

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

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



**IEEE Catalog Number: CFP1941K-POD
ISBN: 978-1-7281-3031-6**

**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:	CFP1941K-POD
ISBN (Print-On-Demand):	978-1-7281-3031-6
ISBN (Online):	978-1-7281-3030-9
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

2019 IEEE/IFIP International Conference on Dependable Systems and Networks Workshops **DSN-W 2019**

Table of Contents

Message from the Workshop Chairs .viii.....	
Message from the DCDS 2019 Organizers .ix.....	
Message from the DSML 2019 Organizers .x.....	
Welcome from the SSIV 2019 Organizers .xi.....	

First Workshop on Data-Centric Dependability and Security (DCDS 2019)

Enhancing Information Sharing and Visualization Capabilities in Security Data Analytic Platforms .1.....	
<i>Gustavo Gonzalez-Granadillo (Atos Research & Innovation, Cybersecurity Laboratory, Spain), Mario Faiella (Atos Research & Innovation, Cybersecurity Laboratory, Spain), Ibéria Medeiros (LASIGE, Faculty of Sciences, University of Lisboa, Portugal), Rui Azevedo (LASIGE, Faculty of Sciences, University of Lisboa, Portugal), and Susana González-Zarzosa (Atos Research & Innovation, Cybersecurity Laboratory, Spain)</i>	
Design of a Classification Model for a Twitter-Based Streaming Threat Monitor .9.....	
<i>Fernando Alves (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal), Pedro Miguel Ferreira (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal), and Alysson Bessani (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal)</i>	
System Misuse Detection Via Informed Behavior Clustering and Modeling .15.....	
<i>Linara Adilova (Fraunhofer IAIS), Livin Natious (Fraunhofer IAIS), Siming Chen (Fraunhofer IAIS, Bonn University), Olivier Thonnard (Amadeus), and Michael Kamp (Fraunhofer IAIS, University Bonn)</i>	

2nd Workshop on Dependable and Secure Machine Learning (DSML 2019)

Adversarial Video Captioning .24.....	
<i>Suman Kalyan Adari (University of Florida), Washington Garcia (University of Florida), and Kevin Butler (University of Florida)</i>	

Universal Adversarial Perturbations for Speech Recognition Systems	
<i>Paarth Neekhara (UC San Diego), Shehzeen Hussain (UC San Diego), Prakhar Pandey (UC San Diego), Shlomo Dubnov (UC San Diego), Julian McAuley (UC San Diego), and Farinaz Koushanfar (UC San Diego)</i>	
Malware Evasion Attack and Defense	34
<i>Yonghong Huang (McAfee LLC), Utkarsh Verma (McAfee LLC), Celeste Fralick (McAfee LLC), Gabriel Infante-Lopez (McAfee LLC), Brajesh Kumar (McAfee LLC), and Carl Woodward (McAfee LLC)</i>	
Mixed Strategy Game Model Against Data Poisoning Attacks	39
<i>Yifan Ou (McMaster University) and Reza Samavi (McMaster University and Vector Institute for Artificial Intelligence)</i>	
NV-DNN: Towards Fault-Tolerant DNN Systems with N-Version Programming	44
<i>Hui Xu (The Chinese University of Hong Kong), Zhuangbin Chen (The Chinese University of Hong Kong), Weibin Wu (The Chinese University of Hong Kong), Zhi Jin (Peking University), Sy-yen Kuo (National Taiwan University), and Michael Lyu (The Chinese University of Hong Kong)</i>	
N-Version Machine Learning Models for Safety Critical Systems	48
<i>Fumio Machida (University of Tsukuba)</i>	
Novelty Detection via Network Saliency in Visual-Based Deep Learning	52
<i>Valerie Chen (Yale University), Man-Ki Yoon (Yale University), and Zhong Shao (Yale University)</i>	
Using Intuition from Empirical Properties to Simplify Adversarial Training Defense	58
<i>Guanxiong Liu (Electrical and Computer Engineering Department, New Jersey Institute of Technology), Issa Khalil (QCRI, Hamad bin Khalifa University), and Abdallah Khreishah (Electrical and Computer Engineering Department, New Jersey Institute of Technology)</i>	

5th International Workshop on Safety and Security of Intelligent Vehicles (SSIV 2019)

Component-Level ASIL Decomposition for Automotive Architectures	62
<i>Alessandro Frigerio (Eindhoven University of Technology), Bart Vermeulen (NXP Semiconductors), and Kees Goossens (Eindhoven University of Technology)</i>	
Autonomous Maneuver Coordination Via Vehicular Communication	70
<i>Wenbo Xu (Institute of Operating Systems and Computer Networks, TU Braunschweig), Alexander Willecke (Institute of Operating Systems and Computer Networks, TU Braunschweig), Martin Wegner (Institute of Operating Systems and Computer Networks, TU Braunschweig), Lars Wolf (Institute of Operating Systems and Computer Networks, TU Braunschweig), and Rüdiger Kapitza (Institute of Operating Systems and Computer Networks, TU Braunschweig)</i>	
Reliability-Driven Task Assignment in Vehicular Crowdsourcing: A Matching Game	78
<i>Talal Halabi (Queen's University) and Mohammad Zulkernine (Queen's University)</i>	

Predictive Runtime Simulation for Building Trust in Cooperative Autonomous Systems .86.....
Emilia Cioroai (Fraunhofer IESE), Daniel Schneider (Fraunhofer IESE), Hanna AlZughbi (Fraunhofer IESE), Jan Reich (Fraunhofer IESE), Rasmus Adler (Fraunhofer IESE), and Tobias Braun (Fraunhofer IESE)

Enabling Security Checking of Automotive ECUs with Formal CSP Models .90.....
John Heneghan (Systems Security Group, Institute of Future Transport and Cities (FTC), Coventry University, United Kingdom), Siraj Ahmed Shaikh (Systems Security Group, Institute of Future Transport and Cities (FTC), Coventry University, United Kingdom), Jeremy Bryans (Systems Security Group, Institute of Future Transport and Cities (FTC), Coventry University, United Kingdom), Madeline Cheah (Horiba MIRA Ltd., Nuneaton, United Kingdom), and Paul Wooderson (Horiba MIRA Ltd., Nuneaton, United Kingdom)

Author Index .99