

2026 IEEE Symposium on Security and Privacy Workshops (SPW 2026)

**San Francisco, California, USA
21 May 2026**

IEEE Catalog Number:
ISBN:

CFP26SPX-POD
979-8-3195-1071-6



Copyright © 2026, IEEE

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:	CFP26SPX-POD
ISBN (Print-On-Demand):	979-8-3195-1071-6
ISBN (Online):	979-8-3195-1070-9
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

TABLE OF CONTENTS

Seventy Years of Parsing: Theoretical and Practical Consequences	1
<i>Zephyr S. Lucas, Prashant Anantharaman, Sean W. Smith</i>	
Tracing MCP Security Vulnerabilities: Constructing and Analyzing an MCP Security Vulnerability Dataset	26
<i>Xu He, Sagar Patel, Shu Wang</i>	
JUNID: Empowering Static Analysis with Asymptotically Optimal Intersection with Incomplete Sentences	35
<i>Eric Alata, Pierre-François Gimenez</i>	
CBCL: Safe Self-Extending Agent Communication	48
<i>Hugo O'Connor</i>	
PAPI: Provenance-Aware Parse Insertion for LangSec Mediation	58
<i>J. Peter Brady, Sean W. Smith</i>	
Object-Centric Tracing for Language-Theoretic Security in Low-Level Interfaces	69
<i>Imani Palmer, Edmond Rogers, Rob Adams</i>	
PickleFuzzer: A Case Study in Fuzzing for Discrepancies Between Python Pickle Implementations	83
<i>Justin Applegate, Andreas Kellas</i>	
Privacy Aware Anatomy Preserving Retinal Image Generation with ControlNet for Zero-False-Negative Glaucoma Screening	95
<i>Mao-Hsiu Hsu, Hsien-Chen Sun, Yu-Ting Hsu</i>	
Supply Chain Security of PCR Tests	106
<i>Noam Barkay, Yair Motro, Jacob Moran-Gilad, Rami Puzis</i>	
Adversarial Genomic Sequences Could Evade Biosecurity Screening	118
<i>Jeyashree Krishnan, Ajay Mandyam Rangarajan, Andrea Loehr, Jason Hoelscher-Obermaier</i>	
DNAS-Bench: Deterministic Nucleic Acid Screener Benchmarking	129
<i>Henry C. Wong, Tadayoshi Kohno, Jeff Nivala</i>	
Artificial Pancreas Implantables - How Healthcare Professionals May Deal with DIY Bio Cases	142
<i>Austin James, Xavier-Lewis Palmer, Lucas Potter, Celisha Oscar</i>	
PCR Automation Threats and Mitigations	150
<i>Naor Dalal, Yossi Oren, Jacob Moran-Gilad, Rami Puzis</i>	
Protecting Individual Identities in Wastewater Data Through Statistical and Differential Privacy Analysis	161
<i>Jiahui Gao, Riya Shah, Ni Trieu, Heewook Lee, R. Halden, Stephanie Forrest</i>	
Investigating TenSEAL's Homomorphic Encryption Through Predicting Encrypted RNA Sequencing Data	174
<i>Logan Choi, Wooyoung Kim</i>	
Towards Enhanced Detection of Genetically Engineered Plasmids	180
<i>Felix M. Quintana, Ryan D. Doughty, Michael G. Nute, Lydia E. Kavraki, Todd J. Treangen</i>	

