

Lecture Notes in Computer Science

2618

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Pierpaolo Degano (Ed.)

Programming Languages and Systems

**12th European Symposium on Programming, ESOP 2003
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2003
Warsaw, Poland, April 7-11, 2003
Proceedings**



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Pierpaolo Degano
Università di Pisa, Dipartimento di Informatica
Via F. Buonarroti, 2, 56127 Pisa, Italy
E-mail: degano@di.unipi.it

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek.
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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

ISSN 0302-9743

ISBN 3-540-00886-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH
Printed on acid-free paper SPIN: 10872938 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2003 was the sixth 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 (FOSSACS, FASE, ESOP, CC, TACAS), 14 satellite workshops (AVIS, CMCS, COCV, FAMAS, Feyerabend, FICS, LDTA, RSKD, SC, TACoS, UniGra, USE, WITS and WOOD), eight invited lectures (not including those that are specific to the satellite events), and several tutorials. We received a record number of submissions to the five conferences this year: over 500, making acceptance rates fall below 30% for every of them. Congratulations to all the authors who made it to the final program! I hope that all the other authors still found a way of participating in this exciting event and I hope you will continue submitting.

A special event was held to honor the 65th birthday of Prof. Wlad Turski, one of the pioneers of our young science. The deaths of some of our “fathers” in the summer of 2002 — Dahl, Dijkstra and Nygaard — reminded us that Software Science and Technology is, perhaps, no longer that young. Against this sobering background, it is a treat to celebrate one of our most prominent scientists and his lifetime of achievements. It gives me particular personal pleasure that we are able to do this for Wlad during my term as chairman of ETAPS.

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 independent 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 2003 was organized by Warsaw University, Institute of Informatics, in cooperation with the Foundation for Information Technology Development, as well as:

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

- ACM SIGACT, SIGSOFT and SIGPLAN.

The organizing team comprised:

Mikołaj Bojańczyk, Jacek Chrząszcz, Piotr Chrząstowski-Wachtel, Grzegorz Grudziński, Kazimierz Grygiel, Piotr Hoffman, Janusz Jabłonowski, Mirosław Kowaluk, Marcin Kubica (publicity), Sławomir Leszczyński (www), Wojciech Moczydłowski, Damian Niwiński (satellite events), Aleksy Schubert, Hanna Sokolowska, Piotr Stańczyk, Krzysztof Szafran, Marcin Szczuka, Łukasz Sznuć, Andrzej Tarlecki (co-chair), Jerzy Tiuryn, Jerzy Tyszkiewicz (book exhibition), Paweł Urzyczyn (co-chair), Daria Walukiewicz-Chrząszcz, Artur Zawłocki.

ETAPS 2003 received support from:¹

- Warsaw University
- European Commission, High-Level Scientific Conferences and Information Society Technologies
- US Navy Office of Naval Research International Field Office,
- European Office of Aerospace Research and Development, US Air Force
- Microsoft Research

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

Egidio Astesiano (Genoa), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Marie-Claude Gaudel (Paris), Evelyn Duesterwald (IBM), Hubert Garavel (Grenoble), Andy Gordon (Microsoft Research, Cambridge), Roberto Gorrieri (Bologna), Susanne Graf (Grenoble), Görel Hedin (Lund), Nigel Horspool (Victoria), Kurt Jensen (Aarhus), Paul Klint (Amsterdam), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Mogens Nielsen (Aarhus), Hanne Riis Nielson (Copenhagen), Fernando Orejas (Barcelona), Mauro Pezzè (Milano), Andreas Podelski (Saarbrücken), Don Sannella (Edinburgh), David Schmidt (Kansas), Bernhard Steffen (Dortmund), Andrzej Tarlecki (Warsaw), Igor Walukiewicz (Bordeaux), Herbert Weber (Berlin).

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, and Springer-Verlag for agreeing to publish the ETAPS proceedings. The final votes of thanks must go, however, to Andrzej Tarlecki and Paweł Urzyczyn. They accepted the risk of organizing what is the first edition of ETAPS in Eastern Europe, at a time of economic uncertainty, but with great courage and determination. They deserve our greatest applause.

Leicester, January 2003

José Luiz Fiadeiro
ETAPS Steering Committee Chair

¹ The contents of this volume do not necessarily reflect the positions or the policies of these organizations and no official endorsement should be inferred.

Preface

This volume contains the 27 papers presented at ESOP 2003, the 12th European Symposium on Programming, which took place in Warsaw, Poland, April 5–13, 2003. The ESOP series began in 1986 with the goal of bridging the gap between theory and practice. The conferences are devoted to fundamental issues in the specification, analysis and implementation of programming languages and systems.

The call for ESOP 2003 encouraged papers addressing the topics traditionally covered by ESOP (but not limited to):

- programming paradigms and their integration;
- semantics;
- calculi of computation;
- security;
- advanced type systems;
- program analysis and transformation;
- practical algorithms based on theoretical developments.

