Lecture Notes in Computer Science 3444

Mooly Sagiv (Ed.)

Programming Languages and Systems

14th European Symposium on Programming, ESOP 2005
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2005
Edinburgh, UK, April 4-8, 2005
Proceedings

Springer

Volume Editor

Mooly Sagiv
Tel Aviv University
School of Computer Science
Tel Aviv 69978, Israel
E-mail: msagiv@post.tau.ac.il

Library of Congress Control Number: 2005922810

CR Subject Classification (1998): D.3, D.1, D.2, F.3, F.4, E.1

ISSN 0302-9743
ISBN-10 3-540-25435-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-25435-5 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11410553 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2005 was the eighth instance of the European Joint Conferences on Theory and Practice of Software. ETAPS is an annual federated conference that was established in 1998 by combining a number of existing and new conferences. This year it comprised five conferences (CC, ESOP, FASE, FOSSACS, TACAS), 17 satellite workshops (AVIS, BYTECODE, CEES, CLASE, CMSB, COCV, FAC, FESCA, FINCO, GCW-DSE, GLPL, LDTA, QAPL, SC, SLAP, TGC, UITP), seven invited lectures (not including those that were specific to the satellite events), and several tutorials. We received over 550 submissions to the five conferences this year, giving acceptance rates below 30% for each one. Congratulations to all the authors who made it to the final program! I hope that most of the other authors still found a way of participating in this exciting event and I hope you will continue submitting.

The events that comprise ETAPS address various aspects of the system development process, including specification, design, implementation, analysis and improvement. The languages, methodologies and tools which support these activities are all well within its scope. Different blends of theory and practice are represented, with an inclination towards theory with a practical motivation on the one hand and soundly based practice on the other. Many of the issues involved in software design apply to systems in general, including hardware systems, and the emphasis on software is not intended to be exclusive.

ETAPS is a loose confederation in which each event retains its own identity, with a separate program committee and proceedings. Its format is open-ended, allowing it to grow and evolve as time goes by. Contributed talks and system demonstrations are in synchronized parallel sessions, with invited lectures in plenary sessions. Two of the invited lectures are reserved for “unifying” talks on topics of interest to the whole range of ETAPS attendees. The aim of cramming all this activity into a single one-week meeting is to create a strong magnet for academic and industrial researchers working on topics within its scope, giving them the opportunity to learn about research in related areas, and thereby to foster new and existing links between work in areas that were formerly addressed in separate meetings.

ETAPS 2005 was organized by the School of Informatics of the University of Edinburgh, in cooperation with

- European Association for Theoretical Computer Science (EATCS);
- European Association for Programming Languages and Systems (EAPLS);
- European Association of Software Science and Technology (EASST).

The organizing team comprised:

- Chair: Don Sannella
- Publicity: David Aspinall
- Satellite Events: Massimo Felici

- Secretariat: Dyane Goodchild
- Local Arrangements: Monika-Jeannette Lekuse
- Tutorials: Alberto Momigliano
- Finances: Ian Stark
- Website: Jennifer Tenzer, Daniel Winterstein
- Fundraising: Phil Wadler

ETAPS 2005 received support from the University of Edinburgh.

Overall planning for ETAPS conferences is the responsibility of its Steering Committee, whose current membership is:

> Perdita Stevens (Edinburgh, Chair), Luca Aceto (Aalborg and Reykjavík), Rastislav Bodik (Berkeley), Maura Cerioli (Genoa), Evelyn Duesterwald (IBM, USA), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Marie-Claude Gaudel (Paris), Roberto Gorrieri (Bologna), Reiko Heckel (Paderborn), Holger Hermanns (Saarbrücken), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Kim Larsen (Aalborg), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Hanne Riis Nielson (Copenhagen), Fernando Orejas (Barcelona), Mooly Sagiv (Tel Aviv), Don Sannella (Edinburgh), Vladimiro Sassone (Sussex), Peter Sestoft (Copenhagen), Michel Wermelinger (Lisbon), Igor Walukiewicz (Bordeaux), Andreas Zeller (Saarbrücken), Lenore Zuck (Chicago).

I would like to express my sincere gratitude to all of these people and organizations, the program committee chairs and PC members of the ETAPS conferences, the organizers of the satellite events, the speakers themselves, the many reviewers, and Springer for agreeing to publish the ETAPS proceedings. Finally, I would like to thank the organizer of ETAPS 2005, Don Sannella. He has been instrumental in the development of ETAPS since its beginning; it is quite beyond the limits of what might be expected that, in addition to all the work he has done as the original ETAPS Steering Committee Chairman and current ETAPS Treasurer, he has been prepared to take on the task of organizing this instance of ETAPS. It gives me particular pleasure to thank him for organizing ETAPS in this wonderful city of Edinburgh in this my first year as ETAPS Steering Committee Chair.

