2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2025)

Naples, Italy
23-26 June 2025

IEEE

IEEE Catalog Number: CFP25048-POD
ISBN: 979-8-3315-1202-6

****** 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:	CFP25048-POD
ISBN (Print-On-Demand):	979-8-3315-1202-6
ISBN (Online):	979-8-3315-1201-9
ISSN:	1530-0889

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

2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)

DSN 2025

Table of Contents

Message from the General Chairs ..... **xiii**
Message from the Program Chairs ..... **xv**
Steering Committee ..... **xvii**
Organizing Committee ..... **xviii**
Research Track Program Committee ..... **xx**
Research Track Reviewers ..... **xxiii**
William C. Carter Award ..... **xxvi**
Rising Star in Dependability Award ..... **xxviii**
Test of Time Award ..... **xxx**
Jean-Claude Laprie Award ..... **xxxi**
Distinguished Artifact Award ..... **xxxiv**
Keynote Addresses ..... **xxxvi**

Research Track

Privacy from 5 PM to 6 AM: Tracking and Transparency Mechanisms in the HbbTV Ecosystem 1
Christian Böttger (Westphalian University of Applied Sciences), Henry Hosseini (Westphalian University of Applied Sciences; University of Münster), Christine Utz (Radboud University), Nurullah Demir (Westphalian University of Applied Sciences), Jan Hörnemann (Westphalian University of Applied Sciences; AWARE7 GmbH), Christian Wressnegger (Karlsruhe Institute of Technology), Thomas Hupperich (University of Münster), Norbert Pohlmann (Westphalian University of Applied Sciences), Matteo Große-Kampmann (Rhine-Waal University of Applied Sciences), and Tobias Urban (Westphalian University of Applied Sciences)

Revisiting Main Memory-Based Covert and Side Channel Attacks in the Context of Processing-in-Memory 16
F. Nisa Bostancı (ETH Zürich), Konstantinos Kanellopoulos (ETH Zürich), Ataberk Olgun (ETH Zürich), A. Giray Yağlıkçı (ETH Zürich), İsmail Emir Yüksel (ETH Zürich), Nika Mansouri Ghiasi (ETH Zürich), Zülal Bingöl (ETH Zürich; Bilkent University), Mohammad Sadrosadati (ETH Zürich), and Onur Mutlu (ETH Zürich)

GTV: Generating Tabular Data via Vertical Federated Learning 33
Zilong Zhao (National University of Singapore, Singapore; Betterdata, Singapore), Han Wu (University of Southampton, UK), Aad van Moorsel (University of Birmingham, UK), and Lydia Y. Chen (University of Neuchâtel, Switzerland)

BASSET: Enhancing Binary Code Clone Searching through Multi-Level Hybrid Semantic Indexing.. 47
Yong Zhao (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ang Xia (State Grid Corporation of China Information and Communication Branch), Jie Yin (Chinese Academy of Sciences, China), Zhi Wang (Zhongguancun Laboratory, China), Yaqin Cao (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xiangyi Zeng (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Yuling Liu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

LAGER: Layer-Wise Graph Feature Extractor for Network Intrusion Detection 61
Ke He (University of Canterbury, New Zealand), Dan Dongseong Kim (The University of Queensland, Australia), and Muhammad Rizwan Asghar (University of Surrey, United Kingdom)

VerifyVFL: Practical Verifiable Vertical Federated Learning 75
Junchen Hou (University of Science and Technology of China, China) and Lan Zhang (University of Science and Technology of China, China)

Towards More Dependable Specifications: An Empirical Study Exploring the Synergy of Traditional and LLM-Based Repair Approaches 88
Md Rashedul Hasan (University of Nebraska-Lincoln, USA), Mohannad Alhanahnah (Chalmers/University of Gothenburg, Sweden), Clay Stevens (Iowa State University, USA), and Hamid Bagheri (University of Nebraska-Lincoln, USA)

PTC: Prefix Tuning CodeT5 for High-Quality Secure Network Measurement Script Generation 102
Yuanda Wang (Peking University, China) and Xinhui Han (Peking University, China)

