Preface

Since 1990, ESORICS has established its reputation as the main event in research on computer security in Europe. Every two years, ESORICS gathers researchers and practitioners of computer security and gives researchers the opportunity to present the most recent advances in security theory as well as the risks related to simplistic implementations of security mechanisms.

Despite possible concurrence with other international events, ESORICS 98 received 57 submissions, coming from 19 countries and 4 continents. All these papers were reviewed by at least three program committee members or other experts at their institutions. Most of the submitted papers were considered as very good, and the program committee quickly agreed on 23 papers that could be organised into consistent sessions. Unfortunately, some high quality papers had to be rejected either because they did not correspond to ESORICS scope or because they did not fit with other papers to constitute a homogeneous session.

As in previous ESORICS, some ESORICS 98 sessions are dedicated to fundamental issues such as the design and specification of security policies, access control modelling and protocol analysis. But these sessions mix both theoretical papers and very practical concerns. Since mobility is a topic of increasing importance, its two main aspects will be discussed in two sessions: one on mobile systems and anonymity, the other on Java and mobile code. A session and a panel are devoted to watermarking, an important technique for the protection of intellectual rights. Finally, two sessions are dedicated to practical issues, one on intrusion detection and prevention, the other dealing with specific threats. In this session, two papers on cryptography have been included for the first time in ESORICS. While previously, we had considered that cryptography papers should be submitted to conferences dedicated to cryptography, these two papers have been accepted because security people can learn from them the risks that can be raised by naive implementation of good cryptographic algorithms.

In summaryy, we hope that this mix between practical and theoretical issues will satisfy the practitioner's curiosity and encourage researchers to pursue their work for the progress of a secure information society.

Yves Deswarte   Catherine Meadows
Programme Chair   Programme Vice-Chair

Organization

Conference Chairs

General Chair: Jean-Jacques Quisquater (UCL, Belgium)
Program Chair: Yves Deswarte (LAAS-CNRS & INRIA, France)
Program Vice-Chair: Catherine Meadows (NRL, USA)

Proceedings Editor

Dieter Gollmann   Microsoft Research, UK

Program Commitee

Elisa Bertino   University of Milan, Italy
Joachim Biskup   University of Dortmund, Germany
Yves Deswarte   LAAS-CNRS & INRIA, France
Gérard Eizenberg   CERT-ONERA, France)
Simon Foley   Cambridge University CCSR, UK & University
                        College Cork, Ireland
Dieter Gollmann   Microsoft Research, UK
Franz-Peter Heider   debis, Germany
Jeremy Jacob   University of York, UK
Sokratis Katsikas   University of the Aegean, Greece
Helmut Kurth   IABG, Germany
Peter Landrock   Århus University, Denmark
Carl Landwehr   NRL, USA
Guy Leduc   University of Liège, Belgium
Teresa Lunt   DARPA, USA
Benoît Macq   UCL, Belgium
Ueli Maurer   ETH Zürich, Switzerland
Catherine Meadows   NRL, USA
Refik Molva   Eurecom, France
Emilio Montolivo   Fondazione Ugo Bordoni, Italy
Roger Needham   Microsoft Research, UK
Pierre Paradinas   Gemplus, France
Jean-Jacques Quisquater UCL, Belgium
Pierre Rolin   France Telecom, France
Peter Ryan   DERA, UK
Pierangela Samarati   University of Milan, Italy
Einar Snekkenes   FFI, Norway
Gene Spafford   Purdue University, USA
Stuart Stubblebine   AT&T, USA
Michael Waidner   IBM, Switzerland

Additional Referees

N. Asokan	IBM Zürich Research Laboratory, Switzerland
Marco Bucci	Fondazione Ugo Bordoni, Italy
Jan Camenisch	ETH Zurich, Switzerland
Cecilia Catalano	Fondazione Ugo Bordoni, Italy
Bruno Crispo	University of Cambridge, UK
Francesco Gentile	Fondazione Ugo Bordoni, Italy
Irfan Ghauri	Institut Eurecom, France
Pierre Girard	Gemplus, France
Luigi Giuri	Fondazione Ugo Bordoni, Italy
Martin Hirt	ETH Zürich, Switzerland
Günter Karjoth	IBM Zürich Research Laboratory, Switzerland
Jean-Louis Lanet	Gemplus, France
Sergio Loureiro	Institut Eurecom, France
Renato Menicocci	Fondazione Ugo Bordoni, Italy
Markus Michels	Ubilab, UBS, Switzerland
Jon Millen	SRI International, USA
Alain Pannetrat	Institut Eurecom, France

Local Organisation Committee

Benoît Macq	Université catholique de Louvain, Belgium
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Catherine Rouyer	Université catholique de Louvain, Belgium
Joos Vandewalle	Katholieke Universiteit Leuven, Belgium

Computer Security - ESORICS 98
5th European Symposium on Research in Computer
Security, Louvain-la-Neuve, Belgium, September 16-18,
1998, Proceedings
Quisquater, J.-J.; Deswarte, Y.; Meadows, C.; Gollmann,
D. (Eds.)
1998, X, 382 p., Softcover
ISBN: 978-3-540-65004-1