PST 2026 — Technical Sessions (Detailed)

[S] = short paper · [REMOTE] = approved remote presentation

Thursday - August 27

Session 1 — Privacy-Preserving & Federated Learning

DMS4120 | 10:45 - 12:15 | Chair: Dr. Rongxing Lu

10:45 [#183] Exact and One-Shot Predictive Modeling with Vertically Partitioned Data: Privacy-Protecting Approaches for Binary Responses
Marie-Pier Domingue, Jean-François Ethier, Simon Lévesque, Anita Burgun and Félix Camirand Lemyre

11:07 [#216] Uncertainty-Aware Feature and Label Transformations for Privacy-Preserving Machine Learning under Local Differential Privacy
Tomoshi Yagishita and Atsuko Miyaji

11:29 [#109] Cross-Round Leakage: Enabling Multiclass Property Inference under Aggregate-Only Federated Updates **[REMOTE]**
Sonia Jerry-Akpan, Ahmad Patooghy and Mahmoud Mahmoud

11:51 [#28] Towards Fairness in Federated Client Selection via JS-Similarity Voting on Distilled Knowledge **[S] [REMOTE]**
Ogobuchi Daniel Okey, Sajjad Dadkhah, Demostenes Zegarra Rodríguez and Joao Henrique Kleinschmidt

Session 2 — Malware Detection & Analysis

DMS4130 | 10:45 - 12:15 | Chair: Dr. Suryadipta Majumdar

10:45 [#83] ANDROVEIL: A Reproducible Dataset of Obfuscated Android Malware
Annan Fu, Weijian Zhao, Jiani Guo, Xinyu Zeng and Maryam Tanha

11:07 [#98] Cost-Aware Active Learning with Noisy LLM Annotations for Android Malware Detection
Zhe Deng, Ants Torim, Hayretdin Bahşi and Sadok Ben Yahia

11:29 [#170] Domain Adaptation for Cross-Architecture IoT Malware Detection under Data Scarcity
Yu-Cheng Lin, Tao Ban, Shin-Ming Cheng and Takeshi Takahashi

11:51 [#95] Explaining Provenance-Based GNN Detectors with Interpretable Graph Structural Features **[S] [REMOTE]**
Kunal Mukherjee, Joshua Wiedemeier, Tianhao Wang, Muhyun Kim, Feng Chen, Murat Kantarcioglu and Kangkook Jee

Session 3 — Access Control & Security Policy

DMS4170 | 10:45 - 12:15 | Chair: Dr. Honghao Fu

10:45 [#151] A Feasibility Analysis of Network-Layer Enforcement for Data Usage Control Requirements
Haydar Qarawlus and Falk Howar

11:07 [#168] NGAC Policy Learning using Access Logs through Constrained Matrix Factorization
Abhimanyu Chawla, Samuel Chamberlain and Indrakshi Ray

11:29 [#105] Fine-Grained Access Control for MongoDB **[S]**
Mahmoud Abdelgawad, Abhimanyu Chawla, Christopher Beall, Brian Tan and Indrakshi Ray

11:51 [#72] Research-Practice Gap in Access Control: An Empirical Study of 56 Interviews with Cybersecurity Practitioners **[S]**
Franck Arnaud Fotso Kuate, Florent Avellaneda and Omer Nguena Timo

Session 4 — Post-Quantum & Quantum-Resilient Security

DMS4120 | 1:30 - 2:40 | Chair: Dr. Jake Doliskani

1:30 [#53] PAPQUIC: Performance Analyzer of Post-Quantum QUIC **[S]**
Pedro Rigon, Honghao Fu, Weverton Cordeiro and Carol Fung

1:52 [#141] A Hybrid PQC-TLS Gateway with Integrated Passkeys Authentication **[REMOTE]**
Abdulrahman Al-Hakawati, Nahla Shameer, Mohamed Aslam, Suha Fatima, Ahmed Satti and Sami Zhioua

2:14 [#14] Quantum Resilient Identity Federation for OIDC and SAML with Hybrid Post Quantum Trust Chains **[REMOTE]**
Ankit Gupta, Shilpi Mittal and Gahangir Hossain

Session 5 — Differential Privacy & Synthetic Data

DMS4130 | 1:30 - 2:40 | Chair: Dr. Carlisle Adams

1:30 **[#163]** Dual-Path Discriminator Architecture for Differentially Private Synthetic Tabular Data Generation
Kateryna Padalko and Helen Chen