5G-STREAM: Service Mesh Tailored for Reliable, Efficient and Authorized Microservices in the Cloud 116
Tolga O. Atalay (Virginia Tech, USA), Alireza Famili (Virginia Tech, USA), Sudip Maitra (Virginia Tech, USA), Dragoslav Stojadinovic (Kryptowire, LLC, USA), Angelos Stavrou (Virginia Tech, USA; Kryptowire, LLC, USA), and Haining Wang (Virginia Tech, USA)

A Human Study of Automatically Generated Decompiler Annotations 129
Yuwei Yang (Vanderbilt University, USA), Skyler Grandel (Vanderbilt University, USA), Jeremy Lacomis (Carnegie Mellon University, USA), Edward Schwartz (Carnegie Mellon University, USA), Bogdan Vasilescu (Carnegie Mellon University, USA), Claire Le Goues (Carnegie Mellon University, USA), and Kevin Leach (Vanderbilt University, USA)

ammBoost: State Growth Control for AMMs 143
Nicolas Michel (University of Connecticut, USA), Mohamed E. Najd (University of Connecticut, USA), and Ghada Almashaqbeh (University of Connecticut, USA)

ReCraft: Self-Contained Split, Merge, and Membership Change of Raft Protocol 157
Kezhi Xiong (Northeastern University), Soonwon Moon (Seoul National University), Joshua H. Kang (Northeastern University), Bryant Curto (Northeastern University), Jieung Kim (Yonsei University), and Ji-Yong Shin (Northeastern University)

Semantically Improved Adversarial Attack Based on Masked Language Model via Context Preservation 171
Hao Tian (South China University of Technology, China), Hao-Tian Wu (Guangzhou University, China; Guangdong Key Laboratory of Industrial Control System Security, China), Yiu-ming Cheung (Hong Kong Baptist University, China), Junhui He (South China University of Technology, China), and Zhihong Tian (Guangzhou University, China; Guangdong Key Laboratory of Industrial Control System Security, China)

Less is More: Boosting Coverage of Web Crawling through Adversarial Multi-Armed Bandit 183
Lorenzo Cazzaro (Università Ca' Foscari Venezia, Italy), Stefano Calzavara (Università Ca' Foscari Venezia, Italy), Maksim Kovalkov (Università Ca' Foscari Venezia, Italy), Aleksei Stafeev (CISPA Helmholtz Center for Information Security, Germany), and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany)

ICSTRACKER: Backtracking Intrusions in Modern Industrial Control Systems 193
Md Raihan Ahmed (University of Utah, USA), Jainta Paul (University of Utah, USA), Levi Taiji Li (University of Utah, USA), Luis Garcia (University of Utah, USA), and Mu Zhang (University of Utah, USA)

GnuZero: A Compiler-Based Zeroization Static Detection Tool for the Masses 208
Pierrick Philippe (Univ Rennes), Mohamed Sabt (Univ Rennes), and Pierre-Alain Fouque (Univ Rennes)

PhishingHook: Catching Phishing Ethereum Smart Contracts Leveraging EVM Opcodes 222
Pasquale De Rosa (University of Neuchâtel, Switzerland), Simon Queyrut (University of Neuchâtel, Switzerland), Yérom-David Bromberg (University of Rennes, France), Pascal Felber (University of Neuchâtel, Switzerland), and Valerio Schiavoni (University of Neuchâtel, Switzerland)

GREAT: Global Representation and Edge-Attention for Hardware Trojan Detection 233
Zhengyi Li (Xiangtan University, China; NUDT, China), Wei Cheng (NUDT, China), Huanrong Tang (Xiangtan University, China), and Yaohua Wang (NUDT, China)

IPMES+: Enhancing Incremental TTP Detection with Frequency and Flow Semantics 246
Hong-Wei Li (Academia Sinica, Taiwan), Ping-Ting Liu (NYCU, Taiwan), Bo-Wei Lin (NYCU, Taiwan), and Yennun Huang (Academia Sinica, Taiwan)

Towards Continuous Integrity Attestation and Its Challenges in Practice: A Case Study of Keylime 256
Margie Ruffin (University of Illinois Urbana-Champaign, USA), Chenkai Wang (University of Illinois Urbana-Champaign, USA), Gheorghe Almasi (IBM Research, USA), Abdulhamid Adebayo (IBM Research, USA), Hubertus Franke (IBM Research, USA), and Gang Wang (University of Illinois Urbana-Champaign, USA)

