

2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) **DSN 2024**

Table of Contents

Message from the General Chairs	xi
Message from the Program Chairs	xiii
Steering Committee	xv
Organizing Committee	xvi
Research Track Program Committee	xviii
Research Track Reviewers	xxi
Keynotes	xxiii
William C. Carter Award	xxvi
Rising Star in Dependability Award	xxviii
Test of Time Award	xxix
Jean-Claude Laprie Award	xxx

Research Track

Mutiny! How does Kubernetes fail, and what can we do about it?	1
<i>Marco Barletta (Università degli Studi di Napoli Federico II, Italy), Marcello Cinque (Università degli Studi di Napoli Federico II, Italy), Catello Di Martino (Nokia Bell Labs, Brazil), Zbigniew T. Kalbarczyk (University of Illinois at Urbana-Champaign, USA), and Ravishankar K. Iyer (University of Illinois at Urbana Champaign, USA)</i>	
Reboot-Based Recovery of Unikernels at the Component Level	15
<i>Takeru Wada (TUAT, Japan) and Hiroshi Yamada (TUAT, Japan)</i>	
On the Correctness of Metadata-Based SBOM Generation: A Differential Analysis Approach	29
<i>Sheng Yu (University of California, Riverside; Deepbits Technology Inc.), Wei Song (Deepbits Technology Inc.), Xunchao Hu (Deepbits Technology Inc.), and Heng Yin (University of California, Riverside; Deepbits Technology Inc.)</i>	
SPP: Safe Persistent Pointers for Memory Safety	37
<i>Dimitrios Stavrakakis (TU Munich & The University of Edinburgh), Alexandrina Panfil (TU Munich), Mjin Nam (TU Munich), and Pramod Bhatotia (TU Munich)</i>	
Byzantine Attacks Exploiting Penalties in Ethereum PoS	53
<i>Ulysse Pavloff (Université Paris-Saclay, CEA, LIST, France), Yackolley Amoussou-Guenou (Université Paris-Panthéon-Assas, CRED, France), and Sara Tucci-Piergiovanni (Université Paris-Saclay, CEA, LIST, France)</i>	

ADSynth: Synthesizing Realistic Active Directory Attack Graphs	66
<i>Nhu Long Nguyen (University of Adelaide, Australia), Nickolas Falkner (University of Adelaide, Australia), and Hung Nguyen (University of Adelaide, Australia)</i>	
Read Disturbance in High Bandwidth Memory: A Detailed Experimental Study on HBM2 DRAM Chips	75
<i>Ataberk Olgun (ETH Zürich), Majd Osseiran (ETH Zürich), A. Giray Yağlıkçı (ETH Zürich), Yahya Can Tuğrul (ETH Zürich), Haocong Luo (ETH Zürich), Steve Rhyner (ETH Zürich), Behzad Salami (BSC), Juan Gomez Luna (ETH Zürich), and Onur Mutlu (ETH Zürich)</i>	
A Fast Low-Level Error Detection Technique	90
<i>Zhengyang He (University of Iowa, USA), Hui Xu (Fudan University, China), and Guanpeng Li (University of Iowa, USA)</i>	
Simultaneous Many-Row Activation in Off-the-Shelf DRAM Chips: Experimental Characterization and Analysis	99
<i>Ismail Emir Yüksel (ETH Zürich), Yahya Can Tuğrul (ETH Zürich; TOBB University of Economics and Technology), F. Nisa Bostancı (ETH Zürich), Geraldo F. Oliveira (ETH Zürich), A. Giray Yağlıkçı (ETH Zürich), Ataberk Olgun (ETH Zürich), Melina Soysal (ETH Zürich), Haocong Luo (ETH Zürich), Juan Gómez-Luna (ETH Zürich), Mohammad Sadrosadati (ETH Zürich), and Onur Mutlu (ETH Zürich)</i>	
Grunt Attack: Exploiting Execution Dependencies in Microservices	115
<i>Xuhang Gu (Louisiana State University), Qingyang Wang (Louisiana State University), Jianshu Liu (Louisiana State University), and Jinpeng Wei (University of North Carolina at Charlotte)</i>	
PAROLE: Profitable Arbitrage in Optimistic Rollup with ERC-721 Token Transactions	129
<i>Alvi Ataur Khalil (Florida International University, USA) and Mohammad Ashiqur Rahman (Florida International University, USA)</i>	
iPrism: Characterize and Mitigate Risk by Quantifying Change in Escape Routes	142
<i>Shengkun Cui (University of Illinois at Urbana-Champaign, USA), Saurabh Jha (IBM Research, USA), Ziheng Chen (University of Illinois at Urbana-Champaign, USA), Zbigniew T. Kalbarczyk (University of Illinois at Urbana-Champaign, USA), and Ravishankar K. Iyer (University of Illinois at Urbana-Champaign, USA)</i>	
JITBULL: Securing JavaScript Runtime with a Go/No-Go Policy for JIT Engine	156
<i>Jean-Baptiste Decourcelle (IRIT, Université de Toulouse, CNRS, Toulouse INP, UT3, France), Boris Teabe (IRIT, Université de Toulouse, CNRS, Toulouse INP, UT3, France), and Daniel Hagimont (IRIT, Université de Toulouse, CNRS, Toulouse INP, UT3, France)</i>	
Privacy Leakage from Logits Attack and Its Defense in Federated Distillation	169
<i>Danyang Xiao (Sun Yat-sen University), Diying Yang (Sun Yat-sen University), Jialun Li (Sun Yat-sen University), Xu Chen (Sun Yat-sen University), and Weigang Wu (Sun Yat-sen University)</i>	
System Call Interposition Without Compromise	183
<i>Adriaan Jacobs (DistriNet, KU Leuven, Belgium), Merve Gülmez (Ericsson Security Research, Sweden; DistriNet, KU Leuven, Belgium), Alicia Andries (DistriNet, KU Leuven, Belgium), Stijn Volckaert (DistriNet, KU Leuven, Belgium), and Alexios Voulimeneas (TU Delft, Netherlands)</i>	

