

2025 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2025)

**Gold Coast, Australia
19-22 October 2025**

Pages 1–487

IEEE Catalog Number:
ISBN:

CFP254AA-POD
979-8-3315-6604-3



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:	CFP254AA-POD
ISBN (Print-On-Demand):	979-8-3315-6604-3
ISBN (Online):	979-8-3315-6603-6

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

TABLE OF CONTENTS

Reconstruction of Differentially Private Text Sanitization via Large Language Models	1
<i>Shuchao Pang, Zhigang Lu, Haichen Wang, Peng Fu, Yongbin Zhou, Minhui Xue</i>	
An In-model Spy in Edge Intelligence	18
<i>Fengxu Yang, Paizhuo Chen, Yihui Yan, Zhice Yang</i>	
VulCodeMark: Adaptive Watermarking for Vulnerability Datasets Protection	35
<i>Di Cao, Shigang Liu, Jun Zhang, Yang Xiang</i>	
Unsupervised Backdoor Detection and Mitigation for Spiking Neural Networks	50
<i>Jiachen Li, Bang Wu, Xiaoyu Xia, Xiaoning Liu, Xun Yi, Xiuzhen Zhang</i>	
Functional Encryption in Secure Neural Network Training: Data Leakage and Practical Mitigations	65
<i>Alexandru Ioniță, Andreea Ioniță</i>	
DEPHP: A Source Code Recovery Method for PHP Bytecode with Improved Structural Analysis	77
<i>Shiwu Zhao, Ningjun Zheng, Haoyu Li, Ruizhi Feng, Xingchen Chen, Ru Tan, Qixu Liu</i>	
SyzRetrospector: A Large-Scale Retrospective Study of Syzbot	92
<i>Joseph Bursey, Ardalan Amiri Sani, Zhiyun Qian</i>	
SyzGrapher: Resource-Centric Graph-Based Kernel Fuzzing	106
<i>Marius Fleischer, Harrison Green, Ilya Grishchenko, Christopher Kruegel, Giovanni Vigna</i>	
SH3ARS: Privilege Reduction for ARMv8.0-A Secure Monitors	122
<i>Jonas Röckl, Julian Funk, Matti Schulze, Tilo Müller</i>	
TypeFlexer: Type Directed Flexible Program Partitioning	138
<i>Arunkumar Bhattar, Liyi Li, Mingwei Zhu, Le Chang, Aravind Machiry</i>	
Perry: A High-level Framework for Accelerating Cyber Deception Experimentation	158
<i>Brian Singer, Yusuf Saquib, Lujo Bauer, Vyas Sekar</i>	
Carbon Filter: Scalable, Efficient, and Secure Alert Triage for Endpoint Detection & Response	174
<i>Muhammad Adil Inam, Jonathan Oliver, Raghav Batta, Adam Bates</i>	
STGraph: Spatio-Temporal Graph Mining for Anomaly Detection in Distributed System Logs	190
<i>Teng Li, Shengkai Zhang, Yebo Feng, Jiahua Xu, Zexu Dang, Yang Liu, Jianfeng Ma</i>	
Detecting and Adapting to Stealthy Label-Inversion Drifts via Conditional Distribution Inference	204
<i>Xiaoli Zhang, Yue Xiao, Qilei Yin, Zhengyang Li, Xinyan Wang, Jianrong Zhang, Ke Xu, Qi Li Xu-Cheng Yin</i>	
NIDP: Solving Feature Distribution Shifts in Network Intrusion Detection via Neural Pruning	220
<i>Jiangtao Ding, Junli Zheng, Chengyang Mo, Zhicheng Xu, Hongbing Cheng</i>	
DeepFW: A DNN-Based Firmware Version Identification Framework for Online IoT Devices	233
<i>Zhen Lei, Nian Xue, Zhen Li, Dan Yu, Xin Huang, Yongle Chen</i>	
TAPPecker: TAP Logic Inference and Violation Detection in Heterogeneous Smart Home Systems	248
<i>Qixiao Lin, Jian Mao, Ziwen Liu, Zhenkai Liang</i>	

Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers	266
<i>Gabriel K. Gegenhuber, Maximilian Günther, Markus Maier, Aljosha Judmayer, Florian Holzbauer Philipp É. Frenzel, Johanna Ullrich</i>	
When (Inter)actions Speak Louder Than (Pass)words: Task-Based Evaluation of Implicit Authentication in Virtual Reality	284
<i>Woojin Jeon, Chaejin Lim, Hyoungshick Kim</i>	
MotionDecipher: General Video-assisted Passcode Inference In Virtual Reality	298
<i>Guanchong Huang, Yan He, Shangqing Zhao, Yi Wu, Song Fang</i>	
A Comprehensive Quantification of Inconsistencies in Memory Dumps	314
<i>Andrea Oliveri, Davide Balzarotti</i>	
MuSAR: Multi-Step Attack Reconstruction from Lightweight Security Logs via Event-Level Semantic Association in Multi-Host Environments	329
<i>Yang Liu, Zisen Xu, Zian Luo, Jin'ao Shang, Shilong Zhang, Haichuan Zhang, Ting Liu</i>	
Exploring Runtime Evolution in Android: A Cross-Version Analysis and Its Implications for Memory Forensics	349
<i>Babangida Bappah, Lauren G Bristol, Lamine Noureddine, Sideeq Bello, Umar Farooq, Aisha Ali-Gombe</i>	
{{alert('CSTI')}}: Large-Scale Detection of Client-Side Template Injection	363
<i>Lorenzo Pisu, Davide Balzarotti, Davide Maiorca, Giorgio Giacinto</i>	
Deep Learning-Based Attacks on Traditional Watermarking Systems in Real-Time Live Video Streams	378
<i>Huixin Wang, Amin Sakzad, Stuart Hall</i>	
Deception Meets Diagnostics: Deception-based Real-Time Threat Detection in Healthcare Web Systems	391
<i>Zeeshan Zulkifl Shah, Muhammad Ikram, Hassan Jameel Asghar, Mohamed Ali Kaafar</i>	
On the Effectiveness of Custom Transformers for Binary Analysis	411
<i>Xuezixiang Li, Lian Gao, Sheng Yu, Yu Qu, Heng Yin</i>	
Developing a Strong CPS Defender: An Evolutionary Approach	425
<i>Qingyuan Hu, Christopher M. Poskitt, Jun Sun, Yuqi Chen</i>	
Scalable and Generalizable RL Agents for Attack Path Discovery via Continuous Invariant Spaces	440
<i>Franco Terranova, Abdelkader Lahmadi, Isabelle Chrisment</i>	
From Text to Actionable Intelligence: Automating STIX Entity and Relationship Extraction	458
<i>Ahmed Lekssays, Husrev Taha Sencar, Ting Yu</i>	
Semantic Heat Guided Relational Privacy Inference Based on Panoptic Scene Graph	474
<i>Qi Hao, Jie Huang, Changhao Ding, Zeping Zhang</i>	
From Concealment to Exposure: Understanding the Lifecycle and Infrastructure of APT Domains	488
<i>Athanasios Avgetidis, Aaron Faulkenberry, Vinny Adjibi, Tillson Galloway, Panagiotis Kintis, Omar Alrawi Zane Ma, Fabian Monrose, Angelos D. Keromytis, Roberto Perdisci, Manos Antonakakis</i>	
The Persistent Threat of DGA-Domains Used by Botnets	506
<i>Arthur Drichel, Ulrike Meyer</i>	

