

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*New York University, NY, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Sabrina De Capitani di Vimercati  
Paul Syverson Dieter Gollmann (Eds.)

# Computer Security – ESORICS 2005

10th European Symposium on Research in Computer Security  
Milan, Italy, September 12-14, 2005  
Proceedings



Springer

## Volume Editors

Sabrina De Capitani di Vimercati  
Università degli Studi di Milano  
Dipartimento di Tecnologie dell'Informazione  
Via Bramante 65, 26013 Crema (CR), Italy  
E-mail: decapita@dti.unimi.it

Paul Syverson  
Naval Research Laboratory Washington  
Center for High Assurance Computer Systems  
Washington DC 20375, USA  
E-mail: syverson@itd.nrl.navy.mil

Dieter Gollmann  
TU Hamburg-Harburg, 21071 Hamburg, Germany  
E-mail: diego@tu-harburg.de

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.5, C.2.0, H.2.0, K.6.5, K.4.4

ISSN 0302-9743  
ISBN-10 3-540-28963-1 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-28963-0 Springer Berlin Heidelberg New York

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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media  
springeronline.com

© Springer-Verlag Berlin Heidelberg 2005  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 11555827 06/3142 5 4 3 2 1 0

# Preface

## Foreword from the Program Chairs

These proceedings contain the papers selected for presentation at the 10th European Symposium on Research in Computer Security (ESORICS), held September 12–14, 2005 in Milan, Italy.

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, holding intensive discussion over a period of two weeks. Of the papers submitted, 27 were selected for presentation at the conference, giving an acceptance rate of about 16%. The conference program also includes an invited talk by Barbara Simons.

There is a long list of people who volunteered their time and energy to put together the symposium and who deserve acknowledgment. Thanks to all the members of the program committee, and the external reviewers, for all their hard work in evaluating and discussing papers. We are also very grateful to all those people whose work ensured a smooth organizational process: Pierangela Samarati, who served as General Chair, Claudio Ardagna, who served as Publicity Chair, Dieter Gollmann who served as Publication Chair and collated this volume, and Emilia Rosti and Olga Scotti for helping with 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.

July 2005

Sabrina De Capitani di Vimercati and Paul Syverson

## Foreword from the General Chair

It is my pleasure to welcome you to the 10th European Symposium On Research In Computer Security in Milan. 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. The conference, hosted for the first time in Milan, offers an outstanding technical program, including one invited talk and 27 selected papers.

An event like this does not just happen; it depends on the volunteer efforts of a host of individuals. I wish to express my sincere appreciation to all the people who volunteered their time and energy to put together the conference and make it possible. First and foremost, thanks are due to Sabrina De Capitani di Vimercati and Paul Syverson and the members of the program committee for selecting the technical papers for presentation and to Barbara Simons for agreeing to deliver the keynote speech. I am also grateful to all those people who ensured a smooth organization process: Dieter Gollmann, for collating the proceedings volume and ensuring that these proceedings be ready for distribution at the conference; Claudio Ardagna for serving as Publicity Chair; Emilia Rosti for helping with the organization and taking care of local arrangements; and Olga Scotti for her help with local arrangements.

Special thanks are due to: the University of Milan, for granting us the conference location and service; the Department of Information Technologies of the University for its support; the Italian Association for Information Processing (AICA) for its financial support and for providing help in the secretarial and registration process; and the sponsors for their support.

Last, but certainly not least, thanks to all of you for attending the conference. I hope you find the program stimulating and enjoy your time in Milan!

