Lecture Notes in Computer Science 5429

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

Fabio Massacci Samuel T. Redwine Jr.
Nicola Zannone (Eds.)

Engineering Secure Software and Systems

First International Symposium, ESSoS 2009
Leuven, Belgium, February 4-6, 2009
Proceedings

Springer

Volume Editors

Fabio Massacci
Università di Trento
Dipartimento di Ingegneria e Scienza dell'Informazione
Via Sommarive 14, 38050 Povo (Trento), Italy
E-mail: fabio.massacci@unitn.it

Samuel T. Redwine Jr.
James Madison University
Department of Computer Science
701 Carrier Drive, Harrisonburg, VA 22807, USA
E-mail: redwinst@cisat.jmu.edu

Nicola Zannone
University of Toronto
Department of Computer Science
40 St. George Street, Toronto, ON M5S 2E4, Canada
E-mail: zannone@cs.toronto.edu

Library of Congress Control Number: Applied for

CR Subject Classification (1998): D.2, D.4.6, H.2.7, J.1, K.6.3, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-00198-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-00198-7 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12612079 06/3180 5 4 3 2 1 0

Preface

It is our pleasure to welcome you to the first edition of the International Symposium on Engineering Secure Software and Systems.

This unique events aims at bringing together researchers from Software Engineering and Security Engineering, helping to unite and further develop the two communities in this and future editions. The parallel technical sponsorships from the ACM SIGSAC (the ACM interest group in security) and ACM SIGSOFT (the ACM interest group in software engineering) and the IEEE TCSE is a clear sign of the importance of this inter-disciplinary research area and its potential.

The difficulty of building secure software systems is no longer focused on mastering security technology such as cryptography or access control models. Other important, and less controllable, factors include the complexity of modern networked software systems, the unpredictability of practical development lifecycles, the intertwining of and trade-off between functionality, security and other qualities, the difficulty of dealing with human factors, and so forth. Over the last few years, an entire research domain has been building up around these problems. And although some battles have been won, the jury is still out on the final verdict.

The conference program included two major keynotes from Axel Van Lamsweerde (U. Louvain) and Wolfram Schulte (Microsoft Research) and an interesting blend of research, industry and idea papers.

In response to the call for paper, 57 papers were submitted. The Program Committee selected 10 papers as research papers (17.5%), presenting new research results in the realm of engineering secure software and systems. It further selected four industry reports, detailing concrete case studies in industry and the lessons that practitioners and researchers can learn out of this experience. We also included four ideas papers that the Program Committee judged as interesting but not yet mature for a full paper presentation.

The program also featured a slate of tutorials by industry representatives on "Security by Construction" by Rod Champan (Praxis), "Management in Practice – Model – Based Security Risk Analysis with the CORAS Method" by Heidi E. I. Dahl and Mass Soldal Lund (SINTEF), "Inside the Biggest of the OWASP Top-10 Issues" by R. van Wyk (KRvW Associates, LLC), and a research tutorial on "Security – Philosophy, Patterns and Practices" by Munawar Hafiz (University of Illinois at Urbana-Champaign).

Many individuals and organizations contributed to the success of this event. First of all, we would like to express our appreciation to the authors of the submitted papers, and to the Program Committee members and external referees, who provided timely and relevant reviews. Many thanks go to the Steering Committee for supporting this and future editions of the symposium, and to all the members of the Organizing Committee for their tremendous work and for

excelling in their respective tasks. Nicola Zannone did a great job by assembling the proceedings for Springer.

We owe gratitude to ACM SIGSAC/SIGSOFT, IEEE TCSE and LNCS for supporting us in this new scientific endeavor.

Last but not least, we would like to thank all sponsors, and the DistriNet research group of the K.U.Leuven in particular, for covering the financial aspects of the event.

November 2008

Bart De Win
Fabio Massacci
Sam Redwine

Organization

General Chair

Bart De Win	Katholieke Universiteit Leuven, Belgium

Program Co-chairs

Fabio Massacci	Università di Trento, Italy
Samuel Redwine	James Madison University, USA

Publication Chair

Nicola Zannone	University of Toronto, Canada

Tutorial Chair

Riccardo Scandariato	Katholieke Universiteit Leuven, Belgium

Financial Chair

Katrien Janssens	Katholieke Universiteit Leuven, Belgium

Local Arrangements Chair

Koen Yskout	Katholieke Universiteit Leuven, Belgium

Steering Committee

Gary McGraw	Cigital, USA
Bashar Nuseibeh	The Open University, UK
Jorge Cuellar	Siemens AG, Germany
Fabio Massacci	Università di Trento, Italy
Samuel Redwine	James Madison University, USA
Wouter Joosen	Katholieke Universiteit Leuven, Belgium

