

# **2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021)**

**Virtual Conference  
21 – 24 June 2021**



**IEEE Catalog Number: CFP21048-POD  
ISBN: 978-1-6654-1194-3**

**Copyright © 2021 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:	CFP21048-POD
ISBN (Print-On-Demand):	978-1-6654-1194-3
ISBN (Online):	978-1-6654-3572-7
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) **DSN 2021**

## Table of Contents

Message from the General Chairs .xiii.....	
Message from the Programme Chairs .xiv.....	
Steering Committee .xv.....	
Organizing Committee .xvi.....	
Programme Committee .xviii.....	
External Reviewers .xx.....	
Best Paper Award .xxii.....	
William C. Carter Award PhD Dissertation Award in Dependability .xxiii.....	
Rising Star in Dependability Award .xxiv.....	
Test-of-Time Award .xxv.....	
Jean-Claude Laprie Award in Dependable Computing .xxvi.....	
Keynotes .xxvii.....	
Sponsors .xxxii.....	

## Best Paper Candidates

A Low-Cost Fault Corrector for Deep Neural Networks through Range Restriction .1.....	
<i>Zitao Chen (University of British Columbia, Canada), Guanpeng Li (University of Iowa, USA), and Karthik Pattabiraman (University of British Columbia, Canada)</i>	
Toward Intrusion Tolerance as a Service: Confidentiality in Partially Cloud-Based BFT Systems .14.....	
<i>Maher Khan (University of Pittsburgh, USA) and Amy Babay (University of Pittsburgh, USA)</i>	
PID-Piper: Recovering Robotic Vehicles from Physical Attacks .26.....	
<i>Pritam Dash (University of British Columbia, Canada), Guanpeng Li (University of Iowa, USA), Zitao Chen (University of British Columbia, Canada), Mehdi Karimibiuki (University of British Columbia, Canada), and Karthik Pattabiraman (University of British Columbia, Canada)</i>	

## R1 - Dependability for Machine Learning

- GARFIELD: System Support for Byzantine Machine Learning .39.....  
*Rachid Guerraoui (EPFL), Arsany Guirguis (EPFL), Jérémy Plassmann (EPFL), Anton Ragot (EPFL), and Sébastien Rouault (EPFL)*
- Plinius: Secure and Persistent Machine Learning Model Training .52.....  
*Peterson Yuhala (University of Neuchâtel, Switzerland), Pascal Felber (University of Neuchâtel, Switzerland), Valerio Schiavoni (University of Neuchâtel, Switzerland), and Alain Tchana (ENS Lyon (Inria), France)*
- Decamouflage: A Framework to Detect Image-Scaling Attacks on CNN .63.....  
*Bedeuro Kim (University of Sungkyunkwan; CSIRO's Data61), Alsharif Abuadbbba (CSIRO's Data61; Cybersecurity CRC), Yansong Gao (CSIRO's Data61; Nanjing University of Science and Technology), Yifeng Zheng (CSIRO's Data61; Harbin Institute of Technology), Muhammad Ejaz Ahmed (CSIRO's Data61;), Surya Nepal (CSIRO's Data61; Cybersecurity CRC), and Hyounghick Kim (University of Sungkyunkwan; CSIRO's Data61)*
- MILR: Mathematically Induced Layer Recovery for Plaintext Space Error Correction of CNNs .75....  
*Jonathan Ponader (University of Central Florida, USA), Kyle Thomas (University of Central Florida, USA), Sandip Kundu (University of Massachusetts, USA), and Yan Solihin (University of Central Florida, USA)*

