

2022 IEEE Conference on Communications and Network Security (CNS 2022)

**Austin, Texas, USA
3 – 5 October 2022**



**IEEE Catalog Number: CFP22CNM-POD
ISBN: 978-1-6654-6256-3**

**Copyright © 2022 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:	CFP22CNM-POD
ISBN (Print-On-Demand):	978-1-6654-6256-3
ISBN (Online):	978-1-6654-6255-6

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

ACADIA: Efficient and Robust Adversarial Attacks Against Deep Reinforcement Learning	1
<i>Haider Ali, Mohannad Al Ameedi, Ananthram Swami, Rui Ning, Jiang Li, Hongyi Wu, Jin-Hee Cho</i>	
MultiEvasion: Evasion Attacks Against Multiple Malware Detectors	10
<i>Hao Liu, Wenhai Sun, Nan Niu, Boyang Wang</i>	
Network-Level Adversaries in Federated Learning.....	19
<i>Giorgio Severi, Matthew Jagielski, Gökberk Yar, Yuxuan Wang, Alina Oprea, Cristina Nita-Rotaru</i>	
Transferability of Adversarial Examples in Machine Learning-Based Malware Detection	28
<i>Yang Hu, Ning Wang, Yimin Chen, Wenjing Lou, Y. Thomas Hou</i>	
5G Messaging: System Insecurity and Defenses	37
<i>Jinghao Zhao, Qianru Li, Zengwen Yuan, Zhehui Zhang, Songwu Lu</i>	
Absolute Security in High-Frequency Wireless Links	46
<i>Alejandro Cohen, Rafael G. L. D'Oliveira, Chia-Yi Yeh, Hichem Guerboukha, Rabi Shrestha, Zhaoji Fang, Edward Knightly, Muriel Médard, Daniel M. Mittleman</i>	
Learning-Based Radio Fingerprinting for RFID Secure Authentication Scheme	55
<i>Jiaqi Xu, Xingya Zhao, Arjun Bakshi, Kannan Srinivasan</i>	
Systematically Analyzing Vulnerabilities in the Connection Establishment Phase of Wi-Fi Systems	64
<i>Naureen Hoque, Hanif Rahbari, Cullen Rezendes</i>	
DASK: Driving-Assisted Secret Key Establishment.....	73
<i>Edwin Yang, Song Fang, Dakun Shen</i>	
HoneyCam: Scalable High-Interaction Honeypot for IoT Cameras Based on 360-Degree Video.....	82
<i>Chongqi Guan, Xianda Chen, Guohong Cao, Sencun Zhu, Thomas La Porta</i>	
A User-Friendly Two-Factor Authentication Method Against Real-Time Phishing Attacks.....	91
<i>Yuanyi Sun, Sencun Zhu, Yan Zhao, Pengfei Sun</i>	
GateKeeper: Operator-Centric Trusted App Management Framework on ARM TrustZone	100
<i>Balachandar Gowrisankar, Daisuke Mashima, Wenshei Ong, Quanqi Ye, Ertem Esiner, Binbin Chen, Zbigniew Kalbarczyk</i>	
Eolo: IoT Proximity-Based Authentication Via Pressure Correlated Variations.....	109
<i>Omar Adel Ibrahim, Gabriele Oligeri, Roberto Di Pietro</i>	
Multi-Protocol IoT Network Reconnaissance	118
<i>Stefan Gvozdenovic, Johannes K Becker, John Mikulskis, David Starobinski</i>	
Agent-Level Differentially Private Federated Learning via Compressed Model Perturbation.....	127
<i>Yuanxiong Guo, Rui Hu, Yanmin Gong</i>	
PRM - Private Interference Discovery for IEEE 802.15.4 Networks	136
<i>Dominik Roy George, Savio Sciancalepore</i>	

