

2025 IEEE Annual Computer Security Applications Conference (ACSAC 2025)

**Honolulu, Hawaii, USA
8-12 December 2025**

Pages 1–657

IEEE Catalog Number: CFP25393-POD
ISBN: 979-8-3315-5719-5



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:	CFP25393-POD
ISBN (Print-On-Demand):	979-8-3315-5719-5
ISBN (Online):	979-8-3315-9414-5
ISSN:	1063-9527

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

Decentralized Privacy-Preserving Authenticated Key Exchange Using Real-World Attributes	1
<i>Ling Chen, Xiao Lan, Hao Ren, Hui Guo, Long Chen, Kunpeng Bai</i>	
Sagitta: Facilitating Post-Fuzzing Root Cause Analysis via Data Flow Differencing	13
<i>Katsunori Aoki, Takahiro Shinagawa</i>	
Gravity of the Situation: Security Analysis on Rocket.Chat E2EE	27
<i>Hayato Kimura, Ryoma Ito, Kazuhiko Minematsu, Takanori Isobe</i>	
DROIDCCT: Cryptographic Compliance Test via Trillion-Scale Measurement	43
<i>Daniel Moghimi, Alexandru-Cosmin Mihai, Borbala Benko, Catherine Vlasov, Elie Bursztein, Kurt Thomas László Siroki, Pedro Barbosa, Rémi Audebert</i>	
Fuzzing Acceleration for Memory Safety Bug Discovery with Slicer	58
<i>Giyeol Kim, Dohyun Ryu, Seungjin Bae, Changyul Lee, Taegyu Kim</i>	
AndroByte: LLM-Driven Privacy Analysis through Bytecode Summarization and Dynamic Dataflow Call Graph Generation	72
<i>Mst Eshita Khatun, Lamine Nouredine, Zhiyong Sui, Aisha Ali-Gombe</i>	
VerDiff: Vulnerability Presence Verification for Comprehensive Reporting Using Constraint Programming	89
<i>Md Sakib Anwar, Carter Yagemann, Zhiqiang Lin</i>	
Supply Chain Reaction: Enhancing the Precision of Vulnerability Triage using Code Reachability Information	104
<i>Harshvardhan Patel, Alexander Snit, Michalis Polychronakis</i>	
REx86: A Local Large Language Model for Assisting in x86 Assembly Reverse Engineering	120
<i>Darrin Lea, James Ghawaly, Golden Richard, Aisha Ali-Gombe, Andrew Case</i>	
TeTRIS: General-purpose Fuzzing for Translation Bugs in Source-to-Source Code Transpilers	135
<i>Yeaseen Arafat, Stefan Nagy</i>	
Recovering Peripheral Maps and Protocols to Expedite Firmware Reverse Engineering	149
<i>Bayan Turkistani, Carter Yagemann</i>	
In Pursuit of Lean OS Kernels: Improving Configuration-Based Debloating	166
<i>Akshith Gunasekaran, Gabriel Ritter, Rakesh B. Bobba</i>	
MimicCall: Bypassing System Call Filters via Kernel Function Redundancy	182
<i>Songah Joo, Minchan Park, Hyerean Jang, Youngjoo Shin</i>	
SMORE: Practical Redzone-Based Stack Memory Error Detection Mechanism for Embedded Systems	196
<i>Jaeyeol Park, Yunju Gu, Donghyun Kwon</i>	
ELK: Effective Lock-and-Key Technique for Temporal Memory Safety on Embedded Devices in ARMv8-M	210
<i>Jeonghwan Kang, Kyoungwan Kim, Donghyun Kwon</i>	
Understanding the Security Impact of CHERI on the Operating System Kernel	224
<i>Zhaofeng Li, Jerry Zhang, Joshua Tlatelpa-Agustin, Xiangdong Chen, Anton Burtsev</i>	