## R2 - Networking

- Fast IPv6 Network Periphery Discovery and Security Implications .88.....  
*Xiang Li (Tsinghua University; Beijing National Research Center for Information Science and Technology, China), Baojun Liu (Tsinghua University, China), Xiaofeng Zheng (Tsinghua University; QI-ANXIN Technology Research Institute, China), Haixin Duan (Tsinghua University; Beijing National Research Center for Information Science and Technology; QI-ANXIN Technology Research Institute; Peng Cheng Laboratory, China), Qi Li (Tsinghua University; Beijing National Research Center for Information Science and Technology, China), and Youjun Huang (Tsinghua University, China)*
- A Comprehensive Study of Bugs in Software Defined Networks .101.....  
*Ayush Bhardwaj (Brown University, USA), Zhenyu Zhou (Duke University, USA), and Theophilus A. Benson (Brown University, USA)*
- Enabling Novel Interconnection Agreements with Path-Aware Networking Architectures .116.....  
*Simon Scherrer (ETH Zurich, Switzerland), Markus Legner (ETH Zurich, Switzerland), Adrian Perrig (ETH Zurich, Switzerland), and Stefan Schmid (Faculty of Computer Science, University of Vienna, Austria)*
- Self-Healing Protocol: Repairing Schedules Online After Link Failures in Time-Triggered Networks .129.....  
*Francisco Pozo (Westermo Network Technologies AB, Sweden), Guillermo Rodriguez-Navas (Nokia Bell Labs, Israel), and Hans Hansson (School of Innovation, Design and Engineering, Mälardalen University, Sweden)*

## R3 - Attacks, Vulnerabilities, and Patches

The Master and Parasite Attack .141.....	141
<i>Lukas Baumann (Fraunhofer Institute for Secure Information Technology, Germany), Elias Heftrig (Fraunhofer Institute for Secure Information Technology, Germany), Haya Shulman (Fraunhofer Institute for Secure Information Technology, Germany), and Michael Waidner (Fraunhofer Institute for Secure Information Technology, Germany)</i>	
PatchDB: A Large-Scale Security Patch Dataset .149.....	149
<i>Xinda Wang (Center for Secure Information Systems, George Mason University, USA), Shu Wang (Center for Secure Information Systems, George Mason University, USA), Pengbin Feng (Center for Secure Information Systems, George Mason University, USA), Kun Sun (Center for Secure Information Systems, George Mason University, USA), and Sushil Jajodia (Center for Secure Information Systems, George Mason University, USA)</i>	
PDGraph: A Large-Scale Empirical Study on Project Dependency of Security Vulnerabilities .161...	161
<i>Qiang Li (Beijing JiaoTong University, China), Jinke Song (Beijing JiaoTong University, China), Dawei Tan (Beijing JiaoTong University, China), Haining Wang (Virginia Polytechnic Institute and State University, USA), and Jiqiang Liu (Beijing JiaoTong University, China)</i>	
OCTOPOCS: Automatic Verification of Propagated Vulnerable Code Using Reformed Proofs of Concept .174.....	174
<i>Seongkyeong Kwon (Korea University), Seunghoon Woo (Korea University), Gangmo Seong (Korea University), and Heejo Lee (Korea University)</i>	

## R4 - Systems Dependability

NVCache: A Plug-and-Play NVMM-Based I/O Booster for Legacy Systems .186.....	186
<i>Rémi Dulong (Université de Neuchâtel, Switzerland), Rafael Pires (Swiss Federal Institute of Technology in Lausanne, Switzerland), Andreia Correia (Université de Neuchâtel, Switzerland), Valerio Schiavoni (Université de Neuchâtel, Switzerland), Pedro Ramalhete (Cisco Systems), Pascal Felber (Université de Neuchâtel, Switzerland), and Gaël Thomas (Telecom SudParis/Insitut Polytechnique de Paris)</i>	
K2: Reading Quickly from Storage Across Many Datacenters .199.....	199
<i>Khiem Ngo (Princeton University, USA), Haonan Lu (Princeton University, USA), and Wyatt Lloyd (Princeton University, USA)</i>	
Horus: Non-Intrusive Causal Analysis of Distributed Systems Logs .212.....	212
<i>Francisco Neves (INESC TEC and U. Minho, Portugal), Nuno Machado (Amazon and INESC TEC, Spain), Ricardo Vilaça (INESC TEC and U. Minho, Portugal), and José Pereira (INESC TEC and U. Minho, Portugal)</i>	

