PST 2023 Program (21 August 2023)

Start Time	End Time	Room M1	Room S09
08:00	09:15	Registration & Breakfast	N/A
09:15	09:30	Welcome Ceremony	
09:30	10:30	Keynote I [Session Chair: Weizhi Meng]	
		Qiang Tang ML-based attack detection: a case study for Telecom networks	
10:30	11:00	Morning Tea Break	
11:00	12:15	Paper Session: Privacy – M1 [Session Chair: Weizhi Meng]	Paper Session: Security – S1 [Session Chair: Wayne Chiu]
		David Hasselquist: PET-Exchange: A Privacy Enhanced Trading Exchange using Homomorphic Encryption	Ahmed Haj Abdel Khaleq: Improving Malicious PDF Detection with a Robust Stacking Ensemble Approach
		Atsuko Miyaji Revisited Privacy-preserving Machine Learning Framework	Furqan Rustam Securing Multi-Environment Networks using Versatile Synthetic Data Augmentation Technique and Machine Learning Algorithms
		Piero Romare: Tapping into Privacy: A Study of User Preferences and Concerns on Trigger-Action Platforms	Dipanwita Roy Chowdhury: Unmasking the dominant threat of Data Manipulation Attack on Implantable Cardioverter Defibrillators
		Xiaoyuan Liu Efficient Homomorphic Convolution for Secure Deep Learning Inference	Soheil Varastehpour Analysis and Comparison of Deepfakes Detection Methods for Cross-Library Generalisation
12:15	14:00	Lunch (At DTU Canteen)	N/A
14:00	15:00	Keynote II [Session Chair: Jaideep Vaidya]	
		Pierangela Samarati Controlled data sharing in distributed collaborative scenarios.	
15:00	15:30	Afternoon Coffee Break	
15:30	16:50	Paper Session: Security – M1 [Session Chair: Fabian Willems]	Paper Session: Privacy – S1 [Session Chair: Jiaxuan Wu]
		Mordechai Guri: EL-GRILLO: Leaking Data Ultrasonically from Air-Gapped PCs via the Tiny Motherboard Buzzer	Rim Salem User Modelling for Privacy-Aware Self-Disclosure
		Rashid Hussain Khokhar UCreDiSSiT: User Credibility Incorportating Domain Interest, Semantics in Social Interactions and Temporal factor	Arnaud Grivet Sébert: Combining Homomorphic Encryption and Differential Privacy in Federated Learning
		Yoonjib Kim	Muhammad Lutfor Rahman

		DDoS Attack Dataset (CICEV2023) against EV Authentication in Charging Infrastructure	Saudi Arabian Perspective of Security, Privacy, and Attitute of Using Facial Recognition Technology
		Nuray Baltaci Akhuseyinoglu Geodemographic Profiling of Malicious IP Addresses	
17:00		Reception (At DTU Building 324 Room 240)	N/A

PST 2023 Program (22 August 2023)

Start Time	End Time	Room M1	Room S09
08:00	09:30	Registration & Breakfast	N/A
09:30	10:30	Paper Session: Privacy – M2 [Session Chair: David Kravitz]	Paper Session: Security – S2 [Session Chair: Peichen Liu]
		Kittiphop Phalakarn: Privacy-Preserving Reputation System Against Dishonest Queries	Gaoning Pan: AMF: Efficient Browser Interprocess Communication Fuzzing
		Akito Yamamoto: Privacy-Preserving Publication of GWAS Statistics using Smooth Sensitivity	Francesco Santini A TCP-based Covert Channel with Integrity Check and Retransmission
		Jiachen Shen: MMDSSE: Multi-client and Multi-Keyboard Dynamic Searchable Symmetric Encryption for Cloud Storage	Yakov Mallah: Risk Oriented Resource Allocation in Robotic Swarm
	(10:35)		Liang Chen A Trust-based Approach for Data Sharing in the MQTT Environment
10:30	11:00	Morning Tea Break	N/A
11:00	12:20	Paper Session: Security – M2 [Session Chair: Fabian Willems]	Paper Session: Privacy – S2 [Session Chair: Wayne Chiu]
		Simon Bertrand: Unsupervised User-Based Insider Threat Detection Using Bayesian Gaussian Mixsure Models	Andres Hernandez-Matamoros: An Efficient Local Differential Privacy Scheme Using Bayesian Ridge Regression
		Ayush Kumar RAPTOR: Advanced Persistent Threat Detection in Industrial IoT via Attack Stage Correlation	Sascha Löbner: Systematizing the State of Knowledge in Detecting Privacy Sensitive Information Using Machine Learning
		Guoqiang Chen Investigating Neural-based Function Name Reassignment from the Perspective of Binary Code Representation	Zhenfu Cao: MDPPC: Efficient Scalable Multiparty Delegated PSI and PSI Cardinality
		Qusay Mahmoud: Building Trust in Deep Learning Models via a Self-Interpretable Visual Architecture	Haoran Deng Attention in Differential Cryptanalysis on Lightweight Block Cipher SPECK
12:20	14:00	Lunch (At DTU Canteen)	N/A
14:00	15:00	Keynote III [Session Chair: Christian D. Jensen]	
		Liqun Chen How to align trusted computing with security and privacy?	
15:00	15:30	Afternoon Coffee Break	
15:30	16:25	Paper Session: Blockchain – M1 [Session Chair: Jiachen Shen]	Paper Session: Privacy – S3 [Session Chair: Xiaofu Chen]

