Lecture Notes in Computer Science 3938

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

Editorial Board

Ralf H. Reussner Judith A. Stafford
Clemens A. Szyperski (Eds.)

Architecting Systems with Trustworthy Components

International Seminar
Dagstuhl Castle, Germany, December 12-17, 2004
Revised Selected Papers

Springer

Volume Editors

Ralf H. Reussner
Universität Karlsruhe (TH)
Fakultät für Informatik
Am Fasanengarten 5, 76131 Karlsruhe, Germany
E-mail: reussner@ipd.uka.de

Judith A. Stafford
Tufts University
Department of Computer Science
161 College Avenue, Medford, MA 02155, USA
E-mail: jas@cs.tufts.edu

Clemens A. Szyperski
Microsoft
One Microsoft Way, Redmond, WA 98053, USA
E-mail: cszypers@microsoft.com

Library of Congress Control Number: 2006905119

CR Subject Classification (1998): C.2.4, D.1.3, D.2, D.4.5, F.2.1-2, D.3, F.3

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

ISSN 0302-9743
ISBN-10 3-540-35800-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-35800-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11786160 06/3142 5 4 3 2 1 0

Preface

Software components are most generally viewed as a means of software re-use and, as such, much past research has been devoted to the study of problems associated with integrating components into cohesive systems. However, even when a collection of trustworthy components have been successfully assembled the quality of the resultant system is not guaranteed. In December 2004, 41 experts on this topic from around the world, from research as well as industrial organizations, came together at Dagstuhl to discuss pressing issues related to *architecting software systems from trustworthy components*.

During the course of the cold, yet sunny, December days in Dagstuhl, discussion sessions addressed topics such as compositional reasoning on various system-level properties (such as deadlocks, live-locks etc.), compositional prediction models for different quality attributes (such as performance or reliability), blame analysis, interaction protocols, and composition frameworks. Using the liberal form of Dagstuhl Seminars, the days of the seminar were filled mostly with discussion in a variety of settings: in working sessions, around the table at meals, small groups in a corner, and also all together in the main meeting room.

Component software technologies attract much attention for their promise to enable scaling of our software industry to new levels of flexibility, diversity, and cost efficiency. Yet, these hopes collide with the reality that assemblies typically suffer from the proverbial "weakest link" phenomenon. If a component is used in a new compositional variation, then it will likely be stressed in a new way. Asserting useful properties of assemblies based on the used composition schema and theory requires a firm handle on the properties of both the components being composed and the communication mechanisms (connectors) that bind them. For such assertions to hold, these composition elements must meet their advertized properties, even if used under circumstances not explicitly envisaged by their developers. A component or connector that fails to do so becomes a weak link of its hosting assembly and may cause the entire assembly to fail to meet its advertized properties.

In contrast, components that promise to be a strong link in their assemblies can be called 'trustworthy' and ways to get to the construction and proper use of such components was the subject of this seminar. Transitively, the seminar was also concerned with trustworthy assemblies: assemblies that reliably meet their requirements based on trustworthy components and solid composition methods.

The weakest link phenomenon is not a new observation, but the recent trends to move to dynamic and late composition of non-trivial components exasperate the problem. A concrete example promising deep widespread relevance are Web services. The problem space is complex and multi-faceted. Practical solutions will have to draw on combined insights from a diverse range of disciplines, including component software technology, software engineering, software architecture, dependable systems, formal methods, as well as areas such as type systems and proof-carrying code.

A lot of good, and sometimes even groundbreaking, work has been performed in the focus area of this seminar, but many problems remain open. To spark discussions, a small set of core problems was prepared by the organizers:

- Measurement and normalization of extra-functional properties
- Modular reasoning over extra-functional properties
- capture of component requirements in interfaces and protocols
- Interference and synergy of top-down and bottom-up aspects
- Duality of componentization and architecture
- System properties (non-deadlocks, liveness, fairness, etc.)
- Opportunities for correctness by construction/static checking

All of these problems are considered hard today and yet, all of them, if solved appropriately, promise the creation of key stepping stones toward an overall approach yielding trustworthy components as well as trustworthy compositions. It is likely that any such approach supports a multitude of more specialized disciplines and methods, targeting different requirement profiles at the assembly level; for example, those with tight resource management or that rely on real-time characteristics.

