

Lecture Notes in Computer Science

875

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

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



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, Ithaca, 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

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 1994

Printed in Germany

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
 Elisa Bertino (Vice-Chair)
 Thomas Beth
 Joachim Biskup
 Peter Bottomley
 Yves Deswarte
 Klaus Dittrich
 Gerard Eizenberg (Chair)
 Simon Foley
 Dieter Gollmann
 Franz-Peter Heider
 Jeremy Jacob
 Sushil Jajodia
 Helmut Kurth
 Teresa Lunt
 Giancarlo Martella
 Cathy Meadows
 Jonathan Millen
 Emilio Montolivo
 Roger Needham
 Andreas Pfitzmann
 Jean-Jacques Quisquater
 Einar Snekkenes

CERT-ONERA
 Università di Milano
 Universität Karlsruhe
 Universität Hildesheim
 DRA
 LAAS-CNRS & INRIA
 Universität Zürich
 CERT-ONERA
 University College Cork
 Royal Holloway, University of London
 GEI
 University of York
 George Mason University
 IABG
 DARPA
 Università di Milano
 Naval Research Laboratories
 MITRE Corporation
 Fondazione Ugo Bordoni
 Cambridge University
 Technische Universität Dresden
 Université de Louvain-la-Neuve
 NDRE

Steering Committee Chair

Yves Deswarte

LAAS-CNRS & INRIA

Organising Committee

Pamela Bye
 Dieter Gollmann

IMA
 Royal Holloway, University of London

Referees

Ross Anderson (*Cambridge University*), Bruno d'Ausbourg (*CERT ONERA*), Elisa Bertino (*Università di Milano*), Thomas Beth (*Universität Karlsruhe*), Pierre Bieber (*CERT ONERA*), Joachim Biskup (*Universität Hildesheim*), Peter Bottomley (*DRA Malvern*), Christel Calas (*CERT ONERA*), Silvana Castano (*Università 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 (*Università di Milano*), John McLean (*NRL*), Catherine Meadows (*NRL*), Jonathan Millen (*MITRE Corporation*), Chris Mitchell (*Royal Holloway, University of London*), Emilio Montolivo (*Fondazione Ugo Bordonis*), 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 (*Università di Milano*), Ravi Sandhu (*George Mason University*), Chris Sennett (*DRA Malvern*), Marek Sergot (*Imperial College*), Einar Snekkenes (*NDRE*), Jacques Stern (*Ecole Normale Supérieure*), 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

Valuation of Trust in Open Networks 3
T. Beth, M. Borcharding, B. Klein

Security Versus Performance Requirements
in Data Communication Systems 19
V. Zorkadis

High Assurance Software

Non-Interference Through Determinism 33
A.W. Roscoe, J.C.P. Woodcock, L. Wulf

Compile-Time Detection of Information Flow in Sequential Programs 55
J.-P. Banâtre, C. Bryce, D. Le Métayer

Security Through Type Analysis 75
C. O'Halloran, C.T. Sennett

Key Management I

Designing Secure Key Exchange Protocols 93
C. Boyd, W. Mao

Robust and Secure Password and Key Change Method 107
R. Hauser, P. Janson, R. Molva, G. Tsudik, E. Van Herreweghen

Authentication

Beacon Based Authentication 125
A. Jiwa, J. Seberry, Y. Zheng

Authentication via Multi-Service Tickets in the Kuperee Server 143
T. Hardjono, J. Seberry

Oblivious Signatures 161
L. Chen

Key Management II

- A Calculus for Secure Channel Establishment in Open Networks 175
U.M. Maurer, P.E. Schmid
- On Strengthening Authentication Protocols to Foil Cryptanalysis 193
W. Mao, C. Boyd

Digital Payment

- An Efficient Electronic Payment System Protecting Privacy 207
J.L. Camenisch, J.M. Piveteau, M.A. Stadler
- The ESPRIT Project CAFE - High Security Digital Payment Systems ... 217
*J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjølsnes,
 F. Muller, T. Pedersen, B. Pfizmann, P. de Rooij, B. Schoenmakers,
 M. Schunter, L. Vallée, M. Waidner*
- Liability and Computer Security: Nine Principles 231
R.J. Anderson

Distributed Systems

- Implementing Secure Dependencies over a Network by Designing
 a Distributed Security SubSystem 249
B. d'Ausbourg
- A Secure Medium Access Control Protocol: Security vs Performances 267
P. Siron, B. d'Ausbourg
- Distributed File System over a Multilevel Secure Architecture -
 Problems and Solutions 281
C. Calas

Access Controls

- On the Expressive Power of the Unary Transformation Model 301
R.S. Sandhu, S. Ganta
- Privilege Graph: an Extension to the Typed Access Matrix Model 319
M. Dacier, Y. Deswarte
- A Consideration of the Modes of Operation for Secure Systems 335
C.L. Robinson, S.R. Wiseman

Database I

Mark-and-Sweep Garbage Collection in Multilevel Secure
 Object-Oriented Database Systems 359
A. Ciampichetti, E. Bertino, L. Mancini

Decomposition of Multilevel Objects in an Object-Oriented Database 375
N. Boulahia-Cuppens, F. Cuppens, A. Gabillon, K. Yazdanian

Supporting Object-Based High-Assurance Write-up in Multilevel
 Databases for the Replicated Architecture 403
R.K. Thomas, R.S. Sandhu

Database II

Aggregation in Relational Databases: Controlled Disclosure
 of Sensitive Information 431
A. Motro, D.G. Marks, S. Jajodia

Information Flow Controls vs Interference Controls:
 An Integrated Approach 447
F. Cuppens, G. Trouessin

List of Authors 469