The volume begins with two invited contributions, both in the area of security. The first belongs to ETAPS as a whole, and accompanies its “unifying invited lecture” entitled *Computer Security from a Programming Language and Static Analysis Perspective*, delivered by Xavier Leroy. The second contribution is *What Makes a Cryptographic Protocol Secure? The Evolution of Requirements Specification in Formal Cryptographic Protocol Analysis*, by the ESOP invited speaker Catherine Meadows. The remaining 25 papers were selected by the Programme Committee from the 99 submissions.

Each submission was reviewed by at least three referees, and papers were selected in the latter stages of a one-week electronic discussion phase. I would like to sincerely thank all members of the ESOP 2003 Programme Committee for the excellent job they did in the very difficult selection process, always carried on in a kind, agreeable atmosphere. Also, I would like to thank all the subreferees for their invaluable contribution. I am also grateful to Michele Curti for the help with the conference management software. Finally, many thanks to the ETAPS Organising Committee, chaired by Andrzej Tarlecki and Pawel Urzyczyn, and to the Steering Committee of ETAPS, in particular to José Luiz Fiadeiro, for their efficient coordination of all the activities leading up to ESOP 2003.

Programme Chair

Pierpaolo Degano

Univ. Pisa, Italy

Programme Committee

Patrick Cousot

ENS Paris, France

Mariangiola Dezani-Ciancaglini

Univ. Torino, Italy

Cedric Fournet

Microsoft Research Cambridge, UK

John Hughes

Chalmers Univ., Sweden

Joshua Guttman

MITRE, USA

John Mitchell

Stanford Univ., USA

Alan Mycroft

Univ. Cambridge, UK

Hanne Riis Nielson

IMM Copenhagen, Denmark

Oscar Nierstrasz

Univ. Berne, Switzerland

Catuscia Palamidessi

INRIA Paris, France & Penn State Univ.,
USA

Dave Schmidt

Kansas State Univ., USA

Helmut Seidl

Univ. Trier, Germany

Perdita Stevenson

Univ. Edinburgh, UK

Referees

Adriana Compagnoni
 Agostino Cortesi
 Alan Lawrence
 Alessandra Di Pierro
 Alexandru Berlea
 Allen Stoughton
 Andrew Kennedy
 Andrew Pitts
 Antoine Miné
 Anupam Datta
 Arnaud Venet
 Bertrand Jeannot
 Bruno Blanchet
 Carlo Montangero
 Charles Consel
 Charles Hymans
 Chiara Bodei
 Chris Hankin
 Christian Haack
 Christopher Anderson
 Christoph Kessler
 Claudio Russo
 Corrado Priami
 Dale Miller
 Dario Colazzo
 Davide Ancona
 Davide Sangiorgi
 David Monniaux
 Don Syme
 Elodie Sims
 Elvira Albert
 Emilio Tuosto
 Fabio Gadducci
 Felice Cardone
 Francesco Logozzo
 Francesco Ranzato
 Francois Maurel
 Francois Pottier
 Frank S. de Boer
 Frank Valencia
 Gabriela Arévalo
 German Puebla
 Giancarlo Mauri
 GianLuigi Ferrari

Giorgio Delzanno
 Giorgio Ghelli
 Gregory Morrisett
 Hans Huttel
 Henning Christiansen
 Henrik Pilegaard
 Hongwei Xi
 Hongyan Sun
 Ian Gent
 Ian Stark
 Iliano Cervesato
 Ivano Salvo
 James Riely
 Jeremy Singer
 Jerome Feret
 John Boyland
 John Longley
 Karol Ostrovsky
 Keith Wansbrough
 Kurt Sieber
 Kurt Stenzel
 Laura Ponisio
 Laurence Melloul
 Laurent Mauborgne
 Luca Becchetti
 Luca Cardelli
 Luigi Liquori
 Marcin Benke
 Marco Danelutto
 Mark Shinwell
 Markus Mueller-Olm
 Martin Abadi
 Martin Elsman
 Martin Fränze
 Martin Grohe
 Martin Sulzmann
 Massimo Bartoletti
 Matthew Parkinson
 Maurizio Gabbriellini
 Michael Hanus
 Michael O'Boyle
 Michael R. Hansen
 Michal Konecny
 Michele Lanza

Mikael Buchholtz
Monica Nesi
Murray Cole
Nadia Busi
Neil Johnson
Nguyen V. Thoai
Nicholas Nethercote
Nick Benton
Nicolas Halbwachs
Paola Giannini
Paolo Manghi
Paula Severi
Paul Fischer
Pawel Urzyczyn
Peter Buneman
Peter Revesz
Peter Sewell
Ralf Laemmel
Raya Leviathan
Rene Rydhof Hansen
Richard Sharp
Roberto Bagnara
Roberto Gorrieri
Robin Milner
Roel Wuyts

Rosario Pugliese
Rustan Leino
Simona Ronchi
Simon Frankau
Simon Peyton-Jones
Stefan Monnier
Stefano Berardi
Stéphane Ducasse
Stephen Freund
Stephen Gilmore
Stuart Anderson
Thomas Noll
Tom Hischowitz
Torben Amtoft
Tudor Girba
Tuomas Aura
Veronique Benzaken
Viviana Bono
Walid Taha
Wolfgang Goerigk
Xavier Leroy
Xavier Rival
Xavier Urbain
Yorck Hunke

