

2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W 2018)

**Luxembourg
25-28 June 2018**



**IEEE Catalog Number: CFP1841K-POD
ISBN: 978-1-5386-6708-8**

**Copyright © 2018 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:	CFP1841K-POD
ISBN (Print-On-Demand):	978-1-5386-6708-8
ISBN (Online):	978-1-5386-6553-4
ISSN:	2325-6648

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

2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops **DSNW 2018**

Table of Contents

Message from the General Chair	xiii
Message from the Workshops Chairs	xiv
Organizing Committee	xvi
Technical Program Committee	xviii
Steering Committee	xxi
External Reviewers	xxii

Industry Track Sessions

Foreword for the Industry Track	1
<i>Sy-Yen Kuo (National Taiwan University, Taiwan), Hari Ramasamy (IBM Corporation), Bob Swarz (Worcester Polytechnic Institute, USA), and Alan Wood (Oracle, USA)</i>	
Autonomous Driving System : Model Based Safety Analysis	2
<i>Mohamed Tlig (IRT SystemX, Paris - Saclay, France), Mathilde Machin (Apsys - Airbus group), Romain Kerneis (IRT SystemX, Paris - Saclay, France), Emmanuel Arbaretier (Apsys - Airbus group), Linda Zhao (SECTOR), Florent Meurville (VALEO), and Jean Van Frank (IRT SystemX, Paris - Saclay, France)</i>	
Measuring and Exploiting Guardbands of Server-Grade ARMv8 CPU Cores and DRAMs	6
<i>Konstantinos Tovletoglou (Queen's University Belfast), Lev Mukhanov (Queen's University Belfast), Georgios Karakonstantis (Queen's University Belfast), Athanasios Chatzidimitriou (University of Athens), George Papadimitriou (University of Athens), Manolis Kaliorakis (University of Athens), Dimitris Gizopoulos (University of Athens), Zacharias Hadjilambrou (University of Cyprus), Yiannakis Sazeides (University of Cyprus), Alejandro Lampropulos (WorldSensing), Shidhartha Das (ARM Ltd.), and Phong Vo (A.M.C.C. Deutschland AMPERE)</i>	
Hardening the Core: Understanding and Detection of XNU Kernel Vulnerabilities	10
<i>Xianyu Liu (Alibaba Inc.), Min Zheng (Alibaba Inc.), Aimin Pan (Alibaba Inc.), and Quan Lu (Alibaba Inc.)</i>	

Hardware Remediation at Scale	14
<i>Fan (Fred) Lin (Facebook Inc.), Matt Beadon (Facebook Inc.), Harish Dattatraya Dixit (Facebook Inc.), Gautham Vunnam (Facebook Inc.), Amol Desai (Facebook Inc.), and Sriram Sankar (Facebook Inc.)</i>	
Cross-Stack Threat Sensing for Cyber Security and Resilience	18
<i>Frederico Araujo (IBM Research), Teryl Taylor (IBM Research), Jialong Zhang (IBM Research), and Marc Stoecklin (IBM Research)</i>	
Lifeguard: Local Health Awareness for More Accurate Failure Detection	22
<i>Armon Dadgar (HashiCorp Inc.), James Phillips (HashiCorp Inc.), and Jon Currey (HashiCorp Inc.)</i>	
Diagnosing Failures of Cloud Management Actions	26
<i>Rohit Ranchal (IBM Watson Health) and Praveen Jayachandran (IBM Research)</i>	
ConfEx: Towards Automating Software Configuration Analytics in the Cloud	30
<i>Ozan Tuncer (Boston University), Nilton Bila (IBM Research), Sastry Duri (IBM Research), Canturk Isci (IBM Research), and Ayse K Coskun (Boston University)</i>	
A Large-Scale System for Real-Time Glucose Monitoring	34
<i>Long Vu (IBM TJ Watson Research Center), Venkata N. Pavuluri (IBM TJ Watson Research Center), Yuan-chi Chang (IBM TJ Watson Research Center), Deepak S. Turaga (IBM TJ Watson Research Center), Alex Zhong (Medtronic Inc.), Pratik Agrawal (Medtronic Inc.), Amit Singh (Medtronic Inc.), Boyi Jiang (Medtronic Inc.), and Krishna Chirutha (Medtronic Inc.)</i>	
Challenges of DB2 Restore in a Distributed Systems Environment and Engineered Solutions	38
<i>Pratik Mukherjee (IBM Watson Health) and Valentina Salapura (IBM Watson Health)</i>	
Dependability in a Multi-tenant Multi-framework Deep Learning as-a-Service Platform	43
<i>Scott Boag (IBM Research AI), Parijat Dube (IBM Research AI), Kaoutar El Maghraoui (IBM Research AI), Benjamin Herta (IBM Research AI), Waldemar Hummer (IBM Research AI), K. R. Jayaram (IBM Research AI), Rania Khalaf (IBM Research AI), Vinod Muthusamy (IBM Research AI), Michael Kalantar (IBM Research AI), and Archit Verma (IBM Research AI)</i>	

