Lecture Notes in Computer Science 4677

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 IV

FOSAD 2006/2007 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

Library of Congress Control Number: 2007933834

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 3-540-74809-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74809-0 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12119967 06/3180 5 4 3 2 1 0

International School on Foundations of Security Analysis and Design

The last decade has witnessed a widespread shifting of real-life and usual practice operations, which are moving from the real-world scenario toward the Internet world, as shown for instance by the success of electronic payments and Internet banking. At the same time, this fast-growing interest toward the new technologies is open to criticism whenever it is not accompanied with an adequate development of the security machinery, as shown in the past by malfunctions in electronic voting and shopping systems.

The critical aspect of security of computer systems is dealt with by an increasing number of academic and industrial research groups, scientific conferences and events. The "International School on Foundations of Security Analysis and Design" (FOSAD, for short) has been one of the foremost events established with the objective of disseminating knowledge in this critical area and favoring the study of foundations for the analysis and the design of security aspects. FOSAD is mainly addressed to young scientists and graduate students at their initial approaches to the field, but also to researchers aiming at establishing novel scientific collaborations and scientists coming from less-favored and non-leading countries in this field.

FOSAD is held annually at the Residential Centre of Bertinoro, Italy, in the fascinating scenario of a former convent and episcopal fortress that has been transformed into a modern conference facility with computing services and Internet access. The first edition of FOSAD was held in 2000, and since then another six editions (including the present one in September 2007) followed, by attracting about 350 participants and 70 leading scientists of the computer security community worldwide. The Web site of the FOSAD series is available at http://www.sti.uniurb.it/events/fosad/.

The present volume gathers a collection of tutorial lectures from FOSAD 2006 and FOSAD 2007. In the past, three volumes published in the Springer LNCS series were dedicated to FOSAD: LNCS 2171 for FOSAD 2000, LNCS 2946 for FOSAD 2001 and 2002, and LNCS 3655 for FOSAD 2004 and 2005. The contributions to this volume, which range from formal methods to software and critical infrastructures security and from identity-based cryptography to trust and reputation systems, are detailed as follows.

The opening paper by Martín Abadi is an introduction to the design and analysis of security protocols. The author presents the principles of protocol design and of a formalism for protocol analysis. Massimo Bartoletti, Pierpaolo Degano, Gian Luigi Ferrari, and Roberto Zunino present a formal framework for designing and composing secure services. The authors show how to employ a core functional calculus for services and a graphical design language in order to correctly plan secure service orchestrations. Daniel Le Métayer provides an overview of the best industrial practices in IT security analysis. In particular, the paper presents recent research results in the area of formal foundations and powerful tools for security analysis. The contribution by Úlfar Erlingsson outlines the general issues of low-level software security. Concrete details of low-level attacks and defenses are given in the case of C and C++ software compiled into machine code. Fabio Martinelli and Paolo Mori describe a solution to improve the Java native security support. Two examples of the application of the proposed solution, with history-based monitoring of the application behavior, are given in the case of grid computing and mobile devices. The purpose of the chapter by Javier Lopez, Cristina Alcaraz, and Rodrigo Roman is to review and discuss critical information infrastructures, and show how to protect their functionalities and performance against attacks. As an example, the chapter also discusses the role of wireless sensor networks technology in the protection of these infrastructures. The paper by Liqun Chen is a survey in the area of asymmetric key cryptographic methodologies for identity-based cryptography. Audun Jøsang gives an overview of the background, current status, and future trend of trust and reputation systems. In the following chapter, Marcin Czenko, Sandro Etalle, Dongyi Li, and William H. Winsborough present the trust management approach to access control in distributed systems. In particular, they focus on the RT family of role-based trust management languages. Chris Mitchell and Eimear Gallery report on the trusted computing technology for the next-generation mobile devices.

We would like to thank all the institutions that have promoted and founded this school and, in particular, 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. FOSAD 2007 was sponsored by CNR-IIT, Università di Bologna, and the EU project ARTIST2, and was 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.

July 2007

Alessandro Aldini
Roberto Gorrieri

Table of Contents

Foundations of Security Analysis and Design