

2025 Annual Computer Security Applications Conference Workshops (ACSAC Workshops 2025)

**Honolulu, Hawaii, USA
8-9 December 2025**

IEEE Catalog Number: CFP250C1-POD
ISBN: 979-8-3315-4537-6



Copyright © 2025, 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:	CFP250C1-POD
ISBN (Print-On-Demand):	979-8-3315-4537-6
ISBN (Online):	979-8-3315-4536-9

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

CYPHER: Adaptive Cyber–Physical Fuzzing for ICS Security	15
<i>Stacy A. Willson, Qian Chen</i>	
Adapting Noise-Driven PUF and AI for Secure WBG ICS: A Proof-of-Concept Study	28
<i>Devon A. Kelly, Christiana Chamon</i>	
Robust Vulnerability Estimation in Industrial Firmware via Incomplete Knowledge Graph Similarity	39
<i>Wei Wang, Mitsuharu Tai, Shota Fujii, Hiroki Yamazaki, Eriko Ando</i>	
Multimodal LLM-Based Identification and Fingerprinting of Internet-Exposed IoT Devices via WebUI Analysis	54
<i>Kotoe Goya, Kano Hayashi, Ryu Kuki, Takayuki Sasaki, Katsunari Yoshioka</i>	
Towards Autonomous Edge-based Machine Learning and Anomaly Detection for Manufacturing	66
<i>Zachary Neal, Curtis R. Taylor</i>	
Under Pressure: Security Analysis and Process Impacts of a Commercial Smart Air Compressor	76
<i>Jad Zarzour, Matthew Jablonski</i>	
Triaging Firmware Updates for Critical Systems to Defend Against Software Supply Chain Threats	87
<i>Nathan Harrison, Dylan Stancil, Marshall Nelson, Samuel Mulder</i>	
Securing Modbus-Based Industrial Control Systems with Refined Multiparty Session Types	99
<i>Max Taylor, Arthur Amorim, Lance Joneckis</i>	
Continuous Monitoring of Cybersecurity in U.S. Rural Hospitals	110
<i>William Yurcik, Rhonda O’Kane, Stephen North, O. Sami Saydjari, Fábio Robero de Miranda Rodolfo da Silva Avelino, Rohan Pluta, Gregory Pluta</i>	
SoK: Hospital Medical Devices as Industrial Control Systems (ICS) - Exposure and Vulnerability	122
<i>J. Malakai Bailey, William Yurcik, O. Sami Saydjari, Rodolfo da Silva Avelino, João Luisi Vieira Pedro Umbelino, Gregory Pluta</i>	
SoK: Hospital at Home Model of Care - Toward Appropriate Use Cases and Other Challenges	134
<i>Rodolfo Da Silva Avelino, Elise Bolda, Guenevere Qian Chen, Diane Dolezel, Jon Mark Hirshon Joseph Kane, Sarah Klein, C. Scott Kruse, Bruce Leff, David M. Levine, Michael Maniaci Monique K. Mansoura, Patricia McGaffigan, John McHugh, Fábio Roberto de Miranda Subhas Mukhopadhyay, Jay Pandit, Gregory Pluta, Martin Pumera, Raj Rajagopalan, Esa Rantanen Richard Rothman, Rami Saydjari, O. Sami Saydjari, Malcolm Schongalla, John Schumacher Naomi Schwartz, Keval K. Sonigara, Natalie Sullivan, Eugene Y. Vasserman, Nalini Venkatasubramanian Thad Wilkins, Christopher Worsham, William Yurcik</i>	
Position Paper: Hospital-at-Home is not Telehealth	157
<i>Bruce Leff, David M. Levine, C. Scott Kruse, William Yurcik</i>	
Change Healthcare – Perspective and Lessons from the Nationwide Pharmacy Supply Chain Failure	159
<i>William Yurcik, Andreas Schick</i>	
PatDiscover: Privacy-Preserving Discoverability of Patients	169
<i>Jan Pennekamp, Johannes Lohmöller, Niels Pressel, Sandra Geisler, Felix M. Mottaghy, Klaus Wehrle</i>	

