2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)

DSN-S 2024

Table of Contents

Message from the Disrupt'24 Chairs x
Message from the Doctoral Forum Chairs xi
Message from the Tutorial Chairs xii
Message from the Industry Chairs xiii
Message from the Poster Track Chairs xiv
Message from the Artifacts Chairs xv
Artifacts Committee xvi

Disrupt

AuSSE: A Novel Framework for Security and Safety Evaluation for Autonomous Vehicles 1
Nhung H. Nguyen (The University of Queensland, Australia), Jin-Hee Cho (Virginia Tech, USA), Terrence J. Moore (US Army Research Laboratory, USA), Seunghyun Yoon (Korea Institute of Energy Technology, USA), Hyuk Lim (Korea Institute of Energy Technology, South Korea), Frederica Nelson (US Army Research Laboratory, USA), Guangdong Bai (The University of Queensland, Australia), and Dan Dongseong Kim (The University of Queensland, Australia)

An Experimental Characterization of Combined RowHammer and RowPress Read Disturbance in Modern DRAM Chips 6
Haocong Luo (ETH Zürich), İsmail Emir Yüksel (ETH Zürich), Ataberk Olgun (ETH Zürich), A. Giray Yağçlıkçı (ETH Zürich), Mohammad Sadrosadati (ETH Zürich), and Onur Mutlu (ETH Zürich)

Exploring Use of Symbolic Execution for Service Analysis 12
Yang Zhang (Tsinghua University), Long Wang (Tsinghua University; Zhongguancun Laboratory), Zhengang Wang (Huawei Corporation), and Dongdong Shangguan (Huawei Corporation)

When Green Computing Meets Performance and Resilience SLOs 17
Haoran Qiu (UIUC), Weichao Mao (UIUC), Chen Wang (IBM Research), Saurabh Jha (IBM Research), Hubertus Franke (IBM Research), Chandra Narayanaswami (IBM Research), Zbigniew Kalbarczyk (UIUC), Tamer Başar (UIUC), and Ravishankar Iyer (UIUC)

Neural Fault Injection: Generating Software Faults from Natural Language 23
Domenico Cotroneo (University of Naples Federico II, Italy) and Pietro Liguori (University of Naples Federico II, Italy)

PANDA: Practical Adversarial Attack Against Network Intrusion Detection 28
Subrat Kumar Swain (UQ-IITD Research Academy), Vireshwar Kumar (Indian Institute of Technology Delhi), Guangdong Bai (The University of Queensland), and Dan Dongseong Kim (The University of Queensland)

Harnessing Explainability to Improve ML Ensemble Resilience 33
Abraham Chan (The University of British Columbia, Canada), Arpan Gujarati (The University of British Columbia, Canada), Karthik Pattabiraman (The University of British Columbia, Canada), and Sathish Gopalakrishnan (The University of British Columbia, Canada)

On the Design of Coordination Services for IoT 38
Tiago Carvalho (Universidade de Lisboa, Portugal), Antonio Casimiro (Universidade de Lisboa, Portugal), and Alysson Bessani (Universidade de Lisboa, Portugal)

Doctoral Forum

Patching the Cracks: Detecting and Addressing Adversarial Examples in Real-World Applications 43
Niklas Bunzel (Fraunhofer SIT/ATHENE/TU-Darmstadt, Germany)

Reducing the gap between theory and Practice in Real-Time Systems with MARS 47
Giann Spilere Nandi (CISTER, Polytechnic Institute of Porto, Portugal), David Pereira (CISTER, Polytechnic Institute of Porto, Portugal), José Proença (CISTER, Polytechnic Institute of Porto, Portugal), Eduardo Tovar (CISTER, Polytechnic Institute of Porto, Portugal), and Luís Nogueira (CISTER, Polytechnic Institute of Porto, Portugal)

