

# **2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2019)**

**Portland, Oregon, USA  
24 – 27 June 2019**



**IEEE Catalog Number: CFP19048-POD  
ISBN: 978-1-7281-0058-6**

**Copyright © 2019 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:	CFP19048-POD
ISBN (Print-On-Demand):	978-1-7281-0058-6
ISBN (Online):	978-1-7281-0057-9
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) **DSN 2019**

## Table of Contents

Message from the General Chair .xiii.....	
Message from the Research Track Chairs .xiv.....	
Steering Committee .xvi.....	
Organizing Committee .xvii.....	
Research Track Program Committee .xviii.....	
Best Paper Award .xx.....	
William C. Carter Award .xxi.....	
The Jean-Claude Laprie Award .xxii.....	
Test-of-Time Award .xxiii.....	
Keynotes .xxiv.....	
Sponsors .xxviii.....	

## Best Paper Award Candidates

GreenFlag: Protecting 3D-Racetrack Memory from Shift Errors .1.....	
<i>Georgios Mappouras (Duke University), Alireza Vahid (University of Colorado Denver), Robert Calderbank (Duke University), and Daniel J. Sorin (Duke University)</i>	
Understanding and Modeling On-Die Error Correction in Modern DRAM: An Experimental Study Using Real Devices .13.....	
<i>Minesh Patel (ETH Zürich), Jeremie S. Kim (Carnegie Mellon University; ETH Zürich), Hasan Hassan (ETH Zürich), and Onur Mutlu (ETH Zürich; Carnegie Mellon University)</i>	
Demystifying Soft Error Assessment Strategies on ARM CPUs: Microarchitectural Fault Injection vs. Neutron Beam Experiments .26.....	
<i>Athanasios Chatzidimitriou (University of Athens), Pablo Bodmann (Federal University of Rio Grande do Sul), George Papadimitriou (University of Athens), Dimitris Gizopoulos (University of Athens), and Paolo Rech (Federal University of Rio Grande do Sul)</i>	

## Session 1 – Machine Learning Security

- A Multiversion Programming Inspired Approach to Detecting Audio Adversarial Examples .39.....  
*Qiang Zeng (University of South Carolina), Jianhai Su (University of South Carolina), Chenglong Fu (Temple University), Golam Kayas (Temple University), Lannan Luo (University of South Carolina), Xiaojiang Du (Temple University), Chiu C. Tan (Temple University), and Jie Wu (Temple University)*
- Classifying Malware Represented as Control Flow Graphs using Deep Graph Convolutional Neural Network .52.....  
*Jiaqi Yan (Illinois Institute of Technology), Guanhua Yan (Binghamton University, State University of New York), and Dong Jin (Illinois Institute of Technology)*
- ZK-GanDef: A GAN Based Zero Knowledge Adversarial Training Defense for Neural Networks .64.....  
*Guanxiong Liu (New Jersey Institute of Technology), Issa Khalil (QCRI, Hamad bin Khalifa University), and Abdallah Khreishah (New Jersey Institute of Technology)*

## Session 2 – Modeling

- Efficient Treatment of Uncertainty in System Reliability Analysis using Importance Measures .76.....  
*Hananeh Aliee (Helmholtz Zentrum München), Faramarz Khosravi (Friedrich-Alexander-Universität Erlangen-Nürnberg), and Jürgen Teich (Friedrich-Alexander-Universität Erlangen-Nürnberg)*
- Extensions of Network Reliability Analysis .88.....  
*Hoang Hai Nguyen (University of Illinois at Urbana-Champaign), Kartik Palani (University of Illinois at Urbana-Champaign), and David M. Nicol (University of Illinois at Urbana-Champaign)*
- An Online Approach to Estimate Parameters of Phase-Type Distributions .100.....  
*Peter Buchholz (TU Dortmund), Iryna Dohndorf (TU Dortmund), and Jan Kriege (TU Dortmund)*

