Lecture Notes in Computer Science 7215

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

Advanced Research in Computing and Software Science
Subline of Lectures Notes in Computer Science

Pierpaolo Degano Joshua D. Guttman (Eds.)

Principles of Security and Trust

First International Conference, POST 2012
Held as Part of the European Joint Conferences
on Theory and Practice of Software, ETAPS 2012
Tallinn, Estonia, March 24 – April 1, 2012
Proceedings

Springer

Volume Editors

Pierpaolo Degano
Università di Pisa
Dipartimento di Informatica
Largo Bruno Pontecorvo, 3
56127 Pisa, Italy
E-mail: degano@di.unipi.it

Joshua D. Guttman
Worcester Polytechnic Institute
Department of Computer Science
100 Institute Road
Worcester, MA 01609, USA
E-mail: guttman@wpi.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-28640-7 e-ISBN 978-3-642-28641-4
DOI 10.1007/978-3-642-28641-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012932616

CR Subject Classification (1998): C.2.0, D.4.6, E.3, K.4.4, K.6.5, D.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

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)

Foreword

ETAPS 2012 is the fifteenth 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 six sister conferences (CC, ESOP, FASE, FOSSACS, POST, TACAS), 21 satellite workshops (ACCAT, AIPA, BX, BYTECODE, CMCS, DICE, FESCA, FICS, FIT, GRAPHITE, GT-VMT, HAS, IWIGP, LDTA, LINEARITY, MBT, MSFP, PLACES, QAPL, VSSE and WRLA), and eight invited lectures (excluding those specific to the satellite events).

The six main conferences received this year 606 submissions (including 21 tool demonstration papers), 159 of which were accepted (6 tool demos), giving an overall acceptance rate just above 26%. Congratulations therefore to all the authors who made it to the final programme! I hope that most of the other authors will still have found a way to participate in this exciting event, and that you will all continue to submit to ETAPS and contribute to making it the best conference on software science and engineering.

The events that comprise ETAPS address various aspects of the system development process, including specification, design, implementation, analysis, security and improvement. The languages, methodologies and tools that 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 confederation in which each event retains its own identity, with a separate Programme 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 synchronised 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.

This year, ETAPS welcomes a new main conference, *Principles of Security and Trust*, as a candidate to become a permanent member conference of ETAPS. POST is the first addition to our main programme since 1998, when the original five conferences met in Lisbon for the first ETAPS event. It combines the practically important subject matter of security and trust with strong technical connections to traditional ETAPS areas.

A step towards the consolidation of ETAPS and its institutional activities has been undertaken by the Steering Committee with the establishment of *ETAPS e.V.*, a non-profit association under German law. ETAPS e.V. was founded on April 1st, 2011 in Saarbrücken, and we are currently in the process of defining its structure, scope and strategy.

ETAPS 2012 was organised by the *Institute of Cybernetics at Tallinn University of Technology*, 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)

and with support from the following sponsors, which we gratefully thank:

Institute of Cybernetics at TUT; Tallinn University of Technology (TUT); Estonian Centre of Excellence in Computer Science (EXCS) funded by the European Regional Development Fund (ERDF); Estonian Convention Bureau; and Microsoft Research.

The organising team comprised:

General Chair:	*Tarmo Uustalu*
Satellite Events:	*Keiko Nakata*
Organising Committee:	*James Chapman, Juhan Ernits, Tiina Laasma, Monika Perkmann* and their colleagues in the *Logic and Semantics* group and *administration* of the *Institute of Cybernetics*

The ETAPS portal at http://www.etaps.org is maintained by *RWTH Aachen University*.

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

Vladimiro Sassone (Southampton, Chair), Roberto Amadio (Paris 7), Gilles Barthe (IMDEA-Software), David Basin (Zürich), Lars Birkedal (Copenhagen), Michael O'Boyle (Edinburgh), Giuseppe Castagna (CNRS Paris), Vittorio Cortellessa (L'Aquila), Koen De Bosschere (Gent), Pierpaolo Degano (Pisa), Matthias Felleisen (Boston), Bernd Finkbeiner (Saarbrücken), Cormac Flanagan (Santa Cruz), Philippa Gardner (Imperial College London), Andrew D. Gordon (MSR Cambridge and Edinburgh), Daniele Gorla (Rome), Joshua Guttman (Worcester USA), Holger Hermanns (Saarbrücken), Mike Hinchey (Lero, the Irish Software Engineering Research Centre), Ranjit Jhala (San Diego), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Barbara König (Duisburg), Juan de Lara (Madrid), Gerald Lüttgen (Bamberg), Tiziana Margaria (Potsdam), Fabio Martinelli (Pisa), John Mitchell (Stanford), Catuscia Palamidessi (INRIA Paris), Frank Pfenning (Pittsburgh), Nir Piterman (Leicester), Don Sannella (Edinburgh), Helmut Seidl (TU Munich),

Scott Smolka (Stony Brook), Gabriele Taentzer (Marburg), Tarmo Uustalu (Tallinn), Dániel Varró (Budapest), Andrea Zisman (London), and Lenore Zuck (Chicago).

