Lecture Notes in Computer Science 11535

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7408

Jorge A. Pérez · Nobuko Yoshida (Eds.)

Formal Techniques for Distributed Objects, Components, and Systems

39th IFIP WG 6.1 International Conference, FORTE 2019
Held as Part of the 14th International Federated Conference on Distributed Computing Techniques, DisCoTec 2019
Kongens Lyngby, Denmark, June 17–21, 2019
Proceedings

Springer

Editors
Jorge A. Pérez
University of Groningen
Groningen, The Netherlands

Nobuko Yoshida
Imperial College London
London, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-21758-7 ISBN 978-3-030-21759-4 (eBook)
https://doi.org/10.1007/978-3-030-21759-4

LNCS Sublibrary: SL2 – Programming and Software Engineering

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

Foreword

The 14th International Federated Conference on Distributed Computing Techniques (DisCoTec) took place in Kongens Lyngby, Denmark, during June 17–21, 2019. It was organized by the Department of Applied Mathematics and Computer Science at the Technical University of Denmark.

The DisCoTec series is one of the major events sponsored by the International Federation for Information Processing (IFIP). It comprised three conferences:

- COORDINATION, the IFIP WG 6.1 21st International Conference on Coordination Models and Languages
- DAIS, the IFIP WG 6.1 19th International Conference on Distributed Applications and Interoperable Systems
- FORTE, the IFIP WG 6.1 39th International Conference on Formal Techniques for Distributed Objects, Components and Systems

Together, these conferences cover a broad spectrum of distributed computing subjects, ranging from theoretical foundations and formal description techniques to systems research issues.

In addition to the individual sessions of each conference, the event included several plenary sessions that gathered attendants from the three conferences. This year, the general chair and the DisCoTec Steering Committee joined the three DisCoTec conferences in the selection and nomination of the plenary keynote speakers, whose number was accordingly increased from the traditional three to five. The five keynote speakers and the title of their talks are listed below:

- Prof. David Basin (ETH Zürich, Switzerland) – "Security Protocols: Model Checking Standards"
- Dr. Anne-Marie Kermarrec (Inria Rennes, France) – "Making Sense of Fast Big Data"
- Prof. Marta Kwiatkowska (University of Oxford, UK) – "Versatile Quantitative Modelling: Verification, Synthesis and Data Inference for Cyber-Physical Systems"
- Prof. Silvio Micali (MIT, USA)—"ALGORAND—The Distributed Ledger for the Borderless Economy"
- Prof. Martin Wirsing (LMU, Germany) – "Toward Formally Designing Collective Adaptive Systems"

As is traditional in DisCoTec, an additional joint session with the best papers from each conference was organized. The best papers were:

- "Representing Dependencies in Event Structures" by G. Michele Pinna (Coordination)
- "FOUGERE: User-Centric Location Privacy in Mobile Crowdsourcing Apps" by Lakhdar Meftah, Romain Rouvoy and Isabelle Chrisment (DAIS)

- "Psi-Calculi Revisited: Connectivity and Compositionality" by Johannes Åman Pohjola (FORTE)

Associated with the federated event were also two satellite events that took place:

- ICE, the 12th International Workshop on Interaction and Concurrency Experience
- DisCoRail, the First International Workshop on Distributed Computing in Future Railway Systems

I would like to thank the Program Committee chairs of the different events for their help and cooperation during the preparation of the conference, and the Steering Committee and Advisory Boards of DisCoTec and their conferences for their guidance and support. The organization of DisCoTec 2019 was only possible thanks to the dedicated work of the Organizing Committee, including Francisco "Kiko" Fernández Reyes and Francesco Tiezzi (publicity chairs), Maurice ter Beek, Valerio Schiavoni, and Andrea Vandin (workshop chairs), Ann-Cathrin Dunker (logistics and finances), as well as all the students and colleagues who volunteered their time to help. Finally, I would like to thank IFIP WG 6.1 for sponsoring this event, Springer's *Lecture Notes in Computer Science* team for their support and sponsorship, EasyChair for providing the reviewing infrastructure, the Nordic IoT Hub for their sponsorship, and the Technical University of Denmark for providing meeting rooms and additional support.

June 2019 Alberto Lluch Lafuente

Preface

This volume contains the papers presented at FORTE 2019: the 39th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems. FORTE 2019 was held as one of three main conferences of the 14th International Federated Conference on Distributed Computing Techniques (DisCoTec), during June 17–21, 2019 in Lyngby, Denmark.

FORTE is a well-established forum for fundamental research on theory, models, tools, and applications for distributed systems, with special interest in:

- Software quality, reliability, availability, and safety
- Security, privacy, and trust in distributed and/or communicating systems
- Service-oriented, ubiquitous, and cloud computing systems
- Component- and model-based design
- Object technology, modularity, software adaptation
- Self-stabilization and self-healing/organizing
- Verification, validation, formal analysis, and testing of the above

The Program Committee received a total of 42 quality submissions, written by authors from 21 different countries. Of these, 18 papers were selected for inclusion in the scientific program: 15 full papers, one short paper, and two "journal first" papers—a new submission category we introduced this year. Each submission was reviewed by at least three Program Committee members with the help of external reviewers in selected cases. There was one submission with which both of us declared ourselves in conflict; Uwe Nestmann kindly agreed to oversee and lead the discussion for this submission, which was eventually accepted.

