

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

Table of Contents

Message from the General Chairs	xiv
Message from the Program Co-Chairs	xv
Organizing Committee	xvii
Program Committee	xviii
Steering Committee	xxi
Reviewers	xxii
Sponsors	xxiii

Adversarial Machine Learning

ViDToken: A Video-Transformer-Based Latent Token Defense for Adversarial Video Detection	1
<i>Wei Song (University of New South Wales, Australia), Zhenchang Xing (CSIRO's Data61, Australia), Liming Zhu (CSIRO's Data61, Australia), Yulei Sui (University of New South Wales, Australia), and Jingling Xue (University of New South Wales, Australia)</i>	
Robust Cross-Modal Deepfake Detection via Facial UV Maps and Momentum Contrastive Learning	18
<i>Yuesen Tang (Southeast University, China), Yuanyang Zhang (Southeast University, China), Wangxiao Mao (Southeast University, China), and Li Yao (Southeast University, China)</i>	
BadLogo: A Physically Realizable Adversarial Sticker for Evaluating the Robustness of Face Recognition Models	32
<i>Fuqi Qi (Xidian University), Haichang Gao (Xidian University), Boling Li (Xidian University), Shiping Guo (Xidian University), Yuming Zheng (Xidian University), and Bingqian Zhou (Xidian University)</i>	
The Adaptive Arms Race: Redefining Robustness in AI Security	46
<i>Ilias Tsingenopoulos (KU Leuven, Belgium), Vera Rimmer (KU Leuven, Belgium), Davy Preuveneers (KU Leuven, Belgium), Fabio Pierazzi (University College London, United Kingdom), Lorenzo Cavallaro (University College London, United Kingdom), and Wouter Joosen (KU Leuven, Belgium)</i>	

Red-Teaming LLMs with Token Control Score: Efficient, Universal, and Transferable Jailbreaks	64
<i>Leo Hyun Park (Yonsei University) and Taekyoung Kwon (Yonsei University)</i>	

Security and Privacy in Federated & Distributed Learning

PRIV-HFL: Privacy-Preserving and Robust Federated Learning for Heterogeneous Clients Against Data Reconstruction Attacks	83
<i>Mohammadreza Najafi (La Trobe University), Hooman Alavizadeh (La Trobe University), Ahmad Salehi Shahraki (La Trobe University), A.S.M Kayes (La Trobe University), and Wenny Rahayu (La Trobe University)</i>	
Guard-GBDT: Efficient Privacy-Preserving Approximated GBDT Training on Vertical Dataset	96
<i>Anxiao Song (Xidian University), Shujie Cui (Monash University), Jianli Bai (Singapore Management University), Ke Cheng (Xidian University), Yulong Shen (Xidian University), and Giovanni Russello (University of Auckland)</i>	
Re-examine Federated Rank Learning: Analyzing Its Robustness Against Poisoning Attacks	112
<i>Xiaofei Huang (Institute of Information Engineering, Chinese Academy of Sciences), Xiaojie Zhu (King Abdullah University of Science and Technology), Chi Chen (Institute of Information Engineering, Chinese Academy of Sciences), and Paulo Esteves-Verissimo (King Abdullah University of Science and Technology)</i>	
BadFU: Backdoor Federated Learning Through Adversarial Machine Unlearning	128
<i>Bingguang Lu (University of Newcastle), Hongsheng Hu (University of Newcastle), Yuantian Miao (University of Newcastle), Shaleeza Sohail (University of Newcastle), Chaoxiang He (Shanghai Jiao Tong University), Shuo Wang (Shanghai Jiao Tong University), and Xiao Chen (University of Newcastle)</i>	
FedSIG: Privacy-Preserving Federated Recommendation via Synthetic Interaction Generation	144
<i>Thirasara Ariyaratna (University of New South Wales, Australia), Salil S. Kanhere (University of New South Wales, Australia), Meisam Mohammady (Iowa State University, USA), and Hye-young Paik (University of New South Wales, Australia)</i>	

Attacks On and Defenses for ML Models

Reconstruction of Differentially Private Text Sanitization via Large Language Models	156
<i>Shuchao Pang (Nanjing University of Science and Technology), Zhigang Lu (Western Sydney University), Haichen Wang (Nanjing University of Science and Technology), Peng Fu (Institute of Information Engineering, Chinese Academy of Sciences), Yongbin Zhou (Nanjing University of Science and Technology), and Minhui Xue (CSIRO's Data61 and Responsible AI Research (RAIR) Centre, The University of Adelaide)</i>	
An In-model Spy in Edge Intelligence	173
<i>Fengxu Yang (ShanghaiTech University, China), Paizhuo Chen (ShanghaiTech University, China), Yihui Yan (Shanghai Maritime University, China), and Zhice Yang (ShanghaiTech University, China)</i>	

