

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

Alfred Kobsa

University of California, Irvine, CA, 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

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

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
Javier Lopez

George Mason University, USA
University of Malaga, Spain

General Chair

Jose M. Troya

University of Malaga, Spain

Program Committee

Vijay Atluri
Michael Backes
David Basin
Gilles Barthe
Marina Blanton
Jan Camenisch
David Chadwick
Bruno Crispo
Frederic Cuppens
Sabrina De Capitani di Vimercati
Josep L. Ferrer
David Galindo
Juan A. Garay
Dieter Gollmann
Antonio Gomez-Skarmeta
Juanma Gonzalez-Nieto
Dimitris Gritzalis
Stefanos Gritzalis

Rutgers University, USA
Saarland University, Germany
ETH Zurich, Switzerland
INRIA, France
University of Notre Dame, USA
IBM Research, Switzerland
University of Kent, UK
University of Trento, Italy
ENST Bretagne, France
Università degli Studi di Milano, Italy
University of the Balearic Islands, Spain
University of Malaga, Spain
Bell Labs, USA
HUT, Germany
University of Murcia, Spain
QUT, Australia
UAEB, Greece
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 Felmetzger, 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 Sornioti, 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 1: Intrusion Detection and Network Vulnerability Analysis

Multiprimary Support for the Availability of Cluster-Based Stateful Firewalls Using FT-FW	1
<i>P. Neira, R.M. Gasca, and L. Lefèvre</i>	
Identifying Critical Attack Assets in Dependency Attack Graphs	18
<i>Reginald E. Sawilla and Xinming Ou</i>	
Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory	35
<i>C.P. Mu, X.J. Li, H.K. Huang, and S.F. Tian</i>	

Session 2: Network Security

Strongly-Resilient and Non-interactive Hierarchical Key-Agreement in MANETs	49
<i>Rosario Gennaro, Shai Halevi, Hugo Krawczyk, Tal Rabin, Steffen Reidt, and Stephen D. Wolthusen</i>	
Efficient Handling of Adversary Attacks in Aggregation Applications . . .	66
<i>Gelareh Taban and Virgil D. Gligor</i>	
Symmetric Key Approaches to Securing BGP – A Little Bit Trust Is Enough	82
<i>Bezawada Bruhadeshwar, Sandeep S. Kulkarni, and Alex X. Liu</i>	

Session 3: Smart Cards and Identity Management

Dismantling MIFARE Classic	97
<i>Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijters, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs</i>	
A Browser-Based Kerberos Authentication Scheme	115
<i>Sebastian Gajek, Tibor Jager, Mark Manulis, and Jörg Schwenk</i>	
CROO: A Universal Infrastructure and Protocol to Detect Identity Fraud	130
<i>D. Nali and P.C. van Oorschot</i>	

Session 4: Data and Applications Security

Disclosure Analysis and Control in Statistical Databases	146
<i>Yingjiu Li and Haibing Lu</i>	
TRACE: Zero-Down-Time Database Damage Tracking, Quarantine, and Cleansing with Negligible Run-Time Overhead	161
<i>Kun Bai, Meng Yu, and Peng Liu</i>	
Access Control Friendly Query Verification for Outsourced Data Publishing	177
<i>Hong Chen, Xiaonan Ma, Windsor Hsu, Ninghui Li, and Qihua Wang</i>	

Session 5: Privacy Enhancing Technologies

Sharemind: A Framework for Fast Privacy-Preserving Computations . . .	192
<i>Dan Bogdanov, Sven Laur, and Jan Willemsen</i>	
Modeling Privacy Insurance Contracts and Their Utilization in Risk Management for ICT Firms	207
<i>Athanassios N. Yannacopoulos, Costas Lambrinoudakis, Stefanos Gritzalis, Stylianos Z. Xanthopoulos, and Sokratis N. Katsikas</i>	
Remote Integrity Check with Dishonest Storage Server	223
<i>Ee-Chien Chang and Jia Xu</i>	