Program Committee

Matt Bishop	University of California (Davis), USA
Brian Chess	Fortify Software, USA
Richard Clayton	Cambridge University, UK
Christian Collberg	University of Arizona, USA
Noopur Davis	Davis Systems, USA

Bart De Win	Katholieke Universiteit Leuven, Belgium
Juergen Doser	ETH, Switzerland
Eduardo Fernández-Medina	University of Castilla-La Mancha, Spain
Dieter Gollmann	Hamburg University of Technology, Germany
Michael Howard	Microsoft, USA
Cynthia Irvine	Naval Postgradual School, USA
Jan Jürjens	Open University, UK
Volkmar Lotz	SAP Labs, France
Antonio Maña	University of Malaga, Spain
Robert Martin	MITRE, USA
Fabio Massacci	Università di Trento, Italy
Mira Mezini	Darmstadt University, Germany
Mattia Monga	Milan University, Italy
Andy Ozment	DoD, USA
Gunther Pernul	Universitat Regensburg, Germany
Domenico Presenza	Engineering, Italy
Samuel Redwine	James Madison University, USA
Riccardo Scandariato	Katholieke Universiteit Leuven, Belgium
Ketil Stølen	Sintef, NO
Eric Vetillard	Trusted Logic, France
Jon Whittle	Lancaster University, UK
Mohammad Zulkernine	Queen's University, Canada

External Reviewers

Mohamed Atef
Sean Barnum
Christian Broser
Istehad Chowdhury
Heidi Dahl
Lieven Desmet
Francois Dupressoir
Stefan Durbeck
Joy Forsythe
Christoph Fritsch
Oliver Gmelch
Wolfgang Hennes
Thomas Heyman
Shahriar Hussein
Jan Kolter
Hristo Koshutanski
Edward Lee
Fredrick Lee
Olav Ligaarden
Matias Madou
Lorenzo Martignoni
Chris McLaughlin
Steven Murdoch
Antonio Muñoz
Brian O'Hanion
Yekaterina O'Neil
Aida Omerovic
Gimena Pujol
Atle Refsdal
Alfonso Rodriguez
Rolf Schillinger
Bjørnar Solhaug
Stefan Taubenberger
Hsiao-Ming Tsou
Lingyu Wang
Jacob West
Michael Yang
Yves Younan
Koen Yskout

Table of Contents

Policy Verification and Enforcement

Verification of Business Process Entailment Constraints Using SPIN 1
Christian Wolter, Philip Miseldine, and Christoph Meinel

From Formal Access Control Policies to Runtime Enforcement Aspects 16
Slim Kallel, Anis Charfi, Mira Mezini, Mohamed Jmaiel, and Karl Klose

Idea: Trusted Emergency Management 32
Timothy E. Levin, Cynthia E. Irvine, Terry V. Benzel, Thuy D. Nguyen, Paul C. Clark, and Ganesha Bhaskara

Model Refinement and Program Transformation

Idea: Action Refinement for Security Properties Enforcement 37
Fabio Martinelli and Ilaria Matteucci

Pattern-Based Confidentiality-Preserving Refinement 43
Holger Schmidt

Architectural Refinement and Notions of Intransitive Noninterference 60
Ron van der Meyden

Systematically Eradicating Data Injection Attacks Using Security-Oriented Program Transformations 75
Munawar Hafiz, Paul Adamczyk, and Ralph Johnson

Secure System Development

Report: Measuring the Attack Surfaces of Enterprise Software 91
Pratyusa K. Manadhata, Yuecel Karabulut, and Jeannette M. Wing

Report: Extensibility and Implementation Independence of the .NET Cryptographic API 101
Pieter Philippaerts, Cédric Boon, and Frank Piessens

Report: CC-Based Design of Secure Application Systems 111
Robin Sharp

Protection Poker: Structuring Software Security Risk Assessment and Knowledge Transfer 122
Laurie Williams, Michael Gegick, and Andrew Meneely

Attack Analysis and Prevention

Toward Non-security Failures as a Predictor of Security Faults and Failures 135
Michael Gegick, Pete Rotella, and Laurie Williams

A Scalable Approach to Full Attack Graphs Generation 150
Feng Chen, Jinshu Su, and Yi Zhang

MEDS: The Memory Error Detection System 164
Jason D. Hiser, Clark L. Coleman, Michele Co, and Jack W. Davidson

Testing and Assurance

Idea: Automatic Security Testing for Web Applications 180
Thanh-Binh Dao and Etsuya Shibayama

Report: Functional Security Testing Closing the Software – Security Testing Gap: A Case from a Telecom Provider 185
Albin Zuccato and Clemens Kögler

Idea: Measuring the Effect of Code Complexity on Static Analysis Results 195
James Walden, Adam Messer, and Alex Kuhl

Author Index 201