Most of the time at Dagstuhl was used for focused discussions in break-out groups; the abstracts of the break-out groups as well as position papers submitted by all participants are available on the seminar Website. In this volume of *Lecture Notes on Computer Science* we present extended papers reflecting work of seminar participants. Among the articles are ten peer-reviewed papers and five invited papers of outstanding researchers whose work is related to the Dagstuhl seminar but were not able to attend. The peer-reviewed papers were submitted by participants after the conclusion of the workshop and were selected based upon the high quality of scholarly work, their timeliness, and their appropriateness to the goals of the seminar, some reflecting ongoing collaboration that grew out of the seminar.

We would like to gratefully acknowledge the friendly and very helpful support of the Dagstuhl administration staff, Alfred Hofmann from Springer for his support during the preparation and publication of the LNCS volume and Klaus Krogmann for preparing the final manuscript for Springer.

Karlsruhe, Medford, and Redmond
February 2006

Ralf Reussner
Judith Stafford
Clemens Szyperski

Organization

Architecting Systems with Trustworthy Components

(Dagstuhl Seminar 04511)

Organizers

Ralf Reussner, Universität Karlsruhe (T.H.), Germany
Judith Stafford, Tufts University, USA
Clemens Szyperski, Microsoft Corp., USA

Participants

Uwe Aßmann, TU Dresden, Germany
Colin Atkinson, University of Mannheim, Germany
Steffen Becker, University of Oldenburg, Germany
Jan Bredereck, TZI, Bremen, Germany
Antonia Brogi, Università di Pisa, Italy
Christian Bunse, Fraunhofer IESE, Germany
Ivica Crnkovic, Mälardalen University, Sweden
Viktoria Firus, University of Oldenburg, Germany
Kathi Fisler, Worcester Polytechnic Institute, USA
Felix C. Freiling, RWTH Aachen, Germany
Sabine Glesner, Universität Karlsruhe (T.H.), Germany
Gerhard Goos, Universität Karlsruhe (T.H.), Germany
Ian Gorton, NICTA, Australia
Lars Grunske, The University of Queensland, Australia
Christine Hofmeister , Lehigh Univ. - Bethlehem, USA
Jens-Holger Jahnke, University of Victoria, Canada
Jean-Marc Jézéquel, IRISA (Univ. Rennes & INRIA), France
Bernd Krämer, FernUniversität in Hagen, Germany
Shriram Krishnamurthi, Brown Univ. - Providence, USA
Juliana Küster-Filipe, The University of Birmingham, UK
Stig Larsson, ABB - Västerås, Sweden
Nicole Levy, University of Versailles, France
Raffaela Mirandola, University of Rome TorVergata, Italy
Sven Overhage, Universität Augsburg, Germany
Frantisek Plasil, Charles University, Czech Republic
Iman Poernomo, King's College London, UK
Alexander Romanovsky, University of Newcastle, UK
Christian Salzmann, BMW Car IT, Germany
Thomas Santen, TU Berlin, Germany

Heinz Schmidt, Monash University, Australia
Jürgen Schneider, IBM - Böblingen, Germany
Asuman Sünbül, SAP Research Labs - Palo Alto, USA
Massimo Tivoli, Univ. degli Studi di L'Aquila, Italy
Kurt Wallnau, Software Engineering Institute, USA
Wolfgang Weck, Independent Software Architect, Switzerland
Rob van Ommering, Philips Research - Eindhoven, The Netherlands
Willem-Jan van den Heuvel, Tilburg University, The Netherlands

Invited Contributions

Antonia Bertolino, ISTI CNR Pisa, Italy
Manfred Broy, TU Munich, Germany
Bertrand Meyer, ETH Zurich, Switzerland
Wolfgang Pree, University of Salzburg, Austria
Heike Wehrheim, University of Paderborn, Germany

Publication date: May 2006

Table of Contents

Invited Articles

Articles by Participants