## R5 - Machine Learning for Dependability

Asteria: Deep Learning-Based AST-Encoding for Cross-Platform Binary Code Similarity Detection .224.....	
<i>Shouguo Yang (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Long Cheng (School of Computing, Clemson University, USA), Yicheng Zeng (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Zhe Lang (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Hongsong Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), and Zhiqiang Shi (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China)</i>	
Sentiment Analysis Based Error Detection for Large-Scale Systems .237.....	
<i>Khalid Ayedh Alharthi (University of Warwick, UK; University of Bisha, KSA), Arshad Jhumka (University of Warwick, UK), Sheng Di (Argonne National Laboratory, USA), Franck Cappello (Argonne National Laboratory, USA; University of Illinois at Urbana-Champaign, USA), and Edward Chuah (Lancaster University, UK)</i>	
Time-Window Based Group-Behavior Supported Method for Accurate Detection of Anomalous Users .250.....	
<i>Lun-Pin Yuan (Pennsylvania State University, USA), Euijin Choo (Qatar Computing Research Institute, Qatar), Ting Yu (Qatar Computing Research Institute, Qatar), Issa Khalil (Qatar Computing Research Institute, Qatar), and Sencun Zhu (Pennsylvania State University, USA)</i>	
General Feature Selection for Failure Prediction in Large-Scale SSD Deployment .263.....	
<i>Fan Xu (Alibaba Group), Shujie Han (The Chinese University of Hong Kong), Patrick P. C. Lee (The Chinese University of Hong Kong), Yi Liu (Alibaba Group), Cheng He (Alibaba Group), and Jiongzhou Liu (Alibaba Group)</i>	

## R6 - GPUs

Data-Centric Reliability Management in GPUs .271.....	
<i>Gurunath Kadam (William &amp; Mary, USA), Evgenia Smirni (William &amp; Mary, USA), and Adwait Jog (William &amp; Mary, USA)</i>	
NVBitFI: Dynamic Fault Injection for GPUs .284.....	
<i>Timothy Tsai (Nvidia), Siva Kumar Sastry Hari (Nvidia), Michael B. Sullivan (Nvidia), Oreste Villa (Nvidia), and Stephen W. Keckler (Nvidia)</i>	

Revealing GPUs Vulnerabilities by Combining Register-Transfer and Software-Level Fault Injection .292.....	
	<i>Fernando F. dos Santos (PPGC, Institute of Informatics, Universidade Federal do Rio Grande do Sul, Brasil), Josie E. Rodriguez Condia (Politecnico di Torino, Italy), Luigi Carro (PPGC, Institute of Informatics, Universidade Federal do Rio Grande do Sul, Brasil), Matteo Sonza Reorda (Politecnico di Torino, Italy), and Paolo Rech (Politecnico di Torino, Italy)</i>
Examining Failures and Repairs on Supercomputers with Multi-GPU Compute Nodes .305.....	
	<i>Amir Taherin (Northeastern University), Tirthak Patel (Northeastern University), Giorgis Georgakoudis (Lawrence Livermore National Laboratory), Ignacio Laguna (Lawrence Livermore National Laboratory), and Devesh Tiwari (Northeastern University)</i>

## R7 - Systems Security

An Application Agnostic Defense Against the Dark Arts of Cryptojacking .314.....	
	<i>Nada Lachtar (University of Michigan, USA), Abdulrahman Abu Elkhail (University of Michigan, USA), Anys Bacha (University of Michigan, USA), and Hafiz Malik (University of Michigan, USA)</i>
Catch You with Cache: Out-of-VM Introspection to Trace Malicious Executions .326.....	
	<i>Chao Su (State Key Lab for Novel Software Tech., Nanjing University, China), Xuhua Ding (School of Information Systems, Singapore Management University), and Qingkai Zeng (State Key Lab for Novel Software Tech., Nanjing University, China)</i>
Towards Optimal Use of Exception Handling Information for Function Detection .338.....	
	<i>Chengbin Pang (Nanjing University; Stevens Institute of Technology), Ruotong Yu (Stevens Institute of Technology), Dongpeng Xu (University of New Hampshire), Eric Koskinen (Stevens Institute of Technology), Georgios Portokalidis (Stevens Institute of Technology), and Jun Xu (Stevens Institute of Technology)</i>
CloudSkulk: A Nested Virtual Machine Based Rootkit and Its Detection .350.....	
	<i>Joseph Connelly (Boise State University, USA), Taylor Roberts (Boise State University, USA), Xing Gao (University of Delaware, USA), Jidong Xiao (Boise State University, USA), Haining Wang (Virginia Tech, USA), and Angelos Stavrou (Virginia Tech, USA)</i>

