

2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2023)

**Porto, Portugal
27 – 30 June 2023**



**IEEE Catalog Number: CFP23048-POD
ISBN: 979-8-3503-4794-4**

**Copyright © 2023 by the Institute of Electrical and Electronics Engineers, Inc.
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:	CFP23048-POD
ISBN (Print-On-Demand):	979-8-3503-4794-4
ISBN (Online):	979-8-3503-4793-7
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

CURRAN ASSOCIATES INC.
proceedings
.com

2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) **DSN 2023**

Table of Contents

Welcome Message from the DSN 2023 General Chairs	xiii
Message from the DSN 2023 Program Chairs	xv
DSN 2023 Organizing Committee	xvii
DSN 2023 Steering Committee	xix
DSN 2023 Research Track Program Committee	xx
William C. Carter Award	xxiii
Rising Star in Dependability Award	xxv
Test of Time Award	xxvii
Jean-Claude Laprie Award	xxviii
Keynotes	xxx

RT-1: Best Paper Candidates

SHATTER: Control and Defense-Aware Attack Analytics for Activity-Driven Smart Home Systems... 1 <i>Nur Imtiazul Haque (Florida International University, USA), Maurice Ngouen (Florida International University, USA), Mohammad Ashiqur Rahman (Florida International University, USA), Selcuk Uluagac (Florida International University, USA), and Laurent Njilla (US Air Force Research Laboratory (AFRL), USA)</i>	
SecDDR: Enabling Low-Cost Secure Memories by Protecting the DDR Interface	14
<i>Ali Fakhrzadehgan (The University of Texas at Austin), Prakash Ramrakhyani (Arm), Moinuddin K. Qureshi (Georgia Tech), and Mattan Erez (The University of Texas at Austin)</i>	
Devils in Your Apps: Vulnerabilities and User Privacy Exposure in Mobile Notification Systems	28
<i>Jiadong Lou (University of Louisiana at Lafayette, USA), Xiaohan Zhang (Xidian University, China), Yihe Zhang (University of Louisiana at Lafayette, USA), Xinghua Li (Xidian University, China), Xu Yuan (University of Louisiana at Lafayette, USA), and Ning Zhang (Washington University in St. Louis, USA)</i>	

RT-2: Vehicles

Breaking Geographic Routing Among Connected Vehicles	42
<i>Zizheng Liu (Purdue University, USA), Shaan Shekhar (Purdue University, USA), and Chunyi Peng (Purdue University, USA)</i>	
NPTSN: RL-Based Network Planning with Guaranteed Reliability for In-Vehicle TSSDN	55
<i>Weijiang Kong (Eindhoven University of Technology, the Netherlands), Majid Nabi (Eindhoven University of Technology, the Netherlands), and Kees Goossens (Eindhoven University of Technology, the Netherlands)</i>	
Get Your Cyber-Physical Tests Done! Data-Driven Vulnerability Assessment of Robotic Aerial Vehicles	67
<i>Aolin Ding (Accenture Labs), Matthew Chan (Rutgers University), Amin Hass (Accenture Labs), Nils Ole Tippenhauer (CISPA Helmholtz Center for Information Security), Shiqing Ma (Rutgers University), and Saman Zonouz (Georgia Tech)</i>	

RT-3: Memory 1

Compiler-Implemented Differential Checksums: Effective Detection and Correction of Transient and Permanent Memory Errors	81
<i>Christoph Borchert (Osnabrück University, Germany), Horst Schirmeier (TU Dresden, Germany), and Olaf Spinczyk (Osnabrück University, Germany)</i>	
PT-Guard: Integrity-Protected Page Tables to Defend Against Breakthrough Rowhammer Attacks... 95	
<i>Anish Saxena (Georgia Institute of Technology), Gururaj Saileshwar (NVIDIA and University of Toronto), Jonas Juffinger (Graz University of Technology), Andreas Kogler (Graz University of Technology), Daniel Gruss (Graz University of Technology), and Moinuddin Qureshi (Georgia Institute of Technology)</i>	
Don't Knock! Rowhammer at the Backdoor of DNN Models	109
<i>M. Caner Tol (Worcester Polytechnic Institute, USA), Saad Islam (Worcester Polytechnic Institute, USA), Andrew J. Adiletta (Worcester Polytechnic Institute, USA), Berk Sunar (Worcester Polytechnic Institute, USA), and Ziming Zhang (Worcester Polytechnic Institute, USA)</i>	

RT-4: Blockchain & Replication

Micro Replication	123
<i>Tobias Distler (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Michael Eischer (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), and Laura Lawniczak (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)</i>	
Heron: Scalable State Machine Replication on Shared Memory	138
<i>Mojtaba Eslahi-Kelorazi (Universita della Svizzera italiana, Switzerland), Long Hoang Le (Universita della Svizzera italiana, Switzerland), and Fernando Pedone (Universita della Svizzera italiana, Switzerland)</i>	

