

## Founding Editors

Gerhard Goos, Germany  
Juris Hartmanis, USA

## Editorial Board Members

Elisa Bertino, USA  
Wen Gao, China  
Bernhard Steffen , Germany

Gerhard Woeginger , Germany  
Moti Yung, 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>


Frank de Boer · Antonio Cerone (Eds.)

# Software Engineering and Formal Methods

18th International Conference, SEFM 2020  
Amsterdam, The Netherlands, September 14–18, 2020  
Proceedings

*Editors*

Frank de Boer  
Informatica  
Centrum voor Wiskunde  
en Informatica (CWI)  
Amsterdam, The Netherlands

Antonio Cerone   
Department of Computer Science  
Nazarbayev University  
Astana, Kazakhstan

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-58767-3              ISBN 978-3-030-58768-0 (eBook)  
<https://doi.org/10.1007/978-3-030-58768-0>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2020

Chapters 1, 7 and 8 are licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapters.

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 18th International Conference on Software Engineering and Formal Methods (SEFM 2020), which was originally planned to take place during September 14–18, 2020, in Amsterdam, The Netherlands (hosted by the Centrum Wiskunde & Informatica – CWI). Because of the COVID-19 pandemic, SEFM 2020 could not take place physically but had to be replaced by a virtual event (still held during September 14–18, 2020).

The general aim of the conference is 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.

There were 58 full paper submissions, which were reviewed for quality, correctness, originality, and relevance. Each submission was reviewed by four Program Committee Members and an online post-reviewing discussion, open to the entire Program Committee, was held to make the final decisions. The committee decided to accept 16 papers (27.6% acceptance rate). This volume contains the revised versions of those 16 papers, which cover a wide variety of topics, including testing, formal verification, program analysis, runtime verification, meta-programming, and software development and evolution. The papers address a wide range of systems, such as IoT systems, human-robot interaction in healthcare scenarios, navigation of maritime autonomous systems, and operating systems.

The conference program also featured three keynote talks by Paola Inverardi (University of L’Aquila, Italy), Roberto Di Cosmo (Paris Diderot University, France), and Eelco Visser (Delft University of Technology, The Netherlands). This volume includes an extended abstract of Paola Inverardi’s talk titled “A Software Exoskeleton to Protect Ethics and Privacy of Users in the Digital World” and a full paper of Eelco Visser’s talk titled “Multi-Purpose Syntax Definition with SDF3” – co-authored by Luís Eduardo de Souza Amorim.

We would like to thank Paola Inverardi, Roberto Di Cosmo, and Eelco Visser for accepting our invitations to give keynote talks, and the authors who submitted their work to SEFM 2020. 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 SEFM Steering Committee for their advices and support, the workshop co-chairs Loek Cleophas (TU/e, The Netherlands) and Mieke Massink (ISTI, Italy), Jacopo Mauro (SDU, Denmark) for taking care of the publicity, and Hans-Dieter Hiep and Benjamin Lion (CWI, The Netherlands) for setting up and maintaining the conference web pages. We would like to thank all people involved in SEFM 2020 for their contributions in these exceptional circumstances of the COVID-19 pandemic.

We greatly appreciated the convenience of the EasyChair system for handling the submission and review processes, and for preparing these proceedings. Finally, we gratefully acknowledge the technical support from CWI.

July 2020

Frank de Boer  
Antonio Cerone

# Organization

## Program Co-chairs

Frank de Boer  
Antonio Cerone

CWI, The Netherlands  
Nazarbayev University, Kazakhstan

## Steering Committee

Frank de Boer  
Radu Calinescu  
Antonio Cerone (Chair)  
Rocco De Nicola  
Peter Ölveczky  
Gwen Salaï  
Marjan Sirjani

CWI, The Netherlands  
University of York, UK  
Nazarbayev University, Kazakhstan  
IMT Lucca, Italy  
University of Oslo, Norway  
University of Grenoble Alpes, France  
Malardalen University, Sweden