Cyberbiosecurity Risk Assessment Framework for Genomic Data Storage in Cloud Environments	186
<i>Abtsega Tesfaye Chufare, Ribka Tiruneh, Sisay Beyene Juja</i>	
Enhancing Biosecurity Incident Response by Predicting Unknown Genetic Circuit Logic	197
<i>William Mo, Christopher A. Vaiana, Chris J. Myers</i>	
Limitations of Biological Risk Evaluation for Llms and Autonomous Science	203
<i>Andy Lin, Brian R. Bartoldson, George T. Bonheyo, Ryan Goldhahn, Bhavya Kalikhura, Greg Klunder Brian P. Mayer, C. Mark Maupin, Sai Munikoti, James S. Oakdale, Lauren A. Phillips, Paul M. Rigor Jonathan H. Tu, Janice R. Van Haeften, Henry Williams, Cindy Gonzales, Karl Pazdernik</i>	
Analysis of Trustworthiness and Fairness in Machine Learning for Healthcare	210
<i>Bingyu Liu</i>	
Targeting Systems, Not Pathogens: Adapting Cybersecurity Threat Modeling for Modern Biosecurity	216
<i>James Diggans, Kevin Flyangolts, Rami Puzis</i>	
Defining Cyberbiosecurity by Biological Consequence	223
<i>Tia Pope</i>	
Mental Damage: Caption Poisoning Attacks on Retrieval-Augmented Text-to-Music Generation	230
<i>Yizhu Wen, Shuhao Zhang, Nan Zhang, Long Cheng, Hanqing Guo</i>	
Auditing Training Data in Generative Music Models via Black-Box Membership Inference	239
<i>Yi Chen Liu, Jiawei Yu, Kexin Cao, Syed Irfan Ali Meerza, Trishika Movva, Jian Liu</i>	
FLEXMark: Evaluating Watermark Robustness and Attribution Reliability Under Redistribution and Adaptive AI Laundering	247
<i>Natalia Ellen Nicholas, Furqan Rustam, Anca Delia Jurcut</i>	
RD-PHash: A Robustness Enhancement for DCT-Based Perceptual Hashing Against Adversarial Bit-Flipping Attacks	259
<i>Nan Jiang, Bangjie Sun, Nayoung Kim, Terence Sim, Jun Han</i>	
On the Mismatch of Disclosure Practices in Security and Privacy Research	266
<i>Simon Koch, Jannik Hartung, Rainer Böhme, David Klein</i>	
Position Paper: On the (Non-)Precision of Psychological Measures in Security and Privacy Research - Reliability Beyond Reporting Alpha	277
<i>Nele Borgert, Tim Ulmann, Robin Merchel</i>	
What's in the Mandatory USENIX Security 2025 Ethics Sections? Results from a Meta-Analysis	284
<i>Rachel Gonzalez Rodriguez, Harshini Sri Ramulu, Yasemin Acar</i>	
Fair Enough? Assessing Open Science Practices on a Top-Tier Security Privacy Conference	288
<i>Tiago Heinrich, Sebastian Giessler, David Klein, Alexandra Dirksen</i>	
Evaluating LLMs Reliability for Coding Adversarial Machine Learning Research Papers	294
<i>Madhav Khanal, Jasser Jasser, Mina Basirat</i>	
Position Paper: Living Artifacts: Enabling Vertical Progress in Cybersecurity Research	302
<i>Jelena Mirkovic, David Balenson</i>	

Experience Paper: Is This the Real Life? Is This Just Fantasy? Hunting for Hallucinated References in Paper Submissions	309
<i>Gianluca Stringhini, Jeremy Blackburn</i>	
Experience Paper: “This Paper Is Quite Unusual:” Metascience and Structural Misalignment in the Security & Privacy Research Community	317
<i>Henry Hosseini, Christian Böttger, Nurullah Demir, Tobias Urban</i>	
Inspectable AI for Science: A Research Object Approach to Generative AI Governance	324
<i>Ruta Binkyte, Sharif Abuaddba, Chamikara Mahawaga Arachchige, Ming Ding, Natasha Fernandes Mario Fritz</i>	
Position Paper: Replication Crisis in Human-Centered Security Research-Are We There Yet?	334
<i>Juliane Schmöser, Jan-Ulrich Holtgrave, Florian Schaub, Sascha Fahl</i>	
From “Available” to “Reusable”: Measuring Transparency and Reproducibility of Industrial Control System Datasets Under Security Artifact Evaluation Policies	340
<i>Mohammad Einaam Alim, Tommy Morris</i>	
CyCoAnalysis: A Dataset of Cybersecurity Conference Metadata for Meta-Science and Policy Decisions	349
<i>Marton Bognar, Lieven Desmet, Frank Piessens</i>	
Position Paper: Corrections Not Found - Post-Publication Integrity in Usable Security and Privacy Research	354
<i>Nele Borgert, Luisa Jansen, Lukas Jung, Theresa Halbritter, Malte Elson</i>	
DART: Data Augmentation of Rare ATT&CK Techniques Using LLM Agents	360
<i>Taya Ambrose, Sergio Valderrama, Younghee Park, Álvaro A. Cárdenas</i>	
An Approach to Predictive Software Threat Modeling Using Public Vulnerability Data	370
<i>Onyeka Ezenwoye, Gokila Dorai</i>	
Flexible Generation of Synthetic Attacks for Host Security Datasets	380
<i>Rahul George, Ashwin Kirandumkara, Teryl Taylor, Frederico Araujo, Trent Jaeger</i>	
Zer0n-Bench: A Provenance-Aware Vulnerability Dataset for Studying Label Reliability	390
<i>Harshil Parmar, Pushti Vyas, Prayers Khristi, Priyank Panchal</i>	
Know-It-All?: A Human-Calibrated LLM Benchmark for Cybersecurity Knowledge	400
<i>Athanasios Theocharis, Armin Buescher, Omer Akgul, Dario Pasquini, Oystein Fladby, Dan Marino Christopher Gates, Petros Efsthathopoulos</i>	