

2024 Annual Computer Security Applications Conference Workshops (ACSAC Workshops 2024)

**Honolulu, Hawaii, USA
9-10 December 2024**



**IEEE Catalog Number: CFP240C1-POD
ISBN: 979-8-3315-3282-6**

**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:	CFP240C1-POD
ISBN (Print-On-Demand):	979-8-3315-3282-6
ISBN (Online):	979-8-3315-3281-9

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

CURRAN ASSOCIATES INC.
proceedings
.com

2024 Annual Computer Security Applications Conference Workshops (ACSAC Workshops) **ACSACW 2024**

Table of Contents

Message from the Conference Chairs	x
Message from the Workshop Chairs	xii
Message from the Sponsor: Applied Computer Security Associates (ACSA)	xiii
ACSA Members	xv

ARTMAN

ML for Cybersecurity

Inherently Interpretable and Uncertainty-Aware Models for Online Learning in Cyber-Security Problems	1
<i>Benjamin Kolicic (The Alan Turing Institute), Alberto Caron (The Alan Turing Institute), Vasilios Mavroudis (The Alan Turing Institute), and Chris Hicks (The Alan Turing Institute)</i>	
Dark Watchdog: A Novel RAG-Driven System for Real-Time Detection and Analysis of Data Leaks on Dark Web Forums	11
<i>Shing-Li Hung (National Tsing Hua University, Taiwan), Chung-Kuan Chen (CyCraft Technology, Taiwan), Keisuke Furumoto (National Institute of Information and Communications Technology, Japan), Takeshi Takahashi (National Institute of Information and Communications Technology, Japan), and Hung-Min Sun (National Tsing Hua University, Taiwan)</i>	
Intrusion Detection Simplified: A Feature-Free Approach to Traffic Classification using Transformers	20
<i>Kohei Miyamoto (National Institute of Information and Communications Technology, Japan), Chansu Han (National Institute of Information and Communications Technology, Japan), Tao Ban (National Institute of Information and Communications Technology, Japan), Takeshi Takahashi (National Institute of Information and Communications Technology, Japan), and Jun'ichi Takeuchi (Kyushu University, Japan)</i>	

Robustness, Privacy and Safety for ML Systems I

Balancing Safety and Security in Autonomous Driving Systems: A Machine Learning Approach with Safety-First Prioritization	30
<i>Afshin Hasani (University of Guilan, Iran), Mehran Alidoost Nia (Shahid Beheshti University, Iran), and Reza Ebrahimi Atani (University of Guilan, Iran)</i>	
Restoring Unintended Model Learning by Error Correcting Code	42
<i>Nami Ashizawa (NTT Social Informatics Laboratories, Japan), Toshiki Shibahara (NTT Social Informatics Laboratories, Japan), Naoto Kiribuchi (NTT Social Informatics Laboratories, Japan), Osamu Saisho (NTT Social Informatics Laboratories, Japan), and Naoto Yanai (Osaka University, Japan)</i>	

Robustness, Privacy and Safety for ML Systems II

Learning to Unfix: Towards ML Robustness in Vulnerability Detection via Structure-Aware Code Generation	51
<i>Muhammad Fakhur Rozi (National Institute of Information and Communications Technology, Japan) and Takeshi Takahashi (National Institute of Information and Communications Technology, Japan)</i>	
Does Prompt-Tuning Enhance Privacy in Large Language Models?	59
<i>Tsunato Nakai (Mitsubishi Electric Corporation, Japan), Kento Oonishi (Mitsubishi Electric Corporation, Japan), and Takuya Higashi (Mitsubishi Electric Corporation, Japan)</i>	