Edinburgh, January 2005

Perdita Stevens
ETAPS Steering Committee Chair

Preface

This volume contains the 29 papers presented at ESOP 2005, the 14th European Symposium on Programming, which took place in Edinburgh, UK, April 6–8, 2005. The ESOP series began in 1986 with the goal of bridging the gap between theory and practice, and the conferences continue to be devoted to explaining fundamental issues in the specification, analysis, and implementation of programming languages and systems.

The volume begins with a summary of an invited contribution by Andrew Myers titled "Programming with Explicit Security Policies," and continues with the 28 papers selected by the Program Committee from 114 submissions. Each submission was reviewed by at least three referees, and papers were selected during a 10-day electronic discussion phase.

I would like to sincerely thank the members of the Program Committee for their thorough reviews and dedicated involvement in the PC discussion. I would also like to thank the subreferees, for their diligent work. Martin Karusseit and Noam Rinetzky helped me with MetaFrame, used as the conference management software. Finally, I would like to thank Anat Lotan-Schwartz for helping me to collect the final papers and prepare these proceedings.

January 2005 Mooly Sagiv

Organization

Program Chair

Mooly Sagiv	Tel Aviv University, Israel

Program Committee

Martín Abadi	University of California at Santa Cruz, USA
Alex Aiken	Stanford University, USA
Bruno Blanchet	École Normale Supérieure, France
Luca Cardelli	Microsoft Research, UK
Patrick Cousot	École Normale Supérieure, France
Oege de Moor	Oxford University, UK
Manuel Fähndrich	Microsoft Research, USA
John Field	IBM, USA
Maurizio Gabbrielli	Università di Bologna, Italy
Chris Hankin	Imperial College London, UK
Manuel Hermenegildo	Universidad Politécnica de Madrid, Spain and University of New Mexico, USA
Xavier Leroy	INRIA Rocquencourt, France
Anders Møller	University of Aarhus, Denmark
Greg Morrisett	Harvard University, USA
David Naumann	Stevens Institute of Technology, USA
Hanne Riis Nielson	IMM, Technical University of Denmark
Peter O'Hearn	University of London, UK
Catuscia Palamidessi	INRIA Futurs Saclay and LIX, France
Thomas Reps	University of Wisconsin-Madison, USA
Martin Rinard	MIT, USA
Andrei Sabelfeld	Chalmers University and Göteborg University, Sweden
David Sangiorgi	Università di Bologna, Italy
David Schmidt	Kansas State University, USA
Scott Stoller	SUNY at Stony Brook, USA

Referees

A. Ahmed
E. Albert
A. Aldini
J. Aldrich
Z. Ariola
A. Askarov
F. Barbanera
M. Barnett
N. Benton
J. Berdine
L. Bettini
G. Bierman

D. Biernacki
C. Bodei
C. Brabrand
K. Bruce
M. Buscemi
N. Busi
B.C. Pierce
C. Calcagno
A. Cavalcanti
K. Chatzikokolakis
S.C. Mu
T. Chothia
M. Codish
A. Corradini
A. Cortesi
V. Cortiero
S. Crafa
F.D. Valenciao
O. Danvy
F. De Boer
P. Degano
G. Delzanno
D. Distefano
D. Dougherty
D. Duggan
R. Ettinger
G. File
C. Flanagan
M. Fluet
R. Focardi
C. Fourned
B. Francisco
J. Garrigue
D. Ghica
R. Giacobazzi
J.C. Godskesen
S. Goldsmith
G. Gonthier
J. Goubault-Larrecq
M.R. Hansen
J. Hickey
T. Hildebrandt
P. Hill
Y. Huenke
J. Hurd
M.J. Jaskelioff
L. Jagadeesan
A. Jeffrey
A. Kennedy
C. Kirkegaard
B. Klin
J. Kodumal
R. Komondoor
S. Krishnamurthi
B. Le Charlier
F. Levi
F. Logozzo
P. Lopez-Garcia
I. Lynagh
R. Majumdar
R. Manevich
M.C. Marinescu
A. Matos
L. Mauborgne
D. Miller
A. Miné
D. Monniaux
M. Naik
U. Neumerkel
F. Nielson
N. Nystrom
R. O'Callahan
L. Ong
L. Paolini
B. Pfitzmann
E. Poll
F. Pottier
M. Proietti
G. Puebla
S. Rajamani
A. Ravara
J. Rehof
J. Reppy
N. Rinetzky
C. Russo
D. Rémy
C. Sacerdoti Cohen
A. Sahai
A. Sasturkar
A. Schmitt
T. Schrijvers
A.S. Christensen
R. Solmi
M. Spivey
F. Spoto
T. Streicher
K. Støvring Sørensen
J.M. Talbot
T. Terauchi
L. Tesei
H. Thielecke
C. Urban
M. Vaziri
T. Veldhuizen
B. Victor
L. Vigano
J. Vouillono
Y. Wang
B. Warinschi
Y. Xie
E. Yahav
E. Zaffanella
S. Zdancewic
T. Zhao
E. Zucca