It's a Non-Stop PARTEE! Practical Multi-Enclave Availability Through Partitioning and Asynchrony	240
<i>Richard Habeeb, Hao Chen, Man-Ki Yoon, Zhong Shao</i>	
Beyond Driver Isolation - Triaging Threats against Driver Isolation	257
<i>Yongzhe Huang, Kaiming Huang, Matthew Ennis, Vikram Narayanan, Anton Burtsev, Trent Jaeger Gang Tan</i>	
AGNOMIN - Architecture Agnostic Multi-Label Function Name Prediction	274
<i>Yonatan Gizachew Achamyelah, Tongtao Zhang, Joshua Hyunki Kim, Gabriel Garcia, Shih-Yuan Yu Anton Kocheturov, Mohammad Abdullah Al Faruque</i>	
PSan: Towards Hybrid Metadata Scheme for Efficient Pointer Checking	290
<i>Shengjie Xu, Eric Liu, Wei Huang, Ilya Grishchenko, David Lie</i>	
OTABase: Enhancing Over-the-Air Testing to Detect Memory Crashes in Cellular Basebands	303
<i>CheolJun Park, Marc Egli, BeomSeok Oh, Tuan Dinh Hoang, Suhwan Jeong, Martin Crettol, Insu Yun Mathias Payer, Yongdae Kim</i>	
False Promises of Passwordless: Defeating Windows Hello through TPM Misuses	320
<i>Jeongho Lee, Minkyong Kang, Seunghwan Lee, Hyoung-Kee Choi</i>	
ProxyPrints: From Database Breach to Spoof, A Plug-and-Play Defense for Biometric Systems	334
<i>Yaniv Hacmon, Keren Gorelik, Gilad Gressel, Yisroel Mirsky</i>	
R+R: Anonymous Authentication and Key Agreement, Revisited	349
<i>Yanqi Zhao, Xiangyu Liu, Min Xie, Xiaoyi Yang, Jianting Ning, Baodong Qin, Haibin Zhang, Yong Yu</i>	
Belt and Braces! Fight against Key Compromising in Single Sign-On Systems	363
<i>Yuan Zhang, Yali Wang, Guowen Xu, Yaqing Song, Hongwei Li</i>	
Compact and Selective Disclosure for Verifiable Credentials	377
<i>Alessandro Buldini, Carlo Mazzocca, Rebecca Montanari, Selcuk Uluagac</i>	
DP-Mix: Differentially Private Routing in Mix Networks	394
<i>Mahdi Rahimi</i>	
FLAME: Flexible and Lightweight Biometric Authentication Scheme in Malicious Environments	411
<i>Fuyi Wang, Fangyuan Sun, Mingyuan Fan, Jianying Zhou, Jin Ma, Chao Chen, Jiangang Shu Leo Yu Zhang</i>	
Seti:Secure Time for Virtualized Systems	425
<i>Adeel Nasrullah, Muhammad Abdullah Soomro, Fatima Muhammad Anwar</i>	
A Cloudy View on Trust Relationships of CVMs: How Confidential Virtual Machines are Falling Short in Public Cloud	440
<i>Jana Eisoldt, Anna Galanou, Andrey Ruzhanskiy, Nils Küchenmeister, Yewgenij Baburkin, Tianxiang Dai Ivan Gudymenko, Stefan Köpsell, Rüdiger Kapitza</i>	
VMIGEN: Utilizing Virtual Machine Introspection for Fuzzing Complex Closed-Source Targets	454
<i>Florian Schweins, Moritz Schloegel, Moritz Bley, Nico Schiller, Thorsten Holz</i>	
TrustLeech: Privileged System Analysis using Nested Virtualization	468
<i>Matti Schulze, Paul Bergmann, Jonas Röckl, Felix Freiling</i>	

Non-Bare-Metal User-Space Control-Flow Attestation	482
<i>Nikita Yadav, Hrushikesh Salunke, Dev Tejas Gandhi, Vinod Ganapathy</i>	
R+R: From Claims to Crashes: A Systematic Re-evaluation of Graph-Based Network Intrusion Detection Systems	499
<i>Chenglong Wang, Pujia Zheng, Jiaping Gui, Cunqing Hua, Wajih Ul Hassan</i>	
Clouseau: A Hierarchical Multi-Agent Approach for Autonomous Attack Investigation	516
<i>Abdullah Aldaihan, Fahad Alotaibi, Sergio Maffei</i>	
Revealing the True Indicators: Understanding and Improving IoC Extraction From Threat Reports	533
<i>Evangelos Froudakis, Athanasios Avgetidis, Sean Tyler Frankum, Roberto Perdisci, Manos Antonakakis Angelos D. Keromytis</i>	
One Detector Fits All: Robust and Adaptive Detection of Malicious Packages from PyPI to Enterprises	550
<i>Biagio Montaruli, Luca Compagna, Serena Elisa Ponta, Davide Balzarotti</i>	
R+R: Revisiting Static Feature-Based Android Malware Detection Using Machine Learning	566
<i>Md Tanvirul Alam, Dipkamal Bhusal, Nidhi Rastogi</i>	
Invisible Ears at Your Fingertips: Acoustic Eavesdropping via Mouse Sensors	583
<i>Mohamad Habib Fakh, Rahul Dharmaji, Youssef Mahmoud, Halima Bouzidi Mohammad Abdullah Al Faruque</i>	
Environmental Rate Manipulation Attacks on Power Grid Security	598
<i>Yonatan Gizachew Achamyeleh, Yang Xiang, Yun-Ping Hsiao, Yasamin Moghaddas Mohammad Abdullah Al Faruque</i>	
SnoopDog: Detecting USB Bus Sniffers Using Responsive EMR	612
<i>Srinivasan Murali, Youngtak Cho, Huadi Zhu, Pan Li, Ming Li</i>	
Controllable Spoofing Attacks on Visual SLAM in Robotic Vehicles	629
<i>Yuan Xu, Gelei Deng, Guanlin Li, Xingshuo Han, Shangwei Guo, Tianwei Zhang</i>	
ORT: Unintended Text Recognition from Eyeglass Reflections in Video Conferencing Environments	646
<i>Jieun Kim, Youngjoo Park, Rokyung Kwon, Jimin Han, Hoorin Park</i>	
The 2FA Illusion: Uncovering Weak Links of Web Account Access in the Wild	658
<i>Ke Coby Wang, Sunpreet S. Arora, Michael K. Reiter</i>	
Uncovering Bigger Truths: Deobfuscating PHP with Phoebe	673
<i>Manuel Karl, Simon Koch, David Klein, Martin Johns</i>	
WAFFLED: Exploiting Parsing Discrepancies to Bypass Web Application Firewalls	689
<i>Seyed Ali Akhavan, Bahruz Jabiyev, Ben Kallus, Cem Topcuoglu, Sergey Bratus, Engin Kirda</i>	
Pathfinder: Exploring Path Diversity for Assessing Internet Censorship Inconsistency	703
<i>Xiaoqin Liang, Guannan Liu, Lin Jin, Shuai Hao, Haining Wang</i>	
PP3D: An In-Browser Vision-Based Defense Against Web Behavior Manipulation Attacks	719
<i>Spencer King, Irfan Ozen, Karthika Subramani, Saranyan Senthivel, Phani Vadrevu, Roberto Perdisci</i>	
Into the Unknown: Fuzzing CPU Non-standard Instructions with MystFuzz	736
<i>Zihui Guo, Wenhao Cui, Liwei Chen, Miaomiao Yuan, Gang Shi, Dan Meng</i>	