Attack to ML Algorithms

The Impact of Active Learning on Availability Data Poisoning for Android Malware Classifiers	73
<i>Shae McFadden (King's College London; The Alan Turing Institute; University College London), Zeliang Kan (King's College London; University College London), Lorenzo Cavallaro (University College London, United Kingdom), and Fabio Pierazzi (University College London; King's College London)</i>	
When AI Meets Code Analysis: A Study of Adversarial Attacks on Deep Learning-Based Code Models via Program Transformation	85
<i>Avilash Rath (The University of Texas at Dallas), Youpeng Li (The University of Texas at Dallas), Troy Davis (Cypress Woods High School), Braden Bronaugh (Cypress Woods High School), Darsh Poddar (Lebanon Trail High School), Sophia Li (Lovejoy High School), and Xinda Wang (The University of Texas at Dallas)</i>	
AdVul: Adversarial Attack against ML-Based Vulnerability Detection	97
<i>Marina Katoh (The University of Tulsa, USA), Weiping Pei (The University of Tulsa, USA), and Youye Xie (University of Illinois Urbana-Champaign, USA)</i>	

ICSS

Assurance of Application Security on IIoT Platforms with Knowledge Augmentation	108
<i>Yannick Landeck (fortiss GmbH, Germany), Dian Balta (fortiss GmbH, Germany), Martin Wimmer (Siemens AG, Germany), and Christian Knierim (Siemens AG, Germany)</i>	
Towards Provable Security in Industrial Control Systems Via Dynamic Protocol Attestation	120
<i>Arthur Amorim (University of Central Florida, USA), Trevor Kann (Carnegie Mellon University, USA), Max Taylor (Idaho National Laboratory, USA), and Lance Joneckis (Idaho National Laboratory, USA)</i>	
MFAA: Historical Hash Based Multi-Factor Authentication and Authorization in IIoT	133
<i>Eyasu Getahun Chekole (Singapore University of Technology and Design, Singapore) and Jianying Zhou (Singapore University of Technology and Design, Singapore)</i>	
Attacks on EtherNet/IP and Migrations through CIP Security	145
<i>Alexander Gebhard (Marquette University, USA) and Debbie Perouli (Marquette University, USA)</i>	
Conducting Attack Scenarios and Forensic Techniques in a Virtual ICS Test Bed	155
<i>Chris Churilla (University of Arizona, USA)</i>	

WAITI with IOT-SCTI

AI-Driven Cybersecurity Solutions for CTI, IoT and Software Infrastructures

MIND-IoT: Machine Intelligence and Data-Mining for IoT Threats	163
<i>Kwabena Aboagye-Otchere (The University of Texas Rio Grande Valley, USA) and Jorge Castillo (The University of Texas Rio Grande Valley, USA)</i>	
A Privacy-Preserving Byzantine-Aware Swarm Learning Framework for CTI	171
<i>Marco Arazzi (University of Pavia, Italy), Dincy R. Arikkat (Cochin University of Science and Technology, India), Mert Cihangiroglu (University of Pavia, Italy), and Sameera K. M. (Cochin University of Science and Technology, India)</i>	
Automating AWS Security Controls: Leveraging Generative AI for Gherkin Script Generation	178
<i>Chen Ling (Emory University), Mina Ghashami (Amazon), Kyuhong Park (Amazon), Ali Torkamani (Amazon), Nivedita Mangam (Amazon), Bhavya Jain (Amazon), Malini SS (Amazon), Felix Candelario (Amazon), Farhan Diwan (Amazon), and Mingrui Cheng (Amazon)</i>	
The Rings of Tracking: Evaluating Security and Privacy in the Smart Ring Ecosystem	186
<i>Johannes Ludwig (Ruhr University Bochum), Veelasha Moonsamy (Ruhr University Bochum), and Matteo Große-Kampmann (Rhine-Waal University of Applied Sciences)</i>	
Cyber Attack Detection for Internet of Health Things through Federated Deep Learning Technique	194
<i>Liyakathunisa Liyakathunisa (Taibah University, Saudi Arabia), Zoya Riyaz Syeda (Rajiv Gandhi University of Health Science, India), and Riyaz Sohale Syed (Independent Researcher, India)</i>	

MAD: A Meta-Learning Approach to Detect Advanced Persistent Threats using Provenance Data in Industrial IoT	201
<i>Bikash Saha (Indian Institute of Technology Kanpur, India), Nanda Rani (Indian Institute of Technology Kanpur, India), and Sandeep Kumar Shukla (Indian Institute of Technology Kanpur, India)</i>	