Protecting Confidential Virtual Machines from Hardware Performance Counter Side Channels	195
<i>Xiaoxuan Lou (Nanyang Technological University), Kangjie Chen (Nanyang Technological University), Guowen Xu (Nanyang Technological University), Han Qiu (Tsinghua University), Shangwei Guo (Chongqing University), and Tianwei Zhang (Nanyang Technological University)</i>	
ZLB: A Blockchain to Tolerate Colluding Majorities	209
<i>Alejandro Ranchal-Pedrosa (University of Sydney and Protocol Labs, Australia) and Vincent Gramoli (University of Sydney and Redbelly Network, Australia)</i>	
ZipChannel: Cache Side-Channel Vulnerabilities in Compression Algorithms	223
<i>Marina Minkin (University of Michigan) and Baris Kasikci (University of Washington)</i>	
ChainNet: A Customized Graph Neural Network Model for Loss-Aware Edge AI Service Deployment	238
<i>Zifeng Niu (Imperial College London), Manuel Roveri (Politecnico di Milano), and Giuliano Casale (Imperial College London)</i>	
Goldfish: An Efficient Federated Unlearning Framework	252
<i>Houzhe Wang (University of Chinese Academy of Sciences, China; Institute of Information Engineering, Chinese Academy of Sciences, China), Xiaojie Zhu (King Abdullah University of Science and Technology, Kingdom of Saudi Arabia), Chi Chen (University of Chinese Academy of Sciences, China; Institute of Information Engineering, Chinese Academy of Sciences, China), and Paulo Esteves-Veríssimo (King Abdullah University of Science and Technology, Kingdom of Saudi Arabia)</i>	
IPMES: A Tool for Incremental TTP Detection over the System Audit Event Stream	265
<i>Hong-Wei Li (Academia Sinica, Taiwan), Ping-Ting Liu (National Yang Ming Chiao Tung University, Taiwan), Bo-Wei Lin (National Yang Ming Chiao Tung University, Taiwan), Yi-Chun Liao (National Taiwan University, Taiwan), and Yennun Huang (Academia Sinica, Taiwan)</i>	
Decentagram: Highly-Available Decentralized Publish/Subscribe Systems	274
<i>Haofan Zheng (UC Santa Cruz), Tuan Tran (UC Santa Cruz), Roy Shadmon (UC Santa Cruz), and Owen Arden (UC Santa Cruz)</i>	
Toward Evaluating Robustness of Reinforcement Learning with Adversarial Policy	288
<i>Xiang Zheng (City University of Hong Kong), Xingjun Ma (Fudan University), Shengjie Wang (Tsinghua University), Xinyu Wang (Tencent Inc.), Chao Shen (Xi'an Jiaotong University), and Cong Wang (City University of Hong Kong)</i>	
Towards Shielding 5G Control Plane Functions	302
<i>Sudip Maitra (Virginia Tech, USA), Tolga O. Atalay (Virginia Tech, USA), Angelos Stavrou (Virginia Tech, USA; Kryptowire LLC, USA), and Haining Wang (Virginia Tech, USA)</i>	
A Comprehensive Study on Drones Resilience in the Presence of Inertial Measurement Unit Faults	316
<i>Anamta Khan (University of Coimbra, Portugal), Naghmeh Ivaki (University of Coimbra, Portugal), and Henrique Madeira (University of Coimbra, Portugal)</i>	