Decoding DNS Centralization: Measuring and Identifying NS Domains Across Hosting Providers. 266
Qihang Peng (Tsinghua University, China), Mingming Zhang (Zhongguancun Laboratory, China), Deliang Chang (QI-ANXIN Technology Research Institute, China), Jia Zhang (Tsinghua University, China), Baojun Liu (Tsinghua University, China), and Haixin Duan (Tsinghua University, China)

ConfBench: A Tool for Easy Evaluation of Confidential Virtual Machines 279
Andrea De Murtas (Sapienza University of Rome, Italy; University of Neuchâtel, Switzerland), Daniele Cono D'Elia (Sapienza University of Rome, Italy), Giuseppe Antonio Di Luna (Sapienza University of Rome, Italy), Pascal Felber (University of Neuchâtel, Switzerland), Leonardo Querzoni (Sapienza University of Rome, Italy,), and Valerio Schiavoni (University of Neuchâtel, Switzerland)

SOUNDBOOST: Effective RCA and Attack Detection for UAV via Acoustic Side-Channel 289
Haoran Wang (Georgia Institute of Technology), Zheng Yang (Georgia Institute of Technology), Sangdon Park (Pohang University of Science and Technology), Yibin Yang (Georgia Institute of Technology), Seulbae Kim (Pohang University of Science and Technology), Willian Lunardi (Technology Innovation Institute), Martin Andreoni (Technology Innovation Institute), Taesoo Kim (Georgia Institute of Technology), and Wenke Lee (Georgia Institute of Technology)

Faster Hash-Based Multi-Valued Validated Asynchronous Byzantine Agreement 303
Hanwen Feng (University of Sydney, Australia), Zhenliang Lu (Nanyang Technological University, Singapore), Tiancheng Mai (University of Sydney, Australia), and Qiang Tang (University of Sydney, Australia)

LiveGuard: Voice Liveness Detection via Wavelet Scattering Transform and Mel Spectrogram Scaling 317
Liqun Shan (University of Louisiana at Lafayette, USA), Xingli Zhang (University of Louisiana at Lafayette, USA), Md Imran Hossen (University of Louisiana at Lafayette, USA), and Xiali Hei (University of Louisiana at Lafayette, USA)

EasyDRAM: An FPGA-Based Infrastructure for Fast and Accurate End-to-End Evaluation of Emerging DRAM Techniques 331
Oğuzhan Canpolat (TOBB ETÜ; ETH Zürich), Ataberk Olgun (ETH Zürich), David Novo (Univ. Montpellier), Oğuz Ergin (University of Sharjah; ETH Zürich; TOBB ETÜ), and Onur Mutlu (ETH Zürich)

What Lies Beneath: An Empirical Study of Silent Vulnerability Fixes in Open-Source Software 345
Jialiang Dong (The University of New South Wales), Xinzhang Chen (The University of New South Wales), Willy Susilo (University of Wollongong), Nan Sun (The University of New South Wales), Arash Shaghaghi (The University of New South Wales), and Siqi Ma (The University of New South Wales)

Attack-Defense Trees with Offensive and Defensive Attributes 358
Danut-Valentin Copae (University of Twente), Reza Soltani (University of Twente), and Milan Lopuhaä-Zwakenberg (University of Twente)

An Analysis of Malicious Packages in Open-Source Software in the Wild 371
Xiaoyan Zhou (Beijing Jiaotong University, China), Ying Zhang (Beijing Jiaotong University, China), Wenjia Niu (Beijing Jiaotong University, China), Jiqiang Liu (Beijing Jiaotong University, China), Haining Wang (Virginia Polytechnic Institute and State University, USA), and Qiang Li (Beijing Jiaotong University, China)

ParaVerser: Harnessing Heterogeneous Parallelism for Affordable Fault Detection in Data Centers 386
Minli Julie Liao (University of Cambridge), Sam Ainsworth (University of Edinburgh), Lev Mukhanov (Queen Mary University of London), Adrian Barredo (Barcelona Supercomputing Center), Markos Kynigos (University of Manchester), and Timothy M. Jones (University of Cambridge)

