

2024 IEEE Conference on Communications and Network Security (CNS 2024)

**Taipei, Taiwan
30 September - 3 October 2024**



**IEEE Catalog Number: CFP24CNM-POD
ISBN: 979-8-3503-7597-8**

**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:	CFP24CNM-POD
ISBN (Print-On-Demand):	979-8-3503-7597-8
ISBN (Online):	979-8-3503-7596-1
ISSN:	2474-025X

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

NetHawk : Hunting Advanced Persistent Threats Via Structural and Temporal Graph Anomalies.....	1
<i>Benjamin Bowman, Isaiah J. King, Rimon Melamed, H. Howie Huang</i>	
Uncovering Recurring Vulnerabilities Through Taint-Extracted Operator Sequences	10
<i>Chang-Ming Yang, Che-Jui Hsu, Tao Ban, Takeshi Takahashi, Hsu-Chun Hsiao</i>	
CommanderGPS: Practical Hidden Command Dissemination Through Pedal Operations	19
<i>Edwin Yang, Guanchong Huang, Song Fang</i>	
Enhancing the McEliece Scheme Based on Concatenation of Polar Codes and Blocked QC-LDPC Codes.....	28
<i>Xin Lin, Yusun Fu, Zihao Wang, Junpeng Yin</i>	
Universal Adversarial Attack for Sybil Detection System.....	34
<i>Xin Yao, Kecheng Huang, Ting Yao</i>	
SAFE-IoT: Attesting Firmware in IoT Swarms Using Volatile Memory and a Mixture of Experts.....	43
<i>Varun Kohli, Muhammad Naveed Aman, Biplab Sikdar</i>	
UQuery: Static Security Analysis of PHP-Based Web Programs Using Graph Models.....	52
<i>Jin Huang, Junjie Zhang, Jialun Liu, Chuang Li, Rui Dai</i>	
Adversarial Attacks on Federated Learning Revisited: A Client-Selection Perspective.....	61
<i>Xingyu Lyu, Shixiong Li, Ning Wang, Tao Li, Danjue Chen, Yimin Chen</i>	
A Blockchain-PUF-Based Secure Mutual Authentication Scheme for IoT	70
<i>Ei-Jie Li, Hui-Tang Lin, Hao-Ren Yang</i>	
RF Sensing-Enabled Interference Mitigation for Wi-Fi-Based IoT Systems: A Deep Learning Approach	79
<i>Chunhui Lin, Gen Li, Xiaonan Zhang, Linke Guo</i>	
W-MIA: Membership Inference Attack Against Deep Learning-Based RF Fingerprinting	88
<i>Yan Zhang, Jiawei Li, Dianqi Han, Yanchao Zhang</i>	
ProFLingo: A Fingerprinting-Based Intellectual Property Protection Scheme for Large Language Models.....	97
<i>Heng Jin, Chaoyu Zhang, Shanghao Shi, Wenjing Lou, Y. Thomas Hou</i>	
Building ToF Resiliency into UWB-Based Secure Distance Bounding Protocols	106
<i>Raphael E. Nkrow, Dutliff Boshoff, Bruno J. Silva, Zhe Liu, Gerhard P. Hancke</i>	
CrossAlert: Enhancing Multi-Stage Attack Detection Through Semantic Embedding of Alerts Across Targeted Domains.....	115
<i>Nadia Niknami, Vahid Mahzoon, Jie Wu</i>	
POP-FA: Paillier and Order-Preserving Encryption-Based Facial Authentication	124
<i>Yatish Dubasi, William Burroughs, Qinghua Li</i>	
Membership Inference Via Self-Comparison	133
<i>Jiadong Lou, Xu Yuan</i>	

