Lecture Notes in Computer Science 5705

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
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 of Computer Science, Saarbruecken, Germany

Alessandro Aldini Gilles Barthe
Roberto Gorrieri (Eds.)

Foundations of Security Analysis and Design V

FOSAD 2007/2008/2009 Tutorial Lectures

Springer

Volume Editors

Alessandro Aldini
Università degli Studi di Urbino "Carlo Bo"
Istituto di Scienze e Tecnologie dell'Informazione
Piazza della Repubblica 13, 61029 Urbino, Italy
E-mail: alessandro.aldini@uniurb.it

Gilles Barthe
Universidad Politécnica de Madrid
Facultad de Informatica
Fundación IMDEA Software
Campus Montegancedo, 28660 Boadilla del Monte, Madrid, Spain
E-mail: gilles.barthe@imdea.org

Roberto Gorrieri
Università degli Studi di Bologna
Dipartimento di Scienze dell'Informazione
Mura Anteo Zamboni 7, 40127 Bologna, Italy
E-mail: gorrieri@cs.unibo.it

Library of Congress Control Number: 2009932255

CR Subject Classification (1998): D.4.6, C.2, K.6.5, K.4, D.3, F.3, E.3

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-03828-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-03828-0 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: 12738250 06/3180 5 4 3 2 1 0

Preface

This book presents a collection of tutorial papers accompanying lectures from the last three editions of the International School on Foundations of Security Analysis and Design (FOSAD).

FOSAD has been one of the foremost educational events established with the goal of disseminating knowledge in the critical area of security in computer systems and networks. The main aim of FOSAD is to offer a good spectrum of current research in foundations of security – ranging from programming languages to analysis of protocols, from cryptographic algorithms to access control policies and trust/identity management – that can be of help for graduate students and young researchers from academia or industry who intend to approach the field. Another objective of FOSAD is to propose panels dedicated to topical open problems and to allow a selected number of participants to give presentations about their ongoing work, in order to favor discussions and novel scientific collaborations.

The topics covered in this book include cryptographic protocol analysis, program and resource certification, identity management and electronic voting, access and authorization control, wireless security, mobile code and communications security.

The opening paper presented by Santiago Escobar, Catherine Meadows, and José Meseguer gives an overview of the Maude-NRL Protocol Analyzer, a tool for the analysis of cryptographic protocols using functions that obey different equational theories. In a proof-carrying code framework, Gilles Barthe and César Kunz present a technique to build, from a certificate of the source program, a certificate for the result of its compilation. The paper by David Chadwick addresses in a survey several different topics concerning federated identity management. Bart Jacobs and Wolter Pieters discuss technical and social aspects of electronic voting systems, by presenting as a case study the system implemented in practice in The Netherlands. The paper by Martín Abadi provides an overview of the role of logic in access control, by covering logical foundations for access control and their applications in languages for security policies. Sebastian Mödersheim and Luca Viganò introduce the open-source fixed-point model checker OFMC for symbolic cryptographic protocol analysis. Rustan Leino, Peter Müller, and Jan Smans describe a verifier for concurrent programs called Chalice, whose methodology centers around permissions and permission transfer. Frédéric Besson, David Cachera, Thomas Jensen and David Pichardie propose a tutorial on building analyzers using the Coq proof assistant. In particular, they propose an interval analysis for the static verification of the absence of array-out-of-bounds accesses. Elvira Albert, Puri Arenas, Samir Genaim, Germán Puebla, and Damiano Zanardini present the COSTA system, a state-of-the-art analyzer that automatically generates precise resource usage information for a large class

of Java programs. In the last paper, Javier Lopez, Rodrigo Roman, and Cristina Alcaraz analyze how different requirements of sensor networks can influence the security mechanisms.

We would like to thank all the institutions that have promoted and founded FOSAD in the last few years. In particular, we are grateful to the IFIP Working Group 1.7 on "Theoretical Foundations of Security Analysis and Design," which was established to promote research and education in security-related issues. Among the sponsors, we would like to mention CNR-IIT, Department of the Navy Grant N00014-08-1-1109 issued by Office of Naval Research Global, EU projects SENSORIA and MOBIUS, International Workshop on Views On Designing Complex Architectures (VODCA), and Università di Bologna. Every year, FOSAD is supported by EATCS-IT, EEF, and ERCIM Working Group on Security and Trust Management.

Finally, we also wish to thank the entire staff of the University Residential Centre of Bertinoro for the organizational and administrative support.

June 2009

Alessandro Aldini
Gilles Barthe
Roberto Gorrieri

Table of Contents

Foundations of Security Analysis and Design

Part I: FOSAD 2007

Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties 1
Santiago Escobar, Catherine Meadows, and José Meseguer

Part II: FOSAD 2008

An Introduction to Certificate Translation 51
Gilles Barthe and César Kunz

Federated Identity Management 96
David W. Chadwick

Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment 121
Bart Jacobs and Wolter Pieters

Part III: FOSAD 2009

Logic in Access Control (Tutorial Notes) 145
Martín Abadi

The Open-Source Fixed-Point Model Checker for Symbolic Analysis of Security Protocols 166
Sebastian Mödersheim and Luca Viganò

Verification of Concurrent Programs with Chalice 195
K. Rustan M. Leino, Peter Müller, and Jan Smans

Certified Static Analysis by Abstract Interpretation 223
Frédéric Besson, David Cachera, Thomas Jensen, and David Pichardie

Resource Usage Analysis and Its Application to Resource Certification 258
Elvira Albert, Puri Arenas, Samir Genaim, Germán Puebla, and Damiano Zanardini

Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks 289
Javier Lopez, Rodrigo Roman, and Cristina Alcaraz

Author Index 339