

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board Members

David Hutchison, UK

Josef Kittler, UK

Friedemann Mattern, Switzerland

Moni Naor, Israel

Bernhard Steffen, Germany

Doug Tygar, USA

Takeo Kanade, USA

Jon M. Kleinberg, USA

John C. Mitchell, USA

C. Pandu Rangan, India

Demetri Terzopoulos, USA

## Formal Methods

Subline of Lectures Notes in Computer Science

## Subline Series Editors

Ana Cavalcanti, *University of York, UK*

Marie-Claude Gaudel, *Université de Paris-Sud, France*

## Subline Advisory Board

Manfred Broy, *TU Munich, Germany*

Annabelle McIver, *Macquarie University, Sydney, NSW, Australia*

Peter Müller, *ETH Zurich, Switzerland*

Erik de Vink, *Eindhoven University of Technology, The Netherlands*

Pamela Zave, *AT&T Laboratories Research, Bedminster, NJ, USA*

More information about this series at <http://www.springer.com/series/7407>

Peter Csaba Ölveczky · Gwen Salaün (Eds.)

# Software Engineering and Formal Methods

17th International Conference, SEFM 2019  
Oslo, Norway, September 18–20, 2019  
Proceedings

*Editors*

Peter Csaba Ölveczky  
University of Oslo  
Oslo, Norway

Gwen Salaün  
University of Grenoble Alpes  
Montbonnot, France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-30445-4

ISBN 978-3-030-30446-1 (eBook)

<https://doi.org/10.1007/978-3-030-30446-1>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This volume contains the proceedings of the 17th International Conference on Software Engineering and Formal Methods (SEFM 2019), which was held during September 18–20, 2019, in Oslo, Norway.

The conference aims to bring together leading researchers and practitioners from academia, industry, and government to advance the state of the art in formal methods, to facilitate their uptake in the software industry, and to encourage their integration within practical software engineering methods and tools.

SEFM 2019 received 89 full paper submissions. Each paper received at least three reviews. Based on the reviews and extensive discussions, the program committee decided to accept 27 papers. This volume contains the revised versions of those 27 papers, which cover a wide variety of topics, including testing, formal verification, program analysis, runtime verification, malware and attack detection, and software development and evolution. The papers address a wide range of systems, such as cyber-physical systems, UAVs, autonomous robots, and feature-oriented and operating systems.

The conference also featured invited talks by Wil van der Aalst (RWTH Aachen University), David Basin (ETH Zürich), and Koushik Sen (University of California, Berkeley). Abstracts of two of these invited talks, and a full paper accompanying the invited talk by van der Aalst, are included in this volume.

Many colleagues and friends contributed to SEFM 2019. We thank Wil van der Aalst, David Basin, and Koushik Sen for accepting our invitations to give invited talks, and the authors who submitted their work to SEFM 2019. We are grateful to the members of the program committee and the external reviewers for providing timely and insightful reviews, as well as for their involvement in the post-reviewing discussions. We would also like to thank the members of the organizing committee, in particular its hard-working co-chair Martin Steffen, for all their work in organizing SEFM 2019, the SEFM steering committee chair Antonio Cerone for useful assistance, the workshop chairs (Javier Camara and Martin Steffen) for supervising the organization of the SEFM 2019 workshops, Lina Marsso for her excellent job attracting submissions, and Ajay Krishna for maintaining the conference web pages.

We appreciated very much the convenience of the EasyChair system for handling the submission and review processes, and for preparing these proceedings. Finally, we gratefully acknowledge financial support from The Research Council of Norway.

September 2019

Peter Csaba Ölveczky  
Gwen Salaün

# Organization

## Program Chairs

Peter Csaba Ölveczky  
Gwen Salaün

University of Oslo, Norway  
University of Grenoble Alpes, France

## Steering Committee

Radu Calinescu  
Antonio Cerone (Chair)  
Rocco De Nicola  
Einar Broch Johnsen  
Peter Csaba Ölveczky  
Gwen Salaün  
Ina Schaefer  
Marjan Sirjani

University of York, UK  
Nazarbayev University, Kazakhstan  
IMT School for Advanced Studies Lucca, Italy  
University of Oslo, Norway  
University of Oslo, Norway  
University of Grenoble Alpes, France  
Technical University of Braunschweig, Germany  
Mälardalen University, Sweden

## Program Committee

Erika Ábrahám  
Cyrille Artho  
Kyungmin Bae

RWTH Aachen University, Germany  
KTH Royal Institute of Technology, Sweden  
Pohang University of Science and Technology,  
South Korea

