2024 IEEE Security and Privacy Workshops (SPW 2024)

San Francisco, California, USA
23 May 2024

IEEE Catalog Number:	CFP24SPX-POD
ISBN:	979-8-3503-5488-1

**Copyright © 2024 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP24SPX-POD
ISBN (Print-On-Demand):	979-8-3503-5488-7
ISBN (Online):	979-8-3503-5487-4
ISSN:	2639-7862

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA

Phone:	(845) 758-0400
Fax:	(845) 758-2633
E-mail:	curran@proceedings.com
Web:	www.proceedings.com

2024 IEEE Security and Privacy Workshops (SPW)

SPW 2024

Table of Contents

SecWeb: Workshop on Designing Security for the Web

A Public and Reproducible Assessment of the Topics API on Real Data 1
Yohan Beugin (University of Wisconsin-Madison) and Patrick McDaniel (University of Wisconsin-Madison)

User Verification System using Location-based Dynamic Questions for Account Recovery 9
Shuji Yamaguchi (LY Research, LY Corporation), Hidehito Gomi (LY Research, LY Corporation), and Tetsutaro Uehara (College of Information Science and Engineering, Ritsumeikan University)

Manufactured Narratives: On the Potential of Manipulating Social Media to Politicize World Events 17
Chris Tsoukaladelis (Stony Brook University) and Nick Nikiforakis (Stony Brook University)

Exploring the Capabilities and Limitations of Video Stream Fingerprinting 28
Tim Walsh (Naval Postgraduate School), Trevor Thomas (Naval Postgraduate School), and Armon Barton (Naval Postgraduate School)

ConPro: 8th Workshop on Technology and Consumer Protection

DLSP: 7th Deep Learning Security and Privacy Workshop

A Performance Analysis for Confidential Federated Learning 40
Iacopo Colonnelli (University of Turin, Italy), Gianluca Mittone (University of Turin, Italy), Robert Renè Maria Birke (University of Turin, Italy), Walter Riviera (University of Verona, Italy), Antonio Sciarappa (Leonardo SpA, Italy), Carlo Cavazzoni (Leonardo SpA, Italy), and Marco Aldinucci (University of Turin)

LocalStyleFool: Regional Video Style Transfer Attack Using Segment Anything Model 48
Yuxin Cao (Tsinghua University, China), Jinghao Li (Shandong University, China), Xi Xiao (Tsinghua University, China), Derui Wang (CSIRO's Data61, Australia), Minhui Xue (CSIRO's Data61, Australia), Hao Ge (Ping An Technology, China), Wei Liu (Shenzhen Institute of Information Technology, China), and Guangwu Hu (Shenzhen Institute of Information Technology, China)

Certifying Safety in Reinforcement Learning under Adversarial Perturbation Attacks 57
Junlin Wu (Washington University in St. Louis), Hussein Sibai (Washington University in St. Louis), and Yevgeniy Vorobeychik (Washington University in St. Louis)

Wendigo: Deep Reinforcement Learning for Denial-of-Service Query Discovery in GraphQL 68
Shae McFadden (King's College London, United Kingdom; The Alan Turing Institute, United Kingdom), Marcello Maugeri (University of Catania, Italy; King's College London, United Kingdom), Chris Hicks (The Alan Turing Institute, United Kingdom), Vasilios Mavroudis (The Alan Turing Institute, United Kingdom), and Fabio Pierazzi (King's College London, United Kingdom)

Mitigating Deep Reinforcement Learning Backdoors in the Neural Activation Space 76
Sanyam Vyas (The Alan Turing Institute), Chris Hicks (Alan Turing Institute), and Vasilios Mavroudis (Alan Turing Institute)

Just another copy and paste? Comparing the security vulnerabilities of ChatGPT generated code and StackOverflow answers 87
Sivana Hamer (North Carolina State University, USA), Marcelo d'Amorim (North Carolina State University, USA), and Laurie Williams (North Carolina State University, USA)

NodeGuard: A Highly Efficient Two-Party Computation Framework for Training Large-Scale Gradient Boosting Decision Tree 95
Tianxiang Dai (Huawei European Research Center, Germany), Yufan Jiang (Huawei European Research Center, Germany; Karlsruhe Institute of Technology, Germany), Yong Li (Huawei European Research Center, Germany), and Fei Mei (Huawei European Research Center, Germany)

The Impact of Uniform Inputs on Activation Sparsity and Energy-Latency Attacks in Computer Vision 104
Andreas Müller (Ruhr University Bochum, Germany) and Erwin Quiring (Ruhr University Bochum, Germany; International Computer Science Institute, USA)

SAGAI: Security Architectures for Generative Artificial Intelligence

Defending Language Models Against Image-Based Prompt Attacks via User-Provided Specifications 112
Reshabh K Sharma (University of Washington, USA), Vinayak Gupta (University of Washington, USA), and Dan Grossman (University of Washington, USA)

