Lecture Notes in Computer Science **11724**

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

Springer

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	University of Oslo, Norway
Gwen Salaün	University of Grenoble Alpes, France

Steering Committee

Radu Calinescu	University of York, UK
Antonio Cerone (Chair)	Nazarbayev University, Kazakhstan
Rocco De Nicola	IMT School for Advanced Studies Lucca, Italy
Einar Broch Johnsen	University of Oslo, Norway
Peter Csaba Ölveczky	University of Oslo, Norway
Gwen Salaün	University of Grenoble Alpes, France
Ina Schaefer	Technical University of Braunschweig, Germany
Marjan Sirjani	Mälardalen University, Sweden

Program Committee

Erika Ábrahám	RWTH Aachen University, Germany
Cyrille Artho	KTH Royal Institute of Technology, Sweden
Kyungmin Bae	Pohang University of Science and Technology, South Korea
Olivier Barais	University of Rennes, France
Luis Barbosa	University of Minho, Portugal
Dirk Beyer	Ludwig-Maximilian University Munich, Germany
Roberto Bruni	University of Pisa, Italy
Ana Cavalcanti	University of York, UK
Alessandro Cimatti	FBK, Italy
Robert Clarisó	Open University of Catalonia, Spain
Rocco De Nicola	IMT School for Advanced Studies Lucca, Italy
John Derrick	University of Sheffield, UK
José Luiz Fiadeiro	Royal Holloway, University of London, UK
Osman Hasan	National University of Sciences and Technology, Pakistan
Klaus Havelund	Jet Propulsion Laboratory, USA
Reiko Heckel	University of Leicester, UK
Marieke Huisman	University of Twente, The Netherlands
Alexander Knapp	Augsburg University, Germany
Nikolai Kosmatov	CEA LIST, France
Frédéric Mallet	University of Nice Sophia Antipolis, France
Tiziana Margaria	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
Michael Abir
Waqar Ahmad
Alif Akbar Pranata
Pedro Antonino
Sebastien Bardin
Flavia Barros
Sarah Beecham
Chiara Bodei
Johann Bourcier
Marco Bozzano
Antonio Bucchiarone
Márton Búr
Nathalie Cauchi
Gabriele Costa
Ferruccio Damiani
Luca Di Stefano
Gidon Ernst
Alessandro Fantechi
Alessio Ferrari
Michael Foster
Leo Freitas
Karlheinz Friedberger
Letterio Galletta
Luca Geatti
Alberto Griggio
Rebecca Haehn
Patrick Healy
Omar Inverso
Shaista Jabeen
Cyrille Jegourel
Seema Jehan
Richard Johansson
Sebastiaan Joosten
Georgia Kapitsaki
Alexander Knüppel
Jürgen König
Ajay Krishna
Dimitrios Kouzapas
Sophie Lathouwers
Jean-Christophe Léchenet
Thomas Lemberger
Yun Lin
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
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

Program Analysis

Relating Models and Implementations

Runtime Verification

Security

Verification