

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Úlfar Erlingsson Roel Wieringa
Nicola Zannone (Eds.)

Engineering Secure Software and Systems

Third International Symposium, ESSoS 2011
Madrid, Spain, February 9-10, 2011
Proceedings

Volume Editors

Úlfar Erlingsson
Google Inc.
1288 Pear Ave, Mountain View, CA 94043, USA
E-mail: ulfar@google.com

Roel Wieringa
University of Twente, Computer Science Department
Drienerlolaan 5, 7522 NB Enschede, The Netherlands
E-mail: r.j.wieringa@ewi.utwente.nl

Nicola Zannone
Eindhoven University of Technology
Faculty of Mathematics and Computer Science
Den Dolech 2, 5612 AZ Eindhoven, The Netherlands
E-mail: n.zannone@tue.nl

ISSN 0302-9743
ISBN 978-3-642-19124-4
DOI 10.1007/978-3-642-19125-1
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-19125-1

Library of Congress Control Number: 2011920029

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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)

Preface

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

This unique event aims at bringing together researchers from software engineering and security engineering, which might help 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) is a clear sign of the importance of this interdisciplinary 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 factors include the complexity of modern networked software systems, the unpredictability of practical development life-cycles, 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.

The conference program include two major keynotes from George Candea (École Polytechnique Fédérale de Lausanne) on automated cloud-based software reliability services and Mark Ryan (University of Birmingham) on the analysis of security properties of electronic voting systems, and an interesting blend of research and idea papers.

In response to the call for papers, 63 papers were submitted. The Program Committee selected 18 contributions as research papers (29%), presenting new research results in the realm of engineering secure software and systems. It further selected three idea papers, which gave crisp expositions of interesting, novel ideas in the early stages of development.

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. The DistriNet research group of the K.U. Leuven did an excellent job for the website and the advertising for the conference. Nicola Zannone did a great job by assembling the proceedings for Springer.

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

December 2010

Úlfar Erlingsson
Roel Wieringa
Manuel Clavel

Conference Organization

General Chair

Manuel Clavel
Imdea Software/Universidad Complutense de
Madrid, Spain

Program Co-chairs

Úlfar Erlingsson
Roel Wieringa
Google Inc., US/Reykjavik University, Iceland
University of Twente, The Netherlands

Publication Chair

Nicola Zannone
Eindhoven University of Technology,
The Netherlands

Publicity Chair

Pieter Philippaerts
Katholieke Universiteit Leuven, Belgium

Local Arrangements Chair

Marina Egea
Imdea Software, Spain

Steering Committee

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

Programme Committee

Thomas Alspaugh
Jo Atlee
Bruno Blanchet
Hao Chen
Frederic Cuppens
Prem Devanbu
University of California at Irvine, USA
University of Waterloo, Canada
Ecole Normale Supérieure, France
University of California, Davis, USA
Ecole Nationale Supérieure de
Télécommunication Bretagne, France
University of California at Davis, USA

Eric Dubois	Centre de Recherche Public Henri Tudor, Luxembourg
Christof Ebert	Vector Consulting, Germany
Manuel Fahndrich	Microsoft Research, USA
Eduardo Fernandez-Medina	Universidad de Castilla-La Mancha, Spain
Robert France	Colorado State University, USA
Vinod Ganapathy	Rutgers University, USA
Dieter Gollman	Hamburg University of Technology, Germany
Siv Hilde Houmb	Telenor, Norway
Martin Johns	SAP Research, Germany
Jan Jurjens	Technische Universität Dortmund, Germany
Yuecel Karabulut	SAP Labs, USA
Seok-Won Lee	University of North Carolina Charlotte, USA
Lin Liu	Tsinghua University, China
Robert Martin	MITRE, USA
Vaclav Matyas	Masaryk University, Czech Republic
Sjouke Mauw	University of Luxembourg, Luxembourg
Chris Mitchell	Royal Holloway, UK
Akito Monden	Nara Institute of Science and Technology, Japan
Haralambos Mouratidis	University of East London, UK
Marcus Peinado	Microsoft Research, USA
Erik Poll	University of Nijmegen, The Netherlands
David Sands	Chalmers University, Sweden
Angela Sasse	University College London, UK
Venkat Venkatakrishnan	University of Illinois at Chicago, USA

