Preface

Foreword from the Program Chairs

These proceedings contain the papers selected for presentation at the 9th European Symposium on Research in Computer Security (ESORICS), held during September 13–15, 2004 in Sophia Antipolis, France.

In response to the call for papers 159 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the program committee. The program committee meeting was held electronically; there was an intensive discussion over a period of two weeks. Of the papers submitted, 27 were selected for presentation at the conference, giving an acceptance rate lower than 17%. The conference program also included an invited talk.

A workshop like this does not just happen; it depends on the volunteer efforts of a host of individuals. There is a long list of people who volunteered their time and energy to put together the workshop and who deserve special thanks. Thanks to all the members of the program committee, and the external reviewers, for all their hard work in the paper evaluation. Due to the large number of submissions the program committee members were really required to work hard in a short time frame, and we are very thankful to them for the commitment they showed with their active participation in the electronic discussion. We are also very grateful to all those people whose work ensured a smooth organization process: Refik Molva, who served as the General Chair, Marc Dacier, the Sponsoring Chair, Yves Roudier, who served as the Publicity Chair and maintained the Web pages, Sabrina de Capitani di Vimercati, who helped in the review process, Dieter Gollmann, who served as the Publication Chair and collated this volume, and Anne Duflos and Laurence Grammare for helping with the local arrangements.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the program stimulating.

Peter Ryan and Pierangela Samarati
(Program Co-chairs)
Foreword from the General Chair

Initially established as the European conference in research on computer security, ESORICS has reached the status of a main international event gathering researchers from all over the world. Taking place in a different European country every other year during its first seven occurrences, it has been a yearly conference since 2003.

ESORICS 2004 was organized by the Institut EURECOM and took place in Sophia Antipolis, France, September 13–15, 2004.

The organization of such an important event required a major effort and we wish to express our sincere appreciation to the organization committee members for their excellent work.

We would like to express our special appreciation to the Program Chairs Pierangela Samarati and Peter Ryan for coming up with a high-quality technical program that was the result of a complex evaluation process they handled very smoothly.

We are also indebted to the Institut EURECOM who not only allowed us and other organization committee members to dedicate considerable time and energy to the organization of this event, but also provided logistic and financial support to host it.

Sophia Antipolis, September 2004

Refik Molva
Program Committee

Vijay Atluri
Giampaolo Bella
Joachim Biskup
Jan Camenisch
Germanno Caronni
David Chadwick
Ernesto Damiani
Sabrina De Capitani di Vimercati
Yves Deswarte
Alberto Escudero-Pascual
Csilla Farkas
Simon Foley
Dieter Gollmann
Joshua D. Guttman
Sushil Jajodia
Sokratis K. Katsikas
Maciej Koutny
Peng Liu
Javier Lopez
Roy Maxion
Patrick McDaniel
John McHugh
Catherine A. Meadows
Refik Molva
Peng Ning
LouAnna Notargiacomo
Eiji Okamoto
Stefano Paraboschi
Andreas Pfitzmann
Bart Preneel
Jean-Jacques Quisquater
Peter Ryan (co-chair)
Pierangela Samarati (co-chair)
Steve Schneider
Christoph Schuba
Michael Steiner
Paul Syverson
Kymie M. C. Tan
Dan Thomsen
Moti Yung

Rutgers University, USA
Università di Catania, Italy
Universität Dortmund, Germany
IBM Research, Switzerland
Sun Microsystems Laboratories, USA
University of Salford, UK
University of Milan, Italy
University of Milan, Italy
LAAS-CNRS, France
Royal Institute of Technology, Sweden
University of South Carolina, USA
University College Cork, Ireland
TU Hamburg-Harburg, Germany
MITRE, USA
George Mason University, USA
University of the Aegean, Greece
University of Newcastle upon Tyne, UK
Pennsylvania State University, USA
University of Malaga, Spain
Carnegie Mellon University, USA
AT&T Labs-Research, USA
CERT/CC, USA
Naval Research Lab, USA
Institut Eurécom, France
NC State University, USA
The MITRE Corporation, USA
University of Tsukuba, Japan
University of Bergamo, Italy
TU Dresden, Germany
Katholieke Universiteit Leuven, Belgium
Microelectronic Laboratory, Belgium
University of Newcastle, UK
University of London, UK
Sun Microsystems Inc., USA
IBM T.J. Watson Research Lab., USA
Naval Research Laboratory, USA
Carnegie Mellon University, USA
Tresys Technology, USA
Columbia University, USA
Additional Reviewers

Carlos Aguilar, Farid Ahmed, Ben Aziz, Walid Bagga, Endre Bangerter, Lejla Batina, Alex Biriyukov, Rainer Böhme, R. Bouroulet, Laurent Bussard, David Byers, Alex Bystrov, Shiping Chen, Ioan Chisalita, Mathieu Ciet, Sebastian Claus, Stefano Crosta, Roberto Delicata, Alex Dent, Thomas Dübendorfer, Claudiu Duma, Neil Evans, Ulrich Flegel, Elke Franz, Qijun Gu, James Heather, Almut Herzog, Manuel Hilty, John Iliadis, Ryszard Janicki, Mohamed Kaâniche, Ioanna Kantzavelou, Kevin Killourhy, Herbert Klimant, Stefan Köpsell, Spyros Kokolakis, Thomas Kriegelstein, Klaus Kursawe, Costas Lambrinoudakis, Thomas Leineweber, Benoît Libert, Donggang Liu, Pietro Michiardi, Jose A. Montenegro, Fabrice Mourlin, Vincent Nicomette, Melek Otenko, Giuseppe Pappalardo, Jörg Parthe, E. Pelz, Olivier Pereira, Thomas Quillinan, Josyula R. Rao, Douglas S. Reeves, Marc Rennhard, Pankaj Rohatgi, Rodrigo Roman, Yves Roudier, Dagmar Schönfeld, Diana Senn, Stefaan Seys, Barbara Sprick, Sandra Steinbrecher, Reto Strobl, Linying Su, Kun Sun, Eduard Turcan, Torben Weibert, Duminda Wijesekera, Sandra Wortmann, Dingbang Xu, Jun Xu, Meng Yu, Wanyu Zang, Christophe Zanon, Hongbin Zhou