VulCodeMark: Adaptive Watermarking for Vulnerability Datasets Protection	190
<i>Di Cao (School of Science, Computing and Emerging Technologies, Swinburne University of Technology), Shigang Liu (Data61, CSIRO), Jun Zhang (School of Science, Computing and Emerging Technologies, Swinburne University of Technology), and Yang Xiang (Digital Research Capability Platform, Swinburne University of Technology)</i>	
Unsupervised Backdoor Detection and Mitigation for Spiking Neural Networks	205
<i>Jiachen Li (RMIT University, Australia), Bang Wu (RMIT University, Australia), Xiaoyu Xia (RMIT University, Australia), Xiaoning Liu (RMIT University, Australia), Xun Yi (RMIT University, Australia), and Xiuzhen Zhang (RMIT University, Australia)</i>	
Functional Encryption in Secure Neural Network Training: Data Leakage and Practical Mitigations	220
<i>Alexandru Ioniță (Alexandru Ioan Cuza University of Iași, Romania) and Andreea Ioniță (Alexandru Ioan Cuza University of Iași, Romania)</i>	

Machine Learning for Security Applications

On the Effectiveness of Custom Transformers for Binary Analysis	232
<i>Xuezixiang Li (University of California Riverside, United States), Lian Gao (University of California Riverside, United States), Sheng Yu (University of California Riverside, United States), Yu Qu (Xi'an Thermal Power Research Institute Co., Ltd, China), and Heng Yin (University of California Riverside, United States)</i>	
Developing a Strong CPS Defender: An Evolutionary Approach	246
<i>Qingyuan Hu (ShanghaiTech University, China), Christopher M. Poskitt (Singapore Management University, Singapore), Jun Sun (Singapore Management University, Singapore), and Yuqi Chen (ShanghaiTech University, China)</i>	
Scalable and Generalizable RL Agents for Attack Path Discovery via Continuous Invariant Spaces	261
<i>Franco Terranova (Université de Lorraine, CNRS, Inria, LORIA), Abdelkader Lahmadi (Université de Lorraine, CNRS, Inria, LORIA), and Isabelle Chrisment (Université de Lorraine, CNRS, Inria, LORIA)</i>	
From Text to Actionable Intelligence: Automating STIX Entity and Relationship Extraction	279
<i>Ahmed Lekssays (Qatar Computing Research Institute), Husrev Taha Sencar (Qatar Computing Research Institute), and Ting Yu (Mohamed bin Zayed University of Artificial Intelligence)</i>	
Semantic Heat Guided Relational Privacy Inference Based on Panoptic Scene Graph	295
<i>Qi Hao (Southeast University, China), Jie Huang (Southeast University, Purple Mountain Laboratories, China), Changhao Ding (Southeast University, China), and Zeping Zhang (Southeast University, China)</i>	

Systems and Software Security

DEPHP: A Source Code Recovery Method for PHP Bytecode with Improved Structural Analysis ...	309
<i>Shiwu Zhao (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ningjun Zheng (Tencent Technology (Shanghai) Co., Ltd, China), Haoyu Li (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ruizhi Feng (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xingchen Chen (Chinese Academy of Sciences, China), Ru Tan (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Qixu Liu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
SyzRetrospector: A Large-Scale Retrospective Study of Syzbot	324
<i>Joseph Bursey (University of California, Irvine), Ardalan Amiri Sani (University of California, Irvine), and Zhiyun Qian (University of California, Riverside)</i>	
SyzGrapher: Resource-Centric Graph-Based Kernel Fuzzing	338
<i>Marius Fleischer (NVIDIA), Harrison Green (Carnegie Mellon University), Ilya Grishchenko (University of Toronto), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)</i>	
SH3ARS: Privilege Reduction for ARMv8.0-A Secure Monitors	354
<i>Jonas Röckl (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Julian Funk (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Matti Schulze (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), and Tilo Müller (Hof University of Applied Sciences, Germany)</i>	
TYPEFLEXER: Type Directed Flexible Program Partitioning	370
<i>Arunkumar Bhattar (Purdue University), Liyi Li (Iowa State University), Mingwei Zhu (University of Maryland, College Park), Le Chang (University of Maryland, College Park), and Aravind Machiry (Purdue University)</i>	