Protecting Activity Sensing Data Privacy Using Hierarchical Information Dissociation.....	142
<i>Guangjing Wang, Hanqing Guo, Yuanda Wang, Bocheng Chen, Ce Zhou, Qiben Yan</i>	
Shared Resource Entanglement Attacks Against Serverless Computing.....	151
<i>Yuwen Cui, Mingkui Wei, Zhuo Lu, Yao Liu</i>	
TrustHeartbeat: A Trustworthy Multimodal Interactive System with Heartbeat Recognition and User Identification.....	160
<i>Yan Zhang</i>	
Channel-Centric Spatio-Temporal Graph Networks for Network-Based Intrusion Detection	169
<i>Eduardo Santos Escriche, Jakob Nyberg, Yeongwoo Kim, György Dán</i>	
mmPalm: Unlocking Ubiquitous User Authentication Through Palm Recognition with mmWave Signals	178
<i>Yucheng Xie, Xiaonan Guo, Yan Wang, Jerry Q. Cheng, Tianfang Zhang, Yingying Chen, Yi Wei, Yuan Ge</i>	
Context-Aware Anomaly-Based Detection for Ransomware Using Multivariate Feature	187
<i>Millati Pratiwi, Yoon-Ho Choi</i>	
Multi-Sensor Data Privacy Protection with Adaptive Privacy Budget for IoT Systems.....	196
<i>Xinyi Liu, Ye Zheng, Zhengxiong Li, Yidan Hu</i>	
A Data-Driven Evaluation of the Current Security State of Android Devices.....	205
<i>Ernst Leierzopf, René Mayrhofer, Michael Roland, Wolfgang Studier, Lawrence Dean, Martin Seiffert, Florentin Putz, Lucas Becker, Daniel R. Thomas</i>	
Thelma: Threat Hunting Enhanced Language Models for Hunt Automation.....	214
<i>Raymund Lin</i>	
SecBeam: Securing mmWave Beam Alignment Against Beam-Stealing Attacks	223
<i>Jingcheng Li, Loukas Lazos, Ming Li</i>	
DisLLM: Distributed LLMs for Privacy Assurance in Resource-Constrained Environments	232
<i>Sumudith Sadeepa, Keshara Kavinda, Emmanuel Hashika, Chamara Sandeepa, Tharindu Gamage, Madhusanka Liyanage</i>	
HoneyLLM: Enabling Shell Honey pots with Large Language Models	241
<i>Chongqi Guan, Guohong Cao, Sencun Zhu</i>	
PLTA: Private Location Task Allocation Using Multidimensional Approximate Agreement	250
<i>Abderrafi Abdeddine, Amine Boussetta, Youssef Iraqi, Loubna Mekouar</i>	
Device-Independent Tokens with Password Protection Against Token Stealing.....	259
<i>Preston Haffey, Reihaneh Safavi-Naini, Sabyasachi Dutta</i>	
Privacy-Preserving Hierarchical Model-Distributed Inference	268
<i>Fatemeh Jafarian Dehkordi, Yasaman Keshtkarjahromi, Hulya Seferoglu</i>	
A Scalable Double-Oracle Algorithm for Multi-Domain Deception Game.....	277
<i>Ahmed Bilal Asghar, Ahmed Hemida, Charles Kamhoua, Jon Kleinberg</i>	
Unlearning Backdoor Attacks in Federated Learning.....	286
<i>Chen Wu, Sencun Zhu, Prasenjit Mitra, Wei Wang</i>	

An Empirical Study on Learning Models and Data Augmentation for IoT Anomaly Detection	295
<i>Alireza Toghiani Khorasgani, Paria Shirani, Suryadipta Majumdar</i>	
Privacy-Preserving Network Anomaly Detection on Homomorphically Encrypted Data.....	304
<i>Tatjana Wingarz, August See, Florian Gondesén, Mathias Fischer</i>	
LLM Honeypot: Leveraging Large Language Models as Advanced Interactive Honeypot Systems	313
<i>Hakan T. Otal, M. Abdullah Canbaz</i>	
Adaptive Privacy-Preserving Task Scheduling with User Device Collaboration in High-Density Edge Computing Environments.....	319
<i>Hung-Chin Jang, Ting-Ching Li</i>	
A Resilient RAP Solution Using Market-Based Multi-Agent Systems	325
<i>Li Bai, Anway Bose, Zhuo Li</i>	
Enhancing Smart Grid Security: An Data-Driven Anomaly Detection Framework	331
<i>Nguyen Khanh Son, Arun Kumar Sangaiah, Darshan Vishwasrao Medhane, Mohammed J. F. Alenazi, Salman A. Alqahtani</i>	
Physical Layer Security: Learning-Aided Attack Detection Based on 5G NR SRS.....	337
<i>Jonas Ninnemann, Felix Rauschert, Paul Schwarzbach, Pascal Kerschke, Oliver Michler</i>	
Remote Attestation with Software Updates in Embedded Systems.....	343
<i>Ahmad B. Usman, Mikael Asplund</i>	
Device-Specific Anomaly Detection Models for IoT Systems.....	349
<i>Shahrzad Golestani, Dwight Makaroff</i>	
Persistent Distance Bounding for Mobile Provers.....	355
<i>Raphael E. Nkrow, Dutliff Boshoff, Bruno J. Silva, Zhe Liu, Gerhard P. Hancke</i>	
Evaluation of the Communication Efficiency in MQTT 5.0 End-To-End Security Architecture.....	361
<i>An-Tong Shih, Hung-Yu Chien, Yuh-Ming Huang</i>	
Explainable Autonomic Cybersecurity System for Smart Power Grid.....	367
<i>Chengjun Zhang, Wenda Shao, Xianglong Wang, Yinzi Cao, Ahmed Hussain J Alhamadah, Yu-Zheng Lin, Pratik Satam, Lanier Watkins</i>	
Quality Analysis in IDS Dataset: Impact on Model Generalization	373
<i>Didik Sudyana, Miel Verkerken, Laurens D'Hooze, Ying-Dar Lin, Ren-Hung Hwang, Yuan- Cheng Lai, Fietyata Yudha, Tim Wauters, Bruno Volckaert, Filip De Turck</i>	
SecFedDrive: Securing Federated Learning for Autonomous Driving Against Backdoor Attacks	379
<i>Rahul Kumar, Gabrielle Ebbrecht, Junaid Farooq, Wenqi Wei, Ying Mao, Juntao Chen</i>	
DQN-Based Adaptive Network Architecture for High-Fidelity NGN Flow Classification.....	385
<i>Ang Peng Chuan Alvin, Purnima Murali Mohan, Peter Loh Kok Keong, Vivek Balachandran, Choo Yuh Joo</i>	

Author Index