Stealthy Peers: Understanding Security and Privacy Risks of Peer-Assisted Video Streaming	324
<i>Siyuan Tang (Indiana University Bloomington), Eihal Alowaisheq (King Saud University), Xianghang Mi (University of Science and Technology of China), Yi Chen (Indiana University Bloomington), XiaoFeng Wang (Indiana University Bloomington), and Yanzhi Dou (Independent Researcher)</i>	
Intrusion Tolerance for Networked Systems through Two-Level Feedback Control	338
<i>Kim Hammar (KTH Royal Institute of Technology, Sweden) and Rolf Stadler (KTH Royal Institute of Technology, Sweden)</i>	
RABIT, a Robot Arm Bug Intervention Tool for Self-Driving Labs	353
<i>Zainab Saeed Wattoo (University of British Columbia, Canada), Petal Vitis (University of British Columbia, Canada), Ruizhe Zhu (University of British Columbia, Canada), Noah Depner (University of British Columbia, Canada), Ivory Zhang (University of British Columbia, Canada), Jason Hein (University of British Columbia, Canada), Arpan Gujarati (University of British Columbia, Canada), and Margo Seltzer (University of British Columbia, Canada)</i>	
Owl: Differential-Based Side-Channel Leakage Detection for CUDA Applications	362
<i>Yu Zhao (Huazhong University of Science and Technology, China), Wenjie Xue (Huazhong University of Science and Technology, China), Weijie Chen (Huazhong University of Science and Technology, China), Weizhong Qiang (Huazhong University of Science and Technology, China; Jinyinhu Laboratory, China), Deqing Zou (Huazhong University of Science and Technology, China; Jinyinhu Laboratory, China), and Hai Jin (Huazhong University of Science and Technology, China)</i>	
AOAB: Optimal and Fair Ordering of Financial Transactions	377
<i>Vincent Gramoli (University of Sydney, Australia; Redbelly Network, Australia), Zhenliang Lu (University of Sydney, Australia), Qiang Tang (University of Sydney, Australia), and Pouriya Zarbafian (University of Sydney, Australia)</i>	
BFTRAND: Low-Latency Random Number Provider for BFT Smart Contracts	389
<i>Jinghui Liao (Southern University of Science and Technology, China; Wayne State University, USA; Neo Foundation), Borui Gong (Southern University of Science and Technology, China; The Hong Kong Polytechnic University, China), Wenhai Sun (Purdue University, USA), Fengwei Zhang (Southern University of Science and Technology, China), Zhenyu Ning (Hunan University, China), Man Ho Au (The Hong Kong Polytechnic University, China), and Weisong Shi (University of Delaware, USA)</i>	
Verifying Randomized Consensus Protocols with Common Coins	403
<i>Song Gao (University of Chinese Academy of Sciences, China; Institute of Software, Chinese Academy of Sciences, China), Bohua Zhan (University of Chinese Academy of Sciences, China; Institute of Software, Chinese Academy of Sciences, China), Zhilin Wu (University of Chinese Academy of Sciences, China; Institute of Software, Chinese Academy of Sciences, China), and Lijun Zhang (University of Chinese Academy of Sciences, China; Institute of Software, Chinese Academy of Sciences, China; Institute of Intelligent Software, China)</i>	