External Reviewers

Aizatulin, Misha	Ochoa, Martin
Berkman, Omer	Phung, Phu H.
Birgisson, Arnar	Poolsappasit, Nayot
Blanco, Carlos	Radomirovic, Sasa
Brucker, Achim D.	Rafnsson, Willard
Cuppens-Boulahia, Nora	Rosado, David G.
Del Tedesco, Filippo	Russo, Alejandro
Dobias, Jaromir	Sánchez, Luis Enrique
Garcia-Alafaro, Joaquin	Schmidt, Holger
Gerguri, Shkodran	Schweitzer, Patrick
Hirsch, Martin	Stetsko, Andriy
Kordy, Barbara	Svenda, Petr
Kur, Jiri	Tucek, Pavel
Magazinius, Jonas	van Deursen, Ton
Nikiforakis, Nick	van Sinderen, Marten J.

Table of Contents

Session 1. Model-Based Security I

Model-Based Refinement of Security Policies in Collaborative Virtual Organisations	1
<i>Benjamin Aziz, Alvaro E. Arenas, and Michael Wilson</i>	
Automatic Conformance Checking of Role-Based Access Control Policies via Alloy	15
<i>David Power, Mark Slaymaker, and Andrew Simpson</i>	
Security Validation of Business Processes via Model-Checking	29
<i>Wihem Arsac, Luca Compagna, Giancarlo Pellegrino, and Serena Elisa Ponta</i>	

Session 2. Tools and Mechanisms

On-Device Control Flow Verification for Java Programs	43
<i>Arnaud Fontaine, Samuel Hym, and Isabelle Simplot-Ryl</i>	
Efficient Symbolic Execution for Analysing Cryptographic Protocol Implementations	58
<i>Ricardo Corin and Felipe Andrés Manzano</i>	
Predictability of Enforcement	73
<i>Nataliia Bielova and Fabio Massacci</i>	

Session 3. Web Security

SessionShield: Lightweight Protection against Session Hijacking	87
<i>Nick Nikiforakis, Wannes Meert, Yves Younan, Martin Johns, and Wouter Joosen</i>	
Security Sensitive Data Flow Coverage Criterion for Automatic Security Testing of Web Applications	101
<i>Thanh Binh Dao and Etsuya Shibayama</i>	
Middleware Support for Complex and Distributed Security Services in Multi-tier Web Applications	114
<i>Philippe De Ryck, Lieven Desmet, and Wouter Joosen</i>	

Session 4. Model-Based Security II

Lightweight Modeling and Analysis of Security Concepts 128
Jörn Eichler

A Tool-Supported Method for the Design and Implementation of Secure Distributed Applications 142
Linda Ariani Gunawan, Frank Alexander Kraemer, and Peter Herrmann

An Architecture-Centric Approach to Detecting Security Patterns in Software 156
Michaela Bunke and Karsten Sohr

Session 5. Security Requirements Engineering

The Security Twin Peaks 167
Thomas Heyman, Koen Yskout, Riccardo Scandariato, Holger Schmidt, and Yijun Yu

Evolution of Security Requirements Tests for Service-Centric Systems 181
Michael Felderer, Berthold Agreiter, and Ruth Breu

After-Life Vulnerabilities: A Study on Firefox Evolution, Its Vulnerabilities, and Fixes 195
Fabio Massacci, Stephan Neuhaus, and Viet Hung Nguyen

Session 6. Authorization

Authorization Enforcement Usability Case Study 209
Steffen Bartsch

Scalable Authorization Middleware for Service Oriented Architectures 221
Tom Goovaerts, Lieven Desmet, and Wouter Joosen

Adaptable Authentication Model: Exploring Security with Weaker Attacker Models 234
Naveed Ahmed and Christian D. Jensen

Session 7. Ideas

Idea: Interactive Support for Secure Software Development 248
Jing Xie, Bill Chu, and Heather Richter Lipford

Idea: A Reference Platform for Systematic Information Security Management Tool Support	256
<i>Ingo Müller, Jun Han, Jean-Guy Schneider, and Steven Versteeg</i>	
Idea: Simulation Based Security Requirement Verification for Transaction Level Models	264
<i>Johannes Loinig, Christian Steger, Reinhold Weiss, and Ernst Haselsteiner</i>	
Author Index	273