Carnegie Mellon University
CyLab
Security and Privacy Institute

Partners Conference 2024

Tuesday, September 24, 2024

Poster #1
Aidan Yang, 4th year PhD, S3D
Title: *Large Language Models for Test-Free Fault Localization*
Advisor: Rubens Martins
Email: aidan@cmu.edu

Poster #2
Alexandra Li, 2nd year PhD Student, S3D
Title: *Design and Evaluation of the Users First Privacy Notice and Choice Threat Analysis* Taxonomy
Advisor: Lorrie Cranor
Email: alexandrali@cmu.edu

Poster #3
Arjun Ramesh
Title: *Empowering Web Assembly with Thin Kernel Interfaces*
Advisor: Lujo Bauerand Vyas Sekar
Email: arjunr2@andrew.cmu.edu

Poster #4
Brian Singer, 5th year PhD student, ECE
Title: *Perry: A Flexible Security Experimentation Platform*
Advisor:Lujo Bauer and Vyas Sekar
Email: briansin@andrew.cmu.edu

Poster #5
Ben Weinshel, 2nd year PhD student, S3D
McKenna McCall, Post Doc, Software and Society Systems
Title: *Reactions to Information Flow Analysis of Smart-Home Automations*
Advisor: Lujo Bauer
Email: dmanohar@andrew.cmu.edu
bweinshel@cmu.edu
mckennak@andrew.cmu.edu

Poster #6
Haoming Jing, 3rd year PhD student, ECE
Title: *Rethinking Safe Control in the Presence of Self-Seeking Humans*
Advisor: Yorie Nakahira
Email: haomingj@andrew.cmu.edu

Poster #7
Kyzyl Monteiro, 2nd year PhD student
Isadora Krsek, 3rd year PhD Student, HCII
Title*: Intelligent Agents to Improve End-User and Practitioner S&P Behaviors*
Advisor: Sauvik Das
Email: kmonteir@andrew.cmu.edu
ikrsek@andrew.cmu.edu

Poster #8
Alexandra Nisenoff, 2nd year PhD student, S3D
Title: *The State of Privacy Sandbox Attestation on the Web*
Advisor: Nicolas Christin and Lorrie Faith Cranor
Email:nisenoff@cmu.edu

Poster #9
Milind Srivastava, 5th year PhD student, ECE
Title: *Circa: Re-imagining Network Telemetry from an Approximation-First Perspective*
Advisor: Vyas Sekar
Email: milindsr@andrew.cmu.edu

Poster #10
Phyllis Poh, 1st year PhD student, ECE
Omer Akgul (postdoc)
Title: *Malware Makeover + Adversarial Training with EXEs: Breaking and Defending ML-based Malware Detectors*
Advisor: Lujo Bauer
Email: ppoh@andrew.cmu.edu
oakgul@andrew.cmu.edu

Poster #11
Pratap Singh, 3rd year, CSD
Title: *Owl: Automatic End to End Verification of Security Protocols*
Advisor: Bryan Parno
Email:pratapsingh@cmu.edu

Poster #12
Sara Mahdizadeh Shahri, 1st Year PhD Student ECE
Title: *Studying Demographic Bias in Web Scheduling Systems*
Advisor: Akshitha Sriraman
Email:smahdiz@cmu.edu

Poster #13
Taylor McCampbell, Graduate Student CyLab
Title: *Investigating the Utilization of K-12 Cyber Security Educational Resources*
Advisor: Hanan Hibshi
Email: tmccampb@andrew.cmu.edu

Poster #14
Weiran Lin, 6th year PhD student, ECE
Title: *LLM Whisperer: An Inconspicuous Attack to Bias LLM Responses*
Advisor: Lujo Bauer
Email: weiranl@andrew.cmu.edu

Poster #15
Xiaoyuan Wu, 3rd year PhD student, SC
Title: *Transparency or Information Overload? Evaluating Users' Comprehension and Perceptions of the iOS App Privacy Report*
Advisor: Lujo Bauer
Email: xiaoyuaw@andrew.cmu.edu