Olivier Barais  
Luis Barbosa  
Dirk Beyer  
Roberto Bruni  
Ana Cavalcanti  
Alessandro Cimatti  
Robert Clarisó  
Rocco De Nicola  
John Derrick  
José Luiz Fiadeiro  
Osman Hasan

University of Rennes, France  
University of Minho, Portugal  
Ludwig-Maximilian University Munich, Germany  
University of Pisa, Italy  
University of York, UK  
FBK, Italy  
Open University of Catalonia, Spain  
IMT School for Advanced Studies Lucca, Italy  
University of Sheffield, UK  
Royal Holloway, University of London, UK  
National University of Sciences and Technology,  
Pakistan

Klaus Havelund  
Reiko Heckel  
Marieke Huisman  
Alexander Knapp  
Nikolai Kosmatov  
Frédéric Mallet  
Tiziana Margaria

Jet Propulsion Laboratory, USA  
University of Leicester, UK  
University of Twente, The Netherlands  
Augsburg University, Germany  
CEA LIST, France  
University of Nice Sophia Antipolis, France  
Lero, Ireland

Hernán Melgratti	University of Buenos Aires, Argentina
Madhavan Mukund	Chennai Mathematical Institute, India
Peter Csaba Ölveczky	University of Oslo, Norway
Marc Pantel	IRIT, INPT, University of Toulouse, France
Anna Philippou	University of Cyprus, Cyprus
Grigore Rosu	University of Illinois, USA
Gwen Salaün	University of Grenoble Alpes, France
Augusto Sampaio	Federal University of Pernambuco, Brazil
César Sánchez	IMDEA Software Institute, Spain
Ina Schaefer	Technical University of Braunschweig, Germany
Gerardo Schneider	University of Gothenburg, Sweden
Graeme Smith	The University of Queensland, Australia
Jun Sun	Singapore University of Technology and Design, Singapore
Maurice H. ter Beek	ISTI-CNR, Italy
Antonio Vallecillo	University of Málaga, Spain
Dániel Varró	Budapest University of Technology and Economics, Hungary and McGill University, Canada
Heike Wehrheim	University of Paderborn, Germany
Franz Wotawa	University of Graz, Austria

## External Reviewers

Yehia Abd	Karlheinz Friedberger
Michael Abir	Letterio Galletta
Waqar Ahmad	Luca Geatti
Alif Akbar Pranata	Alberto Griggio
Pedro Antonino	Rebecca Haehn
Sebastien Bardin	Patrick Healy
Flavia Barros	Omar Inverso
Sarah Beecham	Shaista Jabeen
Chiara Bodei	Cyrille Jegourel
Johann Bourcier	Seema Jehan
Marco Bozzano	Richard Johansson
Antonio Bucchiarone	Sebastiaan Joosten
Márton Búr	Georgia Kapitsaki
Nathalie Cauchi	Alexander Knüppel
Gabriele Costa	Jürgen König
Ferruccio Damiani	Ajay Krishna
Luca Di Stefano	Dimitrios Kouzapas
Gidon Ernst	Sophie Lathouwers
Alessandro Fantechi	Jean-Christophe Léchenet
Alessio Ferrari	Thomas Lemberger
Michael Foster	Yun Lin
Leo Freitas	Sascha Lity

Piergiuseppe Mallozzi  
Carlos Matos  
Ilaria Matteucci  
Marcel Vinicius Medeiros Oliveira  
Vince Molnár  
Carlo Montangero  
Raul Monti  
Alexandre Mota  
Vadim Mutilin  
Sidney C. Nogueira  
Dan O’Keeffe  
Wytse Oortwijn  
Felix Pauck  
Karen Petrie  
Marinella Petrocchi  
Pablo Picazo-Sanchez  
Virgile Prevosto  
Adnan Rashid

Virgile Robles  
Marco Roveri  
Tobias Runge  
Stefan Schupp  
Alexander Schlie  
Oszkár Semeráth  
Umair Siddique  
Arnab Sharma  
Ling Shi  
Martin Spiessl  
Ketil Stølen  
Ivan Stojic  
Ibrahim Tariq-Javed  
Manuel Toews  
Stefano Tonetta  
Evangelia Vanezi  
Philipp Wendler



## **Abstracts of Invited Talks**

# Security Protocols: Model Checking Standards

David Basin

Department of Computer Science, ETH Zurich, Switzerland

The design of security protocols is typically approached as an art, rather than a science, and often with disastrous consequences. But this need not be so! I have been working for ca. 20 years on foundations, methods, and tools, both for developing protocols that are correct by construction [9, 10] and for the post-hoc verification of existing designs [1–4, 8]. In this talk I will introduce my work in this area and describe my experience analyzing, improving, and contributing to different industry standards, both existing and upcoming [5–7].

