

Contents

Frontmatter

Message from the Chairs	iii
ISSTA 2020 Organization	v

Research Papers

Fuzzing

WEIZZ: Automatic Grey-Box Fuzzing for Structured Binary Formats Andrea Fioraldi, Daniele Cono D’Elia, and Emilio Coppa — <i>Sapienza University of Rome, Italy</i>	1
Active Fuzzing for Testing and Securing Cyber-Physical Systems Yuqi Chen, Bohan Xuan, Christopher M. Poskitt, Jun Sun, and Fan Zhang — <i>Singapore Management University, Singapore; Zhejiang University, China; Zhejiang Lab, China; Alibaba-Zhejiang University Joint Institute of Frontier Technologies, China</i>	14
Learning Input Tokens for Effective Fuzzing Björn Mathis, Rahul Gopinath, and Andreas Zeller — <i>CISPA, Germany</i>	27

Symbolic Execution and Constraint Solving

Fast Bit-Vector Satisfiability Peisen Yao, Qingkai Shi, Heqing Huang, and Charles Zhang — <i>Hong Kong University of Science and Technology, China</i>	38
Relocatable Addressing Model for Symbolic Execution David Trabish and Noam Rinetzkyl — <i>Tel Aviv University, Israel</i>	51
Running Symbolic Execution Forever Frank Busse, Martin Nowack, and Cristian Cadar — <i>Imperial College London, UK</i>	63

Repair and Debug

Can Automated Program Repair Refine Fault Localization? A Unified Debugging Approach Yiling Lou, Ali Ghanbari, Xia Li, Lingming Zhang, Haotian Zhang, Dan Hao, and Lu Zhang — <i>Peking University, China; University of Texas at Dallas, USA; Ant Financial Services, China</i>	75
Automated Repair of Feature Interaction Failures in Automated Driving Systems Raja Ben Abdesslem, Annibale Panichella, Shiva Nejati, Lionel C. Briand, and Thomas Stifter — <i>University of Luxembourg, Luxembourg; Delft University of Technology, Netherlands; University of Ottawa, Canada; IEE, Luxembourg</i>	88
CoCoNuT: Combining Context-Aware Neural Translation Models using Ensemble for Program Repair Thibaud Lutellier, Hung Viet Pham, Lawrence Pang, Yitong Li, Moshel Wei, and Lin Tan — <i>University of Waterloo, Canada; Purdue University, USA</i>	101

Mobile Apps

Detecting and Diagnosing Energy Issues for Mobile Applications Xueliang Li, Yuming Yang, Yepang Liu, John P. Gallagher, and Kaishun Wu — <i>Shenzhen University, China; Southern University of Science and Technology, China; Roskilde University, Denmark; IMDEA Software Institute, Spain</i>	115
Automated Classification of Actions in Bug Reports of Mobile Apps Hui Liu, Mingzhu Shen, Jiahao Jin, and Yanjie Jiang — <i>Beijing Institute of Technology, China</i>	128
Data Loss Detector: Automatically Revealing Data Loss Bugs in Android Apps Oliviero Riganelli, Simone Paolo Mottadelli, Claudio Rota, Daniela Micucci, and Leonardo Mariani — <i>University of Milano-Bicocca, Italy</i>	141

Machine Learning I

Reinforcement Learning Based Curiosity-Driven Testing of Android Applications Minxue Pan, An Huang, Guoxin Wang, Tian Zhang, and Xuandong Li — <i>Nanjing University, China</i>	153
Effective White-Box Testing of Deep Neural Networks with Adaptive Neuron-Selection Strategy Seokhyun Lee, Sooyoung Cha, Dain Lee, and Hakjoo Oh — <i>Korea University, South Korea</i>	165