		Leila Rashidi Securing Supply Chain: A Comprehensive Blockchain-based Framework and Risk Assessment	Sigurd Eskeland: Private Set Intersection using RSA Subgroups with Constant-size Encryptions
		David Kravitz: Course-Correct to DeFi Lacking Default Deficiency	Garima Bajwa Selective EEG Signal Anonymization using Multi-Objective Autoencoders
		Alireza Parvizimosaed Protection against Ransomware in Industrial Control Systems through Decentralization using Blockchain	Masaya Kobayashi: Extended k^m-Anonymity for Randomization Applied to Binary Data
	(16:35)		Yuan Cheng A Secure Distributed Learning Framework Using Homomorphic Encryption
18:00		Gala Dinner - Restaurant Fortunen	N/A

PST 2023 Program (23 August 2023)

Start Time	End Time	Room M1	Room S09
08:00	09:30	Registration	N/A
09:30	10:30	Keynote IV [Session Chair: Ali Ghorbani]	
		Mauro Conti: Covert & Side Stories: Threats Evolution in Traditional and Modern Technologies	
10:30	11:00	Morning Tea Break	
11:00	12:05	Paper Session: Trust – M1 [Session Chair: Christian D. Jensen]	Paper Session: Security – S3 [Session Chair: Erik Falk]
		Feiyang Tang Transparency in App Analytics: Analyzing the Collection of User Interaction Data	Vinay Mysore Sachidananda: ThreatLand: Extracting Intelligence from Audit Logs via NLP methods
		Vanessa Bracamonte: Effectiveness and Information Quality Perception of an AI Model Card: A Study Among Non-Experts	Sonia Kawish An Instance-based Transfer Learning Approach, Applied to Intrusion Detection
		Suzana Moreno A Rule-Language Tailored for Financial Inclusion and KYC/AML Compliance	Dakota Staples A Comparison of Machine Learning Algorithms for Multilingual Phishing Detection
			Olufunsho Falowo Exploration of Various Machine Learning Techniques for Identifying and Mitigating DDoS Attacks
12:10	14:00	Lunch	N/A
14:00	15:00	Paper Session: Security – M3 [Session Chair: David Kravitz]	Paper Session: Privacy – S4 [Session Chair: Windhya Hansinie Rankothge]
		Suryadipta Majumdar: Layered Security Analysis for Container Images: Expanding Lightweight Pre-Deployment Scanning	Matthew Roffel Write Blocker for Internet of Things Flash Technologies
		Hua Deng Forward-Secure Customizable Data Sharing in Blockchain-based EHR Systems	Tanveer Khan: Love or Hate? Share or Split? Privacy-Preserving Training Using Split Learning and Homomorphic Encryption
		Lifei Wei An Efficient Federated Learning Framework for Privacy-Preserving Data Aggregation in IoT	Paulina Chametka Security and Privacy Perceptions of Mental Health Chatbots
	(15:05)		Benjamin Fenelon Private UAV-Assisted IoT Data Collection: An Energy-Privacy Trade-Off

15:00	15:30	Afternoon Coffee Break	N/A
15:30	16:30	Paper Session: Privacy – M3 [Session Chair: Simon Bertrand]	Paper Session: Privacy – S5 [Session Chair: Windhya Hansinie Rankothge]
		Fabian Willems: GhostBuy: An All Steps Anonymous Purchase Platform (ASAPP) based on Separation of Data	Kwasi Boakye-Boateng Securing Substations with Trust, Risk Posture, and Multi-Agent Systems: A Comprehensive Approach
		Xiaohui Liang VPASS: Voice Privacy Assistant System for Monitoring In-home Voice Commands	Hossein Abedi Khorasgani Black-Box Attribute Inference Protection With Adversarial Reprogramming
		Nan Cheng: Efficient Three-party Boolean-to-Arithmetic Share Conversion	Jianbing Ni Verifiable and Privacy-Preserving Ad Exchange for Smart Targeted Advertising
16:30		Closing Ceremony	N/A