## References

1. Basin, D.: Lazy infinite-state analysis of security protocols. In: Secure Networking—CQRE [Secure] 1999. LNCS, vol.1740, pp. 30–42. Springer-Verlag, Düsseldorf, November 1999
2. Basin, D., Cremers, C., Dreier, J., Sasse, R.: Symbolically analyzing security protocols using tamarin. SIGLOG News **4**(4), 19–30 (2017). <https://doi.org/10.1145/3157831.3157835>
3. Basin, D., Cremers, C., Meadows, C.: Model checking security protocols. In: Clarke, E., Henzinger, T., Veith, H., Bloem, R. (eds.) Handbook of Model Checking, pp. 727–762. Springer, Cham (2018). [https://doi.org/10.1007/978-3-319-10575-8\\_22](https://doi.org/10.1007/978-3-319-10575-8_22)
4. Basin, D., Mödersheim, S., Viganò, L.: OFMC: a symbolic model checker for security protocols. Int. J. Inf. Secur. **4**(3), 181–208 (2005). Published online December 2004
5. Basin, D., Cremers, C., Meier, S.: Provably repairing the ISO/IEC 9798 standard for entity authentication. J. Comput. Secur. **21**(6), 817–846 (2013)
6. Basin, D., Cremers, C.J.F., Miyazaki, K., Radomirovic, S., Watanabe, D.: Improving the security of cryptographic protocol standards. IEEE Secur. Privac. **13**(3), 24–31 (2015). <https://doi.org/10.1109/MSP.2013.162>
7. Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V.: Formal analysis of 5G authentication. In: Proceedings of the 2018 ACM Conference on Computer and Communications Security (CCS), pp. 1383–1396 (2018)
8. Schmidt, B., Meier, S., Cremers, C., Basin, D.: Automated analysis of Diffie-Hellman protocols and advanced security properties. In: Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF), pp. 78–94 (2012)
9. Sprenger, C., Basin, D.: Refining key establishment. In: Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF), pp. 230–246 (2012)
10. Sprenger, C., Basin, D.: Refining security protocols. J. Comput. Secur. **26**(1), 71–120 (2018). <https://doi.org/10.3233/JCS-16814>

# Automated Test Generation: A Journey from Symbolic Execution to Smart Fuzzing and Beyond

Koushik Sen

EECS Department, UC Berkeley, CA, USA  
ksen@cs.berkeley.edu

**Abstract.** In the last two decades, automation has had a significant impact on software testing and analysis. Automated testing techniques, such as symbolic execution, concolic testing, and feedback-directed fuzzing, have found numerous critical faults, security vulnerabilities, and performance bottlenecks in mature and well-tested software systems. The key strength of automated techniques is their ability to quickly search state spaces by performing repetitive and expensive computational tasks at a rate far beyond the human attention span and computation speed. In this talk, I will give a brief overview of our past and recent research contributions in automated test generation using symbolic execution, program analysis, constraint solving, and fuzzing. I will also describe a new technique, called constraint-directed fuzzing, where given a pre-condition on a program as a logical formula, we can efficiently generate millions of test inputs satisfying the pre-condition.

# Contents

## Invited Paper

Object-Centric Process Mining: Dealing with Divergence and Convergence in Event Data . . . . .	3
<i>Wil M. P. van der Aalst</i>	

## Cooperative Asynchronous Systems

Relating Session Types and Behavioural Contracts: The Asynchronous Case. . . . .	29
<i>Mario Bravetti and Gianluigi Zavattaro</i>	
Asynchronous Cooperative Contracts for Cooperative Scheduling . . . . .	48
<i>Eduard Kamburjan, Crystal Chang Din, Reiner Hähnle, and Einar Broch Johnsen</i>	

## Cyber-Physical Systems

Automatic Failure Explanation in CPS Models . . . . .	69
<i>Ezio Bartocci, Niveditha Manjunath, Leonardo Mariani, Cristinel Mateis, and Dejan Ničković</i>	
Evolution of Formal Model-Based Assurance Cases for Autonomous Robots. . . . .	87
<i>Mario Gleirscher, Simon Foster, and Yakoub Nemouchi</i>	
Towards Integrating Formal Verification of Autonomous Robots with Battery Prognostics and Health Management . . . . .	105
<i>Xingyu Zhao, Matt Osborne, Jenny Lantair, Valentin Robu, David Flynn, Xiaowei Huang, Michael Fisher, Fabio Papacchini, and Angelo Ferrando</i>	

