19th Annual International Conference on Privacy, Security and Trust

Virtual Conference, Fredericton, GMT-3, 22-24 August 2022

PST 2022 TECHNICAL PROGRAM-AT-A-GLANCE (Main Conference)

Aug. 23, 2022, Fredericton **Aug. 23, 2022, Toronto**

(GMT-3) Time in Fredericton, Canada	(GMT-4) Time in Toronto, Canada	
8:50 am – 9:00 am, Aug. 23	7:50 am – 8:00 am, Aug. 23	Welcome Remarks
9:00 am – 9:50 am, Aug. 23	8:00 am – 8:50 am, Aug. 23	Keynote 1: Chair:
9:50 am – 10:00 am, Aug. 23	8:50 am – 9:00 am, Aug. 23	Short Break
10:00 am – 11:20 am, Aug. 23	9:00 am – 10:20 am, Aug. 23	Session 1 (4 papers) Chair:
11:20 am – 11:30 am, Aug. 23	10:20 am – 11:30 am, Aug. 23	Short Break
11:30 am – 12:50 pm, Aug. 23	10:30 am – 11:50 am, Aug. 23	Session 2 (4 papers) Chair:
12:50 am – 14:00 pm, Aug. 23	11:50 am – 13:00 pm, Aug. 23	Lunch Break
14:00 pm – 14:50 pm, Aug. 23	13:00 pm – 13:50 pm, Aug. 23	Keynote 2: Chair:
14:50 pm – 15:00 pm, Aug. 23	13:50 pm – 14:00 pm, Aug. 23	Short Break
15:00 pm – 16:20 pm, Aug. 23	14:00 pm – 15:20 pm, Aug. 23	Session 3 (4 papers) Chair:
16:20 pm – 16:30 pm, Aug. 23	15:20 pm – 15:30 pm, Aug. 23	Short Break
16:30 pm – 17:50 pm, Aug. 23	15:30 pm – 16:50 pm, Aug. 23	Session 4 (4 papers) Chair:
17:50 pm – 18:00 pm, Aug. 23	16:50 pm – 17:00 pm, Aug. 23	Closing Remarks

Aug. 24, 2022, Fredericton **Aug. 24, 2022, Toronto**

(GMT-3) Time in Fredericton, Canada	(GMT-4) Time in Toronto, Canada	
9:00 am – 9:50 am, Aug. 24	8:00 am – 8:50 am, Aug. 24	Keynote 3: Chair:
9:50 am – 10:00 am, Aug. 24	8:50 am – 9:00 am, Aug. 24	Short Break
10:00 am – 11:20 am, Aug. 24	9:00 am – 10:20 am, Aug. 24	Session 5 (4 papers) Chair:
11:20 am – 11:30 am, Aug. 24	10:20 am – 10:30 am, Aug. 24	Short Break
11:30 am – 12:50 am, Aug. 24	10:30 am – 11:50 am, Aug. 24	Session 6 (4 papers) Chair:
12:50 am – 14:00 pm, Aug. 24	11:50 am – 13:00 pm, Aug. 24	Lunch Break
14:00 pm – 14:50 pm, Aug. 24	13:00 pm – 13:50 pm, Aug. 24	Keynote 4: Chair:
14:50 pm – 15:00 pm, Aug. 24	13:50 pm – 14:00 pm, Aug. 24	Short Break
15:00 pm – 16:20 pm, Aug. 24	14:00 pm – 15:20 pm, Aug. 24	Session 7 (4 papers) Chair:
16:20 pm – 16:30 pm, Aug. 24	15:20 pm – 15:30 pm, Aug. 24	Short Break
16:30 pm – 17:30 pm, Aug. 24	15:30 pm – 16:30 pm, Aug. 24	Session 8 (3 papers) Chair:
17:30 pm – 17:40 pm, Aug. 24	16:30 pm – 17:40 pm, Aug. 24	Closing Remarks

Total **31** papers will be presented, together with **4** keynotes.

Each paper has 20 minutes, including 15-minute presentation + 5-minute Q&A.

Program details can be found below, more details can be found at

https://easychair.org/smart-program/PST2022/

Conference Zoom Link: available soon.

