

Lecture Notes in Computer Science

2946

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Riccardo Focardi Roberto Gorrieri (Eds.)

Foundations of Security Analysis and Design II

FOSAD 2001/2002 Tutorial Lectures



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Riccardo Focardi
Università Ca' Foscari di Venezia, Dipartimento di Informatica
Via Torino 155, 30172 Mestre (Venice), Italy
E-mail: focardi@dsi.unive.it

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

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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

ISSN 0302-9743

ISBN 3-540-20955-7 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media
springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10985960 06/3142 5 4 3 2 1 0

International School on Foundations of Security Analysis and Design

17–29 September 2001, 23–27 September 2002, Bertinoro, Italy

Security is a fast-growing area of computer science, with increasing relevance to real-life applications such as Internet transactions and electronic commerce. Foundations for the analysis and the design of security aspects of these applications are badly needed in order to validate and prove (or guarantee) their correctness. Recently an IFIP Working Group on “Theoretical Foundations of Security Analysis and Design” was established (see <http://www.dsi.unive.it/IFIPWG1.7/> for more details) in order to promote research and education in security-related issues.

One of the many initiatives of the IFIP WG 1.7 has been the creation of the “International School on Foundations of Security Analysis and Design” (FOSAD) that is held annually at the Residential Centre of the University of Bologna in Bertinoro, with the goal of disseminating knowledge in this critical area, especially for participants coming from less-favored and non-leading countries. The Residential Center (see <http://www.centrocongressibertinoro.it/>) is 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 this school (FOSAD 2000) was very successful and the collection of tutorial lectures was published in Springer LNCS volume 2171. This second volume collects some of the tutorials given at the two successive schools (FOSAD 2001 and FOSAD 2002) that attracted many participants from all over the world.

This volume collects six tutorial lectures given at these two schools. More precisely:

- Alessandro Aldini, Mario Bravetti, Alessandra Di Pierro, Roberto Gorrieri, Chris Hankin and Herbert Wiklicky (Two Formal Approaches for Approximating Noninterference Properties);
- Carlo Blundo and Paolo D’Arco (The Key Establishment Problem);
- Michele Bugliesi, Giuseppe Castagna, Silvia Crafa, Riccardo Focardi, Vladimiro Sassone (A Survey of Name-Passing Calculi and Cryptoprimitives);
- Roberto Gorrieri, Riccardo Focardi and Fabio Martinelli (Classification of Security Properties – Part II: Network Security);
- Rosario Gennaro (Cryptographic Algorithms for Multimedia Traffic);
- Hanne Riis Nielson, Flemming Nielson and Mikael Buchholtz (Security for Mobility).

We want to thank all the institutions that have supported the initiatives: CNR-IAT, ONR, Università Ca’ Foscari di Venezia, Università di Bologna, Progetto MURST “Metodi Formali per la Sicurezza e il Tempo” (MEFISTO), and

EU-FET project MyThS: Models and Types for Security in Mobile Distributed Systems. Moreover, the school was held under the auspices of the European Association for Theoretical Computer Science (EATCS – Italian Chapter), the International Federation for Information Processing (IFIP – WG 1.7), and the European Educational Forum. Finally, we want to warmly thank the local organizers of the school, especially Alessandro Aldini, Andrea Bandini, Chiara Braghin and Elena Della Godenza.

November 2003

Riccardo Focardi
Roberto Gorrieri

Table of Contents

Two Formal Approaches for Approximating Noninterference Properties . . .	1
<i>Alessandro Aldini, Mario Bravetti, Alessandra Di Pierro, Roberto Gorrieri, Chris Hankin, and Herbert Wiklicky</i>	
The Key Establishment Problem	44
<i>Carlo Blundo and Paolo D'Arco</i>	
A Survey of Name-Passing Calculi and Crypto-Primitives	91
<i>Michele Bugliesi, Giuseppe Castagna, Silvia Crafa, Riccardo Focardi, and Vladimiro Sassone</i>	
Classification of Security Properties (Part II: Network Security)	139
<i>Riccardo Focardi, Roberto Gorrieri, and Fabio Martinelli</i>	
Cryptographic Algorithms for Multimedia Traffic	186
<i>Rosario Gennaro</i>	
Security for Mobility	207
<i>Hanne Riis Nielson, Flemming Nielson, and Mikael Buchholtz</i>	
Author Index	267