break**	
11:30 - 12:50	1. *Balancing privacy and accountability in digital payment methods using zk-SNARKs* Tariq Bontekoe, Maarten Everts, and Andreas Peter 2. *Discovering Non-Metadata Contaminant Features in Intrusion Detection Datasets* Laurens D'Hooge, Miel Verkerken, Bruno Volckaert, Tim Wauters, and Filip De Turck 3. *Security Analysis in Satellite Communication based on Geostationary Orbit* Jacob Krabbe Pedersen, Mikkel Bøchman, and Weizhi Meng 4. *Solving the Kidney Exchange Problem using Privacy-Preserving Integer Programming* Malte Breuer, Pascal Hein, Leonardo Pompe, Ben Temme, Ulrike Meyer, and Susanne Wetzel	*Chair:* **Yunguo Guan**
12:50 - 14:00	**Lunch Break**	
14:00 - 14:50	**Keynote: Unified View of IoT and CPS and Trend of Research on Microcontroller Based IoT** In this talk, I will first present a unified view of Internet of Things (IoT) and Cyber Physical Systems (CPS), and then discuss the trend of research on microcontroller (MCU) based IoT systems. From the perspective of network topologies and structures, IoT and CPS are similar. IoT devices and CPS field devices are controlled by particular types of actuators and controllers. The controllers have the networking functionality, connecting the devices to particular types of local area networks (LANs), which may use proprietary protocols. The LANs may be connected to the Internet so that administrators may access the devices remotely. Particular servers may be installed in LANs or on the Internet facilitating remote control. We will use a smart plug system as an IoT example and smart building as an example CPS to demonstrate the unified view of IoT and CPS. There is a broad spectrum of IoT devices. We can divide them into two categories: powerful microprocessor based IoT systems that can run powerful operating systems (OSs) such as Linux; low-power MCU based IoT systems that often do not run any OS or have limited OS support such as FreeRTOS. We will present an overview of MCU based IoT research from five aspects, including hardware, OS, software, networking, and data, and discuss the trend of research in those fields.	**Dr. Xinwen Fu,** *Professor, University of Massachusetts Lowell* *Chair:* **Xiaodong Lin**
14:50 - 15:00	**Break**	
15:00 - 16:20	1. *Mobile Mental Health Apps: Alternative Intervention or Intrusion?* Shalini Saini, Dhiral Panjwani, and Nitesh Saxena 2. *An Efficient, Verifiable, and Dynamic Searchable Symmetric Encryption with Forward Privacy* Khosro Salmani	*Chair:* **Songnian Zhang**

15:00 - 16:20	3. *A Feistel Network-based Prefix-Preserving Anonymization Approach, Applied to Network Traces* Shaveta Dandyan, Habib Louafi, and Samira Sadaoui 4. *Visualizing and Reasoning about Presentable Digital Forensic Evidence with Knowledge Graphs* Weifeng Xu and Dianxiang Xu	*Chair:* **Songnian Zhang**
16:20 - 16:30	**Break**	
16:30 - 17:50	1. *Towards the development of a realistic multidimensional IoT profiling dataset* Sajjad Dadkhah, Hassan Mahdikhan, Priscilla Kyei Danso, Alireza Zohourian, and Kevin Anh Truong 2. *Privacy Policy Analysis with Sentence Classification* Andrick Adhikari, Sanchari Das and Rinku Dewri 3. *Efficient and Privacy-preserving Worker Selection in Mobile Crowdsensing Over Tentative Future Trajectories* Xichen Zhang, Songnian Zhang, Suprio Ray and Ali A. Ghorbani 4. *Privacy-Preserving Detection of Poisoning Attacks in Federated Learning* Trent Muhr and Wensheng Zhang	*Chair:* **Xichen Zhang**
17:50 - 18:00	**Closing Remarks**	

KEYNOTE SPEAKERS

Dr. N. Asokan

David R. Cheriton Chair in Software Systems, University of Waterloo

Dr. N. Asokan is a Professor of Computer Science at the University of Waterloo where he holds a David R. Cheriton Chair and serves as the Executive Director of the Waterloo Cybersecurity and Privacy Institute. He is also an adjunct professor at Aalto University where he was the founding director of the Helsinki-Aalto Institute for Cybersecurity. He was a Professor of Computer Science at Aalto University from 2013 to 2019 and at the University of Helsinki from 2012 to 2017. Between 1995 and 2012, he worked in industrial research laboratories designing and building secure systems, first at the IBM Zurich Research Laboratory as a Research Staff Member and then at Nokia Research Center, most recently as Distinguished Researcher. Dr. Asokan's primary research theme is systems security broadly, including topics like the development and use of novel platform security features, applying cryptographic techniques to design secure protocols for distributed systems, applying machine learning techniques to security/ privacy problems, and understanding/ addressing the security and privacy of machine learning applications themselves.

