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. The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

ESORICS is coordinated by an independent steering committee. In the past it took place every two years at various locations throughout Europe. Starting this year, it will take place annually.

ESORICS 2003 was organized by Gjøvik University College, and took place in Gjøvik, Norway, October 13–15, 2003.

The program committee received 114 submissions, originating from 26 countries on all continents. Half the papers originated in Europe (57). The most dominant countries were: UK (16), USA (14), Germany (6), South Korea (6), Sweden (6), Italy (5), France (4) and Poland (4). Each submission was reviewed by at least three program committee members or other experts. The program committee chair and co-chair were not allowed to submit papers. The final selection of papers was made at a program committee meeting followed by a week of e-mail discussions. Out of the 114 papers received, only 19 got accepted (17%). In comparison, ESORICS 2000 and 2002 received 75 and 83 papers and accepted 19% and 16%, respectively.

The program reflected the full range of security research, including access control, cryptographic protocols, privacy enhancing technologies, security models, authentication, and intrusion detection.

The program committee gratefully acknowledges 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.
General Chair

Jørn Wroldsen (Gjøvik University College)

Program Committee

Tuomas Aura  
Microsoft Research, UK
Joachim Biskup  
University of Dortmund, Germany
Tønnes Brekne  
Telenor, Norway
Frédéric Cuppens  
ENST-Bretagne, France
Marc Dacier  
Eurecom, France
Sabrina De Captani di Vimercati  
University of Milan, Italy
Hervé Debar  
France Telecom R&D, France
Yves Deswarte  
LAAS-CNRS, France
Simon Foley  
University College Cork, Ireland
Dieter Gollmann  
Microsoft Research, UK
Trent Jaeger  
IBM Research, USA
Kaoru Kurosawa  
Ibaraki University, Japan
Heiko Mantel  
DFKI, Germany
John McHugh  
CERT, USA
Ken Moody  
University of Cambridge, UK
Stefano Paraboschi  
University of Bergamo, Italy
Birgit Pfitzmann  
IBM Research, Switzerland
Avi Rubin  
Johns Hopkins University, USA
Peter Ryan  
University of Newcastle, UK
Pierangela Samarati (co-chair)  
University of Milan, Italy
Tomas Sander  
Hewlett-Packard, USA
Einar Snekkenes (chair)  
Gjøvik University College, Norway
Michael Steiner  
IBM Research, USA
Paul Syverson  
NRL, USA
Michael Waidner  
IBM Research, Switzerland

Additional Reviewers

Anas Abou El Kalam, Carlos Aguilar, Michael Backes, Jeremy Bryans, Laurent Bussard, Christian Cachin, Pau-chen Cheng, Jason Crampton, Roger Dingledine, Ulrich Flegel, Cédric Fournet, Tetsu Iwata, Klaus Julisch, Jan Jürjens, Yücel Karabulut, Wataru Kishimoto, Thomas Leineweber, Shinichiro Matsuo, Ralf Menzel, Refik Molva, Ira Moskowitz, Vincent Nicomette, Yasuhiro Ohtaki, Jörg Parthe, Benny Pinkas, Gerhard Popp, Fabien Pouget, Michael Roe, Ayda Saidane, Pasha Shabalin, Ron Steinfeld, Morton Swimmer, Vu Dong Tô, Sandra Wortmann, Yuliang Zheng, Alf Zugenmaier
Organizing Committee

Birgith Børthus (chair)
Hilding Sponberg (co-chair)
Øivind Kolloen
Rigmor Øvstetun
Fred Johansen
Svein Pettersen