System Forensics and Investigation

A Comprehensive Quantification of Inconsistencies in Memory Dumps	390
<i>Andrea Oliveri (EURECOM, France) and Davide Balzarotti (EURECOM, France)</i>	
MuSAR: Multi-Step Attack Reconstruction from Lightweight Security Logs via Event-Level	
Semantic Association in Multi-Host Environments	405
<i>Yang Liu (Xi'an Jiaotong University), Zisen Xu (Xi'an Jiaotong University), Zian Luo (Xi'an Jiaotong University), Jin'ao Shang (Xi'an Jiaotong University), Shilong Zhang (Xi'an Jiaotong University), Haichuan Zhang (University of Science and Technology of China), and Ting Liu (Xi'an Jiaotong University)</i>	

CasinoLimit: An Offensive Dataset Labeled with MITRE ATT&CK Techniques	425
<i>Sebastien Kilian (CentraleSupélec), Valérie Viet Triem Tong (CentraleSupélec), Jean-François Lalande (CentraleSupélec), Frédéric Majorczyk (DGA, Ministère des Armées), Alexandre Sanchez (Inria), Natan Talon (CentraleSupélec), Pierre-Victor Besson (Inria), Helene Orsini (CentraleSupélec), Pierre Lledo (DGA, Ministère des Armées), and Pierre-François Gimenez (Inria)</i>	
Exploring Runtime Evolution in Android: A Cross Version Analysis and Its implication for Memory Forensics	440
<i>Babangida Bappah (Louisiana State University, USA), Lauren G. Bristol (Louisiana State University, USA), Lamine Noureddine (Louisiana State University, USA), Sideeq Bello (Louisiana State University, USA), Umar Faruq (Louisiana State University, USA), and Aisha Ali-Gombe (Louisiana State University, USA)</i>	

Cybercrime and Threat Intelligence

From Concealment to Exposure: Understanding the Lifecycle and Infrastructure of APT Domains	454
<i>Athanasios Avgetidis (Georgia Institute of Technology), Aaron Faulkenberry (Georgia Institute of Technology), Boladji Vinny Adjibi (Georgia Institute of Technology), Tillson Galloway (Georgia Institute of Technology), Panagiotis Kintis (Georgia Institute of Technology), Omar Alrawi (Georgia Institute of Technology), Zane Ma (Oregon State University), Angelos Keromytis (Georgia Institute of Technology), Fabian Monroe (Georgia Institute of Technology), Roberto Perdisci (University of Georgia), and Manos Antonakakis (Georgia Tech)</i>	
The Persistent Threat of DGA-Domains Used by Botnets	472
<i>Arthur Drichel (RWTH Aachen University) and Ulrike Meyer (RWTH Aachen University)</i>	
A Longitudinal Analysis of LockBit 3.0's Extortion Lifecycle and Response to Law Enforcement	489
<i>Yin Minn Pa Pa (Yokohama National University), Yuji Sekine (Yokohama National University), Yamato Kawaguchi (Yokohama National University), Yogo Tatsuki (Yokohama National University), Kelvin Lubbertsen (Delft University of Technology), Rolf van Wegberg (Delft University of Technology, Yokohama National University), Michel van Eeten (Delft University of Technology, Yokohama National University), and Katsunari Yoshioka (Yokohama National University)</i>	
EventHunter: Dynamic Clustering and Ranking of Security Events from Hacker Forum Discussions	503
<i>Yasir ECH-CHAMMAKHY (Mohammed VI Polytechnic University, Morocco), Anas MOTII (Mohammed VI Polytechnic University, Morocco), Anass RABII (Deloitte Morocco Cyber Center, Morocco), and Jaafar CHBILI (Deloitte Conseil, France)</i>	

Malware Analysis and Detection

Demystifying Feature Engineering in Malware Analysis of API Call Sequences	517
<i>Tianheng Qu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), Hongsong Zhu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), Limin Sun (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), Haining Wang (The Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, USA), Haiqiang Fei (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China), Zheng He (National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China), and Zhi Li (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China)</i>	
Malware and Vulnerability Analysis using Graph-synchronized Language Model	531
<i>Paventhana Vivekanandan (Indiana University Bloomington, USA), Alexander Shroyer (Indiana University Bloomington, USA), and Martin Swamy (Indiana University Bloomington, USA)</i>	
Evaluating LLM-Based Detection of Malicious Package Updates in npm	547
<i>Elizabeth Wyss (University of Kansas), Dominic Tassio (University of Kansas), Lorenzo De Carli (University of Calgary), and Drew Davidson (University of Kansas)</i>	
ADAPT: A Pseudo-labeling Approach to Combat Concept Drift in Malware Detection	562
<i>Md Tanvirul Alam (Rochester Institute of Technology), Aritran Piplai (University of Texas El Paso), and Nidhi Rastogi (Rochester Institute of Technology)</i>	