The selection of accepted submissions was based on electronic discussions via the EasyChair conference management system. Toward the end of this electronic discussion, there was a two-day physical meeting in which we discussed the referee reports for each submission with the relevant Program Committee members. We found this combination of electronic and physical discussion highly effective.

As program chairs, we actively contributed to the selection of the five keynote speakers of DisCoTec 2019:

- Prof. David Basin (ETH Zürich, Switzerland)
- Dr. Anne-Marie Kermarrec (Inria Rennes, France)
- Prof. Marta Kwiatkowska (University of Oxford, UK)
- Prof. Silvio Micali (MIT, USA)
- Prof. Martin Wirsing (LMU, Germany)

We are most grateful to Prof. Basin for accepting our invitation as FORTE-related keynote speaker. This volume includes the abstract of his keynote talk: "Security Protocols: Model Checking Standards."

As is traditional in DisCoTec, a joint session with the best papers from each main conference was organized. The best paper of FORTE 2019 was "Psi-Calculi Revisited: Connectivity and Compositionality" by Johannes Åman Pohjola (Data61/CSIRO, University of New South Wales, Australia).

We wish to thank all the authors of submitted papers, all the members of the Program Committee for their thorough evaluations of the submissions, and the 26 external reviewers who assisted the evaluation process. We are also indebted to the Steering Committee of FORTE for their advice and suggestions. Last but not least, we thank the DisCoTec general chair, Alberto Lluch Lafuente, and his organization team for their hard, effective work on providing an excellent environment for FORTE 2019 and all other conferences and workshops.

April 2019

Jorge A. Pérez
Nobuko Yoshida

Organization

Program Committee

Samik Basu	Iowa State University, USA
Annette Bieniusa	University of Kaiserslautern, Germany
Stefano Calzavara	Università Ca' Foscari Venezia, Italy
Natalia Chechina	Bournemouth University, UK
Mila Dalla Preda	University of Verona, Italy
Rayna Dimitrova	University of Leicester, UK
Patrick Eugster	University of Lugano (USI), Switzerland
Ichiro Hasuo	National Institute of Informatics, Japan
Thomas Hildebrandt	University of Copenhagen, Denmark
Sophia Knight	University of Minnesota, USA
Etienne Lozes	I3S, University of Nice and CNRS, France
Emanuela Merelli	University of Camerino, Italy
Roland Meyer	TU Braunschweig, Germany
Uwe Nestmann	TU Berlin, Germany
Gustavo Petri	IRIF, Paris Diderot, Paris 7, France
Jorge A. Pérez	University of Groningen, The Netherlands
Willard Rafnsson	IT University of Copenhagen, Denmark
Anne Remke	WWU Münster, Germany
Guido Salvaneschi	TU Darmstadt, Germany
Cesar Sanchez	IMDEA Software Institute, Spain
Ana Sokolova	University of Salzburg, Austria
Alexander J. Summers	ETH Zurich, Switzerland
Peter Thiemann	Universität Freiburg, Germany
Jaco van de Pol	Aarhus University, Denmark
Tim Willemse	Eindhoven University of Technology, The Netherlands
Nobuko Yoshida	Imperial College London, UK
Lukasz Ziarek	SUNY Buffalo, USA

Additional Reviewers

Aldini, Alessandro
Alvim, Mario S.
Åman Pohjola, Johannes
Back, Christoffer Olling
Chini, Peter
Courtieu, Pierre
Dubut, Jérémy
Francalanza, Adrian
Inverso, Omar
Keiren, Jeroen
Madiot, Jean-Marie
Maestri, Stefano
Maubert, Bastien
Menikkumbura, Danushka
Neumann, Elisabeth
Otoni, Rodrigo
Pilch, Carina
Radanne, Gabriel
Sasse, Ralf
Savvides, Savvas
Schweizer, Sebastian
Sedwards, Sean
Tesei, Luca
Wolff, Sebastian
Yamada, Akihisa
Zeller, Peter

Security Protocols: Model Checking Standards (Invited Talk)

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. CQRE. LNCS, vol. 1740, pp. 30–42. Springer, Heidelberg (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)
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.A., 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.A., Cremers, C.J.F., Miyazaki, K., Radomirovic, S., Watanabe, D.: Improving the security of cryptographic protocol standards. IEEE Secur. Priv. **13**(3), 24–31 (2015). https://doi.org/10.1109/MSP.2013.162, http://dx.doi.org/10.1109/MSP.2013.162
7. Basin, D.A., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V.: Formal analysis of 5G authentication. CoRR **abs/1806.10360** (2018). http://arxiv.org/abs/1806.10360
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, http://dx.doi.org/10.3233/JCS-16814

Contents

Full Papers

Short and "Journal First" Papers