CasinoLimit: An Offensive Dataset Labeled with MITRE ATT&CK Techniques	523
<i>Sébastien Kilian, Valérie Viet Triem Tong, Jean-François Lalande, Frédéric Majorczyk, Alexandre Sanchez Natan Talon, Pierre-Victor Besson, Hélène Orsini, Pierre Lledo, Pierre-François Gimenez</i>	
A Longitudinal Analysis of LockBit 3.0's Extortion Lifecycle and Response to Law Enforcement	538
<i>Yin Minn Pa Pa, Yuji Sekine, Yamato Kawaguchi, Tatsuki Yogo, Kelvin Lubbertsen, Rolf van Wegberg Michel van Eeten, Katsunari Yoshioka</i>	
EventHunter: Dynamic Clustering and Ranking of Security Events from Hacker Forum Discussions	552
<i>Yasir Ech-Chammakhy, Anas Motii, Anass Rabii, Jaafar Chbili</i>	
ViDToken: A Video-Transformer-Based Latent Token Defense for Adversarial Video Detection	566
<i>Wei Song, Yulei Sui, Zhenchang Xing, Liming Zhu, Jingling Xue</i>	
Robust Cross-Modal Deepfake Detection via Facial UV Maps and Momentum Contrastive Learning	583
<i>Yuesen Tang, Yuanyang Zhang, Wangxiao Mao, Li Yao</i>	
BadLogo: A Physically Realizable Adversarial Sticker for Evaluating the Robustness of Face Recognition Models	597
<i>Fuqi Qi, Haichang Gao, Boling Li, Shiping Guo, Yuming Zheng, Bingqian Zhou</i>	
The Adaptive Arms Race: Redefining Robustness in AI Security	611
<i>Ilias Tsingenopoulos, Vera Rimmer, Davy Preuveneers, Fabio Pierazzi, Lorenzo Cavallaro, Wouter Joosen</i>	
Red-Teaming LLMs with Token Control Score: Efficient, Universal, and Transferable Jailbreaks	629
<i>Leo Hyun Park, Taekyoung Kwon</i>	
Malware and Vulnerability Analysis using Graph-synchronized Language Model	648
<i>Paventhan Vivekanandan, Alexander Shroyer, Martin Swamy</i>	
Demystifying Feature Engineering in Malware Analysis of API Call Sequences	664
<i>Tianheng Qu, Hongsong Zhu, Limin Sun, Haining Wang, Haiqiang Fei, Zheng He, Zhi Li</i>	
Evaluating LLM-Based Detection of Malicious Package Updates in npm	678
<i>Elizabeth Wyss, Dominic Tassio, Lorenzo De Carli, Drew Davidson</i>	
ADAPT: A Pseudo-labeling Approach to Combat Concept Drift in Malware Detection	693
<i>Md Tanvirul Alam, Aritran Piplai, Nidhi Rastogi</i>	
Revealing Informed Scanners by Colocating Reactive and Passive Telescopes	713
<i>Dario Ferrero, George Smaragdakis, Harm Griffioen</i>	
PRIV-HFL: Privacy-Preserving and Robust Federated Learning for Heterogeneous Clients Against Data Reconstruction Attacks	728
<i>Mohammadreza Najafi, Hooman Alavizadeh, Ahmad Salehi Shahraki, A.S. M Kayes, Wenny Rahayu</i>	
Guard-GBDT: Efficient Privacy-Preserving Approximated GBDT Training on Vertical Dataset	741
<i>Anxiao Song, Shujie Cui, Jianli Bai, Ke Cheng, Yulong Shen, Giovanni Russello</i>	
Re-examine Federated Rank Learning: Analyzing Its Robustness Against Poisoning Attacks	757
<i>Xiaofei Huang, Xiaojie Zhu, Chi Chen, Paulo Esteves-Verüssimo</i>	
BadFU: Backdoor Federated Learning through Adversarial Machine Unlearning	773
<i>Bingguang Lu, Hongsheng Hu, Yuantian Miao, Shaleeza Sohail, Chaoxiang He, Shuo Wang, Xiao Chen</i>	

FedSIG: Privacy-Preserving Federated Recommendation via Synthetic Interaction Generation	789
<i>Thirasara Ariyaratna, Salil Kanhere, Meisam Mohammady, Hye-Young Helen Paik</i>	
Portal: Enabling Accurate Siemens PLC Rehosting via Peripheral Proxying and Proactive Interrupt Synchronization	801
<i>Haoran Li, Dakun Shen, Wenbo Shen, Zhen Zhu</i>	
Activation Functions Considered Harmful: Recovering Neural Network Weights through Controlled Channels	815
<i>Jesse Spielman, David Oswald, Mark Ryan, Jo Van Bulck</i>	
Zebrafix: Mitigating Memory-Centric Side-Channel Leakage via Interleaving	835
<i>Anna Pättschke, Jan Wichelmann, Thomas Eisenbarth</i>	
RF-Eye-D: Probing Feasibility of CMOS Camera Watermarking with Radio-Frequency Injection	850
<i>Hui Zhuang, Yan Long, Kevin Fu</i>	
ShuffleV: A Microarchitectural Defense Strategy against Electromagnetic Side-Channel Attacks in Microprocessors	866
<i>Nuntipat Narkthong, Yukui Luo, Xiaolin Xu</i>	
Overlapping IPv4, IPv6, and TCP data: exploring errors, test case context, and multiple overlaps inside network stacks and NIDSes with Pyrolyse	886
<i>Lucas Aubard, Johan Mazel, Gilles Guette, Pierre Chifflier</i>	
Active Attack Resilience in 5G: A New Take on Authentication and Key Agreement	905
<i>Nazatul H. Sultan, Xinlong Guan, Josef Pieprzyk, Wei Ni, Sharif Abuadbbba, Hajime Suzuki</i>	
H2Fuzz: Guided, Black-box, Differential Fuzzing for HTTP/2-to-HTTP/1 Conversion Anomalies	920
<i>Anthony Gavazzi, Weixin Kong, Engin Kirda</i>	
Uncontained Danger: Quantifying Remote Dependencies in Containerized Applications	935
<i>Chris Tsoukaladelis, Roberto Perdisci, Nick Nikiforakis</i>	
RBAClock: Contain RBAC Permissions through Secure Scheduling	950
<i>Qingwang Chen, Ru Tan, Xinyu Liu, Yuqi Shu, Zhou Tong, Haoqiang Wang, Ze Jin, Qixu Liu</i>	
Scalable Active Directory Defense with α -Metagraph	966
<i>Nhu Long Nguyen, Nickolas Falkner, Hung Nguyen</i>	