Dr. Xinwen Fu

Professor, University of Massachusetts Lowell

Dr. Xinwen Fu is a Professor in the Department of Computer Science at the University of Massachusetts Lowell. Previously, he was a tenured Associate Professor at University of Central Florida. His current research interests are in computer and network security and privacy. Dr. Fu has published at prestigious conferences including the four top computer security conferences (Oakland, CCS, USENIX Security, and NDSS), and journals such as ACM/ IEEE Transactions on Networking and IEEE Transactions on Dependable and Secure Computing. He spoke at various technical security conferences including Black Hat. Various media has reported on his research including CNN, Wired, Huffington Post, Forbes, Yahoo, MIT Technology Review, PC Magazine and aired on CNN Domestic and International and the State Science and Education Channel of China (CCTV 10).

ACADEMIC DAY PROGRAM - DAY 2

Wednesday, 24 August 2022

09:00 - 09:50	**Keynote: The Dumbo Protocol Family: Making Asynchronous Consensus Real** Asynchronous consensus is the most robust (assuming least trust on underlying network conditions) consensus protocol, thus critical for blockchains deployed over the open Internet. Unfortunately, all previous protocols suffer from high complexity and essentially none has been widely deployed. In this talk, we will give an overview of a sequence of our recent results of Dumbo protocols on pushing asynchronous BFT consensus to the optimal complexity, and finally, real.	**Dr. Qiang Tang,** *Senior Lecturer,* *University of Sydney* *Chair:* **Rongxing Lu**
09:50 - 10:00	**Break**	
10:00 - 11:20	1. *Quantitative Risk Assessment of Threats on SCADA Systems Using Attack Countermeasure Tree* Xueqin Gao, Tao Shang, Da Li, and Jianwei Liu 2. *Faceless: A Cross-Platform Private Payment scheme for Human-Readable Identifiers* Huang Lin 3. *Achieving Efficient and Secure Query in Blockchain-based Traceability Systems* Chengzhe Lai and Yinzhen Wang 4. *User Behavior Simulation in ICS Cyber Ranges* Chuhan Liu, Wei Yan, Fengkai Xu, Wenlong Yang, and Beibei Li	*Chair:* **Cheng Huang**
11:20 - 11:30	**Break**	

11:30 - 12:50	1. *SATAn: Air-Gap Exfiltration Attack via Radio Signals from SATA Cables* Mordechai Guri 2. *An Efficient and Privacy-Preserving Range Query over Encrypted Cloud Data* Wentao Wang, Yuxuan Jin, and Bin Cao 3. *Designing In-Air Hand Gesture-based User Authentication System via Convex Hul*l Yiming Sun, Weizhi Meng, and Wenjuan Li 4. *Content Analysis of Privacy Policies Before and After GDPR* Nastaran Bateni, Rozita Dara, Jasmin Kaur, and Fei Song	*Chair:* **Yunguo Guan**
12:50 - 14:00	**Lunch Break**	
14:00 - 14:50	**Keynote: "You keep using that word. I do not think it means what you think it means." (Inigo Montoya)** We have come a long way, haven't we? 30 years ago, this summer, the first article on Computational Trust was published and presented in a small Multi-Agent Systems workshop in Italy. At which point lots of interesting things began to happen, for many different reasons, perhaps the biggest of which was the arrival of the public Internet and the Web. The result? Not really what I expected! Multiple models, plenty of applications (perhaps there's a link between the two?!), increased understanding perhaps, increased complexity certainly, and now a bunch of thoughts about AI. And security. Some time ago, Dieter Gollmann pointed out that trust was 'an absolute mess' and was not the unifying theme for security people seem to think it is (or was). Maybe. Probably. But don't vendors love to tell us we can trust their systems? Isn't it lovely when we can look at trust-marks, or reviews, or reputation, and other more violent means of controlling people. Like social credit, for example. Here's the thing: 'trust' is so overloaded a term as to be useless, so it's probably time to figure out what on earth we are talking about when we are talking about trust. Because, as we all know, Inigo Montoya was right.	**Dr. Stephen Marsh,** *Associate Professor of Trust Systems, Ontario Tech University* *Chair:* **Rongxing Lu**
14:50 - 15:00	**Break**	
15:00 - 16:20	1. *An Analytical Study of Selfish Mining Attacks on Chainweb Blockchain* Suyang Wang, Bo Yin, Shuai Zhang, and Yu Cheng 2. *Collaborative DDoS Detection in Distributed Multi-Tenant IoT using Federated Learning* Euclides Neto and Sajjad Dadkhah 3. *Careful What You Wish For: on the Extraction of Adversarially Trained Model*s Kacem Khaled, Gabriela Nicolescu, and Felipe Gohring de Magalhães 4. *Human Brains Can't Detect Fake News: A Neuro-Cognitive Study of Textual Disinformation Susceptibility* Cagri Arisoy, Anuradha Mandal, and Nitesh Saxena	*Chair:* **Songnian Zhang**
16:20 - 16:30	**Break**	