## Session 3 – Machine Learning Reliability

- ML-Based Fault Injection for Autonomous Vehicles: A Case for Bayesian Fault Injection .112.....  
*Saurabh Jha (University of Illinois at Urbana-Champaign), Subho Banerjee (University of Illinois at Urbana-Champaign), Timothy Tsai (NVIDIA Corporation), Siva K. S. Hari (NVIDIA Corporation), Michael B. Sullivan (NVIDIA Corporation), Zbigniew T. Kalbarczyk (University of Illinois at Urbana-Champaign), Stephen W. Keckler (NVIDIA Corporation), and Ravishankar K. Iyer (University of Illinois at Urbana-Champaign)*
- Deep Validation: Toward Detecting Real-World Corner Cases for Deep Neural Networks .125.....  
*Weibin Wu (The Chinese University of Hong Kong), Hui Xu (The Chinese University of Hong Kong), Sanqiang Zhong (The Chinese University of Hong Kong), Michael R. Lyu (The Chinese University of Hong Kong), and Irwin King (The Chinese University of Hong Kong)*

SOTER: A Runtime Assurance Framework for Programming Safe Robotics Systems .138.....  
*Ankush Desai (University of California, Berkeley), Shromona Ghosh (University of California, Berkeley), Sanjit A. Seshia (University of California, Berkeley), Natarajan Shankar (SRI International), and Ashish Tiwari (SRI International and Microsoft)*

## Session 4 – Transactions and Concurrency

OneFile: A Wait-Free Persistent Transactional Memory .151.....  
*Pedro Ramalhete (Cisco Systems), Andreia Correia (University of Neuchatel), Pascal Felber (University of Neuchatel), and Nachshon Cohen (EPFL)*

Sparkle: Speculative Deterministic Concurrency Control for Partially Replicated Transactional Stores .164.....  
*Zhongmiao Li (Universite catholique de Louvain and Instituto Superior Tecnico, Lisbon University & INESC-ID), Paolo Romano (Instituto Superior Tecnico, Lisbon University & INESC-ID), and Peter Van Roy (Universite catholique de Louvain)*

White-Box Atomic Multicast .176.....  
*Alexey Gotsman (IMDEA Software Institute), Anatole Lefort (Télécom SudParis), and Gregory Chockler (Royal Holloway, University of London)*

## Session 5 – Hardware Reliability

Fault Tolerance Through Redundant Execution on COTS Multicores: Exploring Trade-Offs .188.....  
*Yanyan Shen (UNSW Sydney and Data61, CSIRO, Australia), Gernot Heiser (UNSW Sydney and Data61, CSIRO, Australia), and Kevin Elphinstone (UNSW Sydney and Data61, CSIRO, Australia)*

ParaMedic: Heterogeneous Parallel Error Correction .201.....  
*Sam Ainsworth (University of Cambridge) and Timothy M. Jones (University of Cambridge)*

gem5-Approxilyzer: An Open-Source Tool for Application-Level Soft Error Analysis .214.....  
*Radha Venkatagiri (University of Illinois at Urbana-Champaign), Khaliq Ahmed (University of Illinois at Urbana-Champaign), Abdulrahman Mahmoud (University of Illinois at Urbana-Champaign), Sasa Misailovic (University of Illinois at Urbana-Champaign), Darko Marinov (University of Illinois at Urbana-Champaign), Christopher W. Fletcher (University of Illinois at Urbana-Champaign), and Sarita V. Adve (University of Illinois at Urbana-Champaign)*

## Session 6 – IoT Security

- Your IoTs Are (Not) Mine: On the Remote Binding Between IoT Devices and Users .222.....  
*Jiongyi Chen (The Chinese University of Hong Kong), Chaoshun Zuo (The Ohio State University), Wenrui Diao (Jinan University), Shuaike Dong (The Chinese University of Hong Kong), Qingchuan Zhao (The Ohio State University), Menghan Sun (The Chinese University of Hong Kong), Zhiqiang Lin (The Ohio State University), Yinqian Zhang (The Ohio State University), and Kehuan Zhang (The Chinese University of Hong Kong)*
- BenchIoT: A Security Benchmark for the Internet of Things .234.....  
*Naif Saleh Almakhdhub (Purdue University and King Saud University), Abraham A. Clements (Purdue University and Sandia National Laboratories), Mathias Payer (EPFL), and Saurabh Bagchi (Purdue University)*
- Exploiting Memory Corruption Vulnerabilities in Connman for IoT Devices .247.....  
*K. Virgil English (UNC Charlotte), Islam Obaidat (UNC Charlotte), and Meera Sridhar (UNC Charlotte)*