Pierangela Samarati

# Organization

## Program Committee

Rakesh Agrawal	IBM Almaden Research Center, USA
Gerard Allwein	Naval Research Laboratory, USA
Ross Anderson	University of Cambridge, UK
Vijay Atluri	Rutgers University, USA
Michael Backes	IBM Zurich Research Laboratory, Switzerland
Giampaolo Bella	University of Catania, Italy
Jan Camenisch	IBM Zurich Research Laboratory, Switzerland
David Chadwick	University of Kent, UK
LiWu Chang	Naval Research Laboratory, USA
Marc Dacier	Institut Eurécom, France
Ernesto Damiani	Università degli Studi di Milano, Italy
George Danezis	University of Cambridge, UK
Sabrina De Capitani di Vimercati (co-chair)	Università degli Studi di Milano, Italy
Simon Foley	University College Cork, Ireland
Philippe Golle	Palo Alto Research Center, USA
Marit Hansen	ICPP Schleswig-Holstein, Germany
Philippa Hopcroft	Oxford University, UK
Sushil Jajodia	George Mason University, USA
Dogan Kesdogan	RWTH Aachen, Informatik IV, Germany
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Patrick McDaniel	Pennsylvania State University, USA
Heiko Mantel	ETH-Zentrum, Switzerland
Nick Mathewson	The Free Haven Project, USA
Richard E. Newman	University of Florida, USA
Peng Ning	NC State University, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Emilia Rosti	Università degli Studi di Milano, Italy
Peter Ryan	University of Newcastle upon Tyne, UK
Kazue Sako	NEC Corporation, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Paul Syverson (co-chair)	Naval Research Laboratory, USA
Vanessa Teague	University of Melbourne, Australia
Brent Waters	Stanford University, USA
Mariemma I. Yagüe	University of Malaga, Spain
Alec Yasinsac	Florida State University, USA
Sheng Zhong	State University of New York at Buffalo, USA

## Additional Reviewers

Todd Andel,  
Ben Aziz  
Walid Bagga  
Sebastiano Battiato  
Birgit Baum-Waidner  
Meletis Belsis  
Peter Berlich  
Mike Bond  
Kevin Butler  
Achim Brucker  
Jeremy Bryans  
Christian Cachin  
Shiping Chen  
Shu-Ching Chen  
Yannick Chevalier  
Richard Clayton  
Andrew Conway  
Amy Corman  
Lavinia Egidi  
Will Enck  
Jun Furukawa  
Michael Goldsmith  
Steven Greenwald  
Qijun Gu  
Huiping Guo  
Markus Hansen  
Shan He  
Boniface Patrick Hicks  
Martin Hirt  
Dennis Hofheinz  
Susan Hohenberger  
Toshinori Araki  
Toshiyuki Isshiki  
Tobias Kölsch  
Kameswari Kotapati  
Fengjun Li  
Huiyun Li  
Lunquan Li  
Jay Ligatti  
Anyi Liu  
Donggang Liu  
Wesam Lootah  
Gavin Lowe  
Ashwin Machanavaajhala

Todd McDonald  
Martin Meints  
Jose A. Montenegro  
Kengo Mori  
Barry Mulcahy  
Gregory Neven  
Tom Newcomb  
Satoshi Obana  
Jose A. Onieva  
Joseph Pamula  
Chi-Chun Pan  
Udaya Parampalli  
Thea Peacock  
Alexis Pimenidis  
Fabien Pouget  
Thomas Probst  
Ahmad-Reza Sadeghi  
Ralf Rantza  
Arnon Rosenthal  
Sankardas Roy  
Patrizia Scandurra  
Tim Seipold  
Christos Siaterlis  
Barbara Sprick  
Rainer Steinwandt  
Isamu Teranishi  
Patrick Traynor  
Ingrid Verbauwhede  
Frederik Vercauteren  
Ulrich Waldmann  
Hai Wang  
Lingyu Wang  
Xinyuan Wang  
Bogdan Warinshi  
Ralf Wienzek  
Duminda Wijesekera  
Min Wu  
Dingbang Xu  
Jun Xu  
Meng Yu  
Stefano Zanero  
Justin Zhan  
Lei Zhang  
Hongbin Zhou