Program Details

August 23, 2022

Keynote 1 (9:00 am – 9:50 am, Aug. 23, GMT-3)
Speaker: Dr. N. ASOKAN, University of Waterloo **Bio:** N. Asokan is 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 (https://cpi.uwaterloo.ca/). He is also an adjunct professor at Aalto University where he was the founding director of the Helsinki-Aalto Institute for Cybersecurity (https://haic.fi). 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. 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. Asokan received his doctorate in Computer Science from the University of Waterloo, MS in Computer and Information Science from Syracuse University, and BTech (Hons.) in Computer Science and Engineering from the Indian Institute of Technology at Kharagpur. He is an ACM Fellow and an IEEE Fellow. **Title:** Extraction of Complex DNN Models: Real Threat or Boogeyman **Abstract:** 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.

Session 1 (10:00 am – 11:20 am, Aug. 23, GMT-3)
10:00 Kun Peng Efficient Homomorphic E-Voting Based On Batch Proof Techniques 10:20

Xiaodong Qu, Qinglei Kong, Feng Yin and Lexi Xu
A Secure and Privacy-Preserving Dynamic Aggregation Mechanism for V2G System
10:40
Hiroaki Kikuchi, Shun Miyoshi, Takafumi Mori and Andres Hernandez-Matamoros
A Vulnerability in Face Anonymization – Privacy Disclosure from Face-obfuscated video
11:00
Mingchang Liu, Vinay Sachidananda, Hongyi Peng, Rajendra Patil, Sivaanandh Muneeswaran and Mohan Gurusamy
LOG-OFF: A Novel Behavior Based Authentication Compromise Detection Approach

Session 2 (11:30 am – 12:50 pm, Aug. 23, GMT-3)

11:30
Tariq Bontekoe, Maarten Everts and Andreas Peter
Balancing privacy and accountability in digital payment methods using zk-SNARKs
11:50
Laurens D'Hooge, Miel Verkerken, Bruno Volckaert, Tim Wauters and Filip De Turck
Discovering Non-Metadata Contaminant Features in Intrusion Detection Datasets
12:10
Jacob Krabbe Pedersen, Mikkel Bøchman and Weizhi Meng
Security Analysis in Satellite Communication based on Geostationary Orbit
12:30
Malte Breuer, Pascal Hein, Leonardo Pompe, Ben Temme, Ulrike Meyer and Susanne Wetzel
Solving the Kidney Exchange Problem using Privacy-Preserving Integer Programming

Keynote 2 (14:00 pm – 14:50 pm, Aug. 23, GMT-3)

Speaker: Dr. XINWEN FU, University of Massachusetts Lowell

Bio: Dr. Xinwen Fu is a Professor in the Department of Computer Science, University of Massachusetts Lowell. 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 (ToN) and IEEE Transactions on Dependable and Secure Computing (TDSC). He spoke at various technical security conferences including Black Hat. His research was reported by various Media 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).

Title: Unified View of IoT and CPS and Trend of Research on Microcontroller Based IoT

Abstract: 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.

Session 3 (15:00 pm – 16:20 pm, Aug. 23, GMT-3)

15:00
Shalini Saini, Dhiral Panjwani and Nitesh Saxena
Mobile Mental Health Apps: Alternative Intervention or Intrusion?
15:20
Khosro Salmani
An Efficient, Verifiable, and Dynamic Searchable Symmetric Encryption with Forward Privacy
15:40
Shaveta Dandyan, Habib Louafi and Samira Sadaoui
A Feistel Network-based Prefix-Preserving Anonymization Approach, Applied To Network Traces
16:00
Weifeng Xu and Dianxiang Xu
Visualizing and Reasoning about Presentable Digital Forensic Evidence with Knowledge Graphs

Session 4 (16:30 pm – 17:50 pm, Aug. 23, GMT-3)