Fast Abstract Session

Fast Abstract #1

EUBra-BIGSEA, A Cloud-Centric Big Data Scientific Research Platform	47
<i>Ignacio Blanquer (Universitat Politècnica de València) and Wagner Meira Jr. (Universidade Federal de Minas Gerais)</i>	

SWAMP: Smart Water Management Platform Overview and Security Challenges	49
<i>Carlos Kamienski (Federal University of ABC), João Kleinschmidt (Federal University of ABC), Juha-Pekka Soininen (VTT Technical Research Centre of Finland), Kari Kolehmainen (VTT Technical Research Centre of Finland), Luca Roffia (University of Bologna), Marcos Visoli (Brazilian Agricultural Research Corporation (EMBRAPA)), Rodrigo Filev Maia (Centro Universitário da FEI), and Stenio Fernandes (Federal University of Pernambuco)</i>	
ATMOSPHERE: Adaptive, Trustworthy, Manageable, Orchestrated, Secure, Privacy-Assuring, Hybrid Ecosystem for REsilient Cloud Computing	51
<i>Francisco Brasileiro (Universidade Federal de Campina Grande), Andrey Brito (Universidade Federal de Campina Grande), and Ignacio Blanquer (Universitat Politècnica de València)</i>	
SecureCloud: Secure Big Data Processing in Untrusted Clouds	53
<i>Andrey Brito (Universidade Federal de Campina Grande) and Christof Fetzer (Technische Universität Dresden)</i>	
AVFI: Fault Injection for Autonomous Vehicles	55
<i>Saurabh Jha (University of Illinois at Urbana Champaign), Subho S. Banerjee (University of Illinois at Urbana Champaign), James Cyriac (University of Illinois at Urbana Champaign), Zbigniew T. Kalbarczyk (University of Illinois at Urbana Champaign), and Ravishankar K. Iyer (University of Illinois at Urbana Champaign)</i>	
Reconfiguration Strategies for Critical Adaptive Distributed Embedded Systems	57
<i>Alberto Ballesteros (University of the Balearic Islands), Julián Proenza (University of the Balearic Islands), Manuel Barranco (University of the Balearic Islands), and Luis Almeida (Universidade do Porto)</i>	
Towards Lightweight Temporal and Fault Isolation in Mixed-Criticality Systems with Real-Time Containers	59
<i>Marcello Cinque (Federico II University of Naples, Italy) and Domenico Cotroneo (Federico II University of Naples, Italy)</i>	

Fast Abstract #2

Finding Top-k Most Frequent Items in Distributed Streams in the Time-Sliding Window Model	61
<i>Emmanuelle Anceaume (CNRS / IRISA), Yann Busnel (IMT Atlantique / IRISA), and Vasile Cazacu (CNRS / IRISA)</i>	
Mixing Time and Spatial Redundancy Over Time Sensitive Networking	63
<i>Inés Álvarez (Universitat de les Illes Balears), Julián Proenza (Universitat de les Illes Balears), and Manuel Barranco (Universitat de les Illes Balears)</i>	
Stateless Security Risk Assessment for Dynamic Networks	65
<i>Jin Bum Hong (University of Western Australia), Simon Enoch Yusuf (University of Canterbury), Dong Seong Kim (University of Canterbury), and Khaled MD Khan (Qatar University)</i>	