## Session 7 – Network Reliability

- Rigorous, Effortless and Timely Assessment of Cellular Network Changes .256.....  
*Ajay Mahimkar (AT&T), Zihui Ge (AT&T), Sanjeev Ahuja (AT&T), Shomik Pathak (AT&T), and Nauman Shafi (AT&T)*
- An Eventually Perfect Failure Detector for Networks of Arbitrary Topology Connected with ADD Channels Using Time-To-Live Values .264.....  
*Karla Vargas (Universidad Nacional Autónoma de México) and Sergio Rajsbaum (Universidad Nacional Autónoma de México)*
- Bonsai: Efficient Fast Failover Routing Using Small Arborescences .276.....  
*Klaus-Tycho Foerster (Faculty of Computer Science, University of Vienna, Austria), Andrzej Kamisinski (AGH University of Science and Technology, Poland), Yvonne-Anne Pignolet (DFINITY, Switzerland), Stefan Schmid (Faculty of Computer Science, University of Vienna, Austria), and Gilles Tredan (LAAS-CNRS, France)*

## Session 8 – Hardware Security

- SATIN: A Secure and Trustworthy Asynchronous Introspection on Multi-Core ARM Processors .289.  
*Shengye Wan (College of William and Mary), Jianhua Sun (College of William and Mary), Kun Sun (George Mason University), Ning Zhang (Washington University), and Qi Li (Tsinghua University)*
- DeviceVeil: Robust Authentication for Individual USB Devices Using Physical Unclonable Functions .302.....  
*Kuniyasu Suzuki (National Institute of Advanced Industrial Science and Technology), Yohei Hori (National Institute of Advanced Industrial Science and Technology), Kazukuni Kobara (National Institute of Advanced Industrial Science and Technology), and Mohammad Mannan (National Institute of Advanced Industrial Science and Technology)*

Multilayer ROP Protection Via Microarchitectural Units Available in Commodity Hardware .315.....  
*Mateus Tymburibá (CEFET-MG), Hugo Sousa (UFMG), and Fernando Pereira (UFMG)*

## Session 9 – IoT and SCADA Reliability

Deploying Intrusion-Tolerant SCADA for the Power Grid .328.....  
*Amy Babay (Spread Concepts LLC, Johns Hopkins University), John Schultz (Spread Concepts LLC), Thomas Tantillo (Johns Hopkins University), Samuel Beckley (Johns Hopkins University), Eamon Jordan (Resurgo LLC), Kevin Ruddell (Resurgo LLC), Kevin Jordan (Resurgo LLC), and Yair Amir (Johns Hopkins University, Spread Concepts LLC)*

Reaching Data Confidentiality and Model Accountability on the CalTrain .336.....  
*Zhongshu Gu (IBM Research), Hani Jamjoom (IBM Research), Dong Su (IBM Research), Heqing Huang (Bytedance), Jialong Zhang (Bytedance), Tengfei Ma (IBM Research), Dimitrios Pendarakis (IBM Cognitive Systems), and Ian Molloy (IBM Research)*

Tell Me More Than Just Assembly! Reversing Cyber-Physical Execution Semantics of Embedded IoT Controller Software Binaries .349.....  
*Pengfei Sun (Rutgers University), Luis Garcia (University of California, Los Angeles), and Saman Zonouz (Rutgers University)*

## Session 10 – Memory Systems Reliability

Exploiting Latency and Error Tolerance of GPGPU Applications for an Energy-Efficient DRAM .362...  
*Haonan Wang (College of William & Mary) and Adwait Jog (College of William & Mary)*

Leveraging Transverse Reads to Correct Alignment Faults in Domain Wall Memories .375.....  
*Sébastien Ollivier (University of Pittsburgh), Donald Kline, Jr. (University of Pittsburgh), Roxy Kawsher (University of South Florida), Rami Melhem (University of Pittsburgh), Sanjukta Banja (University of South Florida), and Alex K. Jones (University of Pittsburgh)*

