Lecture Notes in Computer Science 5283

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Sushil Jajodia Javier Lopez (Eds.)

Computer Security – ESORICS 2008

13th European Symposium on Research in Computer Security
Málaga, Spain, October 6-8, 2008
Proceedings

Springer

Volume Editors

Sushil Jajodia
Center for Secure Information Systems
George Mason University
Fairfax, VA, USA
E-mail: jajodia@gmu.edu

Javier Lopez
Computer Science Department
University of Málaga
Málaga, Spain
E-mail: jlm@lcc.uma.es

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2.0, H.2.0, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-88312-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-88312-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12538461 06/3180 5 4 3 2 1 0

Preface

These proceedings contain the papers selected for presentation at the 13th European Symposium on Research in Computer Security—ESORICS 2008—held October 6–8, 2008 in Torremolinos (Malaga), Spain, and hosted by the University of Malaga, Computer Science Department.

ESORICS has become *the* European research event in computer security. The symposium started in 1990 and has been organized on alternate years in different European countries. From 2002 it has taken place yearly. It attracts an international audience from both the academic and industrial communities.

In response to the call for papers, 168 papers were submitted to the symposium. 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. Finally, 37 papers were selected for presentation at the symposium, giving an acceptance rate of 22%.

There is a long list of people who volunteered their time and energy to put together the symposium and who deserve acknowledgment. Our thanks to the General Chair, Jose M. Troya, for his valuable support in the organization of the event. Also, to Pablo Najera for preparation and maintenance of the symposium website, and Cristina Alcaraz and Rodrigo Roman for the local organization support. Special thanks to the members of the Program Committee and external reviewers for all their hard work during the review and the selection process. Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees.

We hope that you will find the program stimulating and a source of inspiration for future research.

October 2008

Sushil Jajodia
Javier Lopez

ESORICS 2008
13th European Symposium on Research in Computer Security

Malaga, Spain
October 6–8, 2008

Organized by
Computer Science Department
University of Malaga
Spain

Program Co-chairs

Sushil Jajodia	George Mason University, USA
Javier Lopez	University of Malaga, Spain

General Chair

Jose M. Troya	University of Malaga, Spain

Program Committee

Vijay Atluri	Rutgers University, USA
Michael Backes	Saarland University, Germany
David Basin	ETH Zurich, Switzerland
Gilles Barthe	INRIA, France
Marina Blanton	University of Notre Dame, USA
Jan Camenisch	IBM Research, Switzerland
David Chadwick	University of Kent, UK
Bruno Crispo	University of Trento, Italy
Frederic Cuppens	ENST Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Josep L. Ferrer	University of the Batearic Islands, Spain
David Galindo	University of Malaga, Spain
Juan A. Garay	Bell Labs, USA
Dieter Gollmann	HUT, Germany
Antonio Gomez-Skarmeta	University of Murcia, Spain
Juanma Gonzalez-Nieto	QUT, Australia
Dimitris Gritzalis	UAEB, Greece
Stefanos Gritzalis	University of the Aegean, Greece

Jordi Herrera	UAB, Spain
Aggelos Kiayias	University of Connecticut, USA
Socrates Katsikas	University of Piraeus, Greece
Christopher Kruegel	TU Vienna, Austria
Michiharu Kudo	IBM Tokyo Research, Japan
Kwok-Yan Lam	Tsinghua University, China
Wenke Lee	Georgia Institute of Technology, USA
Yingjiu Li	SMU, Singapore
Peng Liu	Penn State University, USA
Fabio Martinelli	CNR, Italy
Fabio Massacci	University of Trento, Italy
Vashek Matyas	University Brno, Czech Republic
Chris Mitchell	Royal Holloway, UK
Refik Molva	Eurecom, France
Yi Mu	University of Wollongong, Australia
Peng Ning	North Carolina State University, USA
Eiji Okamoto	University of Tsukuba, Japan
Martin Olivier	University of Pretoria, South Africa
Stefano Paraboschi	University of Bergamo, Italy
Jong-Hyuk Park	Kyungnam University, Korea
Guenther Pernul	University of Regensburg, Germany
Bart Preneel	KUL, Belgium
Jean-Jacques Quisquater	UCL, Belgium
Indrakshi Ray	Colorado State University, USA
Peter Ryan	Newcastle University, UK
Pierangela Samarati	Università degli Studi di Milano, Italy
Sean Smith	Dartmouth College, USA
Miguel Soriano	UPC, Spain
Vipin Swarup	MITRE Corporation, USA
Angelos Stavrou	George Mason University, USA
Giovanni Vigna	UCSB, USA
Michael Waidner	IBM Zurich Research, Switzerland
Lingyu Wang	Concordia University, Canada
Avishai Wool	Tel Aviv University, Israel
Jianying Zhou	I2R, Singapore
Sencun Zhu	Pennsylvania State University, USA