Intrusion Detection and Response

Perry: A High-level Framework for Accelerating Cyber Deception Experimentation	582
<i>Brian Singer (Carnegie Mellon University), Yusuf Saquib (Carnegie Mellon University), Lujo Bauer (Carnegie Mellon University), and Vyas Sekar (Carnegie Mellon University)</i>	
Carbon Filter: Scalable, Efficient, and Secure Alert Triage for Endpoint Detection & Response	598
<i>Muhammad Adil Inam (University of Illinois at Urbana-Champaign), Jonathan Oliver (Broadcom Inc.), Raghav Batta (Broadcom Inc.), and Adam Bates (University of Illinois at Urbana-Champaign)</i>	
STGraph: Spatio-Temporal Graph Mining for Anomaly Detection in Distributed System Logs	614
<i>Teng Li (Xidian University), Shengkai Zhang (Xidian University), Yebo Feng (Nanyang Technological University), Jiahua Xu (University College London), Zexu Dang (Xidian University), Yang Liu (Nanyang Technological University), and Jianfeng Ma (Xidian University)</i>	

Detecting and Adapting to Stealthy Label-Inversion Drifts via Conditional Distribution Inference	628
<i>Xiaoli Zhang (University of Science and Technology Beijing), Yue Xiao (Tsinghua University), Qilei Yin (Zhongguancun Laboratory), Zhengyang Li (University of Science and Technology Beijing), Xinyan Wang (China Unicom Digital Tech Co., Ltd), Jianrong Zhang (China Unicom Digital Tech Co., Ltd), Ke Xu (Tsinghua University), Qi Li (Tsinghua University), and Xu-Cheng Yin (University of Science and Technology Beijing)</i>	
NIDP: Solving Feature Distribution Shifts in Network Intrusion Detection via Neural Pruning	644
<i>Jiangtao Ding (Zhejiang University of Technology, China), Junli Zheng (Zhejiang University of Technology, China), Chengyang Mo (China Jiliang University, China), Zhicheng Xu (Zhejiang University of Technology, China), and Hongbing Cheng (Zhejiang University of Technology, China)</i>	

Network and Protocol Security

Overlapping IPv4, IPv6, and TCP data: exploring errors, test case context, and multiple overlaps inside network stacks and NIDSes with PYROLYSE	657
<i>Lucas Aubard (Inria), Johan Mazel (ANSSI), Gilles Guette (IMT Atlantique), and Pierre Chifflier (ANSSI)</i>	
Active Attack Resilience in 5G: A New Take on Authentication and Key Agreement	676
<i>Nazatul H. Sultan (CSIRO's Data61, Australia), Xinlong Guan (CSIRO's Data61, Australia), Josef Pieprzyk (CSIRO's Data61, Australia & Polish Academy of Sciences, Poland), Wei Ni (CSIRO's Data61, Australia), Sharif Abuadbba (CSIRO's Data61, Australia), and Hajime Suzuki (CSIRO's Data61, Australia)</i>	
Revealing Informed Scanners by Colocating Reactive and Passive Telescopes	691
<i>Dario Ferrero (Delft University of Technology, The Netherlands), George Smaragdakis (Delft University of Technology, The Netherlands), and Harm Griffioen (Delft University of Technology, The Netherlands)</i>	

Web and Media Security

{{alert('CSTI')}}: Large-Scale Detection of Client-Side Template Injection	706
<i>Lorenzo Pisu (University of Cagliari, Italy), Davide Balzarotti (Eurecom, France), Davide Maiorca (University of Cagliari, Italy), and Giorgio Giacinto (University of Cagliari and National Interuniversity Consortium for Informatics, Italy)</i>	
Deep Learning-Based Attacks on Traditional Watermarking Systems in Real-Time Live Video Streams	721
<i>Huixin Wang (Monash University), Amin Sakzad (Monash University), and Stuart W. Hall (Monash University)</i>	