Poster #16
Yu Kai Huang, PhD student
Title: *A Reference-Based 3D Semantic-Aware Framework for Accurate Local Facial Attribute Editing*
Advisor: Marios Savvides
Email: yukaih2@andrew.cmu.edu

Wednesday, September 25, 2024

Poster #1
Ian McCormack, 4th year PhD student, S3D
Title: *A Study of Undefined Behavior Across Foreign Function Boundaries in Rust Libraries*
Advisor: Jonathan Aldrich and Joshua Sunshine
Email: icmccorm@andrew.cmu.edu

Poster #2
Shuaiqi Wang, 4th year PhD student, ECE
Title: *Statistic Maximal Leakage*
Advisor: Guilia Fanti
Email: shuaiqiw@andrew.cmu.edu

Poster #3
Twain Byrnes, 1st year PhD student, ECE
Title: *Enforcing Expressive Information Flow Security Policies on Rust Programs*
Advisor: Limin Jia
Email:binarynewts@cmu.edu

Poster #4
Shuli Jiang, 5th year PhD student, RI
Title: *Differentially Private Incremental Gradient (IF) Methods with Public Data*
Advisor: Gauri Joshi
Email:shulij@andrew.cmu.edu

Poster #5
Andrea Gallardo, 5th year PhD student, S3D
Lily Klucinec, Research Assistant in CyLab
Title: *Attitudes Towards AI-enabled Voice Technologies for Decision Making Among Southern U.S. English Speakers*
Advisor: Lujo Bauer, Lorrie Cranor
Email: agallar2@andrew.cmu.edu
laklucin@andrew.cmu.edu

Poster #6
Eric Zeng, Postdoc
Title: *Measuring Risks to Users’ Health Privacy from Online Tracking and Targeted Advertising*
Advisor: Lujo Bauer
Email: ericzeng@cmu.edu

Poster #7
Rex Chen, 5th year PhD student, S3D
Title: *Missing Pieces: How Framing Uncertainty Impacts Longitudinal Trust in AL Decision Aids - A Gig Driver Case Study*
Advisor: Norman Sadeh
Email: rexc@cmu.edu

Poster #8
Tae Hoon Kim, 2nd year MS student, CSD
David Rudo, CMU Undergraduate
Title: *Perspective: A Principled Framework for Pliable and Secure Speculation in Operating Systems*
Advisor: Dimitrios Skarlatos
Email: taehoon2@andrew.cmu.edu

Poster #9
Zichao Zhang, Final year PhD student, ECE.
Hao Kang, CMU Undergraduate
Cheng Zhang, PostDoc
Title: *ProInspector*[1]*: Uncovering Logical Bugs in Protocol Implementations*
Advisor: Limin Jia
Email: zichaoz@andrew.cmu.edu
haok@andrew.cmu.edu
chengz3@andrew.cmu.edu

Poster #10
Alexandra Nisenoff, 3rd year PhD student, S3D
Title: *The State of Privacy Sandbox Attestation on the Web*
Advisor: Nicolas Christin and Lorrie Faith Cranor
Email: nisenoff@cmu.edu

Poster #11
Clement Fung, 6th year PhD student, S3D
Title: *Detecting and Explaining Anomalies in Industrial Control Systems (ICS)*
Advisor: Lujo Bauer
Email: clementf@andrew.cmu.edu

Poster #12
Yiliang Liang, 2nd year PhD student, S3D
Title: *Improving Understanding of Formal Models through Conceptual Visualization*
Advisor: Eunsuk Kang and Joshua Sunshine
Email: yiliangl@andrew.cmu.edu

Poster #13
Xiyu Deng, 2nd year PhD student, ECE
Title: *A Learning and Control Perspective for Microfinance*
Advisor: Yorie Nakahira
Email: xiyud@andrew.cmu.edu

Poster #14
Siddharth Jayashankar, 3rd Year PhD Student, CSD
Title: *Cinnamon: A Scale Out Framework for Encrypted Computing*
Advisor: Wenting Zheng and Dimitrios Skarlatos
Email: sidjay@cmu.edu