Lecture Notes in Computer Science 6659

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

Marco Bernardo Valérie Issarny (Eds.)

Formal Methods for Eternal Networked Software Systems

11th International School on Formal Methods for the Design of Computer, Communication and Software Systems, SFM 2011
Bertinoro, Italy, June 13-18, 2011
Advanced Lectures

Springer

Volume Editors

Marco Bernardo
Università di Urbino "Carlo Bo"
Dipartimento di Scienze di Base e Fondamenti
Piazza della Repubblica 13, 61029 Urbino, Italy
E-mail: bernardo@sti.uniurb.it

Valérie Issarny
INRIA Paris - Rocquencourt
Domaine de Voluceau, B.P. 105
78153 Le Chesnay, France
E-mail: valerie.issarny@inria.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-21454-7 e-ISBN 978-3-642-21455-4
DOI 10.1007/978-3-642-21455-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011928397

CR Subject Classification (1998): D.2.4, D.3.1, F.3-4, C.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume presents a set of papers accompanying the lectures of the 11th International School on Formal Methods for the Design of Computer, Communication and Software Systems (SFM).

This series of schools addresses the use of formal methods in computer science as a prominent approach to the rigorous design of the above-mentioned systems. The main aim of the SFM series is to offer a good spectrum of current research in foundations as well as applications of formal methods, which can be of help for graduate students and young researchers who intend to approach the field.

SFM 2011 was devoted to formal methods for eternal networked software systems and covered several topics including formal foundations for the interoperability of software systems, application-layer and middleware-layer dynamic connector synthesis, interaction behavior monitoring and learning, and quality assurance of connected systems. The school was held in collaboration with the researchers of the EU-funded projects CONNECT and ETERNALS.

This volume comprises 15 articles organized into six parts: (i) architecture and interoperability, (ii) formal foundations for connectors, (iii) connector synthesis, (iv) learning and monitoring, (v) dependability assurance, and (vi) trustworthy eternal systems via evolving software.

The paper by Blair, Paolucci, Grace, and Georgantas examines the issue of interoperability in complex distributed systems by focussing on middleware solutions that are intrinsically based on semantic meaning and advocates a dynamic approach to interoperability based on the concept of emergent middleware. Grace, Georgantas, Bennaceur, Blair, Chauvel, Issarny, Paolucci, Saadi, Souville, and Sykes illustrate how the CONNECT architecture tackles the interoperability problem for heterogeneous systems by observing the networked systems in action, learning their behavior, and then dynamically generating mediator software that will connect the systems.

The paper by Forejt, Kwiatkowska, Norman, and Parker provides an introduction to probabilistic model checking of Markov decision processes and its applications to performance and dependability analysis of networked systems, communication protocols, and randomized distributed algorithms. Baier, Klein, and Klüppelholz present an overview of the modeling concepts for components and connectors using the exogenous coordination languages Reo together with the underlying constraint automata framework for property verification.

The paper by Inverardi, Spalazzese, and Tivoli reports on how to automatically achieve protocol interoperability via connector synthesis by distinguishing between two notions of application-layer connectors: coordinators and mediators. Giannakopoulou and Păsăreanu review techniques for generating component interfaces automatically in order to cope with the fact that the satisfaction of certain properties may depend on the context in which a component will be

dynamically introduced. The paper by Issarny, Bennaceur, and Bromberg deals with middleware interoperability by discussing an approach to the dynamic synthesis of emergent connectors that mediate the interaction protocols executed by networked systems from application down to middleware layers.

Steffen, Howar, and Merten give an introduction to active learning of Mealy machines, which is characterized by the alternation of an exploration phase – during which membership queries are used to construct hypothesis models of a system under test – and a testing phase – during which equivalence queries are used to compare hypothesis models with the actual system – until a valid model of the target system is produced. The paper by Tretmans's presents model-based testing, in which test cases are algorithmically generated from a model specifying the required behavior of a system, and test-based modeling or automata learning, which aims at automatically generating a model from test observations, and shows that test coverage in model-based testing and precision of learned models turn out to be two sides of the same coin. Jonsson's paper is about generating models of communication system components from observations of their external behavior and illustrates how to adapt existing techniques to include data parameters in messages and states.

The paper by Bertolino, Calabró, Di Giandomenico, and Nostro deals with the dependability and performance evaluation of dynamic and evolving systems by means of a framework that can be used off-line for system design and on-line for continuously monitoring system behavior and detecting possible issues arising at run time. Costa, Issarny, Martinelli, Matteucci, and Saadi investigate security and trust as two complementary perspectives on the problem of the correct interaction among software components and propose an approach called security by contract with trust, in which the level of trust measures the adherence of the application to its contract.

The paper by Clarke, Diakov, Hähnle, Johnsen, Schaefer, Schäfer, Schlatte, and Wong describes HATS, an abstract behavioral modeling language for highly configurable distributed systems that supports spatial and temporal variability. Moschitti's paper introduces kernel methods designed within the statistical learning theory in order to overcome the concrete limitations of logic/rule-based approaches to the semantic modeling of the behavior of complex systems. Jürjens, Ochoa, Schmidt, Marchal, Houmb, and Islam recall the UMLsec approach to model-based security, which supports the system specification and design phases as well as maintaining the needed levels of security even through later software evolution.

We believe that this book offers a useful view of what has been done and what is going on worldwide in the field of eternal networked software systems. We wish to thank all the speakers and all the participants for a lively and fruitful school. We also wish to thank the entire staff of the University Residential Center of Bertinoro for the organizational and administrative support.

June 2011

Marco Bernardo
Valérie Issarny

Table of Contents

Part V: Dependability Assurance

Part VI: Trustworthy Eternal Systems via Evolving Software