Table of Contents

Programming with Explicit Security Policies
Andrew C. Myers 1

Trace Partitioning in Abstract Interpretation Based Static Analyzers
Laurent Mauborgne, Xavier Rival 5

The ASTRÉE Analyzer
Patrick Cousot, Radhia Cousot, Jerôme Feret, Laurent Mauborgne, Antoine Miné, David Monniaux, Xavier Rival 21

Interprocedural Herbrand Equalities
Markus Müller-Olm, Helmut Seidl, Bernhard Steffen 31

Analysis of Modular Arithmetic
Markus Müller-Olm, Helmut Seidl 46

Forward Slicing by Conjunctive Partial Deduction and Argument Filtering
Michael Leuschel, Germán Vidal 61

A New Foundation for Control-Dependence and Slicing for Modern Program Structures
Venkatesh Prasad Ranganath, Torben Amtoft, Anindya Banerjee, Matthew B. Dwyer, John Hatcliff 77

Summaries for While Programs with Recursion
Andreas Podelski, Ina Schaefer, Silke Wagner 94

Determinacy Inference for Logic Programs
Lunjin Lu, Andy King 108

Automatic Verification of Pointer Programs Using Grammar-Based Shape Analysis
Oukseh Lee, Hongseok Yang, Kwangkeun Yi 124

A Type Discipline for Authorization Policies
Cédric Fournet, Andrew D. Gordon, Sergio Maffeis 141

Computationally Sound, Automated Proofs for Security Protocols
Véronique Cortier, Bogdan Warinschi 157

Completing the Picture: Soundness of Formal Encryption in the Presence of Active Adversaries (Extended Abstract)
Romain Janvier, Yassine Lakhnech, Laurent Mazaré 172

Analysis of an Electronic Voting Protocol in the Applied Pi Calculus
Steve Kremer, Mark Ryan 186

Streams with a Bottom in Functional Languages
Hideki Tsuiki, Keiji Sugihara 201

Bottom-Up β-Reduction: Uplinks and λ-DAGs
Olin Shivers, Mitchell Wand 217

BI Hyperdoctrines and Higher-Order Separation Logic
Bodil Biering, Lars Birkedal, Noah Torp-Smith 233

Deciding Reachability in Mobile Ambients
Nadia Busi, Gianluigi Zavattaro 248

Denotational Semantics for Abadi and Leino's Logic of Objects
Bernhard Reus, Jan Schwinghammer 263

A Design for a Security-Typed Language with Certificate-Based Declassification
Stephen Tse, Steve Zdancewic 279

Adjoining Declassification and Attack Models by Abstract Interpretation
Roberto Giacobazzi, Isabella Mastroeni 295

Enforcing Resource Bounds via Static Verification of Dynamic Checks
Ajay Chander, David Espinosa, Nayeem Islam, Peter Lee, George Necula 311

Asserting Bytecode Safety
Martin Wildmoser, Tobias Nipkow 326

Subtyping First-Class Polymorphic Components
João Costa Seco, Luís Caires 342

Complexity of Subtype Satisfiability over Posets
Joachim Niehren, Tim Priesnitz, Zhendong Su 357

A Type System Equivalent to a Model Checker
Mayur Naik, Jens Palsberg 374

Instant Polymorphic Type Systems for Mobile Process Calculi: Just Add Reduction Rules and Close
Henning Makholm, J.B. Wells 389

Towards a Type System for Analyzing JavaScript Programs
Peter Thiemann 408

Java Jr.: Fully Abstract Trace Semantics for a Core Java Language
Alan Jeffrey, Julian Rathke 423

Author Index 439