

2025 Silicon Valley Cybersecurity Conference (SVCC 2025)

**San Francisco, California, USA
23-25 June 2025**



**IEEE Catalog Number: CFP25DI5-POD
ISBN: 979-8-3315-3430-1**

**Copyright © 2025 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:	CFP25DI5-POD
ISBN (Print-On-Demand):	979-8-3315-3430-1
ISBN (Online):	979-8-3315-3429-5

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

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Large Language Models (LLMs) and Generative AI in Cybersecurity and Privacy: A Survey of Dual-Use Risks, AI-Generated Malware, Explainability, and Defensive Strategies	1
<i>Kiarash Ahi, Saeed Valizadeh</i>	
Helol Tunnel: Covert Channel Exploitation of TLS Extensibility & Privacy Features	9
<i>Reza Soosahabi, Rakesh Seal</i>	
Encrypted Network Traffic Analysis: to Website Fingerprinting and Beyond	19
<i>Madeline Moran, Joshua Honig, Nathan Ferrell, Shreena Soni, Sophia Homan, Eric Chan-Tin, Mohammed Abuhamad</i>	
A Comparative Study of Trust Management Models for Security Enhancement in Wireless Sensor Networks	26
<i>Pranav Gangwani, Alexander Perez-Pons, Himanshu Upadhyay</i>	
SLAP: Secure Location-Proof and Anonymous Privacy-Preserving Spectrum Access	34
<i>Saleh Darzi, Attila A. Yavuz</i>	
Post-Quantum Digital Signature and Authentication for eSIM in 5G Mobile Networking	42
<i>Qaiser Khan, Sourav Purification, Rono Cheruiyot, Jino Kim, Ikkyun Kim, Sang-Yoon Chang</i>	
FeatNet-IDS: Anomaly Detection based-Features for Industrial Internet of Things Systems	49
<i>Wael Alsabbagh, Bahij Sayegh, Chaerin Kim, Peter Langendorfer</i>	
Synthetic Malware Image Generation Based on Generative Models Against Zero-Day Attacks	57
<i>Arjun Sudheer, Ayesha Ahmed, Fabio Di Troia, Younghee Park</i>	
A Comprehensive Software Vulnerability Dataset Based on OWASP Top Ten Standard	66
<i>Moses Ndebugre, Mahmoud Nabil, Ahmad Patooghy, Abdolhossein Sarrafzadeh</i>	
Clickjacking in the Modern Era: Analyzing Emerging Attack Vectors and Advanced Defense Strategies	74
<i>Dipankar Saha, Bhushan Bhimrao Chavan, Vishalkumar Langaliya</i>	
Specialized Language Models for Combating Audio and Video Spam	82
<i>Arnold Spantzel, Adelheid Spantzel</i>	
Inter-Device User Keystroke Analysis	88
<i>Austin Erwin-Martinetti, Amith Kamath Belman</i>	
CELS (Crystalline Encryption Layered Security): A Security Extension of Messaging Applications Using Post-Quantum Cryptography	93
<i>Noah Loke, Vaibhav Kumar Bajpai, Tingting Chen</i>	
Exploring Secure Machine Learning Through Payload Injection and FGSM Attacks on ResNet-50	100
<i>Umesh Yadav, Suman Niroula, Gaurav Kumar Gupta, Bicky Yadav</i>	
Artificially Insecure: Examining GitHub Copilot's AI-Based Vulnerability Prevention System	107
<i>Nathan Armstrong, Thomas Hartley</i>	
Context-Aware Natural Language Processing for Malware Detection	113
<i>Helen Liu, Summer McCune, Quang Duy Tran, Fabio Di Troia, Younghee Park</i>	