## Program Committee

Erika Abraham  
Wolfgang Ahrendt  
Alessandro Aldini  
Luís Soares Barbosa  
Maurice H. ter Beek  
Dirk Beyer  
Frank de Boer  
Ana Cavalcanti  
Antonio Cerone  
Alessandro Cimatti  
Marieke Huisman  
Alexander Knapp  
Tiziana Margaria  
Paolo Masci  
Jacopo Mauro  
Peter Müller  
Hans de Nivelle  
Catuscia Palamidessi  
Anna Philippou  
Ka I. Pun

RWTH Aachen University, Germany  
Chalmers University of Technology, Sweden  
University of Urbino, Italy  
University of Minho, Portugal  
ISTI-CNR, Italy  
LMU Munich, Germany  
CWI, The Netherlands  
University of York, UK  
Nazarbayev University, Kazakhstan  
Fondazione Bruno Kessler, Italy  
University of Twente, The Netherlands  
Universität Augsburg, Germany  
Lero, Ireland  
National Institute of Aerospace (NIA), USA  
University of Oslo, Norway  
ETH Zurich, Switzerland  
Nazarbayev University, Kazakhstan  
Inria, France  
University of Cyprus, Cyprus  
Western Norway University of Applied Sciences,  
Norway  
University of Illinois at Urbana-Champaign, USA  
University of Grenoble Alpes, France  
Federal University of Pernambuco, Brazil

Grigore Rosu  
Gwen Salaün  
Augusto Sampaio

Ina Schaefer	Technische Universität Braunschweig, Germany
Gerardo Schneider	Chalmers—University of Gothenburg, Sweden
Roberto Segala	University of Verona, Italy
Marjan Sirjani	Malardalen University, Sweden
Martin Steffen	University of Oslo, Norway
Meng Sun	Peking University, China
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway
Simone Tini	University of Insubria, Italy
Elena Troubitsyna	KTH Royal Institute of Technology, Sweden
M. Birna van Riemsdijk	University of Twente, The Netherlands
Heike Wehrheim	University of Paderborn, Germany
Gianluigi Zavattaro	University of Bologna, Italy
Peter Ölveczky	University of Oslo, Norway

### **Additional Reviewers**

Abbaspour Asadollah, Sara	Kristensen, Lars
Amadini, Roberto	König, Jürgen
Antonino, Pedro	Lanotte, Ruggero
Attala, Ziggy	Lathouwers, Sophie
Bagheri, Maryam	Lee, Nian-Ze
Basile, Davide	Lemberger, Thomas
Baxter, James	Lu, Yuteng
Bordis, Tabea	Madeira, Alexandre
Broccia, Giovanna	Mallozzi, Piergiuseppe
Bugariu, Alexandra	Matheja, Christoph
Castiglioni, Valentina	Mazzanti, Franco
Chimento, Jesus Mauricio	Miranda, Breno
Cledou, Guillermina	Monti, Raúl E.
Clochard, Martin	Mota, Alexandre
Din, Crystal Chang	Neves, Renato
Eilers, Marco	Nieke, Michael
Enoiu, Eduard Paul	Oortwijn, Wytse
Filipovikj, Predrag	Park, Daejun
Fontaine, Pascal	Pauck, Felix
Friedberger, Karlheinz	Paulson, Lawrence
Giallorenzo, Saverio	Rasouli, Peyman
Haltermann, Jan	Richter, Cedric
Hnetyuka, Petr	Runge, Tobias
Holzner, Stephan	Safari, Mohsen
Iyoda, Julianio	Sankaranarayanan, Sriram
Khamespanah, Ehsan	Schlatte, Rudolf
Knüppel, Alexander	Sedaghatbaf, Ali
Kouzapas, Dimitrios	Serwe, Wendelin
Krishna, Ajay	Sewell, Thomas



