

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Gilles Barthe Cédric Fournet (Eds.)

Trustworthy Global Computing

Third Symposium, TGC 2007

Sophia-Antipolis, France, November 5-6, 2007

Revised Selected Papers



Springer

Volume Editors

Gilles Barthe
INRIA Sophia-Antipolis Méditerranée
2004 route des lucioles - BP 93, 06902 Sophia Antipolis Cedex, France
E-mail: Gilles.Barthe@inria.fr

Cédric Fournet
Microsoft Research Ltd.
7 J J Thomson Avenue, Cambridge CB3 0FB, UK
E-mail: fournet@microsoft.com

Library of Congress Control Number: 2008922366

CR Subject Classification (1998): C.2.4, D.1.3, D.2, D.4.6, F.2.1-2, D.3, F.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN	0302-9743
ISBN-10	3-540-78662-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-78662-7 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12241507 06/3180 5 4 3 2 1 0

Preface

This volume contains the post-proceedings of the third edition of the International Symposium on Trustworthy Global Computing (TGC 2007), held in Sophia-Antipolis, France, November 5–6, 2007, and tutorial papers of the following Workshop on the Interplay of Programming Languages and Cryptography, held in Sophia Antipolis, November 7, 2007.

The Symposium on Trustworthy Global Computing is an international annual venue dedicated to safe and reliable computation in global computers. It focuses on providing tools and frameworks for constructing well-behaved applications and for reasoning about their behavior and properties in models of computation that incorporate code and data mobility over distributed networks with highly dynamic topologies and heterogeneous devices.

This volume starts with an invited paper from Martin Hofmann. It then includes the revised versions of the 19 contributed papers; these versions take into account both the referee's reports and the discussions that took place during the symposium. The Program Committee selected 19 papers from 48 submissions. Every submission was reviewed by at least three members of the Program Committee. In addition, the Program Committee sought the opinions of additional referees, selected because of their expertise on particular topics. We are grateful to Andrei Voronkov for his EasyChair system that helped us to manage these discussions. We would like to thank the authors who submitted papers to the conference, the members of the Program Committee, and the additional reviewers for their excellent work. We would also like to thank the invited speakers to TGC 2007, Andrew D. Gordon, Martin Hofmann, and Jeff Magee.

The proceedings also include three tutorial papers. These papers were presented at the Workshop on the Interplay of Programming Languages and Cryptography, organized by Ricardo Corin (INRIA, Rocquencourt) and Tamara Rezk (INRIA, Sophia-Antipolis).

We gratefully acknowledge support from INRIA Sophia-Antipolis, Microsoft Research, and the MSR-INRIA Joint Centre, as well as the European Global Computing Initiative through the FET program.

November 2007

Gilles Barthe
Cédric Fournet

Organization

Steering Committee

Gilles Barthe (INRIA)
Rocco De Nicola (University of Florence)
Christos Kaklamanis (University of Patras)
Ugo Montanari (University of Pisa)
Davide Sangiorgi (University of Bologna)
Don Sannella (University of Edinburgh)
Vladimiro Sassone (University of Southampton)
Martin Wirsing (University of Munich)

Program Committee

Gilles Barthe (INRIA)
Roberto Bruni (University of Pisa)
Luis Caires (Universidade Nova de Lisboa)
Bruno Crispo (University of Trento)
Silvano Dal Zilio (CNRS)
Rocco De Nicola (University of Florence)
Cédric Fournet (Microsoft Research)
Manuel Hermenegildo (T.U. of Madrid - UPM)
Alan Jeffrey (Bell Labs - Alcatel Lucent)
Christos Kaklamanis (University of Patras)
Cosimo Laneve (University of Bologna)
Uwe Nestmann (TU Berlin)
Dave Sands (Chalmers University of Technology of Göteborg)
Vladimiro Sassone (University of Southampton)
Ian Stark (University of Edinburgh)
Alan Schmitt (INRIA)
Paul G. Spirakis (University of Patras and RACTI)
Éric Tanter (Universidad de Chile)
Nobuko Yoshida (Imperial College London)

Referees

Lucia Acciai
Peter Barron
Moritz Y. Becker
Martin Berger

Michele Boreale
Johannes Borgström
Didier Le Botlan
Maria Grazia Buscemi

Marco Carbone
Manuel Carro
Amadeo Casas
Roberto Cascella
Mariano Ceccato
Ricardo Corin
William Delobel
Simon Gay
Roberta Gori
Daniel Hedin
Kohei Honda
Fabrice Huet
Samuel Hym
Romain Janvier
Alberto Lluch Lafuente
Ivan Lanese
Cosimo Laneve
Diego Latella
Serguei Lenglet
Vasiliki Liagkou
Michael Lienhardt
Sam Lindley
Michele Loreti
Carbone Marco
Francisco Martins