Using Diverse Detectors for Detecting Malicious Web Scraping Activity	67
<i>Pedro Marques (Universidade de Lisboa, Portugal), Zayani Dabbabi (Amadeus, France), Miruna-Mihaela Mironescu (Amadeus, France), Olivier Thonnard (Amadeus, France), Frances Buontempo (Centre for Software Reliability, City, University of London, United Kingdom), Ilir Gashi (Centre for Software Reliability, City, University of London, United Kingdom), and Alysson Bessani (Universidade de Lisboa, Portugal)</i>	
On Verifying and Assuring the Cloud SLA by Evaluating the Performance of SaaS Web Services Across Multi-cloud Providers	69
<i>Abdallah Ali Zainelabden Abdallah Ibrahim (University of Luxembourg), Sebastien Varrette (University of Luxembourg), and Pascal Bouvry (University of Luxembourg)</i>	
Sources of Variation in Error Sensitivity Measurements, Significant or Not?	71
<i>Fatemeh Ayatollahi (Chalmers University of Technology, Sweden) and Johan Karlsson (Chalmers University of Technology, Sweden)</i>	
Towards Dynamic End-to-End Privacy Preserving Data Classification	73
<i>Rania Talbi (INSA Lyon – LIRIS Lyon, France), Sara Bouchenak (INSA Lyon – LIRIS Lyon, France), and Lydia Y. Chen (IBM Research – Zurich Lab Zurich, Switzerland)</i>	
HIT: Hybrid-Mode Information Flow Tracking with Taint Semantics Extraction and Replay	75
<i>Yu-Hsin Hung (National Chiao Tung University), Hong-Wei Li (National Chiao Tung University), Yu-Sung Wu (National Chiao Tung University), Bing-Jhong Jheng (National Chiao Tung University), and Yen-Nun Huang (Academia Sinica)</i>	
Reforming Industrial Information Assurance: Experiments with OPC UA Honey pots	
<i>Sriharsha Navile Basavaraju (University of Kaiserslautern, Kaiserslautern, Germany), Amritha Raj Herle (University of Kaiserslautern, Kaiserslautern, Germany), and Daniel Fraunholz (German Research Center for Artificial Intelligence, Kaiserslautern, Germany)</i>	
An Analysis of Automated Software Diversity Using Unstructured Text Analytics	79
<i>Andrew S. Gearhart (The Johns Hopkins University Applied Physics Laboratory), Peter A. Hamilton (The Johns Hopkins University Applied Physics Laboratory), and Joel Coffman (The Johns Hopkins University Applied Physics Laboratory)</i>	
Random Mining Group Selection to Prevent 51% Attacks on Bitcoin	81
<i>Jaewon Bae (Gwangju Institute of Science and Technology (GIST)) and Hyuk Lim (Gwangju Institute of Science and Technology (GIST))</i>	

Student Forum Session

PRESEnCE: A Framework for Monitoring, Modelling and Evaluating the Performance of Cloud SaaS Web Services	83
<i>Abdallah Ali Zainelabden Abdallah Ibrahim (University of Luxembourg)</i>	
Mu-Transaction Sagas in Derecho	87
<i>Sagar Jha (Cornell University)</i>	

Enhanced Dependability Evaluation Through Krylov Methods and Matrix Functions: The Case of Load-Sharing Systems	92
<i>Giulio Masetti (ISTI-CNR Pisa)</i>	
Design, Development and Implementation of a Network Intrusion Detection Tool for Air Traffic Management Systems	96
<i>Thobald de Riberolles (Activus)</i>	

Best of SELSE Session

Best of SELSE 2018 Introduction	100
<i>Alan Wood (Oracle Labs)</i>	
Hamartia: A Fast and Accurate Error Injection Framework	101
<i>Chun-Kai Chang (The University of Texas at Austin), Sangkug Lym (The University of Texas at Austin), Nicholas Kelly (The University of Texas at Austin), Michael B. Sullivan (NVIDIA), and Mattan Erez (The University of Texas at Austin)</i>	
Low Cost Transient Fault Protection Using Loop Output Prediction	109
<i>Sunghyun Park (University of Michigan), Shikai Li (University of Michigan), and Scott Mahlke (University of Michigan)</i>	
Parity++: Lightweight Error Correction for Last Level Caches	114
<i>Irina Alam (University of California, Los Angeles), Clayton Schoeny (University of California, Los Angeles), Lara Dolecek (University of California, Los Angeles), and Puneet Gupta (University of California, Los Angeles)</i>	