Sharma, Arnab  
Spiessl, Martin  
Steffen, Bernhard  
Steffen, Martin  
Steinhöfel, Dominic  
Stolz, Volker  
Sun, Weidi  
Syeda, Hira  
Tschaikowski, Max

Turin, Gianluca  
Tveito, Lars  
Valencia, Frank  
van den Bos, Petra  
Vandin, Andrea  
Wendler, Philipp  
Windsor, Matt  
Zhang, Xiyue  
Zhang, Yi

# **A Software Exoskeleton to Protect Ethics and Privacy of Users in the Digital World (Abstract of a Keynote Talk)**

Paola Inverardi

Università dell'Aquila, L'Aquila, Italy

**Abstract.** In recent years there has been an increasingly amount of interest on the impact that the digital society can have on the fundamental rights of individual, citizens and societies. Starting from the raising of the economy of data to the appearance of the present and future AI fueled autonomous systems the level of attention has lifted from privacy concerns to more general ethical ones [6, 7]. Although there is a general consensus on the vulnerability of users and societies this perspective has been only followed by the regulatory approach that by putting at work new regulations, notably GDPR has effectively enhanced the protection of users. Differently, in research the approach is mainly focusing on AI and concerns the systems/software developers and companies by proposing code of ethics and guidelines for the development of trustworthy systems in order to achieve transparency, accountability and explainability of decisions [1, 5].

Therefore, despite the claim for a human centric AI and the recommendation to empower the user, the user is left unpaired in her interactions with digital systems beyond the basic choice of accepting or not accepting the interaction with a system with all the consequences this might imply. From the case of privacy preferences in the app domain [12] to the more complex case of autonomous driving cars [4] the average user is unprotected and inadequate in her interaction with the digital world. In the talk I will present the approach and preliminary results undertaken in the project EXOSOUL [2, 8–11] that stands on the side of users. EXOSOUL aims at equipping humans with an automatically generated exoskeleton, a software shield that protects and empowers them and their personal data in all interactions with the digital world by mediating or discarding those ones that would result in unacceptable or morally wrong behaviors according to the user's ethical and privacy preferences [3].

**Keywords:** Ethics · Privacy · Software exoskeleton

## References

1. European commission: White paper on artificial intelligence. <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020-en.pdf>
2. Autili, M., DiRuscio, D., Inverardi, P., Pelliccione, P., Tivoli, M.: A software exoskeleton to protect and support citizen's ethics and privacy in the digital world. *IEEE Access* **7**, 62011–62021 (2019). <https://doi.org/10.1109/access.2019.2916203>
3. Autili, M., Inverardi, P., Spalazzese, R., Tivoli, M., Mignosi, F.: Automated synthesis of application-layer connectors from automata-based specifications. *J. Comput. Syst. Sci.* **104**, 17–40 (2019). <https://doi.org/10.1016/j.jcss.2019.03.001>
4. Awad, E., et al.: The moral machine experiment. *Nature* **563**, 59–64 (2018). <https://doi.org/10.1038/s41586-018-0637-6>
5. Commission, E.: High-level expert group on artificial intelligence: Ethics guidelines for trustworthy ai (2019)
6. Floridi, L.: Soft ethics and the governance of the digital. *Philos. Technol.* **31**(1), 1–8 (2018). <https://doi.org/10.1007/s13347-018-0303-9>
7. Inverardi, P.: The european perspective on responsible computing. *Commun. ACM* **62**(4), 64–64 (2019). <http://doi.acm.org/10.1145/3311783>
8. Migliarini, P., Scoccia, G.L., Autili, M., Inverardi, P.: On the elicitation of privacy and ethics preferences of mobile users. In: 7th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft 2020), Vision Track (2020)
9. Scoccia, G.L., Autili, M., Inverardi, P.: A self-configuring and adaptive privacy-aware permission system for android apps. In: 1st IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS 2020) (2020)
10. Scoccia, G.L., Fiore, M.M., Pelliccione, P., Autili, M., Inverardi, P., Russo, A.: Hey, my data are mine! active data to empower the user. In: IEEE/ACM 39th International Conference on Software Engineering (ICSE 2017) (ICSE2020-NIER) (2020)
11. Scoccia, G.L., Malavolta, I., Autili, M., DiSalle, A., Inverardi, P.: Enhancing trustability of android applications via user-centric flexible permissions. *IEEE Trans. Softw. Eng.* (2019). <https://doi.org/10.1109/tse.2019.2941936>
12. Scoccia, G.L., Ruberto, S., Malavolta, I., Autili, M., Inverardi, P.: An investigation into android run-time permissions from the end users' perspective. In: 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft 2018) (2018)