Mieke Massink
Manuel Mazzara
Mario Mendez-Lojo
Edison Mera
Leonardo Gaetano Mezzina
Christopher Moore
Matthieu Morel
Stijn Mostinckx
Sebastian Nanz
Jorge Navas
Rocco De Nicola
Carlo Nocentini
Jose Pacheco
Luca Padovani
Giuseppe Persiano
David Pichardie
Antonio Ravara
Tamara Rezk
Cesar Sanchez
Ioannis Stamatou
Daniele Strollo
Josef Svenningsson
Daniele Varacca
Andres Vignaga
Elena Zucca

Sponsoring Institutions

Microsoft Research, Cambridge, UK
MSR-INRIA Joint Centre, Orsay, France
INRIA, Sophia-Antipolis, France

Table of Contents

Trustworthy Global Computing

Invited Papers

Elimination of Ghost Variables in Program Logics	1
<i>Martin Hofmann and Mariela Pavlova</i>	
Web Service Composition: From Analysis to Autonomy (Abstract)	21
<i>Jeff Magee</i>	
Service Combinators for Farming Virtual Machines (Abstract)	22
<i>Karthikeyan Bhargavan, Andrew D. Gordon, and Iman Narasamdya</i>	

Accepted Papers

Combining a Verification Condition Generator for a Bytecode Language with Static Analyses	23
<i>Benjamin Grégoire and Jorge Luis Sacchini</i>	
Extracting Control from Data: User Interfaces of MIDP Applications . . .	41
<i>Pierre Crégut</i>	
Extending Operational Semantics of the Java Bytecode	57
<i>Patryk Czarnik and Aleksy Schubert</i>	
Relational Analysis for Delivery of Services	73
<i>Flemming Nielson, Hanne Riis Nielson, Jörg Bauer, Christoffer Rosenkilde Nielsen, and Henrik Pilegaard</i>	
Logical Networks: Towards Foundations for Programmable Overlay Networks and Overlay Computing Systems	90
<i>Luigi Liquori and Michel Cosnard</i>	
Type-Safe Distributed Programming with ML5	108
<i>Tom Murphy VII, Karl Crary, and Robert Harper</i>	
Transactional Service Level Agreement	124
<i>Maria Grazia Buscemi and Hernán Melgratti</i>	
On the Complexity of Termination Inference for Processes	140
<i>Romain Demangeon, Daniel Hirschkoﬀ, Naoki Kobayashi, and Davide Sangiorgi</i>	

A Practical Approach for Establishing Trust Relationships between Remote Platforms Using Trusted Computing	156
<i>Kurt Dietrich, Martin Pirker, Tobias Vejda, Ronald Toegl, Thomas Winkler, and Peter Lipp</i>	
Access Control Based on Code Identity for Open Distributed Systems	169
<i>Andrew Cirillo and James Riely</i>	
Service Oriented Architectural Design	186
<i>Roberto Bruni, Alberto Lluch Lafuente, Ugo Montanari, and Emilio Tuosto</i>	
Replicating Web Services for Scalability	204
<i>Mario Bravetti, Stephen Gilmore, Claudio Guidi, and Mirco Tribastone</i>	
Location-Aware Quality of Service Measurements for Service-Level Agreements	222
<i>Ashok Argent-Katwala, Jeremy Bradley, Allan Clark, and Stephen Gilmore</i>	
Multipoint Session Types for a Distributed Calculus	240
<i>Eduardo Bonelli and Adriana Compagnoni</i>	
On Progress for Structured Communications	257
<i>Mariangiola Dezani-Ciancaglini, Ugo de'Liguoro, and Nobuko Yoshida</i>	
A Protocol Compiler for Secure Sessions in ML	276
<i>Ricardo Corin and Pierre-Malo Deniélou</i>	
Application of Dependency Graphs to Security Protocol Analysis	294
<i>Ilja Tšahhirov and Peeter Laud</i>	
Formal Proofs of Cryptographic Security of Diffie-Hellman-Based Protocols	312
<i>Arnab Roy, Anupam Datta, and John C. Mitchell</i>	
Anonymity Protocol with Identity Escrow and Analysis in the Applied π -Calculus	330
<i>Aybek Mukhamedov and Mark D. Ryan</i>	

Tutorial Papers

Formal Approaches to Information-Hiding	347
<i>Romain Beauvis, Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Prakash Panangaden</i>	

Computational Soundness of Equational Theories 363
 Steve Kremer

Adversaries and Information Leaks 383
 Geoffrey Smith

Author Index 401