Workshop on Byzantine Consensus and Resilient Blockchains (BCRB 2018)

BCRB 2018 introduction	121
<i>Alysson Bessani (Universidade de Lisboa, Portugal), Hans P. Reiser (University of Passau, Germany), Marko Vukolic (IBM Zurich, Switzerland), and Tobias Distler (FAU Erlangen-Nürnberg, Germany)</i>	
Protecting Early Stage Proof-of-Work Based Public Blockchain	122
<i>Lin Chen (University of Houston), Lei Xu (University of Houston), Zhimin Gao (University of Houston), Yang Lu (University of Houston), and Weidong Shi (University of Houston)</i>	
Challenges and Pitfalls of Partitioning Blockchains	128
<i>Enrique Fynn (Universita della Svizzera italiana (USI), Switzerland) and Fernando Pedone (Universita della Svizzera italiana (USI), Switzerland)</i>	
Towards Model-Driven Engineering of Smart Contracts for Cyber-Physical Systems	134
<i>Péter Garamvölgyi (Budapest University of Technology and Economics), Imre Kocsis (Budapest University of Technology and Economics), Benjámín Gehl (Budapest University of Technology and Economics), and Attila Klenik (Budapest University of Technology and Economics)</i>	

Latency-Aware Leader Selection for Geo-Replicated Byzantine Fault-Tolerant Systems	140
<i>Michael Eischer (Friedrich-Alexander University Erlangen-Nürnberg (FAU)) and Tobias Distler (Friedrich-Alexander University Erlangen-Nürnberg (FAU))</i>	
Towards Low-Latency Byzantine Agreement Protocols Using RDMA	146
<i>Signe Rüsç (TU Braunschweig), Ines Messadi (TU Braunschweig), and Rüdiger Kapitza (TU Braunschweig)</i>	
Visualizing BFT SMR Distributed Systems - Example of BFT-SMaRt	152
<i>Noëlle Rakotondravony (Universität Passau) and Hans P. Reiser (Universität Passau)</i>	
Dynamic State Partitioning in Parallelized Byzantine Fault Tolerance	158
<i>Bijun Li (TU Braunschweig), Wenbo Xu (TU Braunschweig), and Rüdiger Kapitza (TU Braunschweig)</i>	

3rd Workshop on Security and Dependability of Critical Embedded Real-Time Systems (CERTS 2018)

CERTS 2018 Introduction	164
<i>Mikael Asplund (Linköpings Universitet) and Sabin Mohan (University of Illinois at Urbana-Champaign)</i>	
A Systematic Way to Incorporate Security in Safety Analysis	166
<i>Elena Lisova (Mälardalen University), Aida Caušević (Mälardalen University), Kaj Hänninen (Mälardalen University), Henrik Thane (Mälardalen University), and Hans Hansson (Mälardalen University)</i>	
Design for Dependability Through Error Propagation Space Exploration	172
<i>Imre Kocsis (Budapest University of Technology and Economics)</i>	
Validating and Securing DLMS/COSEM Implementations with the ValiDLMS Framework	179
<i>Henrique Mendes (Universidade de Lisboa, Portugal), Ibéria Medeiros (Universidade de Lisboa, Portugal), and Nuno Neves (Universidade de Lisboa, Portugal)</i>	
Real-Time Security Through a TEE	185
<i>Roberto Duenez (University of Houston) and Albert Mo Kim Cheng (University of Houston)</i>	

Dependable and Secure Machine Learning (DSML 2018)

DSML 2018 Introduction	187
<i>Homa Alemzadeh (University of Virginia, USA), Karthik Pattabiraman (University of British Columbia, BC, Canada), and David E. Evans (University of Virginia, USA)</i>	
Fairness and Transparency of Machine Learning for Trustworthy Cloud Services	188
<i>Nuno Antunes (University of Coimbra, Portugal), Leandro Balby (Universidade Federal de Campina Grande, Brazil), Flavio Figueiredo (Universidade Federal de Minas Gerais, Brazil), Nuno Lourenco (University of Coimbra, Portugal), Wagner Meira Jr. (Universidade Federal de Minas Gerais, Brazil), and Walter Santos (Universidade Federal de Minas Gerais, Brazil)</i>	