A Novel Approach to the Detection of Stegomalware in PDFs Using Kolmogorov Complexity	121
<i>Sebastian Alexis</i>	
Cyber-Security Dashboard: An Extensible Intrusion Detection System for Distributed Controls Systems.....	127
<i>Aidan Jones, Ankita Jaswal, Arpitha Srinivas, Regenal Anastacio, Mahima Agumbe Suresh</i>	
GRU-AUNet: A Domain Adaptation Framework for Contactless Fingerprint Presentation Attack Detection	135
<i>Banafsheh Adami, Nima Karimian</i>	
UAV/Drone Detection and Classification Using Radio Frequency Machine Learning.....	143
<i>Dianne Lopez, Michael Tang, Nathan Lee, Mohammad I Husain</i>	
SyntheticPop: Attacking Speaker Verification Systems with Synthetic VoicePops.....	153
<i>Eshaq Jamdar, Amith Kamath Belman</i>	
Poster: Cloudsweeper: Leveraging Large Language Models to Personalize Sensitive Archive Search.....	161
<i>Victor Escuerdo, Sergio Talavera, Gautam Santhanu Thampy, Ivan Torres, Daniel Vega Lojo, Chris Kanich, Magdalini Eirinaki</i>	
Poster: Entropy and MinHash Fingerprints for Layer-7 Traffic Classification.....	164
<i>Simone Mainardi, Kaushal Bansal, Prabhat Singh</i>	
Reinforcement Learning on Tor: Prioritizing Performance Compromises Anonymity	167
<i>Kelei Zhang, Amanul Islam, Sang-Yoon Chang</i>	
Poster: A Deep-Learning Approach for ECG-Based Cryptographic Key Generation	170
<i>Luciano Maldonado Romero, Nima Karimian, Sara Tehranipoor</i>	
Poster: FortNIC: Secure Container Image Registry on SmartNICs.....	173
<i>Shaunak Galvankar, Sean Choi</i>	
Poster: BlinkSecure: Risk-Aware Continuous Authentication Using Blink-based CAPTCHA and Face Recognition.....	176
<i>Ishan Routray, Ashish Kundu</i>	
Poster: A Case Study on Automated Vulnerability Repair Using Pre-Trained Language Models.....	179
<i>Woorim Han, Miseon Yu, Younghan Lee, Hyungon Moon, Yunheung Paek</i>	
Poster: Threat Intelligence & Modeling Practices for IoMT Devices Using Wi-Fi Communications.....	182
<i>Eva Wilson, Cody Ourique, Bernardo Flores</i>	
Poster: Development of Situation Awareness Measurement for Cybersecurity Professionals	185
<i>David Schuster, Crystal Fausett, Maiyi Huang, Sabina M. Patel, Jenna Korentsides, Joseph R. Keebler, Elizabeth H. Lazzara</i>	
Poster: RTOS Security Risks in Telecommunications Hardware	188
<i>Austin Erwin-Martinetti, Amith Kamath Belman</i>	
Poster: on Website Fingerprinting Defenses and User Tolerances.....	191
<i>Joshua Honig, Madeline Moran, Eric Chan-Tin, Mohammed Abuhamad</i>	
Poster: AI-Driven Security: Investigating LLMs for Automated Vulnerability Detection in Code Changes	194
<i>Sai Ram Motupalli, Sean Choi</i>	

Poster: Synthetic Malware Generation Using Generative Models	197
<i>Tiffany Bao, Kylie Trousil, Quang Duy Tran, Fabio Di Troia, Younghee Park</i>	
The Necessity of Designing Effective Trust Indicators for Mobile Communication Applications to Enhance User Security and Confidence	200
<i>Emily Wayne, Narges Zare</i>	
Demo: LLM-Based Browser Extension for Phishing Detection	205
<i>Eric Pham, Thinh Bui, Haoming Chen</i>	
Demo: A Real-Time Multi-Agent Network Attack Detection and Incident Response System.....	208
<i>Arjun Sudheer, Chia-Hong Chou, Shubham Kumar</i>	
Demo: PhishSense: A LLM-Enhanced Multimodal Framework for Phishing Website Detection.....	211
<i>Tiffany Bao, Tingxuan Tang</i>	
Demo: Dynamic Defense Deployment with LLM-Assisted Client-side Fuzzing in Web Applications.....	214
<i>Jianwei Huang</i>	
Demo: ViolentUTF as an Accessible Platform for Generative AI Red Teaming.....	217
<i>Tam N. Nguyen</i>	
Demo: Fixing C/C++ Vulnerabilities with LLMs : Prompt, Detect, Fix: No More Unsafe Code.....	220
<i>Joseph Gerani, Hei Lam, Ngoc Minh Chau Ho</i>	
Demo: LLM-Based Social Engineering Detection System (LSED).....	223
<i>Alan Park, Britney Jaculina, Dimitar Dimitrov</i>	

Author Index