16:30
Sajjad Dadkhah, Hassan Mahdikhan, Priscilla Kyei Danso, Alireza Zohourian and Kevin Anh Truong
Towards the development of a realistic multidimensional IoT profiling dataset
16:50
Andrick Adhikari, Sanchari Das and Rinku Dewri
Privacy Policy Analysis with Sentence Classification
17:10
Xichen Zhang, Songnian Zhang, Suprio Ray and Ali A. Ghorbani
Efficient and Privacy-preserving Worker Selection in Mobile Crowdsensing Over Tentative Future Trajectories
17:30
Trent Muhr and Wensheng Zhang
Privacy-Preserving Detection of Poisoning Attacks in Federated Learning

August 24, 2022

Keynote 3 (9:00 am – 9:50 am, Aug. 24, GMT-3)

Speaker: Dr. QIANG TANG, The University of Sydney

Bio: Dr. Qiang Tang is currently Senior Lecturer (equal to U.S. Associate Professor) at the University of Sydney. From 2016.8 - 2020.12, 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 35, 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.

Title: The Dumbo Protocol Family: Making Asynchronous Consensus Real

Abstract: 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.

Session 5 (10:00 am – 11:20 am, Aug. 24, GMT-3)

10:00
Xueqin Gao, Tao Shang, Da Li and Jianwei Liu
Quantitative Risk Assessment of Threats on SCADA Systems Using Attack Countermeasure Tree

10:20
Huang Lin
Faceless: A Cross-Platform Private Payment scheme for Human-Readable Identifiers

10:40
Chengzhe Lai and Yinzhen Wang
Achieving Efficient and Secure Query in Blockchain-based Traceability Systems

11:00
Chuhan Liu, Wei Yan, Fengkai Xu, Wenlong Yang and Beibei Li
User Behavior Simulation in ICS Cyber Ranges

Session 6 (11:30 am – 12:50 am, Aug. 24, GMT-3)

11:30
Mordechai Guri
SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables

11:50
Wentao Wang, Yuxuan Jin and Bin Cao
An Efficient and Privacy-Preserving Range Query over Encrypted Cloud Data
12:10
Yiming Sun, Weizhi Meng and Wenjuan Li
Designing In-Air Hand Gesture-based User Authentication System via Convex Hull
12:30
Nastaran Bateni, Rozita Dara, Jasmin Kaur and Fei Song
Content Analysis of Privacy Policies Before and After GDPR

Keynote 4 (14:00 pm – 14:50 pm, Aug. 24, GMT-3)

Speaker: Dr. STEPHEN MARSH, Ontario Tech University

Bio: 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 (https://doi.org/10.1016/j.cogsys.2021.11.001). 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 (his album will be out in October!), draws (badly), writes (Trust Systems the textbook is freely available as an Open Educational Resource at https://ecampusontario.pressbooks.pub/trustsystems/, he is currently working on a fiction trilogy and a non-fiction book about Hope), blogs occasionally at https://trustsystems.work and shares life with people, dogs, cats, horses, a pig, sheep, goats, chickens and lizards. He quite possibly also has bats in the belfry.

Title: "You keep using that word. I do not think it means what you think it means." (Inigo Montoya)

Abstract: 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.

Session 7 (15:00 pm – 16:20 pm, Aug. 24, GMT-3)

15:00
Suyang Wang, Bo Yin, Shuai Zhang and Yu Cheng
An Analytical Study of Selfish Mining Attacks on Chainweb Blockchain
15:20
Euclides Neto and Sajjad Dadkhah
Collaborative DDoS Detection in Distributed Multi-Tenant IoT using Federated Learning
15:40
Kacem Khaled, Gabriela Nicolescu and Felipe Gohring de Magalhães
Careful What You Wish For: on the Extraction of Adversarially Trained Models
PRESENTER: Kacem Khaled
16:00
Cagri Arisoy, Anuradha Mandal and Nitesh Saxena
Human Brains Can't Detect Fake News: A Neuro-Cognitive Study of Textual Disinformation Susceptibility

Session 8 (16:30 pm – 17:30 pm, Aug. 24, GMT-3)

16:30
Ahmed Ghanem and Riham Altawy
Garage Door Openers: A Rolling Code Protocol Case Study
16:50
Saul Hughes and Sana Maqsood
Usability of Paper Audit Trails in Electronic Voting Machines
17:10
Jasmin Kaur, Rozita Dara and Ritu Chaturvedi
A Semantic-based Approach to Reduce the Reading Time of Privacy Policies