Analyzing the Performance of the Inter-Blockchain Communication Protocol	151
<i>João Otávio Chervinski (Monash University, Australia; CSIRO's Data61, Australia), Diego Kreutz (Monash University, Australia; Federal University of Pampa, Brazil), Xiwei Xu (CSIRO's Data61, Australia), and Jiangshan Yu (Monash University, Australia)</i>	

RT-5: Software Security

MalAder: Decision-Based Black-Box Attack Against API Sequence Based Malware Detectors	165
<i>Xiaohui Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Lei Cui (Zhongguancun Laboratory, P.R. China), Hui Wen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhi Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Hongsong Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhiyu Hao (Zhongguancun Laboratory, P.R. China), and Limin Sun (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
Tabby: Automated Gadget Chain Detection for Java Deserialization Vulnerabilities	179
<i>Xingchen Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Baizhu Wang (MYbank AntGroup, China), Ze Jin (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yun Feng (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xianglong Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xincheng Feng (FG Security Lab AntGroup, China), and Qixu Liu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
TagClass: A Tool for Extracting Class-Determined Tags from Massive Malware Labels via Incremental Parsing	193
<i>Yongkang Jiang (Shanghai Jiao Tong University, China), Gaolei Li (Shanghai Jiao Tong University, China), and Shenghong Li (Shanghai Jiao Tong University, China)</i>	

RT-6: Memory 2

Āpta: Fault-Tolerant Object-Granular CXL Disaggregated Memory for Accelerating FaaS	201
<i>Adarsh Patil (University of Edinburgh), Vijay Nagarajan (University of Edinburgh), Nikos Nikoleris (Arm), and Nicolai Oswald (University of Edinburgh)</i>	

HiMFP: Hierarchical Intelligent Memory Failure Prediction for Cloud Service Reliability	216
<i>Qiao Yu (Huawei Munich Research Center, Germany; Technical University of Berlin, Germany), Wengui Zhang (Huawei Technologies Co., Ltd, China), Paolo Notaro (Huawei Munich Research Center, Germany; Technical University of Munich, Germany), Soroush Haeri (Huawei Munich Research Center, Germany), Jorge Cardoso (Huawei Munich Research Center, Germany; University of Coimbra, Portugal), and Odej Kao (Technical University of Berlin, Germany)</i>	
SGX Switchless Calls Made Configless	229
<i>Peterson Yuhala (University of Neuchâtel, Switzerland), Michael Paper (ENS de Lyon, France), Timothée Zerbib (Institut Polytechnique de Paris, France), Pascal Felber (University of Neuchâtel, Switzerland), Valerio Schiavoni (University of Neuchâtel, Switzerland), and Alain Tchana (Grenoble INP, France)</i>	

RT-7: Network Security & Privacy

Poisoning Online Learning Filters by Shifting on the Move	239
<i>Wesley Joon-Wie Tann (National University of Singapore, Singapore) and Ee-Chien Chang (National University of Singapore, Singapore)</i>	
YODA: Covert Communication Channel over Public DNS Resolvers	252
<i>Sandip Saha (IIT Madras), Sareena Karapoola (IIT Madras), Chester Rebeiro (IIT Madras), and Kamakoti V (IIT Madras)</i>	
Targeted Privacy Attacks by Fingerprinting Mobile Apps in LTE Radio Layer	261
<i>Jaejong Baek (Arizona State University, USA), Pradeep Kumar Duraisamy Soundrapandian (Vellore Institute of Technology, India), Sukwha Kyung (Arizona State University, USA), Ruoyu Wang (Arizona State University, USA), Yan Shoshitaishvili (Arizona State University, USA), Adam Doupe (Arizona State University, USA), and Gail-Joon Ahn (Arizona State University, USA)</i>	

RT-8: Machine Learning

Fabricated Flips: Poisoning Federated Learning without Data	274
<i>Jiyue Huang (TU Delft, The Netherlands), Zilong Zhao (TU Delft, The Netherlands), Lydia Y. Chen (TU Delft, The Netherlands), and Stefanie Roos (TU Delft, The Netherlands)</i>	
Fortifying Federated Learning against Membership Inference Attacks via Client-Level Input Perturbation	288
<i>Yuchen Yang (Johns Hopkins University), Haolin Yuan (Johns Hopkins University), Bo Hui (Johns Hopkins University), Neil Gong (Duke University), Neil Fendley (Johns Hopkins University; Johns Hopkins Applied Physics Lab), Philippe Burlina (Johns Hopkins Applied Physics Lab), and Yinzhi Cao (Johns Hopkins University)</i>	

