2023 IEEE Conference on Communications and Network Security (CNS 2023)

Orlando, Florida, USA
2-5 October 2023

IEEE Catalog Number: CFP23CNM-POD
ISBN: 979-8-3503-3946-8

Copyright © 2023 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:	CFP23CNM-POD
ISBN (Print-On-Demand):	979-8-3503-3946-8
ISBN (Online):	979-8-3503-3945-1

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

SecureImgStego: A Keyed Shuffling-Based Deep Learning Model for Secure Image Steganography................ 1
Trishna Chakraborty, Imranur Rahman, Hasan Murad, Md Shohrab Hossain, Shagufta Mehnaz

Machine Learning-Based Intrusion Detection for Swarm of Unmanned Aerial Vehicles 10
Umair Ahmad Mughal, Samuel Chase Hassler, Muhammad Ismail

Byzantine-Robust Federated Learning with Variance Reduction and Differential Privacy 19
Zikai Zhang, Rui Hu

When Good Turns Evil: Encrypted 5G/4G Voice Calls Can Leak Your Identities 28
Jingwen Shi, Tian Xie, Guan-Hua Tu, Chunyi Peng, Chi-Yu Li, Andrew Hou, Sihan Wang, Yiwen Hu, Xinyu Lei, Min-Yue Chen, Li Xiao, Xiaoming Liu

Speaker Anonymity and Voice Conversion Vulnerability: A Speaker Recognition Analysis 37
Shalini Saini, Nitesh Saxena

P3LI5: Practical and confidEntial Lawful Interception on the 5G Core... 46
Francesco Intoci, Julian Sturm, Daniel Fraunholz, Apostolos Pyrgelis, Colin Barschel

Enhancing Security in NOMA-Based Networks: An Effective Deceptive Approach to Thwart Multiple Eavesdroppers... 55
Neji Mensi, Danda B. Rawat

Using Phone Sensors to Augment Vehicle Reliability 64
Noah T. Curran, Arun Ganesan, Mert D. Pesé, Kang G. Shin

RMDM: Using Random Meta-Atoms to Send Directional Misinformation to Eavesdroppers 73
Fahid Hassan, Zhambyl Shaikhanov, Hichem Guerboukha, Daniel M. Mittleman, Kaushik Sengupta, Edward W. Knightly

On the Domain Generalizability of RF Fingerprints Through Multifractal Dimension Representation 82
Benjamin Johnson, Bechir Hamdaoui

Inter-Temporal Reward Decisions with Strategic Ethical Hackers.. 91
Jing Hou, Xuyu Wang, Amy Z. Zeng

Are Existing Out-Of-Distribution Techniques Suitable for Network Intrusion Detection?............................. 100
Andrea Corsini, Shanchieh Jay Yang

A Stealthy Inference Attack on Split Learning with a Split-Fuse Defensive Measure 109
Sean Dougherty, Abhinav Kumar, Jie Hou, Reza Tourani, Atena M. Tabakhi

A Needle in a Haystack: Distinguishable Deep Neural Network Features for Domain-Agnostic Device Fingerprinting...118
Abdurrahman Elmaghbub, Bechir Hamdaoui

VeriActor: Dynamic Generation of Challenge-Response Questions for Enhanced Email Sender Verification 127
Basel Abdeen, Ehab Al-Shaer, Waseem Shadid

VetIoT: on Vetting IoT Defenses Enforcing Policies at Runtime 136
Akib Jawad Nafis, Omar Chowdhury, Endadul Hoque

Stealthy False Data Injection Attack on Unmanned Aerial Vehicles with Partial Knowledge 145
Umair Ahmad Mughal, Muhammad Ismail, Syed Ali Asad Rizvi

SmartLens: Robust Detection of Rogue Device Via Frequency Domain Features in LoRa-Enabled IIoT 154
Subir Halder, Amrita Ghosal, Thomas Newe, Sajal K. Das

Protecting Control Commands Using Low-Cost EM Sensors in the Smart Grid 163
Kylie McClanahan, Jingyao Fan, Qinghua Li, Guohong Cao

Characterizing Cyber Attacks Against Space Systems with Missing Data: Framework and Case Study 172
Ekzhin Ear, Jose L. C. Remy, Antonia Feffer, Shouhuai Xu

Toward Adaptive DDoS-Filtering Rule Generation 181
Jun Li, Devkishen Sisodia, Yebo Feng, Lumin Shi, Mingwei Zhang, Christopher Early, Peter Reiher

Autonomous Cyber Defense Against Dynamic Multi-Strategy Infrastructural DDoS Attacks 190
Ashutosh Dutta, Ehab Al-Shaer, Samrat Chatterjee, Qi Duan

Application-Layer Characterization and Traffic Analysis for Encrypted QUIC Transport Protocol 199
Qianqian Zhang, Chi-Jiun Su

Authenticating Outsourced Location-Based Skyline Queries Under Shortest Path Distance 208
Yidan Hu, Yukun Dong, Wenxin Chen, Yingfei Dong, Rui Zhang

FAKEY: Fake Hashed Key Attack on Payment Channel Networks 217
Alvi Ataur Khalil, Mohammad Ashiqur Rahman, Hisham A. Kholidy