Exploiting Programmatic Behavior of LLMs: Dual-Use Through Standard Security Attacks 132
Daniel Kang (UIUC), Xuechen Li (Stanford University), Ion Stoica (UC Berkeley), Carlos Guestrin (Stanford University), Matei Zaharia (UC Berkeley), and Tatsunori Hashimoto (Stanford University)

Pre-trained Encoders in Self-Supervised Learning Improve Secure and Privacy-preserving Supervised Learning 144
Hongbin Liu (Duke University), Wenjie Qu (National University of Singapore), Jinyuan Jia (Pennsylvania State University), and Neil Zhenqiang Gong (Duke University)

LangSec: 10th Workshop on Language-Theoretic Security and Applications

Vulnerability Flow Type Systems 157
Mohsen Lesani (University of California, Santa Cruz)

Weird Machines in Package Managers: A Case Study of Input Language Complexity and Emergent Execution in Software Systems 169
Sameed Ali (Dartmouth College, USA), Michael E. Locasto (Narf Industries, USA), and Sean Smith (Dartmouth College, USA)

Robust Verification of PEG Parser Interpreters 180
Natarajan Shankar (SRI International) and Zephyr Lucas (Dartmouth College)

Research Report: An Optim(l) Approach to Parsing Random-Access Formats 192
Mark Tullsen (Galois, Inc.), Sam Cowger (Galois, Inc.), Mike Dodds (Galois, Inc.), and Peter Wyatt (PDF Association)

Research Report: Not All Move Specifications Are Created Equal 200
Meng Xu (University of Waterloo)

Parsing, Performance, and Pareto in Data Stream Security 215
J Peter Brady (Dartmouth College, USA) and Sean W Smith (Dartmouth College, USA)

Research Report: Enhanced eBPF Verification and eBPF-based Runtime Safety Protection 224
Guang Jin (Trusted Science & Technology, Inc.), Jason Li (Trusted Science & Technology, Inc.), and Greg Briskin (Trusted Science & Technology, Inc.)

Research Report: Testing and Evaluating Artificial Intelligence Application 231
Joshua Ackerman (Dartmouth College) and George Cybenko (Dartmouth College)

SafeThings: 8th Workshop on the Internet of Safe Things

PrivacyOracle: Configuring Sensor Privacy Firewalls with Large Language Models in Smart Built Environments 239
Brian Wang (UCLA), Luis Garcia (University of Utah), and Mani Srivastava (UCLA and Amazon)

Towards Cyber-Physical Representation and Cyber-Resilience Against Attack and Failure within a Hydraulic Network Simulation Toolkit 246
Sean O'Toole (Boise State University) and Hoda Mehrpouyan (Boise State University)

SideGuard: Non-Invasive On-Chip Malware Detection in Heterogeneous IoT Systems by Leveraging Side-Channels 253
Fatemeh Arkannezhad (UCLA, USA), Pooya Aghanoury (UCLA, USA), Justin Feng (UCLA, USA), Hossein Khalili (UCLA, USA), and Nader Sehatbakhsh (UCLA, USA)

Virtual Keymysteries Unveiled: Detecting Keystrokes in VR with External Side-Channels 260
Hossein Khalili (UCLA, USA), Alexander Chen (UCLA, USA), Theodoros Papaiakovou (UCLA, USA), Timothy Jacques (UCLA, USA), Hao-Jen Chien (UCLA, USA), Changwei Liu (Accenture, USA), Aolin Ding (Accenture, USA), Amin Hass (Accenture, USA), Saman Zonouz (Georgia Tech, USA), and Nader Sehatbakhsh (UCLA, USA)

Intercepting Bluetooth Traffic from Wearable Health Devices 267
Qi Liu (University of Virginia, USA), Yizhe Zhang (University of Virginia, USA), and Yixin Sun (University of Virginia, USA)

Security Analysis of Wearable Smart Health Devices and Their Companion Apps 274
Daniel Timko (California State University San Marcos), Mike Sharko (California State University San Marcos), and Yanyan Li (California State University San Marcos)

Seamlessly Insecure: Uncovering Outsider Access Risks in AiDot-Controlled Matter Devices 281
Narmeen Shafqat (Northeastern University, USA) and Aanjhan Ranganathan (Northeastern University, USA)

Adversarial 3D Virtual Patches using Integrated Gradients 289
Chengzeng You (Imperial College London, UK), Zhongyuan Hau (Imperial College London, UK), Binbin Xu (University of Toronto, Canada), and Soteris Demetriou (Imperial College London, UK)

Posters

Poster: Identity-Independent IoT for Overarching Policy Enforcement 296
Luoyao Hao (Columbia University) and Henning Schulzrinne (Columbia University)

Poster: Towards Privacy-Preserving Federated Recommendation via Synthetic Interactions 297
Thirasara Ariyarathna (University of New South Wales, Australia), Salil S. Kanhere (University of New South Wales, Australia), and Hye-Young Paik (University of New South Wales, Australia)

Author Index **299**