Lecture Notes in Computer Science 2502
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Dieter Gollmann   Günter Karjoth
Michael Waidner (Eds.)

Computer Security – ESORICS 2002

7th European Symposium on Research in Computer Security
Zurich, Switzerland, October 14-16, 2002
Proceedings

Springer

Series Editors

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

Volume Editors

Dieter Gollmann
Microsoft Research
7 J J Thomson Avenue, Cambridge CB3 0FB, UK
E-mail: diego@microsoft.com

Günther Karjoth
Michael Waidner
IBM Zurich Research Lab
Säumerstr. 4, 8803 Rüschlikon, Switzerland
E-mail: {gka/wmi}@zurich.ibm.com

Cataloging-in-Publication Data applied for

Bibliograhpic 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.4.5, E.3, C.2.0, H.2.0, K.6.5, K.4.4

ISSN 0302-9743
ISBN 3-540-44345-2 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 Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10870813 06/3142 5 4 3 2 1 0

Preface

ESORICS, the European Symposium on Research in Computer Security, is the leading research-oriented conference on the theory and practice of computer security in Europe. It takes place every two years, at various locations throughout Europe, and is coordinated by an independent Steering Committee.

ESORICS 2002 was jointly organized by the Swiss Federal Institute of Technology (ETH) and the IBM Zurich Research Laboratory, and took place in Zurich, Switzerland, October 14-16, 2002.

The program committee received 83 submissions, originating from 22 countries. For fans of statistics: 55 submissions came from countries in Europe, the Middle East, or Africa, 16 came from Asia, and 12 from North America. The leading countries were USA (11 submissions), Germany (9), France (7), Italy (7), Japan (6), and UK (6). Each submission was reviewed by at least three program committee members or other experts. Each submission coauthored by a program committee member received two additional reviews. The program committee chair and cochair were not allowed to submit papers. The final selection of papers was made at a program committee meeting and resulted in 16 accepted papers. In comparison, ESORICS 2000 received 75 submissions and accepted 19 of them.

The program reflects the full range of security research: we accepted papers on access control, authentication, cryptography, database security, formal methods, intrusion detection, mobile code security, privacy, secure hardware, and secure protocols.

We gratefully acknowledge all authors who submitted papers for their efforts in maintaining the standards of this conference.

It is also my pleasure to thank the members of the program committee, the additional reviewers, and the members of the organization committee for their work and support.

Zurich, October 2002

Michael Waidner

Program Committee

Martín Abadi	University of California at Santa Cruz, USA
Ross Anderson	University of Cambridge, UK
Tuomas Aura	Microsoft Research, UK
Joachim Biskup	University of Dortmund, Germany
Frédéric Cuppens	ONERA, France
Marc Dacier	Eurecom, France
Hervé Debar	France Telecom R&D, France
Yves Deswarte	LAAS-CNRS, France
Simone Fischer-Hübner	Karlstad University, Sweden
Simon Foley	University College Cork, Ireland
Dieter Gollmann	Microsoft Research, UK
Martin Hirt	ETH Zurich, Switzerland
Trent Jaeger	IBM Research, USA
Socratis Katsikas	University of the Aegean, Greece
Kaoru Kurosawa	Ibaraki University, Japan
Heiko Mantel	DFKI, Germany
John McHugh	CERT, USA
David Naccache	Gemplus, France
Birgit Pfitzmann	IBM Research, Switzerland
Avi Rubin	AT&T Labs–Research, USA
Peter Ryan	University of Newcastle, UK
Pierangela Samarati	University of Milan, Italy
Tomas Sander	Intertrust, USA
Einar Snekkenes, Program Co-chair	Norwegian Computer Center, Norway
Michael Steiner	Saarland University, Germany
Gene Tsudik	University of California, Irvine, USA
Dennis Volpano	Naval Postgraduate School, USA
Michael Waidner, Program Chair	IBM Research, Switzerland

Additional Reviewers

Ammar Alkassar, Michael Backes, Sébastien Canard, Jan Camenisch, Nora Cuppens, Xuhua Ding, Thomas Dübendorfer, Alberto Escudero-Pascual, Serge Fehr, Felix Gärtner, Stuart Haber, Thomas Holenstein, Yongdae Kim, Fabien Laguillaumie, Jean-François Misarsky, Maithili Narasimha, Benny Pinkas, Andrei Sabelfeld, Ahmad-Reza Sadeghi, Axel Schairer, Simon Skaria, Jacques Traoré, Jürg Wullschleger

Organization Committee

Endre Bangerter (IBM Research), Dieter Gollmann (Microsoft Research, UK; Publication Chair) Günter Karjoth (IBM Research, Switzerland; General Chair), Jürg Nievergelt (ETH Zurich, Switzerland; General Co-chair), Floris Tschurr (ETH Zurich)

Steering Committee

Joachim Biskup (University of Dortmund, Germany), Frédéric Cuppens (ONERA, France), Yves Deswarte (LAAS-CNRS, France), Gerard Eizenberg (CERT, France), Simon Foley (University College Cork, Ireland), Dieter Gollmann (Microsoft Research, UK), Franz-Peter Heider (debis IT Security Services, Germany), Jeremy Jacob (University of York, UK), Socratis Katsikas (University of the Aegean, Greece), Helmut Kurth (atsec, Germany), Peter Landrock (Cryptomathic, UK), Emilio Montolivo (FUB, Italy), Roger Needham (Microsoft Research, UK), Jean-Jacques Quisquater (UCL, Belgium), Peter Ryan (University of Newcastle, UK: Steering Committee Chair), Pierangela Samarati (University of Milan, Italy), Einar Snekkenes (Norwegian Computer Center, Norway), Michael Waidner (IBM Research, Switzerland).

Table of Contents