A Moonshot for Trustworthy Medical Software Updates Using Automated Insulin Delivery Systems as a Proving Ground	185
<i>Josiah Dykstra, Shannon Lantzy, Eugene Y. Vasserman</i>	
Adversarial use of protein language models for modeling escape	199
<i>Sayantani B. Littlefield, Roy H. Campbell</i>	
The Conficker Worm – A Persistent Hospital Device Malware	203
<i>Marcus H. Sachs</i>	
FedSecRPM: Federated Learning-Based Analytics for Sensor-Based Remote Patient Monitoring	207
<i>Subrahmanya Chandra Bhamidipati, Mauro Lemus Alarcon, Tanner Kuchar, Judah Robbins Bernal Prasad Calyam</i>	
Secure and Privacy-Preserving Secondary Data Use: A Framework for Cross-Domain Computation in the Encrypted Domain	212
<i>Dimitra Papatsaroucha, Cristina Regueiro, Marisa Escalante, Maurizio Martignano, Velislava Hillman Evangelos K. Markakis</i>	
Applying Public Health Systematic Approaches to Cybersecurity: The Economics of Collective Defense	222
<i>Josiah Dykstra, William Yurcik</i>	
Probing Challenges and Future Research of SBOM Generation for Medical Devices	230
<i>Hui Zhuang, Yan Long, Duyeong Kim, Jennifer R. Amos, Heejo Lee, Kevin Fu</i>	
Compliance v. Completeness: A Case Study on SBOMs in Consideration of FDA Premarket Cybersecurity Guidance	236
<i>Logan Kostick, Michael Rushanan, Tushar M. Jois</i>	
The SBOM Transparency v. Exposure Dilemma: A Case Study on Adversarial Access to Public SBOMs in Healthcare	242
<i>Jiarou Deng, Yang Yang, Michael Rushanan</i>	
AI/ML Trustworthiness for Medical Predictions – Experimental Results	248
<i>Mohimenul Karim, Tanmoy Sarkar Pias, Bimal Viswanath, Danfeng Daphne Yao</i>	
AI on Trial: LLM-as-a-Judge for Private and Reliable Clinical Decision-Making	256
<i>Tanveer Khan, Maaz Rafiq, Antonis Michalas</i>	
Security Risks in Medical AI: Logo-Based Trojan Attacks on Deep Learning Models	263
<i>Pavan Reddy, Nithin Reddy</i>	
CRASHCART: Truckin’ in a Backup System to Revive Hospitals During Computer Outages	271
<i>Almog Bar-Yossef, Kartikeyan Subramanyam, Jonathon Guthrie, Alex Gao, Christian Dameff, Jeff Tully Aaron Schulman</i>	
A Game-Theoretic and AI Approach to Secure and Intelligent Hospital at Home Monitoring	281
<i>Desiree Rivers, Qian Chen</i>	
Goal-Driven Risk Assessment for LLM-Powered Systems: A Healthcare Case Study	290
<i>Neha Nagaraja, Hayretin Bahsi</i>	

EmpathAI: A Trustworthy and Secure Conversational Agent for Mental Healthcare	298
<i>Vani Seth, Ashish Pandey, Kavya Gundlapalli, Mahesh Duvvuri, Rithvik Mettu, Iris Zachary Prasad Calyam</i>	
Evaluating Systemic Risk in DAO Networks	302
<i>Abylay Satybaldy, Kamil J. Tylinski, Marco Alberto Javarone, Paolo Tasca</i>	
ZK-Disclosure: Privacy-Preserving Information Disclosure for Digital Evidence with C2PA and zk-SNARKs	309
<i>Johnny Marinho, Eryk Schiller, Arthur Debaugé, Noria Foukia</i>	
Framework for GDPR and HIPAA Compliance in Healthcare Applications using Zero-Knowledge Proofs	316
<i>Mohammad Madine, Yousuf Alsalami, Khaled Salah, Raja Jayaraman</i>	
Assure-exam: A blockchain-based assurance framework for secure and transparent Exam Paper Distribution	323
<i>Maruf Farhan, Madhuki Rajapakshe, Rejwan Bin Sulaiman, Usman Butt</i>	
Building A Secure Agentic AI Application Leveraging Google's A2A Protocol	332
<i>Vineeth Sai Narajala, Idan Habler, Ken Huang, Prashant Kulkarni</i>	
Prompting the Priorities: Evaluating LLMs for Organization-Specific Vulnerability Prioritization	341
<i>Osama Al Haddad, Muhammad Ikram, Muhammad Ejaz Ahmed, Young Lee</i>	
PrivPicket: Privacy Preserving Serverless Workflows via Optimized Dummy Node Insertion	349
<i>Surabhi Garg, Ratul Kishore Saha, Manju Ramesh, Rajan M A, Dheeraj Chahal</i>	
ByteFlow: A Byte-Level LLM for Deep Packet Inspection and Network Intelligence	357
<i>Abanisenioluwa Orojo, Emmanuelli El-Mahmoud, Erika Leal, Pablo Rivas</i>	
Database Deception using Large Language Models	366
<i>Jason Landsborough, Neil C. Rowe, Thuy D. Nguyen</i>	
IntelForge: Multi-Agent LLM Framework for Cyber Threat Intelligence Enrichment	374
<i>Noam Tarshish, Daniel Hodisan, Asaf Shabtai</i>	
Securebert 2.0: Advanced Language Model for Cybersecurity Intelligence	382
<i>Ehsan Aghaei, Sarthak Jain, Prashanth Arun, Arjun Sambamoorthy</i>	
Can Current Detectors Catch Face-to-Voice Deepfake Attacks?	389
<i>Nguyen Linh Bao Nguyen, Alsharif Abuadbba, Kristen Moore, Tingmin Wu</i>	
SCORE: Syntactic Code Representations for Static Script Malware Detection	397
<i>Ecenaz Erdemir, Kyuhong Park, Yi Fan</i>	
Proof-Carrying Answers: A Systematic Protocol for Verifiable Retrieval-Augmented Generation with Cryptographic Provenance	405
<i>Shivani Shukla, Himanshu Joshi</i>	
Cybersecurity Threat Intelligence for Audit: LLM Scoping, Evidence Guardrails, and Materiality	414
<i>Gurkan Akalin, Ning Zhou</i>	
On the Potential of LLMs for Offensive Security: Benchmarks vs. Operational Reality	420
<i>Ruben Missotten, Vera Rimmer, Wim Mees, Lieven Desmet</i>	