H2FUZZ: Guided, Black-box, Differential Fuzzing for HTTP/2-to-HTTP/1 Conversion Anomalies .	734
<i>Anthony Gavazzi (Northeastern University, United States), Weixin Kong (Northeastern University, United States), and Engin Kirda (Northeastern University, United States)</i>	
Deception Meets Diagnostics: Deception-based Real-Time Threat Detection in Healthcare Web Systems	749
<i>Zeeshan Zulkifl Shah (Macquarie University, Sydney, Australia), Muhammad Ikram (Macquarie University, Sydney, Australia), Hassan Jameel Asghar (Macquarie University, Sydney, Australia), and Mohamed Ali Kaafar (Macquarie University, Sydney, Australia)</i>	
Portal: Enabling Accurate Siemens PLC Rehosting via Peripheral Proxying and Proactive Interrupt Synchronization	769
<i>Haoran Li (Zhejiang University, China), Dakun Shen (Zhejiang University, China), Wenbo Shen (Zhejiang University, China), and Zhen Zhu (Zhejiang Lab, China)</i>	
Activation Functions Considered Harmful: Recovering Neural Network Weights through Controlled Channels	783
<i>Jesse Spielman (University of Birmingham, UK), David Oswald (University of Birmingham, UK and University of Durham, UK), Mark Ryan (University of Birmingham, UK), and Jo Van Bulck (KU Leuven, Belgium)</i>	
Zebrafix: Mitigating Memory-Centric Side-Channel Leakage via Interleaving	803
<i>Anna Pätschke (University of Luebeck, Germany), Jan Wichelmann (University of Luebeck, Germany), and Thomas Eisenbarth (University of Luebeck, Germany)</i>	
RF-Eye-D: Probing Feasibility of CMOS Camera Watermarking with Radio-Frequency Injection	818
<i>Hui Zhuang (Northeastern University), Yan Long (Northeastern University), and Kevin Fu (Northeastern University)</i>	
ShuffleV: A Microarchitectural Defense Strategy against Electromagnetic Side-Channel Attacks in Microprocessors	834
<i>Nuntipat Narkthong (Northeastern University), Yukui Luo (Binghamton University), and Xiaolin Xu (Northeastern University)</i>	

IoT, Mobile and VR Security

DeepFW: A DNN-Based Firmware Version Identification Framework for Online IoT Devices	854
<i>Zhen Lei (Taiyuan University of Technology, China), Nian Xue (Shandong University of Technology, China), Zhen Li (Shandong University of Technology, China), Dan Yu (Taiyuan University of Technology, China), Xin Huang (Taiyuan University of Technology, China), and Yongle Chen (Taiyuan University of Technology, China)</i>	
TAPPecker: TAP Logic Inference and Violation Detection in Heterogeneous Smart Home Systems.	869
<i>Qixiao Lin (Beihang University, China), Jian Mao (Beihang University, China; Tianmushan Laboratory, China; Hangzhou Innovation Institute, China; Zhongguancun Laboratory, China), Ziwen Liu (Beihang University, China), and Zhenkai Liang (National University of Singapore, Singapore)</i>	

Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers	887
<i>Gabriel K. Gegenhuber (University of Vienna), Maximilian Günther (University of Vienna), Markus Maier (University of Vienna), Aljosha Judmayer (University of Vienna), Florian Holzbauer (University of Vienna), Philipp É. Frenzel (SBA Research), and Johanna Ullrich (University of Vienna)</i>	
When (Inter)actions Speak Louder Than (Pass)words: Task-Based Evaluation of Implicit Authentication in Virtual Reality	905
<i>Woojin Jeon (Sungkyunkwan University, Republic of Korea), Chaejin Lim (Sungkyunkwan University, Republic of Korea), and Hyoungshick Kim (Sungkyunkwan University, Republic of Korea)</i>	
MotionDecipher: General Video-assisted Passcode Inference In Virtual Reality	919
<i>Guanchong Huang (University of Oklahoma, USA), Yan He (University of Oklahoma, USA), Shangqing Zhao (University of Oklahoma, USA), Yi Wu (University of Oklahoma, USA), and Song Fang (University of Oklahoma, USA)</i>	

Enterprise Cloud and Infrastructure Security

Uncontained Danger: Quantifying Remote Dependencies in Containerized Applications	935
<i>Chris Tsoukaladelis (Stony Brook University), Roberto Perdisci (University of Georgia), and Nick Nikiforakis (Stony Brook University)</i>	
RBAClock: Contain RBAC Permissions through Secure Scheduling	950
<i>Qingwang Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ru Tan (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xinyu Liu (Institute of Information Engineering, Chinese Academy of Sciences, China), Yuqi Shu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhou Tong (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Haoqiang Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ze Jin (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Qixu Liu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
Scalable Active Directory Defense with α -Metagraph	966
<i>Nhu Long Nguyen (University of Adelaide), Nickolas Falkner (University of Adelaide), and Hung Nguyen (University of Adelaide)</i>	

Author Index	987
--------------------	-----