Lecture Notes in Computer Science 2171
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
*Berlin*
*Heidelberg*
*New York*
*Barcelona*
*Hong Kong*
*London*
*Milan*
*Paris*
*Tokyo*

Riccardo Focardi Roberto Gorrieri (Eds.)

# Foundations of Security Analysis and Design

## Tutorial Lectures

Springer

Volume Editors

Riccardo Focardi
Università Ca' Foscari di Venezia
Dipartimento di Matematica Applicata e Informatica
Via Torino 155, 30173 Mestre (Ve), 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

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Foundations of security analysis and design : tutorial lectures /
Riccardo Focardi ; Roberto Gorrieri (ed.). - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2171)
ISBN 3-540-42896-8

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

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

ISSN 0302-9743
ISBN 3-540-42896-8 Springer-Verlag Berlin Heidelberg New York



Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de



Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN 10840402 06/3142 5 4 3 2 1 0

# International School on Foundations of Security Analysis and Design

*18-30 September 2000, 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" has been established (see http://www.dsi.unive.it/IFIPWG1_7/ for more details) in order to pursue a number objectives, which include the following:

- to investigate the theoretical foundations of security as an independent discipline with firm grounds in logic, semantics, and complexity;
- to discover and promote new areas of application of theoretical techniques in computer security;
- to make formal methods amenable to the security practitioners, hence increasing awareness of formal verification techniques for security in the computer science community at large.

Hence, the scope of the IFIP Working Group 1.7 encompasses all aspects of the fundamental mathematical theory of system specification and verification, which shares with IFIP TC1 the basic fields of logic (first-order logic, temporal logic, epistemic logic), semantics (static analysis, type theory), formal methods and related approaches (model-checking, theorem-proving, process algebra), and complexity.

Among the many initiatives promoted and partly founded by the WG 1.7, there is also the "International School on Foundations of Security Analysis and Design" (FOSAD) held at the Residential Center 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 is an ex-convent and Episcopal fortress that has been transformed into a modern conference facility with computing services and Internet access. Bertinoro lies approximately half-way between Bologna and the Adriatic coast town of Rimini. Bertinoro is perched on the foothills of the Appenine Mountains overlooking the Po Valley to the North and the Tuscan-Emilian hills to the South.

The topics covered by the school (see http://www.cs.unibo.it/ aldini/fosad/ for more details) included: Security in Programming Languages and Process Calculi; Mathematical Models of Computer Security (e.g. non interference); Logics and Models for Security Protocols Specification (e.g. belief logic, strand spaces); Cryptographic Protocol Analysis (e.g. by model checking or theorem proving);

Cryptographic Protocols at Work (e.g. in electronic commerce); Access Control and Personal Identification. The school was composed of eight main courses, each one lasting six or eight hours. Additionally, four further courses, lasting two hours each, were offered.

This volume collects six tutorial lectures given at the school. More precisely:

- Andrew D. Gordon, Microsoft, Cambridge (Nominal Calculi for Security and Mobility);
- Roberto Gorrieri, University of Bologna, and Riccardo Forcardi, University of Venice (Classification of Security Properties);
- Joshua Guttman, Mitre, Bedford, (Security Goals: Packet Trajectories, and Strand Spaces);
- Peter Ryan, CMU, Pittsburgh, (Mathematical Models of Computer Security);
- Pierangela Samarati, University of Milan (Access Control: Policies, Models, Architectures, and Mechanisms);
- Paul Syverson, Naval Research Lab, Washington, (The Logic of Security Protocols).

The school attracted a lot of people. We received almost 100 applications from all over the world. Typical applicants were PhD students, young researchers, a few senior researchers in different areas, some industrial researchers, a few governmental institution members. We selected 60 participants from 4 continents (47 European, 5 Asian, 6 American, 2 African participants), a few more than initially planned, due to the enormous pressure of the applicants that firmly wanted to take part in the event. All participants will receive this special volume of the Springer-Verlag Lecture Notes of Computer Science series.

We would like to thank all the institutions that have supported the initiative: EU (High Level Scientific Conferences programme), UNESCO Venice Office, Ser.In.Ar., University of Bologna, Fondazione Cassa di Risparmio di Forli'. Moreover, the school was held under the auspices of the European Association of Theoretical Computer Science (EATCS – Italian Chapter), International Federation for Information Processing (IFIP – WG 1.7), European Educational Forum. Finally, we would like to warmly thank the local organizers of the school, especially Alessandro Aldini, Andrea Bandini, Mario Bravetti, and Roberta Poggi.

September 2001

Riccardo Focardi
Roberto Gorrieri

# Table of Contents