Session 6: Anonymity and RFID Privacy

A Low-Variance Random-Walk Procedure to Provide Anonymity in Overlay Networks	238
<i>J.P. Muñoz-Gea, J. Malgosa-Sanahuja, P. Manzanares-Lopez, J.C. Sanchez-Aarnoutse, and J. Garcia-Haro</i>	
RFID Privacy Models Revisited	251
<i>Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini</i>	
A New Formal Proof Model for RFID Location Privacy	267
<i>JungHoon Ha, SangJae Moon, Jianying Zhou, and JaeCheol Ha</i>	

Session 7: Access Control and Trust Negotiation

Distributed Authorization by Multiparty Trust Negotiation	282
<i>Charles C. Zhang and Marianne Winslett</i>	

Compositional Refinement of Policies in UML – Exemplified for Access Control	300
<i>Bjørnar Solhaug and Ketil Stølen</i>	

On the Security of Delegation in Access Control Systems	317
<i>Qihua Wang, Ninghui Li, and Hong Chen</i>	

Session 8: Information Flow and Non-transferability

Termination-Insensitive Noninterference Leaks More Than Just a Bit ...	333
<i>Aslan Askarov, Sebastian Hunt, Andrei Sabelfeld, and David Sands</i>	

Security Provisioning in Pervasive Environments Using Multi-objective Optimization	349
<i>Rinku Dewri, Indrakshi Ray, Indrajit Ray, and Darrell Whitley</i>	

Improved Security Notions and Protocols for Non-transferable Identification	364
<i>Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, and Ivan Visconti</i>	

Session 9: Secure Electronic Voting and Web Applications Security

Human Readable Paper Verification of Prêt à Voter	379
<i>David Lundin and Peter Y.A. Ryan</i>	

A Distributed Implementation of the Certified Information Access Service	396
<i>Carlo Blundo, Emiliano De Cristofaro, Aniello Del Sorbo, Clemente Galdi, and Giuseppe Persiano</i>	

Exploring User Reactions to New Browser Cues for Extended Validation Certificates	411
<i>Jennifer Sobey, Robert Biddle, P.C. van Oorschot, and Andrew S. Patrick</i>	

A Framework for the Analysis of Mix-Based Steganographic File Systems	428
<i>Claudia Diaz, Carmela Troncoso, and Bart Preneel</i>	

Session 10: VoIP Security, Malware, and DRM

An Adaptive Policy-Based Approach to SPIT Management	446
<i>Yannis Soupionis, Stelios Dritsas, and Dimitris Gritzalis</i>	

Structured Peer-to-Peer Overlay Networks: Ideal Botnets Command and Control Infrastructures?	461
<i>Carlton R. Davis, Stephen Neville, José M. Fernandez, Jean-Marc Robert, and John McHugh</i>	
Eureka: A Framework for Enabling Static Malware Analysis	481
<i>Monirul Sharif, Vinod Yegneswaran, Hassen Saidi, Phillip Porras, and Wenke Lee</i>	
New Considerations about the Correct Design of Turbo Fingerprinting Codes	501
<i>Joan Tomàs-Buliart, Marcel Fernández, and Miguel Soriano</i>	
Session 11: Formal Models and Cryptographic Protocols	
Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks	517
<i>Michael Backes and Boris Köpf</i>	
Cryptographic Protocol Explication and End-Point Projection	533
<i>Jay McCarthy and Shriram Krishnamurthi</i>	
State Space Reduction in the Maude-NRL Protocol Analyzer	548
<i>Santiago Escobar, Catherine Meadows, and José Meseguer</i>	
Session 12: Language-Based and Hardware Security	
Code-Carrying Authorization	563
<i>Sergio Maffei, Martín Abadi, Cédric Fournet, and Andrew D. Gordon</i>	
CPU Bugs, CPU Backdoors and Consequences on Security	580
<i>Loïc Duflot</i>	
Author Index	601