High-Speed OFDM Physical-Layer Key Exchange 226
Radi Abubaker, Guang Gong

BeamSec: A Practical mmWave Physical Layer Security Scheme Against Strong Adversaries 235
Afifa Ishtiaq, Arash Asadi, Ladan Khaloopour, Waqar Ahmed, Vahid Jamali, Matthias Hollick

Homomorphic Comparison Method Based on Dynamically Polynomial Composite Approximating Sign Function 244
Xiameng Feng, Xiaodong Li, Suya Zhou, Xin Jin

SecDINT: Preventing Data-Oriented Attacks Via Intel SGX Escorted Data Integrity 253
Dakun Shen, Tao Hou, Zhuo Lu, Yao Liu, Tao Wang

MMIO Access-Based Coverage for Firmware Analysis 262
Ken Yihang Bai, Tuba Yavuz

Empirical Analysis of Software Vulnerabilities Causing Timing Side Channels 271
M. Mehdi Kholoosi, M. Ali Babar, Cemal Yilmaz

Enhancing ML-Based DoS Attack Detection Through Combinatorial Fusion Analysis 280
Evans Owusu, Mohamed Rahouti, D. Frank Hsu, Kaiqi Xiong, Yufeng Xin

Early-Stage Conflict Detection in HLF-based Delay-critical IoT Networks 286
Aditya Pathak, Irfan Al-Anbagi, Howard J. Hamilton

Analysis of Decoy Strategies for Detecting Ransomware 292
Byron Denham, Dale R. Thompson

Towards Evaluation and Understanding of Large Language Models for Cyber Operation Automation 298
Madeena Sultana, Adrian Taylor, Li Li, Suryadipta Majumdar

The Tables Have Turned: GPT-3 Distinguishing Passwords from Honeywords 304
Nilesh Chakraborty, Youssef Yamout, Mohammad Zulkernine

Exploring the Dark Side of AI: Advanced Phishing Attack Design and Deployment Using ChatGPT 309
Nils Begou, Jérémy Vinoy, Andrzej Duda, Maciej Korczynski

Lightweight Impact Assessment and Projection of Lateral Movement and Malware Infection 315
Martin Husák, Michal Javorník

Attack Resilient Wireless Backhaul Connectivity with Optimized Fronthaul Coverage in UAV Networks 321
Xingqi Wu, Junaid Farooq

Adversarial Manipulation of Learning in Linear-Quadratic Zero-Sum Differential Games Via Cost Poisoning 327
Son Tung Do, Gabrielle Ebbrecht, Juntao Chen

Adversarial Attacks on Deep Learning-Based UAV Navigation Systems 333
Mohammed Mynuddin, Sultan Uddin Khan, Mahmoud Nabil Mahmoud, Ahmad Alsharif

Self-Similarity Based Network Anomaly Detection for Industrial Control Systems 339
Bryan Martin, Chad A. Bollmann

Leveraging Neuro-Inspired Reinforcement Learning for Secure Reputation-based Communication in Connected Vehicles 345
Heena Rathore, Henry Griffith

Security Analysis of Trust on the Controller in the Matter Protocol Specification 351
Kumar Shashwat, Francis Hahn, Xinming Ou, Anoop Singhal

A Smart Grid Ontology: Vulnerabilities, Attacks, and Security Policies 357
Utku Tefek, Ertem Esiner, Carmen Cheh, Daisuke Mashima

A BERT-Based Empirical Study of Privacy Policies' Compliance with GDPR 363
Lu Zhang, Nabil Moukafih, Hamad Alamri, Gregory Epiphaniou, Carsten Maple

Towards Adaptive Zero Trust Model for Secure AI 369
Kexin Zhang, Shengjie Xu, Bongsik Shin

Cross-Layer Device Identification for Smart Grid Substation Networks : IEEE CNS 23 Poster 371
Venkat Sai Suman Lamba Karanam, Fahmida Afrin, Byrav Ramamurthy, Nirnimesh Ghose

Enhancing ML-Based DoS Attack Detection with Feature Engineering : IEEE CNS 23 Poster 373
Shujun Zhao, Lesther Santana, Evans Owusu, Mohamed Rahouti, Kaiqi Xiong, Yufeng Xin

Universal Network Traffic Analysis for Malicious Traffic Detection Using RappNet: A Privacy-Preserving Approach : IEEE CNS 23 Poster 375
Onur Barut, Lulin Deng, David Lu

A Key Generation Scheme from Sensing Data for IoT Security : IEEE CNS 23 Poster 377
Xiaokai Ye, Tao Lv, Xiaohan Sun

The Impact of Dynamic Learning on Adversarial Attacks in Networks (IEEE CNS 23 Poster) 379
Mohamed El Shehaby, Ashraf Matrawy

Detection of Zero-Day Attacks Using CNN and LSTM in Networked Autonomous Systems 'IEEE CNS 23 Poster' 381
Hassan El Alami, Danda B. Rawat

IEEE CNS 23 Poster: Cooperative Omnidirectional Beamformation for THz Band Phy-Security................. 383
Mehzabien Iqbal, Ahmad Y. Javaid

SHIP: Securing Hashed Timelock Contracts in Payment Channel Networks 385
Alvi Ataur Khalil, Mohammad Ashiqur Rahman

Author Index