Real-Time Intrusion Detection and Prevention with Neural Network in Kernel using eBPF	416
<i>Junyu Zhang (Sun Yat-sen University, China), Pengfei Chen (Sun Yat-sen University, China), Zilong He (Sun Yat-sen University, China), Hongyang Chen (Sun Yat-sen University, China), and Xiaoyun Li (Sun Yat-sen University, China)</i>	
PagPassGPT: Pattern Guided Password Guessing via Generative Pretrained Transformer	429
<i>Xingyu Su (University of Chinese Academy of Sciences, China; Institute of Information Engineering, Chinese Academy of Sciences, China), Xiaojie Zhu (King Abdullah University of Science and Technology, Kingdom of Saudi Arabia), Yang Li (University of Chinese Academy of Sciences, China; Institute of Information Engineering, Chinese Academy of Sciences, China), Yong Li (Institute of Information Engineering, Chinese Academy of Sciences, China), Chi Chen (University of Chinese Academy of Sciences, China; Institute of Information Engineering, Chinese Academy of Sciences, China), and Paulo Esteves-Verissimo (King Abdullah University of Science and Technology, Kingdom of Saudi Arabia)</i>	
Iniva: Inclusive and Incentive-Compatible Vote Aggregation	443
<i>Arian Baloochestani (University of Stavanger, Norway), Hanish Gogada (University of Stavanger, Norway), Leander Jehl (University of Stavanger, Norway), and Hein Meling (University of Stavanger, Norway)</i>	
Delphi: Efficient Asynchronous Approximate Agreement for Distributed Oracles	456
<i>Akhil Bandrupalli (Purdue University), Adithya Bhat (Visa Research), Saurabh Bagchi (Purdue University), Aniket Kate (Purdue University; Supra Research), Chen-Da Liu-Zhang (Lucerne University of Applied Sciences and Arts; Web3 Foundation), and Michael K. Reiter (Duke University; Chainlink Labs)</i>	
Moonshot: Optimizing Block Period and Commit Latency in Chain-Based Rotating Leader BFT	470
<i>Isaac Doidge (Supra Research), Raghavendra Ramesh (Supra Research), Nibesh Shrestha (Supra Research), and Joshua Tobkin (Supra Research)</i>	
SyRep: Efficient Synthesis and Repair of Fast Re-Route Forwarding Tables for Resilient Networks	483
<i>Csaba Györgyi (University of Vienna), Kim G. Larsen (Aalborg University), Stefan Schmid (University of Vienna; TU Berlin), and Jiri Srba (Aalborg University)</i>	
FIRMRES: Exposing Broken Device-Cloud Access Control in IoT Through Static Firmware Analysis	495
<i>Yuting Xiao (Hunan University, China), Jiongyi Chen (National University of Defense Technology, China), Yupeng Hu (Hunan University, China), and Jing Huang (Hunan University, China)</i>	
ChatScam: Unveiling the Rising Impact of ChatGPT on Domain Name Abuse	507
<i>Mingxuan Liu (Zhongguancun Laboratory, China), Zhenglong Jin (Tsinghua University, China), Jiahai Yang (Fuzhou University, China), Baojun Liu (Tsinghua University, China), Haixin Duan (Zhongguancun Laboratory, China; Tsinghua University, China), Ying Liu (Tsinghua University, China; Zhongguancun Laboratory, China), Ximeng Liu (Fuzhou University, China), and Shujun Tang (QI-ANXIN Technology Research Institute, China)</i>	

SEDSpec: Securing Emulated Devices by Enforcing Execution Specification	522
<i>Yang Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Shengzhi Zhang (Boston University, USA), Xiaoqi Jia (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Qihang Zhou (Institute of Information Engineering, Chinese Academy of Sciences, China), Heqing Huang (Institute of Information Engineering, Chinese Academy of Sciences, China), Shaowen Xu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Haichao Du (Institute of Information Engineering, Chinese Academy of Sciences, China)</i>	
OffRAMPS: An FPGA-Based Intermediary for Analysis and Modification of Additive Manufacturing Control Systems	535
<i>Jason Blocklove (New York University, USA), Raz Raz (New York University, USA), Prithwish Basu Roy (New York University Abu Dhabi, UAE), Hammond Pearce (University of New South Wales, Australia), Prashanth Krishnamurthy (New York University, USA), Farshad Khorrami (New York University, USA), and Ramesh Karri (New York University, USA)</i>	
Author Index	545