Detecting Code Vulnerabilities using LLMs 401
Larry Huynh (The University of Western Australia, Australia), Yinghao Zhang (The University of Western Australia, Australia), Djimon Jayasundera (The University of Western Australia, Australia), Woojin Jeon (Sungkyunkwan University, South Korea), Hyoungshick Kim (Sungkyunkwan University, South Korea), Tingting Bi (The University of Western Australia, Australia), and Jin B. Hong (The University of Western Australia, Australia)

Privacy Analysis of Oblivious DNS over HTTPS: A Website Fingerprinting Study 415
Mohammad Amir Salari (Saint Louis University, USA), Abhinav Kumar (Saint Louis University, USA), Federico Rinaudi (Politecnico di Torino, Italy), Reza Tourani (Saint Louis University, USA), Alessio Sacco (Politecnico di Torino, Italy), and Flavio Esposito (Saint Louis University, USA)

Securing In-Network Traffic Control Systems with P4Auth 429
K Ranjitha (IIT Hyderabad, India), Medha Rachel Panna (IIT Hyderabad, India; New York University, USA), Stavan Nilesh Christian (New York University, USA), Karuturi Havya Sree (IIT Hyderabad, India; New York University, USA), Sri Hari Malla (IIT Hyderabad, India; New York University, USA), Dheekshitha Bheemanath (IIT Hyderabad, India; New York University, USA), Rinku Shah (IIIT-Delhi, India), and Praveen Tammana (IIT Hyderabad, India)

MichiCAN: Spoofing and Denial-of-Service Protection using Integrated CAN Controllers 443
Mert D. Pesé (Clemson University), Bulut Gozubuyuk (Clemson University), Eric Andrechek (University of Michigan), Habeeb Olufowobi (University of Texas at Arlington), Mohammad Hamad (Technical University of Munich), and Kang G. Shin (University of Michigan)

SemiAF: Semi-Supervised App Fingerprinting on Unknown Traffic via Graph Neural Network 457
Xiaodong Lei (National University of Defense Technology, China), Yongjun Wang (National University of Defense Technology, China), Lin Liu (National University of Defense Technology, China), Jun-Jie Huang (National University of Defense Technology, China), Jiangyong Shi (National University of Defense Technology, China), and Luming Yang (National University of Defense Technology, China)

MalTAG: Encrypted Malware Traffic Detection Framework via Graph Based Flow Interaction Mining 470
Renjie Li (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhou Zhou (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Hao Miao (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Fengyuan Shi (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Qingyun Liu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Valkyrie: A Response Framework to Augment Runtime Detection of Time-Progressive Attacks 483
Nikhilesh Singh (Technische Universität Darmstadt, Germany) and Chester Rebeiro (Indian Institute of Technology Madras, India)

KubeFence: Security Hardening of the Kubernetes Attack Surface 497
Carmine Cesarano (Università degli Studi di Napoli Federico II, Italy) and Roberto Natella (Università degli Studi di Napoli Federico II, Italy)

Hierarchical Model-Based Approach for Concurrent Testing of Neuromorphic Architecture 511
Suman Kumar (Drexel University, USA), Abhishek Mishra (Drexel University, USA), Anup Das (Drexel University, USA), and Nagarajan Kandasamy (Drexel University, USA)

QUIC-Aware Load Balancing: Attacks and Mitigations 524
Liliana Kistenmacher (University of Hamburg), Anum Talpur (University of Hamburg), and Mathias Fischer (University of Hamburg)

RAVAGE: Robotic Autonomous Vehicles' Attack Generation Engine 537
Pritam Dash (University of British Columbia) and Karthik Pattabiraman (University of British Columbia)

Prompting the Unseen: Detecting Hidden Backdoors in Black-Box Models 547
Zi-Xuan Huang (National Yang Ming Chiao Tung University, Taiwan), Jia-Wei Chen (National Yang Ming Chiao Tung University, Taiwan), Zhi-Peng Zhang (National Yang Ming Chiao Tung University, Taiwan), and Chia-Mu Yu (National Yang Ming Chiao Tung University, Taiwan)

MicroSampler: A Framework for Microarchitecture-Level Leakage Detection in Constant Time Execution 562
Moein Ghaniyoun (The Ohio State University), Kristin Barber (Google), Yinqian Zhang (SUSTech), and Radu Teodorescu (The Ohio State University)