ReFace: Adversarial Transformation Networks for Real-Time Attacks on Face Recognition Systems	302
<i>Shehzeen Hussain (University of California San Diego), Todd Huster (Peraton Labs), Chris Mesterharm (Peraton Labs), Paarth Neekhara (University of California San Diego), and Farinaz Koushanfar (University of California San Diego)</i>	

RT-9: Obfuscation

No Free Lunch: On the Increased Code Reuse Attack Surface of Obfuscated Programs	313
<i>Naiqian Zhang (University of New Hampshire), Daroc Alden (University of New Hampshire), Dongpeng Xu (University of New Hampshire), Shuai Wang (Hong Kong University of Science and Technology), Trent Jaeger (The Pennsylvania State University), and Wheeler Ruml (University of New Hampshire)</i>	
TransAST: A Machine Translation-Based Approach for Obfuscated Malicious JavaScript Detection	327
<i>Yan Qin (Central South University, China), Weiping Wang (Central South University, China), Zixian Chen (Central South University, China), Hong Song (Central South University, China), and Shigeng Zhang (Central South University, China)</i>	
JSRevealer: A Robust Malicious JavaScript Detector against Obfuscation	339
<i>Kunlun Ren (Huazhong University of Science and Technology, China), Weizhong Qiang (Huazhong University of Science and Technology, China; Jinyinhu Laboratory, China), Yueming Wu (Nanyang Technological University, Singapore), Yi Zhou (Huazhong University of Science and Technology, China), Deqing Zou (Huazhong University of Science and Technology, China; Jinyinhu Laboratory, China), and Jin Hai (Huazhong University of Science and Technology, China; Jinyinhu Laboratory, China)</i>	

RT-10: Cyberphysical Systems

Detection of e-Mobility-based Attacks on the Power Grid	352
<i>Dustin Kern (Darmstadt University of Applied Sciences, Germany) and Christoph Krauß (Darmstadt University of Applied Sciences, Germany)</i>	
SwarmFuzz: Discovering GPS Spoofing Attacks in Drone Swarms	366
<i>Yingao Yao (The University of British Columbia), Pritam Dash (The University of British Columbia), and Karthik Pattabiraman (The University of British Columbia)</i>	
DNAttest: Digital-Twin-based Non-Intrusive Attestation under Transient Uncertainty	376
<i>Wei Lin (Singapore University of Technology and Design, Singapore), Heng Chuan Tan (Advanced Digital Sciences Center, Singapore), Binbin Chen (Singapore University of Technology and Design, Singapore), and Fan Zhang (Zhejiang University, China)</i>	

RT-11: Virtualization

IRIS: a Record and Replay Framework to Enable Hardware-Assisted Virtualization Fuzzing	389
<i>Carmine Cesarano (Università degli Studi di Napoli Federico II, Italy), Marcello Cinque (Università degli Studi di Napoli Federico II, Italy), Domenico Cotroneo (Università degli Studi di Napoli Federico II, Italy), Luigi De Simone (Università degli Studi di Napoli Federico II, Italy), and Giorgio Farina (Università degli Studi di Napoli Federico II, Italy)</i>	
Rewind & Discard: Improving Software Resilience using Isolated Domains	402
<i>Merve Gülmez (Ericsson Security Research, KU Leuven), Thomas Nyman (Ericsson Product Security), Christoph Baumann (Ericsson Research), and Jan Tobias Mühlberg (imec-DistriNet, KU Leuven; Université Libre de Bruxelles)</i>	
Intrusion Injection for Virtualized Systems: Concepts and Approach	417
<i>Charles F. Gonçalves (University of Coimbra, Portugal; Board of Information Technology, Brazil), Nuno Antunes (University of Coimbra, Portugal), and Marco Vieira (University of Coimbra, Portugal)</i>	

RT-12: Web Security

vWitness: Certifying Web Page Interactions with Computer Vision	431
<i>He Shuang (University of Toronto), Lianying Zhao (Carleton University), and David Lie (University of Toronto)</i>	
Adaptive Webpage Fingerprinting from TLS Traces	445
<i>Vasilios Mavroudis (Alan Turing Institute) and Jamie Hayes (University College London)</i>	
IDTracker: Discovering Illicit Website Communities via Third-Party Service IDs	459
<i>Chenxu Wang (Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences), Zhao Li (Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences), Jiangyi Yin (Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences), Zhenni Liu (Chinese Academy of Sciences, National Engineering Research Center of Information Security; University of Chinese Academy of Sciences), Zhongyi Zhang (Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences), and Qingyun Liu (Chinese Academy of Sciences; National Engineering Research Center of Information Security)</i>	

