

Proceedings

Sixth IEEE International Conference on Software Engineering and Formal Methods

SEFM 2008

10-14 November 2008 • Cape Town, South Africa

Sponsors

IEEE Computer Society
International Institute for Software Technology
of the United Nations University
Formal Methods Europe
University of Cape Town



Los Alamitos, California
Washington • Tokyo



TABLE OF CONTENTS

TUTORIAL

| | |
|---|---|
| Abstract Interpretation in Code Security | 1 |
| <i>Roberto Giacobazzi</i> | |

KEYNOTE SPEAKER 1

| | |
|--|---|
| Hiding Information in Completeness Holes: New Perspectives in Code Obfuscation and Watermarking | 2 |
| <i>Roberto Giacobazzi</i> | |

SESSION 1: ABSTRACT INTERPRETATION

| | |
|---|----|
| Nullness Analysis in Boolean Form | 14 |
| <i>Fausto Spoto</i> | |
| Widening Operators for Abstract Interpretation..... | 24 |
| <i>Agostino Cortesi</i> | |
| Static Analysis of the Determinism of Multithreaded Programs | 34 |
| <i>Pietro Ferrara</i> | |

SESSION 2: MODEL CHECKING

| | |
|---|----|
| Cheap and Small Counterexamples..... | 44 |
| <i>Henri Hansen, Jaco Geldenhuys</i> | |
| Efficient Model Checking for Duration Calculus Based on Branching-Time Approximations..... | 54 |
| <i>Martin Fränzle, Michael R. Hansen</i> | |
| Flash-Efficient LTL Model Checking with Minimal Counterexamples..... | 64 |
| <i>Stefan Edelkamp, Damian Sulewski</i> | |

SESSION 3: VERIFICATION OF EMBEDDED SYSTEMS

| | |
|--|----|
| Algebraic View Reconciliation..... | 74 |
| <i>Peter Höfner, Ridha Khedri, Bernhard Möller</i> | |
| Compositional Reasoning in Model-Based Verification of Adaptive Embedded Systems..... | 84 |
| <i>Ina Schaefer, Arnd Poetzsch-Heffter</i> | |

SESSION 4: SECURITY

| | |
|---|-----|
| Extracting Conditional Confidentiality Policies | 94 |
| <i>Michael Carl Tschantz, Jeannette M. Wing</i> | |
| Testing Privacy Policies Using Models | 104 |
| <i>Percy Pari Salas, Padmanabhan Krishnan</i> | |
| Preservation of Proof Obligations for Hybrid Verification Methods..... | 114 |
| <i>Gilles Barthe, César Kunz, David Pichardie, Julián Samborski-Forlese</i> | |

SESSION 5: TESTING I

| | |
|---|-----|
| A Generalized Model-Based Test Generation Method | 124 |
| <i>Adilson Luiz Bonifácio, Arnaldo Vieira Moura, Adenilso da Silva Simão</i> | |
| Specification-Based Testing for Software Product Lines..... | 134 |
| <i>Temesghen Kahsai, Markus Roggenbach, Bernd-Holger Schlingloff</i> | |
| Verification-Based Test Case Generation for Full Feasible Branch Coverage..... | 144 |
| <i>Christoph Gladisch</i> | |

SESSION 6: TESTING II

| | |
|---|-----|
| Tagging Makes Local Testing of Message-Passing Systems Feasible..... | 154 |
| <i>Puneet Bhateja, Madhavan Mukund</i> | |
| Using Formal Verification to Reduce Test Space of Fault-Tolerant Programs..... | 164 |
| <i>Kleber S. Xavier, Simone Hanazumi, Ana C. V. de Melo</i> | |
| Behaviour Directed Testing of Auto-code Generators..... | 174 |
| <i>Prahladavaradan Sampath, A. C. Rajeev, S. Ramesh, K. C. Shashidhar</i> | |
| Extending Stream X-Machines to Specify and Test Systems with Timeouts | 184 |
| <i>Mercedes G. Merayo, Robert M. Hierons, Manuel Núñez</i> | |