# Table of Contents

Computerized Voting Machines: A View from the Trenches <i>Barbara Simons</i> .....	1
XML Access Control with Policy Matching Tree <i>Naizhen Qi, Michiharu Kudo</i> .....	3
Semantic Access Control Model: A Formal Specification <i>Mariemma I. Yagüe, María-del-Mar Gallardo, Antonio Maña</i> .....	24
A Generic XACML Based Declarative Authorization Scheme for Java – Architecture and Implementation <i>Rajeev Gupta, Manish Bhide</i> .....	44
Specification and Validation of Authorisation Constraints Using UML and OCL <i>Karsten Sohr, Gail-Joon Ahn, Martin Gogolla, Lars Migge</i> .....	64
Unified Index for Mobile Object Data and Authorizations <i>Vijayalakshmi Atluri, Qi Guo</i> .....	80
On Obligations <i>Manuel Hilty, David Basin, Alexander Pretschner</i> .....	98
A Practical Voter-Verifiable Election Scheme <i>David Chaum, Peter Y.A. Ryan, Steve Schneider</i> .....	118
Machine-Checked Security Proofs of Cryptographic Signature Schemes <i>Sabrina Tarento</i> .....	140
Sanitizable Signatures <i>Giuseppe Ateniese, Daniel H. Chou, Breno de Medeiros, Gene Tsudik</i> .....	159
Limits of the Cryptographic Realization of Dolev-Yao-Style XOR <i>Michael Backes, Birgit Pfitzmann</i> .....	178
Security-Typed Languages for Implementation of Cryptographic Protocols: A Case Study <i>Aslan Askarov, Andrei Sabelfeld</i> .....	197



Augmented Oblivious Polynomial Evaluation Protocol and Its Applications <i>Huafei Zhu, Feng Bao</i> .....	222
Using Attack Trees to Identify Malicious Attacks from Authorized Insiders <i>Indrajit Ray, Nayot Poolsapassit</i> .....	231
An Efficient and Unified Approach to Correlating, Hypothesizing, and Predicting Intrusion Alerts <i>Lingyu Wang, Anyi Liu, Sushil Jajodia</i> .....	247
Towards a Theory of Intrusion Detection <i>Giovanni Di Crescenzo, Abhrajit Ghosh, Rajesh Talpade</i> .....	267
On Scalability and Modularisation in the Modelling of Network Security Systems <i>João Porto de Albuquerque, Heiko Krumm, Paulo Lício de Geus</i> .....	287
Sybil-Resistant DHT Routing <i>George Danezis, Chris Lesniewski-Laas, M. Frans Kaashoek, Ross Anderson</i> .....	305
Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks <i>Felix C. Freiling, Thorsten Holz, Georg Wicherski</i> .....	319
Quantifying Probabilistic Information Flow in Computational Reactive Systems <i>Michael Backes</i> .....	336
Enforcing Non-safety Security Policies with Program Monitors <i>Jay Ligatti, Lujo Bauer, David Walker</i> .....	355
Soundness of Formal Encryption in the Presence of Key-Cycles <i>Pedro Adão, Gergei Bana, Jonathan Herzog, Andre Scedrov</i> .....	374
Privacy Preserving Clustering <i>Somesh Jha, Luis Kruger, Patrick McDaniel</i> .....	397
Abstractions Preserving Parameter Confidentiality <i>Sigrid Gürgens, Peter Ochsenschläger, Carsten Rudolph</i> .....	418
Minimal Disclosure in Hierarchical Hippocratic Databases with Delegation <i>Fabio Massacci, John Mylopoulos, Nicola Zannone</i> .....	438

Security Notions for Disk Encryption <i>Kristian Gjølsteen</i> .....	455
Local View Attack on Anonymous Communication <i>Marcin Gogolewski, Marek Klonowski, Mirosław Kutylowski</i> .....	475
Browser Model for Security Analysis of Browser-Based Protocols <i>Thomas Groß, Birgit Pfitzmann, Ahmad-Reza Sadeghi</i> .....	489
<b>Author Index</b> .....	509