Revisiting Prime+Prune+Probe: Pitfalls and Remedies	751
<i>Moritz Peters, Florian Stolz, Jan Philipp Thoma, Tim Güneysu, Yuval Yarom</i>	
EM-Flow: Advanced Electromagnetic Control Flow Verification for Embedded Systems	767
<i>Carson Stillman, Jennifer Sheldon, Ian Y. Garrett, Patrick Traynor, Ryan M. Gerdes, Sara Rampazzi</i> <i>Kevin R. B. Butler</i>	
Retain the Date: Detecting Recycled Chips in the Supply Chain Through SRAM's Data Retention Behavior	784
<i>Jubayer Mahmod, Matthew Hicks</i>	
CarDS - Controller Area Network and Automotive Ethernet Realistic Data Set	798
<i>Wouter Hellemans, Jannis Hamborg, Timm Lauser, Md Masoom Rabbani, Bart Preneel, Christoph Krauß</i> <i>Nele Mentens</i>	
A Period-Adaptive Traffic Fingerprint-Based Method for Smart Home Device Identification	815
<i>Yingjie Hu, Weiping Wang, Shigeng Zhang, Hong Song, Shilei Kuang</i>	
R+R: IoT Device Identification Under Realistic Conditions	828
<i>Chakshu Gupta, Andreas Peter, Andrea Continella</i>	
Zeus-IoT: Comprehensive Code Signing to Prevent IoT Device Weaponization	845
<i>Alireza Roshandel, Manuel Egele</i>	
InteractionShield: Harnessing Event Relations for Interaction Threat Detection and Resolution in Smart Homes	858
<i>Zhaohui Wang, Bo Luo, Fengjun Li</i>	
Octopus: Fast Homomorphic Convolution for Secure Neural Network Inference	875
<i>Yu Tong, Yu Fu, Tianshi Xu, Cheng Hong, Meng Li, Wei Wang, Dengguo Feng, Jingqiang Lin</i>	
Enhancing Noisy Functional Encryption for Privacy-Preserving Machine Learning	889
<i>Linda Scheu-Hachtel, Jasmin Zalonis</i>	
Mizar: Boosting Secure Three-Party Deep Learning with Co-Designed Sign-Bit Extraction and GPU Acceleration	905
<i>Ye Dong, Xudong Chen, Xiangfu Song, Yaxi Yang, Tianwei Zhang, Jin-Song Dong</i>	
DeepProv: Behavioral Characterization and Repair of Neural Networks via Inference Provenance Graph Analysis	922
<i>Firas Ben Hmida, Abderrahmen Amich, Ata Kaboudi, Birhanu Eshete</i>	
Contextual Adversarial Triggers with Masked Language Models	939
<i>Jiaqi Wu, Chen Chen, Chunyan Hou, Hanwen Xing, Xiaojie Yuan</i>	
Securing On-device Transformer with Hardware Binding and Reversible Obfuscation	956
<i>Peichun Hua, Hanxiu Zhang, Tuo Li, Yue Zheng</i>	
CAUA: A Realistic and Effective Attack on Machine Unlearning Under Limited Information	973
<i>Jing Zhang, Yichen Zhang, Jie Cui, Xianfeng Xie, Chunyang Fan, Bei Li</i>	
Flashy Backdoor: Real-world Environment Backdoor Attack on SNNs with DVS Cameras	986
<i>Roberto Ríaño, Gorka Abad, Stjepan Picek, Aitor Urbieto</i>	