MTD in Plain Sight: Hiding Network Behavior in Moving Target Defenses 50
Tina Moghaddam (The University of Queensland, Australia), Guowei Yang (The University of Queensland, Australia), Chandra Thapa (CSIRO Data61, Australia), Seyit Camtepe (CSIRO Data61, Australia), and Dan Dongseong Kim (The University of Queensland, Australia)

Advancing NDN Security for IoT: Harnessing Machine Learning to Detect Attacks 53
Sai Gautam Mandapati (School of Information Technology), Chathurika Ranaweera (School of Information Technology), and Robin Doss (Deakin University, Australia)

Novel CAN Bus Fuzzing Framework for Finding Vulnerabilities in Automotive Systems 56
Manu Jo Varghese (Deakin University, Australia), Adnan Anwar (Deakin University, Australia), Frank Jiang (Deakin University, Australia), and Robin Doss (Deakin University, Australia)

Secure Data Provenance in Internet of Vehicles with Verifiable Credentials for Security and Privacy 59
Anuj Nepal (Deakin University, Australia), Robin Doss (Deakin University, Australia), and Frank Jiang (Deakin University, Australia)

(Re)-Envisioning Approximate Agreement for Distributed Cryptography and Oracles 62
Akhil Bandarupalli (Purdue University), Saurabh Bagchi (Purdue University), and Aniket Kate (Purdue University and Supra Research)

Tutorial

Tutorial: Safe, Secure, and Trustworthy Artificial Intelligence (AI) via Formal Verification of Neural Networks and Autonomous Cyber-Physical Systems (CPS) with NNV 65
Taylor T. Johnson (Vanderbilt University, TN), Diego Manzanas Lopez (Vanderbilt University, TN), and Hoang-Dung Tran (University of Nebraska Lincoln, NE)

Zero-Knowledge Proofs for Blockchains 67
Sushmita Ruj (University of New South Wales, Australia)

Evaluating Performance and Dependability of Blockchain Protocols with Diablo 69
Andrei Lebedev (University of Sydney, Australia) and Vincent Gramoli (University of Sydney and Redbelly Network, Australia)

Tutorial: LLTFI and the Art of Fault Injection 71
Karthik Pattabiraman (The University of British Columbia (UBC), Canada) and Abraham Chan (The University of British Columbia (UBC), Canada)

Industry

Intrusion Detection at Scale with the Assistance of a Command-line Language Model 73
Jiongliang Lin (Sun Yat-sen University, China), Yiwen Guo (Unaffliated, China), and Hao Chen (UC Davis, USA)

Bridging the Gap: A Study of AI-Based Vulnerability Management between Industry and Academia 80
Shengye Wan (Meta Platforms, Inc.), Joshua Saxe (Meta Platforms, Inc.), Craig Gomes (Meta Platforms, Inc.), Sahana Chennabasappa (Meta Platforms, Inc.), Avilash Rath (The University of Texas at Dallas), Kun Sun (George Mason University), and Xinda Wang (The University of Texas at Dallas)

Investigating Memory Failure Prediction Across CPU Architectures 88
Qiao Yu (Huawei Munich Research Center, Germany; Technical University of Berlin, Germany), Wengui Zhang (Huawei Technologies Co., Ltd, China), Min Zhou (Huawei Technologies Co., Ltd, China), Jialiang Yu (Huawei Technologies Co., Ltd, China), Zhenli Sheng (Huawei Technologies Co., Ltd, China), Jasmin Bogatinovski (Technical University of Berlin, Germany), Jorge Cardoso (Huawei Munich Research Center, Germany; University of Coimbra, Portugal), and Odej Kao (Technical University of Berlin, Germany)

Federated Unlearning in the Internet of Vehicles 96
Guofeng Li (Southeast University, China), Xia Feng (Hainan University, China), Liangmin Wang (Southeast University, China), Haiqin Wu (East China Normal University, China), and Boris Düdder (University of Copenhagen, Denmark)