16:30 - 17:30	1. *Garage Door Openers: A Rolling Code Protocol Case Study* Ahmed Ghanem and Riham Altawy 2. *Usability of Paper Audit Trails in Electronic Voting Machines* Saul Hughes and Sana Maqsood 3. *A Semantic-based Approach to Reduce the Reading Time of Privacy Policies* Jasmin Kaur, Rozita Dara, and Ritu Chaturvedi	*Chair:* **Cheng Huang**
17:30-17:40	**Closing Remarks**	

KEYNOTE SPEAKERS

Dr. Stephen Marsh
Associate Professor of Trust Systems, Ontario Tech University

Dr. Stephen Marsh is an Associate Professor of Trust Systems at Ontario Tech University. His research expertise covers areas as diverse as human-computer interaction, wisdom, trust, regret, forgiveness, energy management, hope, privacy, communications security, socially adept technology, and democracy. He is currently examining Trustworthy AI from the perspective of AI trusting people as well as the other way around. His seminal work on Computational Trust brought together disciplines of cognitive science, psychology, philosophy, sociology, and computational sciences, founded a new research field in Computational Trust, and has continued to influence the field for almost three decades. Steve lives on a nano-farm in Eastern Ontario, from where he builds stuff, teaches, makes music, draws, writes (Trust Systems the textbook is freely available as an Open Educational Resource), blogs occasionally, and shares life with people, dogs, cats, horses, a pig, sheep, goats, chickens, and lizards. He quite possibly also has bats in the belfry.

Dr. Qiang Tang
Senior Lecturer, University of Sydney

Dr. Qiang Tang is currently Senior Lecturer (equal to U.S. Associate Professor) at the University of Sydney. From 2016 - 2020, he was an assistant professor at New Jersey Institute of Technology and director of JD-NJIT-ISCAS Joint Blockchain Research Lab. Before joining NJIT, he was a postdoc at Cornell. His research spans broadly on theoretical and applied cryptography, and blockchain technology, and his work appeared mostly in top security/crypto/distributed computing venues such as Crypto, Eurocrypt, Asiacrypt, TCC, CCS, USENIX Sec, NDSS, PODC and others. He won a few prestigious awards including MIT Technical Review 35 Chinese Innovators under thirty-five, Google Faculty Award, NJIT Research Award, and more. His research is supported by various federal agencies and big tech, as well as leading blockchain foundations including Ethereum, Stellar, Filecoin, Algorand, and more.

CONFERENCE RESEARCH

Posters

Twenty-one posters discussing research projects related to real-world cybersecurity issues will be also displayed at the Cybersecurity Industry Summit and will be made available on the conference website.

