Lecture Notes in Computer Science 6858

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

Alessandro Aldini Roberto Gorrieri (Eds.)

Foundations of Security Analysis and Design VI

FOSAD Tutorial Lectures

Springer

Volume Editors

Alessandro Aldini
Università degli Studi di Urbino "Carlo Bo"
Dipartimento di Scienze di Base e Fondamenti
Piazza della Repubblica 13
61029 Urbino, Italy
E-mail: alessandro.aldini@uniurb.it

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-23081-3 e-ISBN 978-3-642-23082-0
DOI 10.1007/978-3-642-23082-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011934268

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

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)

International School on Foundations of Security Analysis and Design

This book is the sixth in a series of volumes collecting tutorial papers accompanying lectures presented at FOSAD, the International Summer School on Foundations of Security Analysis and Design, which has been held yearly since 2000 at the University Residential Center of Bertinoro, Italy. 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.

Every year, FOSAD offers 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. The spirit of FOSAD is also characterized by the "open session", which represents a series of presentations given by selected participants about their ongoing work. The objective of this initiative is to encourage discussions, propose new ideas, comment on open problems, and favor novel scientific collaborations.

The topics covered in this book include privacy and data protection, security APIs, cryptographic verification by typing, model-driven security, noninterference analysis, security in governance, risk, and compliance, lattice cryptography, quantitative information flow analysis, and risk analysis.

The opening paper presented by Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati gives an overview of the techniques developed for protecting data and ensuring privacy. Riccardo Focardi, Flaminia Luccio, and Graham Steel discuss the subtleties behind the design of secure application program interfaces (security APIs) and show that their analysis through formal techniques has recently proved highly successful both in finding new flaws and verifying security properties of improved designs. The tutorial paper by Cédric Fournet, Karthikeyan Bhargavan, and Andrew Gordon shows the use of types for verifying authenticity properties of cryptographic protocols. The paper by David Basin, Manuel Clavel, Marina Egea, Miguel García de Dios, Carolina Dania, Gonzalo Ortiz, and Javier Valdazo is a survey of a very promising instance of model-driven security. The authors present an approach and a toolkit supporting the construction of security, data, and graphical user interface (GUI) models together with related Web applications. Roberto Gorrieri and Matteo Vernali extend the notion of intransitive noninterference by Rushby to the frameworks of deterministic labelled transition systems, nondeterministic automata, and the class of Petri nets called elementary net systems. Yudistira Asnar and Fabio Massacci describe a methodology to design systems trading information security with governance, risk, and compliance (GRC) management. Daniele Micciancio gives an introduction to the mathematical theory and appli-

cation of lattice cryptography, which is one of the hottest and fast-moving areas in mathematical cryptography today. Mário Alvim, Miguel Andrés, Konstantinos Chatzikokolakis, and Catuscia Palamidessi review two information-theoretic approaches to the quantitative analysis of information flows, namely, the one based on Shannon entropy, and the one based on Rényi min-entropy. In the last paper, Mass Soldal Lunda, Bjørnar Solhauga, and Ketil Stølen introduce general techniques and guidelines for dealing with risk analysis in systems evolving over time. In particular, the authors propose the CORAS approach to model-driven risk analysis.

This year, FOSAD was organized in cooperation with the Network of Excellence on Engineering Secure Future Internet Software Services and Systems (EU FP7 Project NESSoS). Obviously, we would like to thank all the institutions that have promoted and founded FOSAD in the last few years. Finally, we also wish to thank all the staff of the University Residential Center of Bertinoro for the organizational and administrative support.

August 2011

Alessandro Aldini
Roberto Gorrieri

Table of Contents

Foundations of Security Analysis and Design