1:52 **[#214]** Beyond the Stitching Assumption: A Unified Framework for Multimodal Synthetic Data Evaluation via Semantic Quantization
Yefeng Yuan

2:14 **[#100]** Concentrated Reference-Panel Exposure in HAPNEST-Generated Synthetic Genomic Data: A Membership Inference Attack Evaluation on the CanPath Cohort
Reem Al-Saidi, Ziad Kobti and Amy Li

Session 6 — Blockchain, Supply Chain & Chains of Trust

DMS4170 | 1:30 - 2:40 | Chair: Dr. Jeremy Clark

1:30 **[#24]** DarkChain: Weaponizing the Ethereum State Trie as a Censorship-Resistant Distribution Network for Illicit Content
Luke Beard and Nikolay Ivanov

1:52 **[#143]** A Logic for Chains of Trust **[S]**
Niels Voorneveld and Peeter Laud

2:14 **[#49]** STEPchain: Platform for Secure, Scalable, and Privacy-Preserving Supply Chain Tracing and Counterfeit Protection **[REMOTE]**
Moritz Finke, Alexandra Dmitrienko and Jayasree Sengupta

Friday - August 28

Session 7 — LLM Security & Safety

DMS4120 | 9:00 - 10:30 | Chair: Dr. Ali Miri

10:30 **[#67]** Black-Box Behavioral Distillation Breaks Safety Alignment in Medical LLMs
Mohammed Al Duniawi, Sohely Jahan and Ruimin Sun

10:52 **[#205]** CDDO: Consensus Driven Diagnostic Override Through Adaptive Exploitation of Medical LLMs
Sher Safi, Ali Miri and Shadan Ghaffaripour

11:14 **[#13]** Payload-as-Data:A Structural Argument and Measurement Study of Prompt Injection in LLM-Integrated SOCs
Zhaolong Chu, Li Zhang and Carol Fung

11:36 **[#139]** From Prompt to Physical Actuation: Holistic Threat Modeling of LLM-Enabled Robotic Systems **[S]** **[REMOTE]**
Neha Nagaraja, Hayretdin Bahsi and Carlo R. da Cunha

Session 8 — CPS, Smart Grid & Automotive Security

DMS4130 | 9:00 - 10:30 | Chair: Dr. Jun Yan

10:30 **[#142]** GridWhisper: Disrupting an Islanded Campus Microgrid via Protocol-Layer Attacks
Shabnam Saderi Oskouei, Nethmi Hettiarachchi and Kalikinkar Mandal

10:52 **[#32]** Blocking Post-Aggregation Tampering in Federated Net-Load Forecasting: A Real-Data Study with PTProsumer **[S]**
Parventanis Murthy and Kwok-Yan Lam

11:14 **[#144]** OTARQ: Adaptive and Automated Risk Quantification Method for OTA Updates in SDVs **[REMOTE]**
Khaoula Sghaier, Ghada Gharbi, Badis Hammi, Pierre Merdrignac, Pierre Parrend and Didier Verna

11:36 **[#23]** From Tabular Flow Features to LLMs: Text Serialization for Smart Grid Intrusion Detection **[REMOTE]**
Eman Saleh, Hayretdin Bahsi and Andrii Chub

Session 9 — Systems, Hardware & Device Security

DMS4170 | 9:00 - 10:30 | Chair: Dr. Jake Doliskani

10:30 [#47] What's My Age Again? How Old is Too Old For Small Office/Home Office (SOHO) Router Use?
Douglas Healy, Steven Hart and Karl Olson

10:52 [#66] Write Data, Wrong Address: ECC-Based Detection of DRAM Aliasing in Trusted Execution Environments **[S]**
Griffyn Young, Abraham Fernandez Rubio, Pepe Vila and Stavros Kalafatis

11:14 [#125] Canary in the Container: Deception-Based Monitoring for Private Container Images **[S]**
Billy Tsouvalas and Nick Nikiforakis

11:36 [#211] Practical Stabilization of XLATE/Prime+Probe Cache Attacks under Noisy Execution Conditions **[S] [REMOTE]**
Ankit Pulkit, Smita Naval, Shagun Lamba, Parvez Faruki, Vijay Laxmi and Manoj Gaur

Session 10 — Trustworthy AI Agents & LLM Privacy

DMS4120 | 1:15 - 2:45 | Chair: Dr. Indrakshi Ray

1:15 [#97] Argox: A Framework for Securing Large Language Models from Model Inversion Attacks
Mansi Krishnakant Modi, Robert Hortua Leal, Maryam Tanha, Hamed Jelodar and Sajjad Dadkhah