Towards Automatic Triage and Taxonomy of Adversary Shell-Scripts	428
<i>Jared Chandler</i>	
AgentNIRS: An LLM-Driven Agent for Network Intrusion Response	436
<i>Rachida Saroui, Thomas Marchioro, Alexis Olivereau</i>	
AthenaBench: A Dynamic Benchmark for Evaluating LLMs in Cyber Threat Intelligence	443
<i>Md Tanvirul Alam, Dipkamal Bhusal, Salman Ahmad, Nidhi Rastogi, Peter Worth</i>	
AgentCyTE: Leveraging Agentic AI to Generate Cybersecurity Training & Experimentation Scenarios	451
<i>Ana M. Rodriguez, Jaime Acosta, Anantaa Kotal, Aritran Piplai</i>	
Trust-Calibrated Multi-Stage Large Language Model Pipeline for Vulnerability Assessment in DevSecOps Workflows	459
<i>Adiba Mahmud, Yasmeen Rawajfih, Ross Arnold</i>	
Performance-Efficiency Trade-offs in Anomaly Detection Architectures for Zero-Day IoT Attack Detection: A Systematic Benchmark on CIIoT2023	467
<i>Raymond Lee, Yunpeng Zhang</i>	
Trust-Adaptive Agentic Retrieval Framework for LLM-Based Cyber Threat Intelligence	473
<i>Jayesh Guntupalli, Kentarou Watanabe</i>	
Attacks & Defenses Against LLM Fingerprinting	480
<i>Kevin Kurian, Ethan Holland, Sean Oesch</i>	
Ransomware in Active Directory: A Dataset and Analysis of Early-Stage Behavior	491
<i>Prajna Bhandary, Charles Nicholas, Robert J. Joyce, Bojing Li</i>	
User Study of a Network Debugger on FABRIC	501
<i>Alexander Wolosewicz, Vinod Yegneswaran, Ashish Gehani, Nik Sultana</i>	
CTIGuardian: A Few-Shot Framework for Mitigating Privacy Leakage in Fine-Tuned LLMs	510
<i>Shashie Dilhara Batan Arachchige, Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Dinusha Vatsalan Dali Kaafar</i>	
A Multi-Cloud Framework for Zero Trust Workload Authentication	523
<i>Saurabh Deochake, Ryan Murphy, Jeremiah Gearheart</i>	
NOPoutNG: Improving the Effectiveness of Hardware-assisted Control-flow Integrity via Dynamic Landing Pad Elision	531
<i>Alexander J. Gaidis, Jamie Gabbay, Joao Moreira, Vasileios P. Kemerlis</i>	
Not Discrete Enough: On the Inherent Insecurity of dTPMs for Measured Boot	546
<i>Christian Werling, Tahmid Zahin, Jean-Pierre Seifert</i>	
A New Hope for DARPA OpTC	551
<i>Frédéric Majorczyk, Barbara Pilastre, Fanny Dijoud</i>	
Autopwn: Automatic Code-Reuse Exploit Generation Framework with Agentic AI	562
<i>Kaleb Bacztub, Dylan Christensen, Arun Ravindran, Meera Sridhar</i>	
Systematic evaluation of security attacks to household consumer smart doorbells	569
<i>Ashley Mark Brown, Nilufer Tuptuk, Enrico Mariconti, Shane D Johnson</i>	

Open 5G Testbed: A Cyber Range Platform for Security Research	579
<i>Azza H. Ahmed, Thomas Dreibholz, Foivos Ioannis Michelinakis, Tarik Čičić</i>	
MudHunter: Internet-Scale DNS Cache Snooping for Cyber Threat Intelligence	587
<i>Bassel Succar, Joseph Khoury, Antonia Affinito, Elias Bou-Harb</i>	