Table of Contents

Invited Talks

Computer Security from a Programming Language and Static Analysis Perspective	1
<i>Xavier Leroy (INRIA Rocquencourt and Trusted Logic S.A.)</i>	
What Makes a Cryptographic Protocol Secure? The Evolution of Requirements Specification in Formal Cryptographic Protocol Analysis.....	10
<i>Catherine Meadows (Center for High Assurance Computer Systems)</i>	

Contributed Papers

A Tail-Recursive Semantics for Stack Inspections.....	22
<i>John Clements and Matthias Felleisen (Northeastern University)</i>	
Flexible Models for Dynamic Linking	38
<i>Sophia Drossopoulou (Imperial College), Giovanni Lagorio (University of Genova), and Susan Eisenbach (Imperial College)</i>	
Correction of Functional Logic Programs.....	54
<i>Maria Alpuente (DSIC, Univ. Polit�cnica de Valencia), Demis Ballis (Dipartimento di Matematica e Informatica, Universit� di Udine), Francisco J. Correa (DIS, Univ Eafit), and Moreno Falaschi (Dipartimento di Matematica e Informatica, Universit� di Udine)</i>	
Approximate Pruning in Tabled Logic Programming.....	69
<i>Lu�s F. Castro and David S. Warren (SUNY at Stony Brook)</i>	
Goal-Independent Suspension Analysis for Logic Programs with Dynamic Scheduling.....	84
<i>Samir Genaim (Ben-Gurion University of the Negev) and Andy King (University of Kent at Canterbury)</i>	
Security Properties: Two Agents Are Sufficient.....	99
<i>Hubert Comon-Lundh and V�ronique Cortier (LSV, ENS Cachan and CNRS)</i>	
A Simple Language for Real-Time Cryptographic Protocol Analysis.....	114
<i>Roberto Gorrieri , Enrico Locatelli (Universit� di Bologna), and Fabio Martinelli (IIT-CNR)</i>	

Rule Formats for Non Interference	129
<i>Simone Tini (Università dell'Insubria)</i>	
On the Secure Implementation of Security Protocols	144
<i>Pablo Giambiagi and Mads Dam (Swedish Institute of Computer Science)</i>	
Handling Encryption in an Analysis for Secure Information Flow	159
<i>Peeter Laud (Tartu University and Cybernetica AS)</i>	
Using Controller Synthesis to Build Property-Enforcing Layers	174
<i>Karine Altisen (VERIMAG/INPG), Aurélie Clodic (LAAS/CNRS), Florence Maraninchi (VERIMAG/INPG), and Eric Rutten (INRIA Rhône-Alpes)</i>	
Automatic Software Model Checking Using CLP	189
<i>Cormac Flanagan (Systems Research Center, Hewlett Packard Laboratories)</i>	
Verifying Temporal Heap Properties Specified via Evolution Logic	204
<i>Eran Yahav (Tel-Aviv University), Thomas Reps (University of Wisconsin), Mooly Sagiv (Tel-Aviv University), and Reinhard Wilhelm (Universität des Saarlandes)</i>	
Correctness of Data Representations Involving Heap Data Structures	223
<i>Uday S. Reddy (University of Birmingham) and Hongseok Yang (Korean Advanced Institute of Science and Technology)</i>	
Modeling Web Interactions	238
<i>Paul Graunke (Northeastern University), Robert Bruce Findler (University of Chicago), Shriram Krishnamurthi (Brown University), and Matthias Felleisen (Northeastern University)</i>	
Type Inference for a Distributed π -Calculus	253
<i>Cédric Lhousseine (COGS, University of Sussex)</i>	
Type-Safe Update Programming	269
<i>Martin Erwig and Deling Ren (Oregon State University)</i>	
Type Error Slicing in Implicitly Typed Higher-Order Languages	284
<i>Christian Haack and J.B. Wells (Heriot-Watt University)</i>	

Core Formal Molecular Biology	302
<i>Vincent Danos (CNRS University of Paris 7) and Cosimo Laneve (University of Bologna)</i>	
Requirements on the Execution of Kahn Process Networks	319
<i>Marc Geilen and Twan Basten (Eindhoven University of Technology)</i>	
Tagging, Encoding, and Jones Optimality	335
<i>Olivier Danvy (BRICS, University of Aarhus) and Pablo E. Martínez López (LIFIA, UNLP)</i>	
The Rely-Guarantee Method in Isabelle/HOL	348
<i>Leonor Prensa Nieto (INRIA Sophia-Antipolis)</i>	
Building Certified Libraries for PCC: Dynamic Storage Allocation	363
<i>Dachuan Yu, Nadeem A. Hamid, and Zhong Shao (Yale University)</i>	
Finite Differencing of Logical Formulas for Static Analysis	380
<i>Thomas Reps (University of Wisconsin), Mooly Sagiv (Tel-Aviv University), and Alexey Loginov (University of Wisconsin)</i>	
Register Allocation by Proof Transformation	399
<i>Atsushi Ohori (Japan Advanced Institute of Science and Technology)</i>	
Author Index	415