## R8 - Fault Injection

FIRestarter: Practical Software Crash Recovery with Targeted Library-Level Fault Injection.363.....	
	<i>Koustubha Bhat (Vrije Universiteit Amsterdam, The Netherlands), Erik van der Kouwe (Vrije Universiteit Amsterdam, The Netherlands), Herbert Bos (Vrije Universiteit Amsterdam, The Netherlands), and Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands)</i>

- WazaBee: Attacking Zigbee Networks by Diverting Bluetooth Low Energy Chips .376.....  
*Romain Cayre (CNRS, LAAS, France), Florent Galtier (CNRS, LAAS, France), Guillaume Auriol (CNRS, LAAS, France; †Univ de Toulouse, INSA, LAAS), Vincent Nicomette (CNRS, LAAS, France; †Univ de Toulouse, INSA, LAAS), Mohamed Kaâniche (CNRS, LAAS, France), and Géraldine Marconato (APSYS.Lab, APSYS)*
- InjectaBLE: Injecting Malicious Traffic into Established Bluetooth Low Energy Connections .388....  
*Romain Cayre (CNRS, LAAS; APSYS.Lab, APSYS), Florent Galtier (CNRS, LAAS, France), Guillaume Auriol (CNRS, LAAS; Univ de Toulouse, INSA, LAAS), Vincent Nicomette (CNRS, LAAS; Univ de Toulouse, INSA, LAAS), Mohamed Kaâniche (CNRS, LAAS, France), and Géraldine Marconato (APSYS.Lab, APSYS)*
- Glitching Demystified: Analyzing Control-Flow-Based Glitching Attacks and Defenses .400.....  
*Chad Spensky (Allthenticate; IBM T.J. Watson Research Center; UC Santa Barbara), Aravind Machiry (Purdue University), Nathan Burow (MIT Lincoln Laboratory), Hamed Okhravi (MIT Lincoln Laboratory), Rick Housley (River Loop Security), Zhongshu Gu (IBM T.J. Watson Research Center), Hani Jamjoom (IBM T.J. Watson Research Center), Christopher Kruegel (UC Santa Barbara), and Giovanni Vigna (UC Santa Barbara)*

## R9 - Trusted Execution Environments

- Practical and Efficient in-Enclave Verification of Privacy Compliance .413.....  
*Weijie Liu (Indiana University Bloomington, USA), Wenhao Wang (Institute of Information Engineering, CAS, China), Hongbo Chen (Indiana University Bloomington, USA), XiaoFeng Wang (Indiana University Bloomington, USA), Yaosong Lu (Institute of Information Engineering, CAS, China), Kai Chen (Institute of Information Engineering, CAS, China), Xinyu Wang (Shanghai Jiao Tong University, China), Qintao Shen (Institute of Information Engineering, CAS, China), Yi Chen (The Chinese University of Hong Kong), and Haixu Tang (Indiana University Bloomington, USA)*
- ADAM-CS: Advanced Asynchronous Monotonic Counter Service .426.....  
*André Martin (TU Dresden, Germany), Cong Lian (TU Dresden, Germany), Franz Gregor (TU Dresden, Germany), Robert Krahn (TU Dresden, Germany), Valerio Schiavoni (Université de Neuchâtel, Switzerland), Pascal Felber (Université de Neuchâtel, Switzerland), and Christof Fetzner (TU Dresden, Germany)*
- EncDBDB: Searchable Encrypted, Fast, Compressed, In-Memory Database Using Enclaves .438.....  
*Benny Fuhry (SAP Security Research, Germany), Jayanth Jain H A (SAP Security Research, Germany), and Florian Kerschbaum (University of Waterloo, Canada)*