Organisation Committee

Refik Molva (General Chair), Yves Roudier (Publicity Chair), Marc Dacier (Sponsoring Chair), Dieter Gollmann (Publication Chair), Anne Duflos (Conference Secretary), and Laurence Grammare (Communications)

ESORICS 2004 was supported by SAP, @sec, and Conseil Régional Provence Alpes Côte d’Azur.

Steering Committee

Elisa Bertino (University of Milan, I), Joachim Biskup (Universität Dortmund, D), Frédéric Cuppens (ENST-Bretagne, F), Marc Dacier (Eurecom, F), Yves Deswarte (LAAS-CNRS, F), Gérard Eizenberg (ONERA, F), Simon Foley (University College Cork, IE), Dieter Gollmann (TU Hamburg-Harburg, D), Franz-Peter Heider (debis IT Security Services, D), Jeremy Jacob (University of York, UK), Sokratis Katsikas (University of the Aegean, GR), Helmut Kurth (atsec, D), Peter Landrock (Cryptomathic, UK), Jean-Jacques Quisquater (UCL, B), Peter Ryan (University of Newcastle, UK: Steering Committee Chair), Pierangela Samarati (University of Milan, I: Steering Committee Vice-Chair), Einar Snekkenes (Gjøvik University College, N), Michael Waidner (IBM Research, CH).
# Table of Contents

Incorporating Dynamic Constraints in the Flexible Authorization Framework ............................................. 1  
*Shiping Chen, Duminda Wijesekera, and Sushil Jajodia*

Access-Condition-Table-Driven Access Control for XML Databases ............... 17  
*Naizhen Qi (Naishin Seki) and Michiharu Kudo*

An Algebra for Composing Enterprise Privacy Policies ................................. 33  
*Michael Backes, Markus Dürmuth, and Rainer Steinwandt*

Deriving, Attacking and Defending the GDOI Protocol ........................................ 53  
*Catherine Meadows and Dusko Pavlovic*

Better Privacy for Trusted Computing Platforms ........................................ 73  
*Jan Camenisch*

A Cryptographically Sound Dolev-Yao Style Security Proof of the Otway-Rees Protocol ........................................ 89  
*Michael Backes*

A Formalization of Anonymity and Onion Routing ........................................ 109  
*S. Mauw, J.H.S. Verschuren, and E.P. de Vink*

Breaking Cauchy Model-Based JPEG Steganography with First Order Statistics ........................................ 125  
*Rainer Böhme and Andreas Westfeld*

Comparison Between Two Practical Mix Designs ........................................ 141  
*Claudia Díaz, Len Sassaman, and Evelyne Dewitte*

Signature Bouquets: Immutability for Aggregated/Condensed Signatures .......... 160  
*Einar Mykletun, Maithili Narasimha, and Gene Tsudik*

Towards a Theory of Data Entanglement .................................................. 177  
*James Aspnes, Joan Feigenbaum, Aleksandr Yampolskiy, and Sheng Zhong*

Portable and Flexible Document Access Control Mechanisms .......................... 193  
*Mikhail Atallah and Marina Bykova*

Possibilistic Information Flow Control in the Presence of Encrypted Communication ........................................ 209  
*Dieter Hutter and Axel Schairer*
Table of Contents

Information Flow Control Revisited:
Noninfluence = Noninterference + Nonleakage .......................... 225
   David von Oheimb

Security Property Based Administrative Controls ...................... 244
   Jon A. Solworth and Robert H. Sloan

A Vector Model of Trust for Developing Trustworthy Systems .......... 260
   Indrajit Ray and Sudip Chakraborty

Parameterized Authentication ............................................. 276
   Michael J. Covington, Mustaque Ahamad, Irfan Essa,
   and H. Venkateswaran

Combinatorial Design of Key Distribution Mechanisms
for Wireless Sensor Networks ............................................. 293
   Seyit A. Çamtepe and Bülent Yener

Hindering Eavesdropping via IPv6 Opportunistic Encryption .......... 309
   Claude Castelluccia, Gabriel Montenegro, Julien Laganier,
   and Christoph Neumann

On the Role of Key Schedules in Attacks on Iterated Ciphers .......... 322
   Lars R. Knudsen and John E. Mathiassen

A Public-Key Encryption Scheme with Pseudo-random Ciphertexts ...... 335
   Bodo Möller

A Host Intrusion Prevention System for Windows Operating Systems ... 352
   Roberto Battistoni, Emanuele Gabrielli, and Luigi V. Mancini

Re-establishing Trust in Compromised Systems:
Recovering from Rootkits That Trojan the System Call Table .......... 369
   Julian B. Grizzard, John G. Levine, and Henry L. Owen

ARCHERR: Runtime Environment Driven Program Safety ............... 385
   Ramkumar Chinchani, Anusha Iyer, Bharat Jayaraman,
   and Shambhu Upadhyaya

Sets, Bags, and Rock and Roll –
Analyzing Large Data Sets of Network Data ............................ 407
   John McHugh

Redundancy and Diversity in Security ..................................... 423
   Bev Littlewood and Lorenzo Strigini

Discovering Novel Attack Strategies from INFOSEC Alerts .......... 439
   Xinzhou Qin and Wenke Lee

Author Index ................................................................. 457