Steering Committee

Elisa Bertino (University of Milan, Italy)
Joachim Biskup (University of Dortmund, Germany)
Frédéric Cuppens (ENST-Bretagne, France)
Marc Dacier (Eurecom, France)
Yves Deswarte (LAAS-CNRS, France)
Gérard Eizenberg (ONERA, 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)
Sokratis Katsikas (University of the Aegean, Greece)
Helmut Kurth (atsec, Germany)
Peter Landrock (Cryptomathic, UK)
Jean-Jacques Quisquater (UCL, Belgium)
Peter Ryan (University of Newcastle, UK; Steering Committee Chair)
Pierangela Samarati (University of Milan, Italy)
Einar Snekkenes (Gjøvik University College, Norway)
Michael Waidner (IBM Research, Switzerland)
# Table of Contents

Signature and Access Control Policies for XML Documents .......... 1
   *Elisa Bertino, Elena Ferrari, and Loredana Parasiliti Provenza*

Authorization and Access Control in Adaptive Workflows .......... 23
   *Dulce Domingos, António Rito-Silva, and Pedro Veiga*

Flexible Regulation of Distributed Coalitions ................. 39
   *Xuhui Ao and Naftaly H. Minsky*

Initiator-Resilient Universally Composable Key Exchange .......... 61
   *Dennis Hofheinz, Jörn Müller-Quade, and Rainer Steinwandt*

Multi-round Secure Light-Weight Broadcast Exclusion Protocol
with Pre-processing ........................................... 85
   *Yuji Watanabe and Masayuki Numao*

Precisely Answering Multi-dimensional Range Queries
without Privacy Breaches ..................................... 100
   *Lingyu Wang, Yingjiu Li, Duminda Wijesekera, and Sushil Jajodia*

Passive Attack Analysis for Connection-Based Anonymity Systems .. 116
   *Andrei Serjantov and Peter Sewell*

Rapid Mixing and Security of Chaum’s Visual Electronic Voting .. 132
   *Marcin Gomulkiewicz, Marek Klonowski, and Mirosław Kutylowski*

Towards Accountable Management of Privacy and Identity Information . 146
   *Marco Casassa Mont, Siani Pearson, and Pete Bramhall*

A Toolkit for Managing Enterprise Privacy Policies ................. 162
   *Michael Backes, Birgit Pfitzmann, and Matthias Schunter*

Authenticating Mandatory Access Controls and Preserving Privacy
for a High-Assurance Smart Card ................................ 181
   *Helmut Scherzer, Ran Canetti, Paul A. Karger, Hugo Krawczyk,
     Tal Rabin, and David C. Toll*

Hardware Encapsulation of Security Services ........................ 201
   *Adrian Baldwin and Simon Shiu*

A Formal Security Model of the Infineon SLE 88 Smart Card
Memory Management .......................................... 217
   *David von Oheimb, Georg Walter, and Volkmar Lotz*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridging Model-Based and Language-Based Security</td>
<td>235</td>
</tr>
<tr>
<td>Rogardt Heldal and Fredrik Hultin</td>
<td></td>
</tr>
<tr>
<td>An On-the-Fly Model-Checker for Security Protocol Analysis</td>
<td>253</td>
</tr>
<tr>
<td>David Basin, Sebastian Mödersheim, and Luca Viganò</td>
<td></td>
</tr>
<tr>
<td>Symmetric Authentication within a Simulatable Cryptographic Library</td>
<td>271</td>
</tr>
<tr>
<td>Michael Backes, Birgit Pfitzmann, and Michael Waidner</td>
<td></td>
</tr>
<tr>
<td>An Improved Reference Flow Control Model for Policy-Based Intrusion Detection</td>
<td>291</td>
</tr>
<tr>
<td>Jacob Zimmermann, Ludovic Mé, and Christophe Bidan</td>
<td></td>
</tr>
<tr>
<td>Visualisation for Intrusion Detection</td>
<td>309</td>
</tr>
<tr>
<td>Stefan Axelsson</td>
<td></td>
</tr>
<tr>
<td>On the Detection of Anomalous System Call Arguments</td>
<td>326</td>
</tr>
<tr>
<td>Christopher Kruegel, Darren Mutz, Fredrik Valeur, and Giovanni Vigna</td>
<td></td>
</tr>
</tbody>
</table>

**Author Index** | 345