I would like to express my sincere gratitude to all of these people and organisations, the Programme Committee Chairs and PC members of the ETAPS conferences, the organisers of the satellite events, the speakers themselves, the many reviewers, all the participants, and Springer-Verlag for agreeing to publish the ETAPS proceedings in the ARCoSS subline.

Finally, I would like to thank the Organising Chair of ETAPS 2012, Tarmo Uustalu, and his Organising Committee, for arranging to have ETAPS in the most beautiful surroundings of Tallinn.

January 2012

Vladimiro Sassone
ETAPS SC Chair

Preface

The first conference on Principles of Security and Trust (POST) was held 25–27 March 2012 in Tallinn, as part of ETAPS 2012. POST resulted from an alliance among the workshops it will replace: Automated Reasoning and Security Protocol Analysis (ARSPA), Formal Aspects of Security and Trust (FAST), Security in Concurrency (SecCo), and the Workshop on Issues in the Theory of Security (WITS). Some of these events met jointly, affiliated with ETAPS, in 2011 under the name Theory of Security and Applications (TOSCA). The IFIP WG 1.7 on Theoretical Foundations of Security Analysis and Design has long helped to nourish this community.

We are pleased that POST attracted 67 submissions for its first occurrence, from which the committee selected 20. This volume also contains an abstract of the talk given by our invited speaker, Cynthia Dwork, and a paper by Bruno Blanchet, an ETAPS unifying speaker. We would like to thank them for their contributions.

We are grateful to our dedicated and collegial Program Committee, and to the ETAPS Steering Committee for start-up help. We thank the Organizing Committee in Tallinn. Finally, Andrei Voronkov very helpfully ensured that Easychair worked smoothly.

January 2012
Pisa and Boston

Pierpaolo Degano
Joshua Guttman

Organization

Program Committee

Michael Backes	Saarland University and MPI-SWS
Anindya Banerjee	IMDEA Software Institute
Gilles Barthe	IMDEA Software Institute
David Basin	ETH Zurich
Véronique Cortier	CNRS, Loria
Pierpaolo Degano	Università di Pisa
Andy Gordon	Microsoft Research and University of Edinburgh
Joshua Guttman	Worcester Polytechnic Institute
Steve Kremer	ENS Cachan, INRIA
Ralf Küsters	University of Trier
Peeter Laud	Cybernetica AS and University of Tartu
Gavin Lowe	University of Oxford
Heiko Mantel	Technische Universität Darmstadt
Sjouke Mauw	Université du Luxembourg
Catherine Meadows	Naval Research Laboratory
John Mitchell	Stanford University
Carroll Morgan	University of New South Wales
Sebastian A. Mödersheim	Danish Technical University
Mogens Nielsen	University of Aarhus
Catuscia Palamidessi	École Polytechnique, INRIA
Andrei Sabelfeld	Chalmers University of Technology
Nikhil Swamy	Microsoft Research
Luca Viganò	Università di Verona

Additional Reviewers

Aderhold, Markus
Arapinis, Myrto
Barletta, Michele
Bartoletti, Massimo
Bello, Luciano
Berard, Beatrice
Birgisson, Arnar
Bodei, Chiara
Boreale, Michele
Calvi, Alberto
Chen, Xihui
Chevalier, Yannick
Chong, Stephen
Ciobaca, Stefan
Clarckson, Michael
Cremers, Cas
Crespo, Juan Manuel
De Caso, Guido
Delaune, Stéphanie
Eggert, Sebastian
Elsalamouny, Ehab
Ereth, Sarah

Ferrari, Gianluigi
Fournet, Cédric
Garcia, Flavio D.
Gay, Richard
Gibbons, Jeremy
Gibson-Robinson, Thomas
Goldsmith, Michael
Heam, Pierre-Cyrille
Hritcu, Catalin
Jonker, Hugo
Klaedtke, Felix
Kordy, Barbara
Kramer, Simon
Lux, Alexander
Malkis, Alexander
Mezzetti, Gianluca
Morvan, Christophe
Muller, Tim
Murawski, Andrzej
Naumann, David
Nguyen, Long
Perner, Matthias
Peroli, Michele
Petrocchi, Marinella
Radomirovic, Sasa
Rafnsson, Willard
Ryan, P.Y.A.
Schmidt, Benedikt
Seifert, Christian
Smyth, Ben
Sprenger, Christoph
Sprick, Barbara
Starostin, Artem
Strub, Pierre-Yves
Syverson, Paul
Tiu, Alwen
Truderung, Tomasz
Tuengerthal, Max
Van Delft, Bart
Vogt, Andreas
Wang, Rui
Zalinescu, Eugen
Zunino, Roberto

Table of Contents