KEYNOTE SPEAKER 2

| | |
|----------------------------|-----|
| Tools for CSP | 194 |
| <i>Markus Roggenbach</i> | |

SESSION 7: ASPECT-ORIENTED DEVELOPMENT

| | |
|--|-----|
| Laws of Object-Orientation with Reference Semantics | 196 |
| <i>Leila Silva, Augusto Sampaio, Zhiming Liu</i> | |
| Specialized Aspect Languages Preserving Classes of Properties | 206 |
| <i>Simplice Djoko Djoko, Rémi Douence, Pascal Fradet</i> | |
| Tableau-Based Decision Procedure for the Multi-agent Epistemic Logic with Operators of Common and Distributed Knowledge | 216 |
| <i>Valentin Goranko, Dmitry Shkatov</i> | |

SESSION 8: REQUIREMENT AND PROGRAM ANALYSIS

| | |
|--|-----|
| Object Models with Temporal Constraints..... | 226 |
| <i>Alessandro Cimatti, Marco Roveri, Angelo Susi, Stefano Tonetta</i> | |
| A Fast Algorithm to Compute Heap Memory Bounds of Java Card Applets | 236 |
| <i>Tuan-Hung Pham, Anh-Hoang Truong, Ninh-Thuan Truong, Wei-Ngan Chin</i> | |
| PED: Proof-Guided Error Diagnosis by Triangulation of Program Error Causes..... | 245 |
| <i>Gogul Balakrishnan, Malay Ganai</i> | |

SESSION 9: TOOL PAPERS

| | |
|---|-----|
| CRefine: Support for the Circus Refinement Calculus | 256 |
| <i>M. V. M. Oliveira, A. C. Gurgel, C. G. Castro</i> | |
| An Environment for Measuring and Scheduling Time-Critical Embedded Systems with Energy Constraints | 266 |
| <i>Eduardo Tavares, Bruno Silva, Paulo Maciel</i> | |

SESSION 10: COORDINATION LANGUAGES

| | |
|--|-----|
| Modeling Component Connectors: Synchronisation and Context-Dependency | 276 |
| <i>Mohammad Izadi, Marcello M. Bonsangue, Dave Clarke</i> | |
| Generation of Service Wrapper Protocols from Choreography Specifications | 286 |
| <i>Gwen Salauen</i> | |
| Bridging the Gap between Interaction- and Process-Oriented Choreographies | 296 |
| <i>Ivan Lanese, Claudio Guidi, Fabrizio Montesi, Gianluigi Zavattaro</i> | |

SESSION 11: COMMUNICATION, MOBILE, AND INTERACTIVE SYSTEMS

| | |
|--|-----|
| Formal Change Impact Analyses of Extended Finite State Machines Using a Theorem Prover..... | 306 |
| <i>Bo Guo, Mahadevan Subramaniam</i> | |
| Restricted Broadcast Process Theory..... | 316 |
| <i>Fatemeh Ghassemi, Wan Fokkink, Ali Movaghar</i> | |
| Modelling Rational User Behaviour as Games between an Angel and a Demon..... | 326 |
| <i>Rimvydas Rukšinas, Paul Curzon, Ann Blandford</i> | |

SESSION 12: SHORT PAPERS

| | |
|---|-----|
| Formal Methods and Innovation Economy: Facing New Challenges..... | 336 |
| <i>Alexander K. Petrenko, Olga L. Petrenko</i> | |
| Behavioral Compatibility of Active Components..... | 341 |
| <i>Youcef Hammal</i> | |
| Contract-Based Verification of Hierarchical Systems of Components..... | 346 |
| <i>Sophie Quinton, Susanne Graf</i> | |

Checking Interface Interaction Protocols Using Aspect-Oriented Programming.....351

*Anh-Hoang Truong, Thanh-Binh Trinh, Dang Van_Hung, Viet-Ha Nguyen, Nguyen Thi Thu Trang,
Pham Dinh Hung*

Ontology-Based Automatic Model Transformations356

Kurt Geihs, Philipp Baer, Roland Reichle, Jens Wollenhaupt

Author Index