DeepGini: Prioritizing Massive Tests to Enhance the Robustness of Deep Neural Networks Yang Feng, Qingkai Shi, Xinyu Gao, Jun Wan, Chunrong Fang, and Zhenyu Chen — <i>Nanjing University, China; Hong Kong University of Science and Technology, China; Ant Financial Services, China</i>	177
Machine Learning II	
Detecting and Understanding Real-World Differential Performance Bugs in Machine Learning Libraries Saeid Tizpaz-Niari, Pavol Černý, and Ashutosh Trivedi — <i>University of Colorado Boulder, USA; TU Vienna, Austria</i>	189
Higher Income, Larger Loan? Monotonicity Testing of Machine Learning Models Arnab Sharma and Heike Wehrheim — <i>University of Paderborn, Germany</i>	200
Detecting Flaky Tests in Probabilistic and Machine Learning Applications Saikat Dutta, August Shi, Rutvik Choudhary, Zhekun Zhang, Aryaman Jain, and Sasa Misailovic — <i>University of Illinois at Urbana-Champaign, USA</i>	211
Bug Localization and Test Isolation	
Scaffle: Bug Localization on Millions of Files Michael Pradel, Vijayaraghavan Murali, Rebecca Qian, Mateusz Machalica, Erik Meijer, and Satish Chandra — <i>University of Stuttgart, Germany; Facebook, USA</i>	225
Abstracting Failure-Inducing Inputs Rahul Gopinath, Alexander Kampmann, Nikolas Havrikov, Ezekiel O. Soremekun, and Andreas Zeller — <i>CISPA, Germany</i>	237
Debugging the Performance of Maven’s Test Isolation: Experience Report Pengyu Nie, Ahmet Celik, Matthew Coley, Aleksandar Milicevic, Jonathan Bell, and Milos Gligoric — <i>University of Texas at Austin, USA; Facebook, USA; George Mason University, USA; Microsoft, USA</i>	249
Security	
Feedback-Driven Side-Channel Analysis for Networked Applications İsmet Burak Kadron, Nicolás Rosner, and Tevfik Bultan — <i>University of California at Santa Barbara, USA</i>	260
Scalable Analysis of Interaction Threats in IoT Systems Mohannad Alhanahnah, Clay Stevens, and Hamid Bagheri — <i>University of Nebraska-Lincoln, USA</i>	272
DeepSQLi: Deep Semantic Learning for Testing SQL Injection Muyang Liu, Ke Li, and Tao Chen — <i>University of Electronic Science and Technology of China, China; University of Exeter, UK; Loughborough University, UK</i>	286
Regression Testing	
Dependent-Test-Aware Regression Testing Techniques Wing Lam, August Shi, Reed Oei, Sai Zhang, Michael D. Ernst, and Tao Xie — <i>University of Illinois at Urbana-Champaign, USA; Google, USA; University of Washington, USA; Peking University, China</i>	298
Differential Regression Testing for REST APIs Patrice Godefroid, Daniel Lehmann, and Marina Polishchuk — <i>Microsoft Research, USA; University of Stuttgart, Germany</i>	312
Empirically Revisiting and Enhancing IR-Based Test-Case Prioritization Qianyang Peng, August Shi, and Lingming Zhang — <i>University of Illinois at Urbana-Champaign, USA; University of Texas at Dallas, USA</i>	324
Challenging Domains	
Intermittently Failing Tests in the Embedded Systems Domain Per Erik Strandberg, Thomas J. Ostrand, Elaine J. Weyuker, Wasif Afzal, and Daniel Sundmark — <i>Westermo Network Technologies, Sweden; Mälardalen University, Sweden; University of Central Florida, USA</i>	337
Feasible and Stressful Trajectory Generation for Mobile Robots Carl Hildebrandt, Sebastian Elbaum, Nicola Bezzo, and Matthew B. Dwyer — <i>University of Virginia, USA</i>	349
Detecting Cache-Related Bugs in Spark Applications Hui Li, Dong Wang, Tianze Huang, Yu Gao, Wensheng Dou, Lijie Xu, Wei Wang, Jun Wei, and Hua Zhong — <i>Institute of Software at Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Beijing University of Posts and Telecommunications, China</i>	363
Binary Analysis	
Patch Based Vulnerability Matching for Binary Programs Yifei Xu, Zhengzi Xu, Bihuan Chen, Fu Song, Yang Liu, and Ting Liu — <i>Xi’an Jiaotong University, China; Nanyang Technological University, Singapore; Fudan University, China; ShanghaiTech University, China; Zhejiang University, China</i>	376