SuDoku: Tolerating High-Rate of Transient Failures for Enabling Scalable STTRAM .388.....  
*Prashant J. Nair (University of British Columbia), Bahar Asgari (Georgia Institute of Technology), and Moinuddin K. Qureshi (Georgia Institute of Technology)*

## Session 11 – Trusted Computing

NeXUS: Practical and Secure Access Control on Untrusted Storage Platforms using Client-Side SGX .401.....  
*Judicael B. Djoko (University of Pittsburgh), Jack Lange (University of Pittsburgh), and Adam J. Lee (University of Pittsburgh)*

TEE-Perf: A Profiler for Trusted Execution Environments .414.....  
*Maurice Bailleu (The University of Edinburgh), Donald Dragoti (TU Dresden), Pramod Bhatotia (The University of Edinburgh), and Christof Fetzer (TU Dresden)*

EPA-RIMM : An Efficient, Performance-Aware Runtime Integrity Measurement Mechanism for Modern Server Platforms .422.....  
*Brian Delgado (Portland State University / Intel), Tejaswini Vibhute (Intel), John Fastabend (Portland State University), and Karen Karavanic (Portland State University)*

## Session 12 – Network Security

Pseudo-Honeypot: Toward Efficient and Scalable Spam Sniffer .435.....  
*Yihe Zhang (University of Louisiana at Lafayette), Hao Zhang (Oracle Corporation, USA), Xu Yuan (University of Louisiana at Lafayette), and Nian-Feng Tzeng (University of Louisiana at Lafayette)*

Controller-Oblivious Dynamic Access Control in Software-Defined Networks .447.....  
*Steven R. Gomez (MIT Lincoln Laboratory), Samuel Jero (MIT Lincoln Laboratory), Richard Skowrya (MIT Lincoln Laboratory), Jason Martin (MIT Lincoln Laboratory), Patrick Sullivan (MIT Lincoln Laboratory), David Bigelow (MIT Lincoln Laboratory), Zachary Ellenbogen (MIT Lincoln Laboratory), Bryan C. Ward (MIT Lincoln Laboratory), Hamed Okhravi (MIT Lincoln Laboratory), and James W. Landry (MIT Lincoln Laboratory)*

BorderPatrol: Securing BYOD using Fine-Grained Contextual Information .460.....  
*Onur Zungur (Boston University), Guillermo Suarez-Tangil (King's College London), Gianluca Stringhini (Boston University), and Manuel Egele (Boston University)*

## Session 13 – Empirical Studies

Characterizing and Understanding HPC Job Failures Over The 2K-Day Life of IBM BlueGene/Q System .473.....  
*Sheng Di (Argonne National Laboratory), Hanqi Guo (Argonne National Laboratory), Eric Pershey (Argonne National Laboratory), Marc Snir (University of Illinois at Urbana-Champaign), and Franck Cappello (Argonne National Laboratory, University of Illinois at Urbana-Champaign)*

Detecting "0-Day" Vulnerability: An Empirical Study of Secret Security Patch in OSS .485.....  
*Xinda Wang (George Mason University), Kun Sun (George Mason University), Archer Batcheller (Northrop Grumman), and Sushil Jajodia (George Mason University)*

Where Are You Taking Me? Behavioral Analysis of Open DNS Resolvers .493.....  
*Jeman Park (University of Central Florida), Aminollah Khormali (University of Central Florida), Manar Mohaisen (Korea University of Technology and Education), and Aziz Mohaisen (University of Central Florida)*



## Session 14 – Randomization and Vulnerabilities

- POLaR: Per-Allocation Object Layout Randomization .505.....  
*Jonghwan Kim (KAIST), Daehee Jang (KAIST), Yunjong Jeong (KAIST), and Brent Byunghoon Kang (KAIST)*
- The Strength of Weak Randomization: Easily Deployable, Efficiently Searchable Encryption with Minimal Leakage .517.....  
*David Pouliot (Portland State University), Scott Griffy (Portland State University), and Charles V. Wright (Portland State University)*
- HeapTherapy+: Efficient Handling of (Almost) All Heap Vulnerabilities Using Targeted Calling-Context Encoding .530.....  
*Qiang Zeng (University of South Carolina), Golam Kayas (Temple University), Emil Mohammed (Temple University), Lannan Luo (University of South Carolina), Xiaojiang Du (Temple University), and Junghwan Rhee (NEC Lab)*