Model, Data and Reward Repair: Trusted Machine Learning for Markov Decision Processes	194
<i>Shalini Ghosh, Susmit Jha (SRI International), Ashish Tiwari (Microsoft), Patrick Lincoln (SRI International), and Xiaojin Zhu (Univ. of Wisconsin, Madison)</i>	
On the Limitation of MagNet Defense Against L1-Based Adversarial Examples	200
<i>Pei-Hsuan Lu (National Chung Hsing University), Pin-Yu Chen (AI Foundations Learning Group, IBM Thomas J. Watson Research Center), Kang-Cheng Chen (Yuan Ze University), and Chia-Mu Yu (National Chung Hsing University)</i>	
DCN: Detector-Corrector Network Against Evasion Attacks on Deep Neural Networks	215
<i>Jing Wen (The University of Hong Kong), Lucas C.K. Hui (Hong Kong Applied Science and Technology Research Institute), Siu-Ming Yiu (The University of Hong Kong), and Ruoqing Zhang (The University of Hong Kong)</i>	

4th Workshop on Safety and Security of Intelligent Vehicles (SSIV 2018)

SSIV 2018 Introduction	222
<i>João Carlos Cunha (Centro de Informática e Sistemas da Universidade de Coimbra, Portugal), Kalinka Branco (Universidade de São Paulo, Brazil), and Michaël Lauer (LAAS-CNRS, France)</i>	
Risk Assessment and Security Countermeasures for Vehicular Instrument Clusters	223
<i>Eugen Horatiu Gurban (Politehnica University of Timisoara), Bogdan Groza (Politehnica University of Timisoara), and Pal-Stefan Murvay (Politehnica University of Timisoara)</i>	
Detection of Automotive CAN Cyber-Attacks by Identifying Packet Timing Anomalies in Time Windows	231
<i>Andrew Tomlinson (Coventry University), Jeremy Bryans (Coventry University), Siraj Ahmed Shaikh (Coventry University), and Harsha Kumara Kalutarage (Queen's University Belfast)</i>	
Fuzz Testing for Automotive Cyber-Security	239
<i>Daniel S. Fowler (Coventry University), Jeremy Bryans (Coventry University), Siraj Ahmed Shaikh (Coventry University), and Paul Wooderson (HORIBA MIRA Ltd.)</i>	
Evaluating Optical Flow Vectors Under Varying Computer-Generated Snow Intensities and Pixel Density for Autonomous Vehicles	247
<i>Vikas Agrawal (University of Tuebingen), Marcel Frueh (University of Tuebingen), Oliver Bringmann (University of Tuebingen), and Wolfgang Rosenstiel (University of Tuebingen)</i>	
Prototyping Automotive Smart Ecosystems	255
<i>Emilia Cioroica (Fraunhofer IESE), Thomas Kuhn (Fraunhofer IESE), and Thomas Bauer (Fraunhofer IESE)</i>	
Model-Based Dependability Analysis of Unmanned Aerial Vehicles - A Case Study	263
<i>Matheus Lopes Franco (Universidade de São Paulo), Kalinka R. J. L. Branco (Universidade de São Paulo), Rosana T.V. Braga (Universidade de São Paulo), Andre Luiz de Oliveira (Universidade Federal de Juiz de Fora), Catherine Dezan (Université de Bretagne Occidentale), and Jean-Philippe Diguët (CNRS)</i>	

On the Safety of Automotive Systems Incorporating Machine Learning Based Components: A Position Paper	271
<i>Mohamad Gharib (University of Florence, Italy), Paolo Lollini (University of Florence, Italy), Marco Botta (University of Torino, Italy), Elvio Amparore (University of Torino, Italy), Susanna Donatelli (University of Torino, Italy), and Andrea Bondavalli (University of Florence, Italy)</i>	
FMEDA-Based Fault Injection and Data Analysis in Compliance with ISO-26262	275
<i>Kuen-Long Lu (National Taipei University, Taiwan), Yung-Yuan Chen (National Taipei University, Taiwan), and Li-Ren Huang (Industrial Technology Research Institute (ITRI), Taiwan)</i>	
Author Index	279