## Feature-Oriented and Versioned Systems

SAT Encodings of the At-Most- $k$ Constraint: A Case Study on Configuring University Courses . . . . .	127
<i>Paul Maximilian Bittner, Thomas Thüm, and Ina Schaefer</i>	
Software Evolution with a Typeful Version Control System . . . . .	145
<i>Luís Carvalho and João Costa Seco</i>	

Compositional Feature-Oriented Systems . . . . .	162
<i>Clemens Dubslaff</i>	
<b>Model-Based Testing</b>	
Multi-objective Search for Effective Testing of Cyber-Physical Systems. . . . .	183
<i>Hugo Araujo, Gustavo Carvalho, Mohammad Reza Mousavi, and Augusto Sampaio</i>	
Mutation Testing with Hyperproperties . . . . .	203
<i>Andreas Fellner, Mitra Tabaei Befrouei, and Georg Weissenbacher</i>	
Test Model Coverage Analysis Under Uncertainty. . . . .	222
<i>I. S. W. B. Prasetya and Rick Klomp</i>	
<b>Model Inference</b>	
Learning Minimal DFA: Taking Inspiration from RPNI to Improve SAT Approach. . . . .	243
<i>Florent Avellaneda and Alexandre Petrenko</i>	
Incorporating Data into EFSM Inference . . . . .	257
<i>Michael Foster, Achim D. Brucker, Ramsay G. Taylor, Siobhán North, and John Derrick</i>	
<b>Ontologies and Machine Learning</b>	
Isabelle/DOF: Design and Implementation . . . . .	275
<i>Achim D. Brucker and Burkhart Wolff</i>	
Towards Logical Specification of Statistical Machine Learning . . . . .	293
<i>Yusuke Kawamoto</i>	
<b>Operating Systems</b>	
Efficient Formal Verification for the Linux Kernel . . . . .	315
<i>Daniel Bristot de Oliveira, Tommaso Cucinotta, and Rômulo Silva de Oliveira</i>	
Reproducible Execution of POSIX Programs with DiOS. . . . .	333
<i>Petr Ročkal, Zuzana Baranová, Jan Mrázek, Katarína Kejstová, and Jiří Barnat</i>	

## Program Analysis

Using Relational Verification for Program Slicing . . . . .	353
<i>Bernhard Beckert, Thorsten Bormer, Stephan Gocht, Mihai Herda, Daniel Lentzsch, and Mattias Ulbrich</i>	
Local Nontermination Detection for Parallel C++ Programs . . . . .	373
<i>Vladimír Štill and Jiří Barnat</i>	

## Relating Models and Implementations

An Implementation Relation for Cyclic Systems with Refusals and Discrete Time. . . . .	393
<i>Raluca Lefticaru, Robert M. Hierons, and Manuel Núñez</i>	
Modular Indirect Push-Button Formal Verification of Multi-threaded Code Generators . . . . .	410
<i>Anton Wijs and Maciej Wilkowski</i>	

## Runtime Verification

An Operational Guide to Monitorability . . . . .	433
<i>Luca Aceto, Antonis Achilleos, Adrian Francalanza, Anna Ingólfssdóttir, and Karoliina Lehtinen</i>	
Let's Prove It Later—Verification at Different Points in Time . . . . .	454
<i>Martin Ring and Christoph Lüth</i>	

## Security

Using Threat Analysis Techniques to Guide Formal Verification: A Case Study of Cooperative Awareness Messages . . . . .	471
<i>Marie Farrell, Matthew Bradbury, Michael Fisher, Louise A. Dennis, Clare Dixon, Hu Yuan, and Carsten Maple</i>	
Towards Detecting Trigger-Based Behavior in Binaries: Uncovering the Correct Environment . . . . .	491
<i>Dorottya Papp, Thorsten Tarrach, and Levente Buttyán</i>	

## Verification

Formal Verification of Rewriting Rules for Dynamic Fault Trees . . . . .	513
<i>Yassmeen Elderhalli, Matthias Volk, Osman Hasan, Joost-Pieter Katoen, and Sofiène Tahar</i>	

<b>Partially Bounded Context-Aware Verification . . . . .</b>	<b>532</b>
<i>Luka Le Roux and Ciprian Teodorov</i>	
<b>Author Index . . . . .</b>	<b>549</b>