## Session 15 – Storage Systems and Blockchain

- FabZK: Supporting Privacy-Preserving, Auditable Smart Contracts in Hyperledger Fabric .543.....  
*Hui Kang (IBM Research), Ting Dai (NC State University), Nerla Jean-Louis (IBM Research), Shu Tao (IBM Research), and Xiaohui Gu (NC State University)*
- Fast Predictive Repair in Erasure-Coded Storage .556.....  
*Zhirong Shen (The Chinese University of Hong Kong), Xiaolu Li (The Chinese University of Hong Kong), and Patrick P. C. Lee (The Chinese University of Hong Kong)*
- SBFT: A Scalable and Decentralized Trust Infrastructure .568.....  
*Guy Golan Gueta (VMware), Ittai Abraham (VMware), Shelly Grossman (Tel Aviv University), Dahlia Malkhi (VMware), Benny Pinkas (Bar Ilan University), Michael Reiter (UNC-Chapel Hill), Dragos-Adrian Seredinschi (EPFL), Orr Tamir (Tel Aviv University), and Alin Tomescu (MIT)*

## Session 16 – Symbolic Execution

- UChecker: Automatically Detecting PHP-Based Unrestricted File Upload Vulnerabilities .581.....  
*Jin Huang (Wright State University), Yu Li (Wright State University), Junjie Zhang (Wright State University), and Rui Dai (University of Cincinnati)*
- PrivAnalyzer: Measuring the Efficacy of Linux Privilege Use .593.....  
*John Criswell (University of Rochester), Jie Zhou (University of Rochester), Spyridoula Gravani (University of Rochester), and Xiaoyu Hu (BitFusion.io Inc.)*

1dVul: Discovering 1-Day Vulnerabilities through Binary Patches .605.....  
*Jiaqi Peng (Institute of Information Engineering, Chinese Academy of Sciences), Feng Li (Institute of Information Engineering, Chinese Academy of Sciences), Bingchang Liu (Institute of Information Engineering, Chinese Academy of Sciences), Lili Xu (Institute of Information Engineering, Chinese Academy of Sciences), Binghong Liu (Institute of Information Engineering, Chinese Academy of Sciences), Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences), and Wei Huo (Institute of Information Engineering, Chinese Academy of Sciences)*

## Session 17 – Potpourri

Revisiting Client Puzzles for State Exhaustion Attacks Resilience .617.....  
*Mohammad A. Nouredine (University of Illinois at Urbana Champaign), Ahmed M. Fawaz (University of Illinois at Urbana Champaign), Amanda Hsu (University of Illinois at Urbana Champaign), Cody Guldner (University of Illinois at Urbana Champaign), Sameer Vijay (University of Illinois at Urbana Champaign), Tamer Baar (University of Illinois at Urbana Champaign), and William H. Sanders (University of Illinois at Urbana Champaign)*

Robust Anomaly Detection on Unreliable Data .630.....  
*Zilong Zhao (Université Grenoble Alpes, France), Sophie Cerf (Université Grenoble Alpes, France), Robert Birke (ABB Research, Switzerland), Bogdan Robu (Université Grenoble Alpes, France), Sara Bouchenak (INSA Lyon, France), Sonia Ben Mokhtar (INSA Lyon, France), and Lydia Y Chen (TU Delft, Netherlands)*

Pupillography as Indicator of Programmers' Mental Effort and Cognitive Overload .638.....  
*Ricardo Couceiro (CISUC, University of Coimbra), Gonçalo Duarte (CISUC, University of Coimbra), João Durães (CISUC, Polytechnic Institute of Coimbra), João Castelhana (ICNAS, University of Coimbra), Catarina Duarte (ICNAS, University of Coimbra), Cesar Teixeira (CISUC, University of Coimbra), Miguel Castelo Branco (ICNAS/CIBIT, University of Coimbra), Paulo Carvalho (CISUC, University of Coimbra), and Henrique Madeira (CISUC, University of Coimbra)*

**Author Index 645** .....