Lecture Notes in Computer Science 875

Dieter Gollmann (Ed.)

Computer Security – ESORICS 94

Third European Symposium on
Research in Computer Security
Brighton, United Kingdom, November 7-9, 1994
Proceedings

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

Series Editors

Gerhard Goos
Universität Karlsruhe
Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis
Department of Computer Science, Cornell University
4130 Upson Hall, Ithaka, NY 14853, USA

Jan van Leeuwen
Department of Computer Science, Utrecht University
Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editor

Dieter Gollmann
Department of Computer Science
Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom

CR Subject Classification (1991): D.4.6, E.3, C.2.0, H.2.0, K.6.5

ISBN 3-540-58618-0 Springer-Verlag Berlin Heidelberg New York

CIP data applied for

Typesetting: Camera-ready by author
SPIN: 10479219 45/3140-543210 - Printed on acid-free paper

Preface

This year for the first time ESORICS is being held outside France. This is an important step for a European Symposium, which should evidently not get fixed in any one country. Making the move revealed various unsuspected dependencies on the former organisational background, and we are all highly indebted to Dieter Gollmann and Pamela Bye who cheerfully and energetically made things happen when there was some local turbulence.

We are grateful to the Fondazione Ugo Bordoni for a grant to the IMA in support of their work for the Symposium, and to Codes & Ciphers Ltd for a timely loan. LAAS-CNRS, through the good will of Yves Deswarte, gave valuable assistance with a mailing, and distributed details electronically.

The Programme Committee coped uncomplainingly with the increased workload generated by the needed extension of submission date, and we are also greatly indebted to the referees who ensured at short notice that good professional opinions were always available.

I feel confident that we shall all have a valuable Symposium at Brighton.

Roger Needham
General Chairman

Programme Chair's Preface

Twenty-six papers were selected for the European Symposium on Research in Computer Security, ESORICS'94, held November 7-9, 1994 in Brighton, UK. This year's symposium is the third in the ESORICS series created in 1990 and renewed in 1992 by AFCET in France. The IMA organised ESORICS'94 in co-operation with AFCET, BCS Computer Security Specialist Group, CERT-ONERA, AICA and GI. Its proceedings are the object of this volume.

Progressively organised in a series of European countries, the symposium is confirmed as the European research event in Computer Security. The seventy-one submitted papers came from the five continents. Considering the high average quality of the submissions, the programme committee decided to select many of them, which led to a dense programme. The papers were grouped in sessions devoted to high security assurance software, key management, authentication, digital payment, distributed systems, access controls, databases and measures. As the evaluation of security was not sufficiently addressed in the submitted research papers, the programme committee organised a panel session devoted to it. In addition, to amplify the contribution to the symposium of the digital payment topic, it invited Professor Henry Beker to talk about "Security Research for the Financial Sector".

The authors of all submitted papers deserve the main acknowledgement. The successful continuation of a top-grade international symposium depends on them. The efficiency of the programme committee members made possible a timely review of quality. The signatories thank Professor Roger Needham for his help in the global review process they had to perform.

Gerard Eizenberg
Programme Chair

Elisa Bertino
Programme Vice-Chair

ESORICS'94

General Chair

Roger Needham	Cambridge University

Programme Committee

Bruno d'Ausbourg	CERT-ONERA
Elisa Bertino (Vice-Chair)	Universitá di Milano
Thomas Beth	Universität Karlsruhe
Joachim Biskup	Universität Hildesheim
Peter Bottomley	DRA
Yves Deswarte	LAAS-CNRS & INRIA
Klaus Dittrich	Universität Zürich
Gerard Eizenberg (Chair)	CERT-ONERA
Simon Foley	University College Cork
Dieter Gollmann	Royal Holloway, University of London
Franz-Peter Heider	GEI
Jeremy Jacob	University of York
Sushil Jajodia	George Mason University
Helmut Kurth	IABG
Teresa Lunt	DARPA
Giancarlo Martella	Universitá di Milano
Cathy Meadows	Naval Research Laboratories
Jonathan Millen	MITRE Corporation
Emilio Montolivo	Fondazione Ugo Bordoni
Roger Needham	Cambridge University
Andreas Pfitzmann	Technische Universität Dresden
Jean-Jacques Quisquater	Université de Louvain-la-Neuve
Einar Snekkenes	NDRE

Steering Committee Chair

Yves Deswarte	LAAS-CNRS & INRIA

Organising Committee

Pamela Bye	IMA
Dieter Gollmann	Royal Holloway, University of London

Referees

Ross Anderson *(Cambridge University)*, Bruno d'Ausbourg *(CERT ONERA)*, Elisa Bertino *(Universitá di Milano)*, Thomas Beth *(Universität Karlsruhe)*, Pierre Bieber *(CERT ONERA)*, Joachim Biskup *(Universität Hildesheim)*, Peter Bottomley *(DRA Malvern)*, Christel Calas *(CERT ONERA)*, Silvana Castano *(Universitá di Milano)*, Jacques Cazin *(CERT ONERA)*, John Clark *(University of York)*, Frédéric Cuppens *(CERT ONERA)*, Marc Dacier *(LAAS)*, Robert Demolombe *(CERT ONERA)*, Yves Deswarte *(LAAS-CNRS & INRIA)*, Gerard Eizenberg *(CERT ONERA)*, Simon Foley *(University College, Cork)*, Alban Gabillon *(CERT ONERA)*, Dieter Gollmann *(Royal Holloway, University of London)*, Franz-Peter Heider *(GEI)*, Jeremy Jacob *(University of York)*, Sushil Jajodia *(George Mason University)*, Dirk Jonscher *(Universität Zürich)*, Detlef Kraus *(GEI)*, Helmut Kurth *(IABG)*, Michel Lemoine *(CERT ONERA)*, Jean-Henri Llareus *(ENSAE)*, Mark Lomas *(Cambridge University)*, Teresa Lunt *(DARPA)*, Betty Mackman *(DRA Malvern)*, Giancarlo Martella *(Universitá di Milano)*, John McLean *(NRL)*, Catherine Meadows *(NRL)*, Jonathan Millen *(MITRE Corporation)*, Chris Mitchell *(Royal Holloway, University of London)*, Emilio Montolivo *(Fondazione Ugo Bordoni)*, Roger Needham *(Cambridge University)*, Colin O'Halloran *(DRA Malvern)*, Andreas Pfitzmann *(Technische Universität Dresden)*, Jean-Jacques Quisquater *(Universite Catholique de Louvain)*, Clare Robinson *(DRA Malvern)*, John Rushby *(SRI)*, Pierangela Samarati *(Universitá di Milano)*, Ravi Sandhu *(George Mason University)*, Chris Sennett *(DRA Malvern)*, Marek Sergot *(Imperial College)*, Einar Snekkenes *(NDRE)*, Jacques Stern *(Ecole Normale Superieure)*, Erich Van Wickeren *(GEI)*, Simon Wiseman *(DRA Malvern)*, John Wood *(DRA Malvern)*, Raphael Yahalom *(The Hebrew University of Jerusalem)*, Kioumars Yazdanian *(CERT ONERA)*

Contents

Measures

High Assurance Software

Key Management I

Authentication

Key Management II

Digital Payment

Distributed Systems

Access Controls

Database I

Database II