Leveraging Large Language Models for Cybersecurity and Threat Intelligence

Generating Abuse Stories and Misuse Cases using Large Language Models	208
<i>Carmen Cheh (Illinois Advanced Research Center at Singapore Ltd., Singapore), Nan Shing Kham Shing (Singapore University of Technology and Design, Singapore), Reuben Lim (Illinois Advanced Research Center at Singapore Ltd., Singapore), and Binbin Chen (Singapore University of Technology and Design, Singapore)</i>	
Software Vulnerability Detection using LLM: Does Additional Information Help?	216
<i>Samiha Shimmi (Northern Illinois University, USA), Yash Saini (Northern Illinois University, USA), Mark Schaefer (Northern Illinois University, USA), Hamed Okhravi (MIT Lincoln Laboratory, USA), and Mona Rahimi (Northern Illinois University, USA)</i>	
Retrieval of Network Packets Information using a Generated Latent Space Representation for Network Analysis in Cyber Security	224
<i>Ofir Manor (Fujitsu Research of Europe, UK), Ortal Lavi (Fujitsu Research of Europe, Israel), Tomer Schwartz (Fujitsu Research of Europe, Israel), Motoyoshi Sekiya (Fujitsu Research of Europe, UK), Junichi Suga (Fujitsu Limited, Japan), Kenji Hikichi (Fujitsu Limited, Japan), Yuki Unno (Fujitsu Limited, Japan), and Andrés F. Murillo (Fujitsu Research of Europe, UK)</i>	
Formal Trust and Threat Modeling using Large Language Models	232
<i>Zhihao Yao (New Jersey Institute of Technology, USA)</i>	
Fine-Tuning Large Language Models for DGA and DNS Exfiltration Detection	240
<i>Md Abu Sayed (University of Texas at El Paso, USA), Asif Rahman (University of Texas at El Paso, USA), Christopher Kiekintveld (University of Texas at El Paso, USA), and Sebastian García (CTU - Czech Technical University, Czech Republic)</i>	
Exploring Large Language Models for Semantic Analysis and Categorization of Android Malware	248
<i>Brandon J Walton (Louisiana State University, USA), Mst Eshita Khatun (Louisiana State University, USA), James M Ghawaly (Louisiana State University, USA), and Aisha Ali-Gombe (Louisiana State University, USA)</i>	
Advancing TTP Analysis: Harnessing the Power of Large Language Models with Retrieval Augmented Generation	255
<i>Reza Fayyazi (Rochester Institute of Technology, USA), Rozhina Taghdimi (Rochester Institute of Technology, USA), and Shanchieh Jay Yang (Gonzaga University, USA)</i>	

WEB3SEC

Automated Vulnerability Detection in Smart Contracts using Control Flow Graphs and Machine Learning	262
<i>Charles Lohest (UCLouvain, Belgium), Samy Bettaieb (UCLouvain, Belgium), and Axel Legay (UCLouvain, Belgium)</i>	
Privacy-Preserving Financial Anomaly Detection via Federated Learning & Multi-Party Computation	270
<i>Sunpreet Arora (Visa Research), Andrew Beams (Visa Research), Panagiotis Chatzigiannis (Visa Research), Sebastian Meiser (University of Lübeck), Karan Patel (Visa Research), Srinivasan Raghuraman (Visa Research), Peter Rindal (Visa Research), Harshal Shah (Visa Research), Yizhen Wang (Visa Research), Yuhang Wu (IndicatorLab), Hao Yang (Splunk Inc.), and Mahdi Zamani (Visa Research)</i>	
Fast and Secure Consensus Protocol for Ethereum 2.0	280
<i>Shinsaku Naito (The University of Tokyo, Japan) and Kanta Matsuura (The University of Tokyo, Japan)</i>	
Blockchain-Based Sustainability, Traceability, and Certification of Hydrogen Production	288
<i>Sultan Alshehhi (Khalifa University, United Arab Emirates), Ahmad Musamih (Khalifa University, United Arab Emirates), Khaled Salah (Khalifa University, United Arab Emirates), Ahmad Mayyas (Khalifa University, United Arab Emirates), and Raja Jayaraman (New Mexico State University, USA)</i>	
Author Index	299