Lecture Notes in Computer Science 648
Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer

Y. Deswarte G. Eizenberg J.-J. Quisquater (Eds.)

Computer Security – ESORICS 92

Second European Symposium on
Research in Computer Security
Toulouse, France, November 23-25, 1992
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Cornell University
Department of Computer Science
5149 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Yves Deswarte
LAAS-CNRS and INRIA, 7 avenue du Colonel Roche
F-31077 Toulouse, France

Gérard Eizenberg
ONERA-CERT, 2 avenue Edouard Belin
F-31055 Toulouse, France

Jean-Jacques Quisquater
Université Catholique de Louvain, Unité DICE
3 Place du Levant, B-1348 Louvain-la-Neuve, Belgium

CR Subject Classification (1991): D.4.6, K.6.5, C.2.0, H.2.0

ISBN 3-540-56246-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56246-X Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author/editor
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

The first European Symposium on Research in Computer Security took place in October 1990 in Toulouse. The proceedings of ESORICS 90 contained 24 papers from 8 different countries and were published by AFCET. ESORICS 92, whose proceedings are the object of this volume, is the second symposium in what we hope will be a regular European event with a growing international character.

ESORICS could not happen without the cooperation and support of many organizations, and this collaboration will be a major factor in its future success. The early and continuous support of DGA/DRET deserves a special acknowledgement.

The specificity of ESORICS is progressively affirmed, thanks to the high standard of both the programme committee and the papers that were submitted. Authors of all proposed papers therefore deserve the main acknowledgement, since this high quality is the key for the successful continuation of a top-grade international symposium.

September 1992

Gérard Eizenberg, Symposium Chair

Jean-Jacques Quisquater, Programme Committee Chair

Yves Deswarte, Organization Committee Chair

ESORICS 92

was organized by AFCET
Association française des sciences et technologies de l'information et des systèmes
156 boulevard Péreire, 75017 Paris, France

in co-operation with

BCS (The British Computer Society), DISSI (Délégation Interministérielle pour la Sécurité des Systèmes d'Information), ERCIM (European Research Consortium for Informatics and Mathematics), Fondazione Ugo Bordoni, GI (Gesellschaft für Informatik), IEE (The Institution of Electrical Engineers), INRIA (Institut National de Recherche en Informatique et Automatique), LAAS (Laboratoire d'Automatique et d'Analyse des Systèmes du CNRS), NGI (Nederlands Genootschap voor Informatica), ONERA-CERT (Centre d'Etudes et de Recherches de Toulouse)

with the support of

Bull, CNRS (Centre National de la Recherche Scientifique), Conseil Régional de Midi-Pyrénées, DRET (Direction des Recherches Etudes et Techniques).

Symposium Chair

Gérard Eizenberg (ONERA-CERT)

Programme Committee

Jean-Jacques Quisquater (UCL), *Chair*

Bruno d'Ausbourg (ONERA-CERT)
Joachim Biskup (Univ. of Hildesheim)
Peter Bottomley (RSRE)
Yvo Desmedt (Univ. of Wisconsin-Milwaukee)
Yves Deswarte (LAAS-CNRS & INRIA)
Gérard Eizenberg (ONERA-CERT)
Amos Fiat (Univ. of Tel-Aviv)
Dieter Gollmann (Univ. of London)
Franz-Peter Heider (GEI)
Jeremy Jacob (Oxford Univ.)
Helmut Kurth (IABG)
Jean-Claude Laprie (LAAS-CNRS)
Peter Landrock (Aarhus Univ.)
Teresa Lunt (SRI International)
John McDermid (Univ. of York)
John McLean (NRL)
Catherine Meadows (NRL)
Jonathan Millen (MITRE)
Emilio Montolivo (Fondazione Ugo Bordoni)
Roger Needham (Univ. of Cambridge)
Alfredo de Santis (Univ. of Salerno)
Einar Snekkenes (NDRE)
Marie-Jeanne Toussaint (Univ. of Liège)
Kioumars Yazdanian (ONERA-CERT)

Organization Committee

Yves Deswarte (LAAS-CNRS & INRIA), *Chair*

Laurent Cabirol (SCSSI)
Jean-Francois Cornet (Consultant)
Michel Dupuy (ENST)
Marie-Thérèse Ippolito (LAAS-CNRS)
Marie-France Kalogera (AFCET)
Paul Richy (CNET)
Pierre Rolin (ENST Bretagne)
Kioumars Yazdanian (ONERA-CERT)

Referees

Bruno d'Ausbourg	ONERA-CERT
Joachim Biskup	Universität Hildesheim
Peter Bottomley	RSRE
Oliver Costich	George Mason University
Frédéric Cuppens	ONERA-CERT
Yvo Desmedt	University of Wisconsin-Milwaukee
Yves Deswarte	LAAS-CNRS & INRIA
Gérard Eizenberg	ONERA-CERT
Amos Fiat	University of Tel-Aviv
Fred Gilham	SRI International
Dieter Gollmann	University of London
Ira Greenberg	SRI International
Franz-Peter Heider	GEI
Donovan Hsieh	SRI International
Jeremy Jacob	Oxford University
Myong Kang	Naval Research Laboratory
Helmut Kurth	IABG
Jean-Claude Laprie	LAAS-CNRS
Peter Landrock	Aarhus University
Teresa Lunt	SRI International
John McDermid	University of York
John McDermott	Naval Research Laboratory
John McLean	Naval Research Laboratory
Catherine Meadows	Naval Research Laboratory
Jonathan Millen	MITRE
Emilio Montolivo	Fondazione Ugo Bordoni
Roger Needham	University of Cambridge
Andreas Pfitzmann	Universität Hildesheim
Xiaolei Qian	SRI International
Jean-Jacques Quisquater	Université Catholique de Louvain
Alfredo de Santis	Università di Salerno
Einar Snekkenes	NDRE
Marie-Jeanne Toussaint	Université de Liège
Gilles Trouessin	ONERA-CERT
Kioumars Yazdanian	ONERA-CERT

Contents

Authentication I

Distributed Systems

Authentication II

Database Security

System Architectures

Applications