Lecture Notes in Computer Science 3655

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

Editorial Board

Alessandro Aldini Roberto Gorrieri
Fabio Martinelli (Eds.)

Foundations of Security Analysis and Design III

FOSAD 2004/2005 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: aldini@sti.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

Fabio Martinelli
Istituto di Informatica e Telematica - IIT
National Research Council - C.N.R., Pisa Research Area
Via G. Moruzzi 1, 56100 Pisa, Italy
E-mail: Fabio.Martinelli@iit.cnr.it

Library of Congress Control Number: 2005931798

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

ISSN 0302-9743
ISBN-10 3-540-28955-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28955-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11554578 06/3142 5 4 3 2 1 0

Preface

The increasing relevance of security to real-life applications, such as electronic commerce and Internet banking, is attested by the fast-growing number of research groups, events, conferences, and summer schools that address the study of foundations for the analysis and the design of security aspects. The "International School on Foundations of Security Analysis and Design" (FOSAD, see http://www.sti.uniurb.it/events/fosad/) has been one of the foremost events established with the goal of disseminating knowledge in this critical area, especially for young researchers approaching the field and graduate students coming from less-favoured and non-leading countries.

The FOSAD school is held annually at the Residential Centre of Bertinoro (http://www.ceub.it/), in the fascinating setting of a former convent and episcopal fortress that has been transformed into a modern conference facility with computing services and Internet access. Since the first school, in 2000, FOSAD has attracted more than 250 participants and 50 lecturers from all over the world. A collection of tutorial lectures from FOSAD 2000 was published in Springer's LNCS volume 2171. Some of the tutorials given at the two successive schools (FOSAD 2001 and 2002) are gathered in a second volume, LNCS 2946. To continue this tradition, the present volume collects a set of tutorials from the fourth FOSAD, held in 2004, and from FOSAD 2005.

The opening paper by Michael Backes, Birgit Pfitzmann, and Michael Waidner, reports on the integration between the classical Dolev-Yao model of security and the computational view of cryptography. In particular, the authors present an idealized cryptographic library that extends the applicability of the Dolev-Yao model for automated proofs of cryptographic protocols to provably secure cryptographic implementations. Jan Jürjens gives an overview of UMLsec, an extension of the Unified Modelling Language that allows the expression of security-relevant information within the diagrams in a system specification. François Koeune and François-Xavier Standaert present a survey on implementation-specific attacks, which attempt to exploit the physical constraints of any real-life cryptographic device (running time, power consumption, ...) to expose the device's secrets. The authors provide a tutorial on this subject, overviewing the main kinds of attacks and highlighting their underlying principles. Riccardo Focardi's paper presents the basics of authentication protocols and illustrates a specific technique for statically analyzing protocol specifications. The technique works in the presence of both malicious outsiders and compromized insiders, with no limitation on the number of parallel sessions.

Gilles Barthe and Guillaume Dufay illustrate some applications of formal methods to increase the reliability of smartcards and trusted personal devices, with respect to both platform correctness and applet validation. Their paper focuses on devices that embed Java Virtual Machines or their variants, in par-

ticular Java Card Virtual Machines. Elisa Bertino, Ji-Won Byun, and Ninghui Li deal with various aspects of privacy-preserving data management systems. In particular, they focus on database management systems that are able to enforce privacy promises encoded in privacy languages such as P3P. Herve Debar and Jouni Viinikka's paper covers intrusion detection and security information management technologies, focusing on data sources and analysis techniques. To conclude, Fabio Massacci, Paolo Giorgini, and Nicola Zannone review the state of the art in security requirements engineering and discuss their approach to modelling and analyzing security, the Secure Tropos methodology.

We think that this tutorial book offers an interesting view of what is going on worldwide at present in the security field. We would like to thank all the institutions that have promoted and founded this school and, in particular, the IFIP Working Group on "Theoretical Foundations of Security Analysis and Design" (http://www.dsi.unive.it/IFIPWG1_7/), which was established to promote research and education in security-related issues. FOSAD 2005 was sponsored by CNR-IIT, Create-Net, and the Università di Bologna, and has been supported by EATCS-IT, EEF, and the ERCIM Working Group on Security and Trust Management (http://www.iit.cnr.it/STM-WG/). Finally, we also wish to thank the whole staff of the University Residential Centre of Bertinoro for the organizational and administrative support.

June 2005

Alessandro Aldini
Roberto Gorrieri
Fabio Martinelli

Table of Contents

Part I: FOSAD 2004 (6-11 September 2004)

Part II: FOSAD 2005 (19-24 September 2005)