Reentrancy Redux: The Evolution of Real-World Reentrancy Attacks on Blockchains 576
Yuqi Liu (University of British Columbia), Rui Xi (University of British Columbia), and Karthik Pattabiraman (University of British Columbia)

On Security Vulnerabilities in Transportation IoT Devices 589
Jason Yih (University of Maryland, MD), Katerina Goseva-Popstojanova (West Virginia University, WV), and Michel Cukier (University of Maryland, MD)

Safety Interventions against Adversarial Patches in an Open-Source Driver Assistance System 599
Cheng Chen (Louisiana State University, LA), Grant Xiao (University of Virginia, VA), Daehyun Lee (George Mason University, VA), Lishan Yang (George Mason University, VA), Evgenia Smirni (William & Mary, VA), Homa Alemzadeh (University of Virginia, VA), and Xugui Zhou (Louisiana State University, LA)

Secure Access to Network Data for Mobile Network Traffic Analysis Applications 609
Djob Mvondo (Univ Rennes) and Yerom-David Bromberg (Univ Rennes)

Zero-Interference Containers: A Framework to Orchestrate Mixed-Criticality Applications 627
Daniele Ottaviano (Technical University of Munich), Marco Barletta (Huawei Edinburgh Research Center), and Francesco Boccola (Università degli Studi di Napoli Federico II)

Mitigating Front-Running Attacks through Fair and Resilient Transaction Dissemination 637
Wassim Yahyaoui (Univ. of Luxembourg), Joachim Bruneau-Queyreix (Univ. Bordeaux, France), Jérémie Decouchant (Delft University of Technology), and Marcus Völp (Univ. of Luxembourg)

A Closer Look At Modern Evasive Phishing Emails 650
Elyssa Boulila (Amadeus IT Group, France; EURECOM, France), Marc Dacier (KAUST, Saudi Arabia), Siva Prem Vengadessa Peroumal (Amadeus IT Group, France), Nicolas Veys (Amadeus IT Group, France), and Simone Aonzo (EURECOM, France)

Towards Automated and Explainable Threat Hunting with Generative AI 664
Moumita Das Purba (University of North Carolina at Charlotte, USA), Bill Chu (University of North Carolina at Charlotte, USA), and Will French (University of North Carolina at Charlotte, USA)

ZCOVER: Uncovering Z-Wave Controller Vulnerabilities Through Systematic Security Analysis of Application Layer Implementation 678
Nkuba Kayembe Carlos (Korea University), Jimin Kang (Korea University), Seunghoon Woo (Korea University), and Heejo Lee (Korea University)

ReMlX: Resilience for ML Ensembles using XAI at Inference against Faulty Training Data 691
Abraham Chan (The University of British Columbia (UBC), Canada), Arpan Gujarati (The University of British Columbia (UBC), Canada), Karthik Pattabiraman (The University of British Columbia (UBC), Canada), and Sathish Gopalakrishnan (The University of British Columbia (UBC), Canada)

"I will always be by your side": A Side-Channel Aided PWM-based Holistic Attack Recovery for Unmanned Aerial Vehicles 706
Muneeba Asif (Florida International University, USA), Jean C Tonday Rodriguez (Florida International University, USA), Mohammad Kumail Kazmi (Florida International University, USA), Mohammad Ashiqur Rahman (Florida International University, USA), and Kemal Akkaya (Florida International University, USA)

Multi-Version Machine Learning and Rejuvenation for Resilient Perception in Safety-Critical Systems 720
Qiang Wen (University of Tsukuba, Japan), Júlio Mendonça (University of Luxembourg, Luxembourg), Fumio Machida (University of Tsukuba, Japan), and Marcus Völp (University of Luxembourg, Luxembourg)

Automatically Generating Rules of Malicious Software Packages via Large Language Model 734
XiangRui Zhang (Beijing Jiaotong University, China), XueJie Du (Beijing Jiaotong University, China), HaoYu Chen (Beijing Jiaotong University, China), Yongzhong He (Beijing Jiaotong University, China), Wenjia Niu (Beijing Jiaotong University, China), and Qiang Li (Beijing Jiaotong University, China)

Author Index **749**