Zone-Hopping: Sensitive Information Leakage Prevention for DNSSEC-NSEC 104
Fatema Bannat Wala (ESnet, Lawrence Berkeley National Lab, USA) and Stephan Bohacek (University of Delaware, USA)

Optimizing Large-Scale Fault Injection Experiments through Martingale Hypothesis: A Systematic Approach for Reliability Assessment of Safety-Critical Systems 111
Saurabh Hukerikar (NVIDIA, USA), Atieh Lotfi (NVIDIA, USA), Yanxiang Huang (NVIDIA, USA), Jason Campbell (NVIDIA, USA), and Nirmal Saxena (NVIDIA, USA)

Active Learning Omnivariate Decision Trees for Fault Diagnosis in Robotic Systems 118
Casidhe Hutchison (Carnegie Mellon University), Milda Zizyte (Carnegie Mellon University), David Guttendorf (Carnegie Mellon University), Claire Le Goues (Carnegie Mellon University), and Philip Koopman (Carnegie Mellon University)

Empowering Data Centers with Computational Storage Drive-Based Deep Learning Inference Functionality to Combat Ransomware 125
Kurt Friday (Louisiana State University), Elias Bou-Harb (Louisiana State University), Ron Lee (Samsung Memory Solutions Lab), Pramod Peethambaran (Samsung Memory Solutions Lab), and Mayank Saxena (Samsung Memory Solutions Lab)

Road Decals as Trojans: Disrupting Autonomous Vehicle Navigation with Adversarial Patterns..... 133
Wei-Jia Chen (NYCU), Chia-Yi Hsu (NYCU), Wei-Bin Lee (Hon Hai (Foxconn) Research Institute), Chia-Mu Yu (NYCU), and Chun-Ying Huang (NYCU)

Fault Localization Using Interventional Causal Learning for Cloud-Native Applications 141
Saurabh Jha (IBM Research), Jesus Rios (IBM Research), Naoki Abe (IBM Research), Frank Bagehorn (IBM Research), and Laura Shwartz (IBM Research)

Poster

Federated Anomaly Detection 148
Chunjiong Zhang (Ajou University, Korea), Byeong-hee Roh (Ajou University, Korea), and Gaoyang Shan (Ajou University, Korea)

Mitigating False Positives in DGA Detection for Non-English Domain Names 150
Huiju Lee (Korea University, Republic of Korea) and Huy Kang Kim (Korea University, Republic of Korea)

Cryptography-Based Bootstrapping Scheme for Permissionless Sharding Blockchain 152
Ziqiang Xu (La Trobe University, Australia), Ahmad Salehi S. (La Trobe University, Australia), and Naveen Chilamkurti (La Trobe University, Australia)

Poster: Optimizing Tree-Based Quorum Certification for BFT Systems at Planetary-Scale 154
Christian Berger (University of Passau, Germany) and Hans P. Reiser (Reykjavík University, Iceland)

Boosting Communication Efficiency of Federated Learning's Secure Aggregation 157
Niousha Nazemi (The University of Sydney, Australia), Omid Tavallaie (The University of Sydney, Australia), Shuaijun Chen (The University of Sydney, Australia), Albert Y. Zomaya (The University of Sydney, Australia), and Ralph Holz (The University of Sydney, Australia; University of Münster, Germany)

Balancing Privacy and Attack Utility: Calibrating Sample Difficulty for Membership Inference Attacks in Transfer Learning 159
Shuwen Liu (China University of Geosciences), Yongfeng Qian (China University of Geosciences), and Yixue Hao (Huazhong University of Science and Technology)

Synergizing GCN and GAT for Hardware Trojan Detection and Localization 161
Yu-Chen Hsiao (National Yang Ming Chiao Tung University, Taiwan), Chia-Heng Yen (National Yang Ming Chiao Tung University, Taiwan), Bo-Yang Ke (National Yang Ming Chiao Tung University, Taiwan), and Kai-Chiang Wu (National Yang Ming Chiao Tung University, Taiwan)

Author Index **163**