## R10 - Modeling

- Conservative Confidence Bounds in Safety, from Generalised Claims of Improvement & Statistical Evidence .451.....  
*Kizito Salako (Centre for Software Reliability City, University of London, UK), Lorenzo Strigini (Centre for Software Reliability City, University of London, UK), and Xingyu Zhao (University of Liverpool, UK)*
- Model Checking the Multi-formalism Language FIGARO .463.....  
*Shahid Khan (RWTH Aachen University, Germany), Matthias Volk (RWTH Aachen University, Germany), Joost-Pieter Katoen (RWTH Aachen University, Germany), Alexis Braibant (Électricité de France, France), and Marc Bouissou (Électricité de France, France)*
- Avis: In-Situ Model Checking for Unmanned Aerial Vehicles .471.....  
*Max Taylor (The Ohio State University, USA), Haicheng Chen (The Ohio State University, USA), Feng Qin (The Ohio State University, USA), and Christopher Stewart (The Ohio State University, USA)*

## R11 - IoT and Cyber Physical Systems

- Data-Driven Design of Context-Aware Monitors for Hazard Prediction in Artificial Pancreas Systems .484.....  
*Xugui Zhou (University of Virginia, USA), Bulbul Ahmed (University of Florida, USA), James H. Aylor (University of Virginia, USA), Philip Asare (University of Toronto, Canada), and Homa Alemzadeh (University of Virginia, USA)*
- Sanitizing the IoT Cyber Security Posture: An Operational CTI Feed Backed up by Internet Measurements .497.....  
*Morteza Safaei Pour (The Cyber Center for Security and Analytics, University of Texas at San Antonio, USA), Dylan Watson (The Cyber Center for Security and Analytics, University of Texas at San Antonio, USA), and Elias Bou-Harb (The Cyber Center for Security and Analytics, University of Texas at San Antonio, USA)*
- Physics-Aware Security Monitoring Against Structural Integrity Attacks in 3D Printers .507.....  
*Sriharsha Etigowni (Rutgers University, USA), Sizhuang Liang (Georgia Institute of Technology, USA), Saman Zonouz (Rutgers University, USA), and Raheem Beyah (Georgia Institute of Technology, USA)*
- Compromised Computers Meet Voice Assistants: Stealthily Exfiltrating Data as Voice over Telephony .519.....  
*Zhengxian He (Georgia Institute of Technology, USA), Mohit Narayan Rajput (Citrix Systems), and Mustaque Ahamad (Georgia Institute of Technology, USA)*

## R12 - Software Dependability

- BigMap: Future-Proofing Fuzzers with Efficient Large Maps .531.....  
*Alif Ahmed (University of Virginia, USA), Jason D. Hiser (University of Virginia, USA), Anh Nguyen Tuong (University of Virginia, USA), Jack W. Davidson (University of Virginia, USA), and Kevin Skadron (University of Virginia, USA)*

When Program Analysis Meets Bytecode Search: Targeted and Efficient Inter-Procedural Analysis of Modern Android Apps in BackDroid .543.....  
*Daoyuan Wu (The Chinese University of Hong Kong, China), Debin Gao (School of Information Systems, Singapore Management University, Singapore), Robert H. Deng (School of Information Systems, Singapore Management University, Singapore), and Rocky K. C. Chang (The Hong Kong Polytechnic University, China)*

Hiding in the Particles: When Return-Oriented Programming Meets Program Obfuscation .555.....  
*Pietro Borrello (Sapienza University of Rome), Emilio Coppa (Sapienza University of Rome), and Daniele Cono D'Elia (Sapienza University of Rome)*

Statically Detecting JavaScript Obfuscation and Minification Techniques in the Wild .569.....  
*Marvin Moog (Saarland University; CISA Helmholtz Center for Information Security), Markus Demmel (Saarland University), Michael Backes (CISA Helmholtz Center for Information Security), and Aurore Fass (CISA Helmholtz Center for Information Security)*

**Author Index 581**.....