Identifying Java Calls in Native Code via Binary Scanning George Fourtounis, Leonidas Triantafyllou, and Yannis Smaragdakis — <i>University of Athens, Greece</i>	388
An Empirical Study on ARM Disassembly Tools Muhui Jiang, Yajin Zhou, Xiapu Luo, Ruoyu Wang, Yang Liu, and Kui Ren — <i>Hong Kong Polytechnic University, China; Zhejiang University, China; Arizona State University, USA; Nanyang Technological University, Singapore</i>	401
Static Analysis and Search-Based Testing	
How Effective Are Smart Contract Analysis Tools? Evaluating Smart Contract Static Analysis Tools using Bug Injection Asem Ghaleb and Karthik Pattabiraman — <i>University of British Columbia, Canada</i>	415
A Programming Model for Semi-implicit Parallelization of Static Analyses Dominik Helm, Florian Kübler, Jan Thomas Kölzer, Philipp Haller, Michael Eichberg, Guido Salvaneschi, and Mira Mezini — <i>TU Darmstadt, Germany; KTH, Sweden</i>	428
Recovering Fitness Gradients for Interprocedural Boolean Flags in Search-Based Testing Yun Lin, Jun Sun, Gordon Fraser, Ziheng Xiu, Ting Liu, and Jin Song Dong — <i>National University of Singapore, Singapore; Singapore Management University, Singapore; University of Passau, Germany; Xi'an Jiaotong University, China</i>	440
Build Testing	
Scalable Build Service System with Smart Scheduling Service Kaiyuan Wang, Greg Tener, Vijay Gullapalli, Xin Huang, Ahmed Gad, and Daniel Rall — <i>Google, USA</i>	452
Escaping Dependency Hell: Finding Build Dependency Errors with the Unified Dependency Graph Gang Fan, Chengpeng Wang, Rongxin Wu, Xiao Xiao, Qingkai Shi, and Charles Zhang — <i>Hong Kong University of Science and Technology, China; Xiamen University, China; Sourcebrella, China</i>	463
How Far We Have Come: Testing Decompilation Correctness of C Decompilers Zhibo Liu and Shuai Wang — <i>Hong Kong University of Science and Technology, China</i>	475
Numerical Software Analysis and Clone Detection	
Discovering Discrepancies in Numerical Libraries Jackson Vanover, Xuan Deng, and Cindy Rubio-González — <i>University of California at Davis, USA</i>	488
Testing High Performance Numerical Simulation Programs: Experience, Lessons Learned, and Open Issues Xiao He, Xingwei Wang, Jia Shi, and Yi Liu — <i>University of Science and Technology Beijing, China; CNCERT/CC, China</i>	502
Functional Code Clone Detection with Syntax and Semantics Fusion Learning Chunrong Fang, Zixi Liu, Yangyang Shi, Jeff Huang, and Qingkai Shi — <i>Nanjing University, China; Texas A&M University, USA; Hong Kong University of Science and Technology, China</i>	516
Learning to Detect Table Clones in Spreadsheets Yakun Zhang, Wensheng Dou, Jiaxin Zhu, Liang Xu, Zhiyong Zhou, Jun Wei, Dan Ye, and Bo Yang — <i>Institute of Software at Chinese Academy of Sciences, China; Jinling Institute of Technology, China; North China University of Technology, China</i>	528
Tool Demonstrations	
ObjSim: Lightweight Automatic Patch Prioritization via Object Similarity Ali Ghanbari — <i>University of Texas at Dallas, USA</i>	541
Crowdsourced Requirements Generation for Automatic Testing via Knowledge Graph Chao Guo, Tiek He, Wei Yuan, Yue Guo, and Rui Hao — <i>Nanjing University, China</i>	545
TauJud: Test Augmentation of Machine Learning in Judicial Documents Zichen Guo, Jiawei Liu, Tiek He, Zhuoyang Li, and Peitian Zhangzhu — <i>Nanjing University, China</i>	549
EShield: Protect Smart Contracts against Reverse Engineering Wentian Yan, Jianbo Gao, Zhenhao Wu, Yue Li, Zhi Guan, Qingshan Li, and Zhong Chen — <i>Peking University, China; Boya Blockchain, China</i>	553
Echidna: Effective, Usable, and Fast Fuzzing for Smart Contracts Gustavo Grieco, Will Song, Artur Cygan, Josselin Feist, and Alex Groce — <i>Trail of Bits, USA; Northern Arizona University, USA</i>	557
ProFL: A Fault Localization Framework for Prolog George Thompson and Allison K. Sullivan — <i>North Carolina A&T State University, USA; University of Texas at Arlington, USA</i>	561
FineLock: Automatically Refactoring Coarse-Grained Locks into Fine-Grained Locks Yang Zhang, Shuai Shao, Juan Zhai, and Shiqing Ma — <i>Hebei University of Science and Technology, China; Rutgers University, USA</i>	565

CPSDebug: A Tool for Explanation of Failures in Cyber-Physical Systems

Ezio Bartocci, Niveditha Manjunath, Leonardo Mariani, Cristinel Mateis, Dejan Ničković, and Fabrizio Pastore — *TU Vienna, Austria; Austrian Institute of Technology, Austria; University of Milano-Bicocca, Italy; University of Luxembourg, Luxembourg* 569

Test Recommendation System Based on Slicing Coverage Filtering

Ruixiang Qian, Yuan Zhao, Duo Men, Yang Feng, Qingkai Shi, Yong Huang, and Zhenyu Chen — *Nanjing University, China; Hong Kong University of Science and Technology, China; Mooctest, China* 573

Doctoral Symposium

Automated Mobile Apps Testing from Visual Perspective

Feng Xue — *Northwestern Polytechnical University, China* 577

Program-Aware Fuzzing for MQTT Applications

Luis Gustavo Araujo Rodriguez and Daniel Macêdo Batista — *University of São Paulo, Brazil* 582

Automatic Support for the Identification of Infeasible Testing Requirements

João Choma Neto — *University of São Paulo, Brazil* 587

Author Index 592