TrafficSpy: Disaggregating VPN-Encrypted IoT Network Traffic for User Privacy Inference.....	145
<i>Qi Li, Keyang Yu, Dong Chen, Mo Sha, Long Cheng</i>	
An Active Learning Approach to Dynamic Alert Prioritization for Real-Time Situational Awareness	154
<i>Yeongwoo Kim, György Dán</i>	
<i>AutoDefense</i> : Reinforcement Learning Based Autoreactive Defense Against Network Attacks	163
<i>Yu Mi, David Mohaisen, An Wang</i>	
Returning to Port: Efficient Detection of Home Router Devices	172
<i>Thomas Papastergiou, Roberto Perdisci, Manos Antonakakis</i>	
Supporting Law-Enforcement to Cope with Blacklisted Websites: Framework and Case Study	181
<i>Mir Mehedi Ahsan Pritom, Shouhuai Xu</i>	
RadioNet: Robust Deep-Learning Based Radio Fingerprinting	190
<i>Haipeng Li, Kaustubh Gupta, Chenggang Wang, Nirnimesh Ghose, Boyang Wang</i>	
Securing Wireless Channels: Reliable Shared Secret Extraction Through OTFS	199
<i>Usama Saeed, Lingjia Liu, Kai Zeng, Robert Calderbank</i>	
Stealthy Off-Target Coupled-Control-Plane Jamming	208
<i>Shreya Gupta, Chia-Yi Yeh, Edward W. Knightly</i>	
A Study on the Testing of Android Security Patches	217
<i>Christopher D. Brant, Tuba Yavuz</i>	
Performant Binary Fuzzing Without Source Code Using Static Instrumentation	226
<i>Eric Pauley, Gang Tan, Danfeng Zhang, Patrick McDaniel</i>	
SysCap: Profiling and Crosschecking Syscall and Capability Configurations for Docker Images	236
<i>Yunlong Xing, Jiahao Cao, Xinda Wang, Sadegh Torabi, Kun Sun, Fei Yan, Qi Li</i>	
HallMonitor: A Framework for Identifying Network Policy Violations in Software.....	245
<i>Daniel Olszewski, Weidong Zhu, Sandeep Sathyanarayana, Kevin Butler, Patrick Traynor</i>	
Error Prevalence in NIDS Datasets: A Case Study on CIC-IDS-2017 and CSE-CIC-IDS-2018.....	254
<i>Lisa Liu, Gints Engelen, Timothy Lynar, Daryl Essam, Wouter Joosen</i>	
Enhancing Load Balancing by Intrusion Detection System Chain on SDN Data Plane.....	264
<i>Nadia Niknami, Jie Wu</i>	
Detecting DNS Hijacking by Using NetFlow Data.....	273
<i>Martin Fejrskov, Jens Myrup Pedersen, Emmanouil Vasilomanolakis</i>	
Refining Network Message Segmentation with Principal Component Analysis.....	281
<i>Stephan Kleber, Frank Kargl</i>	
When Third-Party JavaScript Meets Cache: Explosively Amplifying Security Risks on the Internet	290
<i>Tao Hou, Shengping Bi, Mingkui Wei, Tao Wang, Zhuo Lu, Yao Liu</i>	
Membership Inference Attack in Face of Data Transformations.....	299
<i>Jiyu Chen, Yiwon Guo, Hao Chen, Neil Gong</i>	
Efficient Public Verification of Confidential Supply-Chain Transactions	308
<i>Kilian Becher, Mirko Schäfer, Axel Schropfer, Thorsten Strufe</i>	

On Security of Proof-of-Policy (PoP) in the Execute-Order-Validate Blockchain Paradigm	317
<i>Shan Wang, Ming Yang, Bryan Pearson, Tingjian Ge, Xinwen Fu, Wei Zhao</i>	
Ransomware Detection in Databases Through Dynamic Analysis of Query Sequences.....	326
<i>Christoph Sendner, Lukas Iffländer, Sebastian Schindler, Michael Jobst, Alexandra Dmitrienko, Samuel Kounev</i>	
Securing Communication Against Leaky Switches.....	335
<i>Leila Rashidi, Sogand Sadrhaghighi, Majid Ghaderi, Cristina Nita-Rotaru, Reihaneh Safavi-Naini</i>	
Security Analysis of Mixed RF-FSO Blockage Attack Over Generalized RF Fading and Atmospheric Turbulence	344
<i>Neji Mensi, Danda B. Rawat, Chunmei Liu</i>	
On SDPN: Integrating the Software-Defined Perimeter (SDP) and the Software-Defined Network (SDN) Paradigms	353
<i>Michael Lefebvre, Daniel W. Engels, Suku Nair</i>	
Trust Threshold Policy for Explainable and Adaptive Zero-Trust Defense in Enterprise Networks	359
<i>Yunfei Ge, Quanyan Zhu</i>	
Free-Rider Games for Federated Learning with Selfish Clients in NextG Wireless Networks.....	365
<i>Yalin E. Sagduyu</i>	
Proactive and Resilient UAV Orchestration for QoS Driven Connectivity and Coverage of Ground Users.....	371
<i>Yuhui Wang, Junaid Farooq</i>	
On the Role of Risk Perceptions in Cyber Insurance Contracts	377
<i>Shutian Liu, Quanyan Zhu</i>	
A Secured Certificateless Sign-Encrypted Blockchain Communication for Intelligent Transport System	383
<i>Rizwan Patan, Reza M. Parizi, Seyedamin Pouriyeh, Mohammad S Khan, Amir H. Gandomi</i>	
Machine Learning-Based False Data Injection Attack Detection and Localization in Power Grids	390
<i>Bruno P. Leao, Jagannadh Vempati, Ulrich Muenz, Shashank Shekhar, Amit Pandey, David Hingos, Siddharth Bhela, Jing Wang, Chris Bilby</i>	
A Novel Secure Physical Layer Key Generation Method in Connected and Autonomous Vehicles (CAVs)	398
<i>Md Shah Alam, Sarkar Marshia Hossain, Jared Oluoch, Junghwan Kim</i>	
Highly Efficient FDD Secret Key Generation Using ESPRIT and Jump Removal on Phase Differences	404
<i>Ehsan Olyaei Torshizi, Utkrist Uprety, Werner Henkel</i>	
Real World Snapshot of Trends in IoT Device and Protocol Deployment: IEEE CNS 22 Poster	410
<i>Daniel Brown, Gabriele Cianfarani, Natalija Vlajic</i>	
Survey of Remote TLS Vulnerability Scanning Tools and Snapshot of TLS Use in Banking Sector	412
<i>Jay Chung, Natalija Vlajic</i>	
Expectation Entropy as a Password Strength Metric.....	414
<i>Khan Reaz, Gerhard Wunder</i>	

Author Index