External Reviewers

Efthimia Aivaloglou, Claudio A. Ardagna, Aslan Askarov, Yudistira Asnar, Man Ho Au, Gildas Avoine, Kun Bai, Theodoros Balopoulos, Erik-Oliver Blass, Yacine Bouzida, Colin Boyd, Roberto Cascella, Lorenzo Cavallaro, Siu-Leung Chung, Robert Cole, Ricardo Corin, Cas Cremers, Nora Cuppens, Mohammad Torabi Dashti, Paul Drielsma, Stelios Dritsas, Stefan Dürbeck, Inger Fabris-Rotelli, Vika Felmetsger, Marcel Fernandez, Sara Foresti, Christoph Fritsch, Ludwig Fuchs, Felix J. Garcia Clemente, Flavio Garcia, Meng Ge, Thomas Genet, Benedikt Gierlichs, Manuel Gil

Pérez, Bob Gilbert, Oliver Gmelch, Felix Gómez Marmol, Qijun Gu, Satoshi Hada, Diala Abi Haidar, Helena Handschuh, Juan Hernandez-Serrano, Susan Hohenberger, Guo Hua, Xinyi Huang, Yoon-Chan Jhi, Seny Kamara, Wael Kanoun, Guenter Karjoth, Irene Karybali, Maria Karyda, Eike Kiltz, Jongsung Kim, Yeong-Deok Kim, Jan Kolter, Elisavet Konstantinou, Maciej Koutny, Jan Krhovjak, Marek Kumpost, Pascal Lafourcade, Costas Lambrinoudakis, Aliaksandr Lazouoski, Yuseop Lee, Fengjun Li, Lunquan Li, Bing Liang, Benoît Libert, Wenming Liu, Gabriel López Millán, Haibing Lu, Olivier de Marneffe, Josep Maria Mateo, Daniel Martínez Manzano, Jon Millen, Takuya Mishina, José L. Muñoz-Tapia, Katsiarina Naliuka, Gregory Neven, Melek Onen, Marinella Petrocchi, Alexander Pretschner, Tamara Rezk, Helena Rifà-Pous, William Robertson, Manuel Sanchez Cuenca, Amitabh Saxena, Patrick Schaller, Rolf Schillinger, Emre Sezer, Jinyang Shi, Abdullatif Shikfa, Alessandro Sorniotti, Yannis Soupionis, Georgios Spathoulas, François-Xavier Standaert, Andriy Stetsko, Thorsten Strufe, Willy Susilo, Marianthi Theoharidou, Julien Alexandre Thomas, Joan Tomàs-Buliart, Angeliki Tsochou, Bill Tsoumas, Christina Tziviskou, Martijn Warnier, Yuji Watanabe, Wei Wu, Xi Xiong, Zhi Xu, Carmen Yago Sánchez, Yanjiang Yang, Yi Yang, Artsiom Yautsiukhin, Sang-Soo Yeo, Tsz Hon Yuen.

Table of Contents

Session 4: Data and Applications Security

Session 5: Privacy Enhancing Technologies

Session 6: Anonymity and RFID Privacy

Session 7: Access Control and Trust Negotiation

Session 8: Information Flow and Non-transferability

Session 9: Secure Electronic Voting and Web Applications Security

Session 10: VoIP Security, Malware, and DRM

Session 11: Formal Models and Cryptographic Protocols

Session 12: Language-Based and Hardware Security