AdvOSD: Adversarial One-Step Diffusion for Generalizable and Efficient Fake Image Detection	1003
<i>Liqun Shan, Kaiying Han, Yazhou Tu, Xiali Hei</i>	
PIM-ORAM: Towards Oblivious RAM Primitives in Commodity Processing-In-Memory	1018
<i>Byeongsu Woo, Kha Dinh Duy, Youngkwang Han, Brent Byunghoon Kang, Hojoon Lee</i>	
Analysis of Encryption Key Zeroization from System-Wide Perspective	1034
<i>Toyofumi Sawa, Kuniyasu Suzuki</i>	
XPOZ-HUB: Privacy Infiltration in Payment Channel Hubs through Balance Probing and Transaction Discovery	1051
<i>Alvi Ataur Khalil, Mohammad Ashiqur Rahman</i>	
No Fish Is Too Big for Flash Boys! Frontrunning on DAG-Based Blockchains	1065
<i>Jianting Zhang, Aniket Kate</i>	
Splash: Adversarial Defense with Short Perturbation Blocks Against Adversarial Training Aided Website Fingerprinting	1081
<i>Runsheng Ma, Chengshang Hou, Gaopeng Gou, Junzheng Shi, Zhen Li, Gang Xiong</i>	
End-to-End Encrypted Applications with Strong Consistency Under Byzantine Actors	1097
<i>Natalie Popescu, Shai Caspin, Leon Schuermann, Jingyuan Chen, Amit Levy</i>	
Enabling Plausible Deniability in Flash-based Storage through Data Permutation	1111
<i>Weidong Zhu, Wenxuan Bao, Vincent Bindschaedler, Sara Rampazzi, Kevin R.B. Butler</i>	
Leaking Queries On Secure Stream Processing Systems	1128
<i>Hung Pham, Viet Vo, Tien Tuan Anh Dinh, Duc Tran, Shuhao Zhang</i>	
MOEVIL: Poisoning Experts to Compromise the Safety of Mixture-of-Experts LLMs	1144
<i>Jaehan Kim, Seung Ho Na, Minkyoo Song, Seungwon Shin, Sooel Son</i>	
Learned, Lagged, LLM-Splained: LLM Responses to End User Security Questions	1161
<i>Vijay Prakash, Kevin Lee, Arkaprabha Bhattacharya, Danny Yuxing Huang, Jessica Staddon</i>	
Rescuing the Unpoisoned: Efficient Defense Against Knowledge Corruption Attacks on RAG Systems	1178
<i>Minseok Kim, Hankook Lee, Hyungjoon Koo</i>	
APILOT: Improving the Security and Usability of LLM Code Suggestions via Outdated API Mitigation	1193
<i>Weiheng Bai, Keyang Xuan, Pengxiang Huang, Qiushi Wu, Jianing Wen, Jingjing Wu, Kangjie Lu</i>	
Siren: A Learning-Based Multi-Turn Attack Framework for Simulating Real-World Human Jailbreak Behaviors	1209
<i>Yi Zhao, Youzhi Zhang</i>	
GET /large. file HTTP /1.1: Connection-Based TCP Amplification Attacks	1221
<i>Yepeng Pan, Lars Richter, Christian Rossow</i>	
TempoNet: Learning Realistic Communication and Timing Patterns for Network Traffic Simulation	1238
<i>Kristen Moore, Diksha Goel, Cody James Christopher, Zhen Wang, Minjune Kim, Ahmed Ibrahim Ahmad Mohsin, Seyit Camtepe</i>	
Fix it - If you Can! Towards Understanding the Impact of Tool Support and Domain Owners' Reactions to SSHFP Misconfigurations	1255
<i>Anne Hennig, Sebastian Neef, Peter Mayer</i>	

Big Broker is Tracking You! A Privacy Assessment of Large-Scale Location Trace Datasets	1272
<i>Kevin De Boeck, Jenno Verdonck, Michiel Willocx, Vincent Naessens</i>	
Fooling Machine's Eyes: Unicode Modifier Letter Evasion Attack	1288
<i>Chao Gao, Guanglu Sun, Xin Liu, Feiyan Liu</i>	