# Contents

Multi-purpose Syntax Definition with SDF3 . . . . .	1
<i>Luís Eduardo de Souza Amorim and Eelco Visser</i>	
Finding and Fixing a Mismatch Between the Go Memory Model and Data-Race Detector: A Story on Applied Formal Methods . . . . .	24
<i>Daniel Schnetzer Fava</i>	
Formal Verification of COLREG-Based Navigation of Maritime Autonomous Systems . . . . .	41
<i>Fatima Shokri-Manninen, Jüri Vain, and Marina Waldén</i>	
End-to-End Verification of Initial and Transition Properties of GR(1) Designs in SPARK . . . . .	60
<i>Laura R. Humphrey, James Hamil, and Joffrey Hugué</i>	
Affine Systems of ODEs in Isabelle/HOL for Hybrid-Program Verification . . . .	77
<i>Jonathan Julián Huerta y Munive</i>	
Interoperability and Integration Testing Methods for IoT Systems: A Systematic Mapping Study . . . . .	93
<i>Miroslav Bures, Matej Klima, Vaclav Rechtberger, Xavier Bellekens, Christos Tachtatzis, Robert Atkinson, and Bestoun S. Ahmed</i>	
FRÉD: Conditional Model Checking via Reducers and Folders . . . . .	113
<i>Dirk Beyer and Marie-Christine Jakobs</i>	
Difference Verification with Conditions . . . . .	133
<i>Dirk Beyer, Marie-Christine Jakobs, and Thomas Lemberger</i>	
A Formal Modeling Approach for Portable Low-Level OS Functionality . . . .	155
<i>Renata Martins Gomes, Bernhard Aichernig, and Marcel Baunach</i>	
Model-Based Testing Under Parametric Variability of Uncertain Beliefs . . . .	175
<i>Matteo Camilli and Barbara Russo</i>	
Hoare-Style Logic for Unstructured Programs . . . . .	193
<i>Didrik Lundberg, Roberto Guanciale, Andreas Lindner, and Mads Dam</i>	
Synthesis of P-Stable Abstractions. . . . .	214
<i>Anna Becchi, Alessandro Cimatti, and Enea Zaffanella</i>	

**Runtime Verification of Contracts with Themulus . . . . .** 231  
*Alberto Aranda García, María-Emilia Cambroner, Christian Colombo,  
Luis Llana, and Gordon J. Pace*

**Sound C Code Decompilation for a Subset of x86-64 Binaries . . . . .** 247  
*Freek Verbeek, Pierre Olivier, and Binoy Ravindran*

**Statically Checking REST API Consumers. . . . .** 265  
*Nuno Burnay, Antónia Lopes, and Vasco T. Vasconcelos*

**A Layered Implementation of DR-BIP Supporting Run-Time Monitoring  
and Analysis. . . . .** 284  
*Antoine El-Hokayem, Saddek Bensalem, Marius Bozga,  
and Joseph Sifakis*

**Formal Verification of Human-Robot Interaction in Healthcare Scenarios. . . . .** 303  
*Livia Lestingi, Mehrnoosh Askarpour, Marcello M. Bersani,  
and Matteo Rossi*

**Author Index . . . . .** 325