1:37 [#76] A Reinforcement Learning Framework for Reducing Sensitive-Data Leakage in Locally Deployed Open-Source Large Language Models **[S]**
Jason Greige, Adel Abusitta and Quentin Cappart

1:59 [#165] ToolMinimize: Auditing and Rewriting LLM Agent Tool Calls to Minimize Privacy Exposure
Wenbiao Li and Yuqiao Xu

2:21 [#43] A framework for the estimation of policy-based trustworthiness of AI agents **[REMOTE]**
Anirban Basu, Yosuke Kaga and Keisei Fujiwara

Session 11 — Cryptographic Foundations & Confidential Computing

DMS4130 | 1:15 - 2:45 | Chair: Dr. Carlisle Adams

1:15 [#35] The ABCs of Jolt: Advice and Bytecode Commitments
Quang Dao, Amirhossein Khajehpour, Omid Bodaghi, Giuseppe Vitto and Thomas Kim

1:37 [#89] Search to Decision Reduction for Dihedral Cosets and a Quantum Public-Key Encryption
Jake Doliskani

1:59 [#58] Trustless Confidential Containers: Verifiable Execution from Code to Runtime **[S]**
Naoki Higo and Arifumi Matsumoto

2:21 [#33] Rational Deterrence for FHE Integrity: A Hybrid TEE–ZKP Architecture with Probabilistic Auditing **[REMOTE]**
Asuman Dumlu

Session 12 — Authentication, Fraud & Media Forensics

DMS4170 | 1:15 - 2:45 | Chair: Dr. Rongxing Lu

1:15 [#217] Enforcing Sender Authenticity by Construction: A Document-Oriented, Sessional Signature Scheme for Email Anti-Phishing **[REMOTE]**
Ye Li

1:37 [#31] Forensic Schema for Psychological Manipulation in Cyber Fraud: LLM-Driven Victim Reports Analysis **[REMOTE]**
Zikai Alex Wen, Corrazon Ogot, Juan Li and Yan Bai

1:59 [#4] A Million Keys to Try: The Economics of OTP Brute-Force Attacks **[S]**
Zhaolong Chu, Doha Mekouar and Carol Fung

2:21 [#155] Interpretable Deepfake Detection in Videos via Explicit Forensic Features and Temporal Modeling
Benhama Chahira, Mohand Said Allili and Assia Hamadene

Session 13 — Vulnerability Analysis & Software Security

DMS4120 | 3:15 - 4:30 | Chair: Dr. Suryadipta Majumdar

3:15 **[#25]** Measuring Security Hardening Adoption in Infrastructure as Code: An Empirical Study of Public Repositories
Ruining Yang and Nick Nikiforakis

3:37 **[#209]** A Lifecycle-Aware EPSS Correction for Trustworthy Vulnerability Prioritization **[S]**
Boyao You

3:59 **[#169]** ReVEX: DSPy-Optimized ReAct Agents for Exploitability Verification of Container Vulnerabilities **[REMOTE]**
Satyam Thakur, Sarker Monojit Asish, Wesam Al Amiri, Mohammad Farmani and Arijet Sarker

Session 14 — Network & Wireless Security

DMS4130 | 3:15 - 4:30 | Chair: Dr. Lianying Zhao

3:15 **[#194]** Unsupervised DoS Attack Detection in O-RAN with Adaptive Thresholding and Autoencoder Models
Mohammad Abdelhalim, Md. Shamim Towhid and Nashid Shahriar

3:37 **[#158]** Information flow detection in the Internet of Things **[S]**
Gildas Kouko, Josée Desharnais and Nadia Tawbi

3:59 **[#152]** Replicating the Signature: Unsupervised Targeted Impersonation Attack on RF Fingerprinting **[REMOTE]**
Haytham Albousayri and Bechir Hamdaoui

Session 15 — Model Protection & Trustworthy ML

DMS4170 | 3:15 - 4:30 | Chair: Dr. Jun Yan

3:15 **[#96]** Model Protection in CNNs via Partial Parameter Concealment **[S]**
Haruki Arai and Hayato Yamana

3:37 **[#200]** Human-Aware Trust Framework for AI-Driven Vulnerability Patch Generation **[S]**
Natasha Naorem

3:59 **[#127]** Prismo: A Decision Support System for Privacy-Preserving Machine Learning Frameworks Selection **[REMOTE]**
Nges Brian Njungle, Eric Jahns, Luigi Mastromauro, Edwin P. Kayang, Milan Stojkov and Michel A. Kinsy