RT-13: Mobile Systems & IoT

Creating a Large-Scale Memory Error IoT Botnet Using NS3DockerEmulator	470
<i>Islam Obaidat (UNC Charlotte, Charlotte, USA), Bennett Kahn (Tulane University, USA), Fatemeh Tavakoli (UNC Charlotte, USA), and Meera Sridhar (UNC Charlotte, USA)</i>	

DARPA: Combating Asymmetric Dark UI Patterns on Android with Run-Time View Decorator ...	480
<i>Zhaoxin Cai (Sun Yat-sen University, China), Yuhong Nan (Sun Yat-sen University, China), Xueqiang Wang (University of Central Florida, USA), Mengyi Long (Sun Yat-sen University, China), Qihua Ou (Sun Yat-sen University, China), Min Yang (Fudan University, China), and Zibin Zheng (Sun Yat-sen University, China)</i>	
IoT Anomaly Detection Via Device Interaction Graph	494
<i>Jincheng Wang (The Chinese University of Hong Kong, China), Zhuohua Li (The Chinese University of Hong Kong, China), Mingshen Sun (Independent Researcher, USA), Bin Yuan (Huazhong University of Science and Technology, China), and John C.S. Lui (The Chinese University of Hong Kong, China)</i>	

RT-14: Potpourri

Time Machine: Generative Real-Time Model For Failure (and Lead Time) Prediction in HPC Systems	508
<i>Khalid Ayed Alharthi (University of Warwick, UK; University of Bisha, KSA; The Alan Turing Institute, UK), Arshad Jhumka (University of Warwick, UK), Sheng Di (The University of Chicago, USA), Lin Gui (King's College London), Franck Cappello (The University of Chicago, USA; University of Illinois at Urbana-Champaign, USA), and Simon McIntosh-Smith (Bristol University, UK)</i>	
How Different are The Cloud Workloads? Characterizing Large-Scale Private and Public Cloud Workloads	522
<i>Xiaoting Qin (Microsoft), Minghua Ma (Microsoft), Yuheng Zhao (Microsoft), Jue Zhang (Microsoft), Chao Du (Microsoft), Yudong Liu (Microsoft), Anjaly Parayil (Microsoft), Chetan Bansal (Microsoft), Saravan Rajmohan (Microsoft), Íñigo Goiri (Microsoft), Eli Cortez (Microsoft), Si Qin (Microsoft), Qingwei Lin (Microsoft), and Dongmei Zhang (Microsoft)</i>	
On Adversarial Robustness of Point Cloud Semantic Segmentation	531
<i>Jiacen Xu (University of California, Irvine), Zhe Zhou (Fudan University), Boyuan Feng (University of California, Santa Barbara), Yufei Ding (University of California, Santa Barbara), and Zhou Li (University of California, Irvine)</i>	

RT-15: System Analysis & Modelling

Cost-Damage Analysis of Attack Trees	545
<i>Milan Lopuhaä-Zwakenberg (University of Twente) and Mariëlle Stoelinga (University of Twente; Radboud University)</i>	
PASTA: Pragmatic Automated System-Theoretic Process Analysis	559
<i>Jette Petzold (Kiel University, Germany), Jana Kreiß (Kiel University, Germany), and Reinhard von Hanxleden (Kiel University, Germany)</i>	

Practical Asynchronous Distributed Key Generation: Improved Efficiency, Weaker Assumption, and Standard Model	568
<i>Haibin Zhang (Beijing Institute of Technology), Sisi Duan (Tsinghua University; Zhongguancun Laboratory), Chao Liu (Shandong University), Boxin Zhao (Zhongguancun Laboratory), Xuanji Meng (Tsinghua University), Shengli Liu (Shanghai Jiao Tong University), Yong Yu (Shaanxi Normal University), Fangguo Zhang (Sun Yat-sen University), and Liehuang Zhu (Beijing Institute of Technology)</i>	

RT-16: Smart Home

VoiceGuard: An Effective and Practical Approach for Detecting and Blocking Unauthorized Voice Commands to Smart Speakers	582
<i>Xuening Xu (Stevens Institute of Technology, USA), Chenglong Fu (UNC Charlotte, USA), Xiaojiang Du (Stevens Institute of Technology, USA), and E. Paul Ratazzi (Air Force Research Laboratory, USA)</i>	
Speaker Orientation-Aware Privacy Control to Thwart Misactivation of Voice Assistants	597
<i>Shaohu Zhang (North Carolina State University, USA), Aafaq Sabir (North Carolina State University, USA), and Anupam Das (North Carolina State University, USA)</i>	

Author Index	611
---------------------------	------------