- **Achieving Efficient and Privacy-Preserving Dynamic Skyline Query in Online Medical Diagnosis** *by Songnian Zhang, Suprio Ray, Rongxing Lu, Yandong Zheng, Yunguo Guan, and Jun Shao*
- **Achieving Privacy-Preserving Secure Electric Vehicle and Charging Stations** *by Soheil Shirvani and Professor A. Ghorbani*
- **An Effective Approach for Adversarial Attack on Deep Learning-based Network Intrusion Detection Systems** *by Hesamodin Mohammadian, Ali Ghorbani, and Arash Habibi Lashkari*
- **Converged Security for Supply Chains** *by Rashid Khokhar, Windhya Rankothge, Leila Rashidi, and Hessam Mohammadian*
- **DGL22: An efficient Measurement-Device-Independent Quantum Key Distribution Scheme** *by Mohammed Al-Darwbi, Ali Ghorbani, and Arash Lashkari*
- **Early Fake New Detection** *by Bahman Jamshidi and Saqib Hakak*
- **Efficient and Privacy-preserving Federated Learning-based approach for next word prediction** *by Amir Firouzi*
- **Efficient Privacy-Preserving Federated Learning** *by Hadiseh Izadi Yekta and Rongxing Lu*
- **Ensemble-based Intrusion Detection for Internet of Things devices** *by Priscilla Kyei Danso, Alireza Zohourian, Sajjad Dadkhah, Euclides Carlos Pinto Neto, and Ali Ghorbani*
- **EVRQ: Achieving Efficient and Verifiable Range Query over Encrypted Traffic Data** *by Yunguo Guan, Pulei Xiong, and Rongxing Lu*
- **Identifying Malicious Actors: Windows Malware Code Signing** *by Michal Widomski and Kalikinkar Mandal*
- **Improve Credibility and Security in Data Exchange in Internet of Vehicle (IoV) Network** *by Hamideh Taslimasa and Euclides Carlos Pinto Neto*
- **IoT Network Monitoring using IoT Device Profiling, Fingerprinting, and Identification** *by Alireza Zohourian, Sajjad Dadkhah, and Euclides Carlos Pinto Neto*
- **IoT systems attack detection using provenance graphs** *by Erfan Ghiasvand, Dr. Suprio Ray, and Dr. Ali Ghorbani*
- **Label Noise Detection in IoT Security based on Decision Tree and Active Learning** *by Mahdi Abrishami, Sajjad Dadkhah, Euclides Carlos Pinto Neto, and Ali Ghorbani*
- **Leveraging Partial Propagation Cascades and News Content for Fake News Early Detection on Social Media** *by Asma Sormeily and Xichen Zhang*
- **Preventing Proof-of-Work Mining Attacks** *by Hamid Azimy, Ali Ghorbani, and Ebrahim Bagheri*
- **Reasoning for fake news detection through few-shot prompting** *by Mohammadamin Kanaani and Xichen Zhang*
- **Rethinking MITRE ATT&CK data Visualization** *by Griffin Higgins and Haruna Isah*
- **Towards Malware Packers Identification** *by Ehab M. Alkhateeb, Ali Ghorbani, and Arash Habibi*
- **ZTSGrid: A Zero-trust Approach for the SCADA System in the Smart Grid** *by Gaurav Uttarkar, Oyonika Samazder, Shabnam Saderi, and Kalikinkar Mandal*

HYBRID WORKSHOP SESSION

Thursday, 25 August 2022

QUANTUM COMPUTING: INTRODUCTION, SECURITY RISK, & MIGRATION

- *Introduction of Quantum Computing*
- *Security Risks in Quantum Computing*
- *Migration Strategy & Recommendations*

10:00 - 12:00

Mohammed Yahya Al-Darwbi
Ph.D. Candidate, Canadian Institute for Cybersecurity

Dr. Yaser Baseri
Cybersecurity Researcher, Canadian Institute for Cybersecurity

SUBSTATION SIMULATION: ATTACKS & TESTBED SETUP

- *Different Types of Attacks for Smart Grids*
- *Introduction on Substation and Testbeds*
- *Demos on Attacks and Testbed Setups*

13:00 - 15:00

Kwasi Boakye-Boateng
Ph.D. Candidate, Canadian Institute for Cybersecurity

Dr. Ratinder Kaur
Cybersecurity Researcher Cyber Defense

UNDERSTANDING SOCIAL ENGINEERING & ETHICAL HACKING

- *Human Factors in Cybersecurity*
- *Social Engineering Framework and Tools*
- *Practical Ethical Hacking*

15:00 - 17:00

Dr. Haruna Isah
Research Associate, Canadian Institute for Cybersecurity

Dr. Xichen Zhang
Research Scientist, Canadian Institute for Cybersecurity

CALL FOR PAPERS

www.pstnet.ca

20th Annual International Conference on Privacy, Security & Trust

PST2023

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.

CONFERENCE SPONSORS

Atlantic Canada
Opportunities
Agency

Agence de
promotion économique
du Canada atlantique

Canada

IGNITE

IEEE New Brunswick Section

TECHNICAL CO-SPONSORS

IEEE
computer
society

UNB
EST. 1785
UNIVERSITY OF NEW BRUNSWICK

Canadian
Institute for
Cybersecurity

IEEE

IEEE and its members inspire a global community to innovate for a better tomorrow through highly cited publications, conferences, technology standards, and professional and educational activities. IEEE is the trusted "voice" for engineering, computing, and technology information around the globe.

19th Annual International Conference
on Privacy, Security & Trust

pstnet.ca

#PST2022