Lecture Notes in Computer Science 4189

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
University of California, Los Angeles, CA, 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

Dieter Gollmann Jan Meier
Andrei Sabelfeld (Eds.)

Computer Security – ESORICS 2006

11th European Symposium on
Research in Computer Security
Hamburg, Germany, September 18-20, 2006
Proceedings

Springer

Volume Editors

Dieter Gollmann
Jan Meier
TU Hamburg-Harburg
Harburger Schlossstr. 20, 21079 Hamburg-Harburg, Germany
E-mail: diego@tu-harburg.de, j.meier@tuhh.de

Andrei Sabelfeld
Chalmers University of Technology
Dept. of Computer Science and Engineering
EDIT Bldg., Rännvägen 6B, 41296 Gothenborg, Sweden
E-mail: andrei@cs.chalmers.se

Library of Congress Control Number: 2006932266

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-44601-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-44601-9 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 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11863908 06/3142 5 4 3 2 1 0

Foreword

These proceedings contain the papers selected for presentation at the 11th European Symposium on Research in Computer Security – ESORICS, held in Hamburg, Germany, September 18-20, 2006.

The 160 papers submitted to ESORICS were each reviewed by at least three members of the program committee. A two-week discussion phase was then held electronically, where committee members could comment on all papers and all reviews. Finally, 32 papers were selected for presentation at ESORICS, giving an acceptance rate of about 21%.

In 2005, three specialized security workshops were organized in affiliation with ESORICS. This trend has continued. In addition to RAID, which is already a well established event in its own right, there were four more workshops this year, ESAS 2006, EuDiRights 06, STM 06, and FEE2, further strengthening the rôle of ESORICS as the major European conference on security research.

There were many volunteers who offered their time and energy to put together the symposium and who deserve our acknowledgment. We want to thank all the members of the program committee and the external reviewers for their hard work in evaluating and discussing the submissions. We are also very grateful to all those people whose work ensured a smooth organization: Joachim Posegga, who served as General Chair; Andreas Günter and his team at HITeC for taking on the conference management; Klaus-Peter Kossakowski for his efforts as Sponsorship Chair; Jan Meier for managing the ESORICS Web site, and Joachim Stehmann for the Web design; and Martin Johns for dealing with the growing number of affiliated workshops.

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

July 2006 Dieter Gollmann and Andrei Sabelfeld

Organization

General Chair

Joachim Posegga	University of Hamburg, Germany

Program Committee

Tuomas Aura	Microsoft Research, UK
Michael Backes	Saarland University, Germany
Gilles Barthe	INRIA Sophia-Antipolis, France
Lynn Batten	Deakin University, Australia
Giampaolo Bella	University of Catania, Italy
Joachim Biskup	University of Dortmund, Germany
Jan Camenisch	IBM Zurich Research Laboratory, Switzerland
Jason Crampton	Royal Holloway, UK
Frederic Cuppens	ENST Bretagne, France
Marc Dacier	Institut Eurécom, France
George Danezis	University of Leuven, Belgium
Sabrina De Capitani di Vimercati	University of Milan, Italy
Robert Deng	Singapore Management University, Singapore
Ulfar Erlingsson	Microsoft Research, USA
Simon Foley	University College Cork, Ireland
Philippe Golle	Palo Alto Research Center, USA
Dieter Gollmann (co-chair)	Hamburg University of Technology, Germany
Pieter Hartel	Twente University, Netherlands
Jaap-Henk Hoepman	Radboud University Nijmegen, Netherlands
Sushil Jajodia	George Mason University, USA
Alan Jeffrey	Bell Labs, USA
Audun Jøsang	QUT, Australia
Jan Jürjens	TU Munich, Germany
Markus Kuhn	University of Cambridge, UK
Xuejia Lai	Shanghai Jiaotong University, PR China
Kwok-Yan Lam	Tsinghua University, PR China
Volkmar Lotz	SAP, France
Heiko Mantel	RWTH Aachen, Germany
Vashek Matyas	Masaryk University Brno, Czech Republic
Flemming Nielson	DTU, Denmark

Peter Ryan	University of Newcastle upon Tyne, UK
Andrei Sabelfeld (co-chair)	Chalmers University, Sweden
Babak Sadighi	SICS, Sweden
Kazue Sako	NEC Corporation, Japan
Andre Scedrov	U. Pennsylvania, USA
Einar Snekkenes	Gjøvik University College, Norway
Eijiro Sumii	Tohoku University, Japan
Paul Syverson	Naval Research Laboratory, USA
Mariemma I. Yagüe	University of Malaga, Spain
Alf Zugenmaier	DoCoMo Labs Europe, Germany

Additional Reviewers

Imad Aad, Pedro Adão, Ana Almeida Matos, Toshinori Araki, Olav Bandmann, Vicente Benjumea, Gustavo Betarte, Stefano Bistarelli, Bruno Blanchet, Damiano Bolzoni, Ahmed Bouabdallah, Jeremy Bryans, Marzia Buscemi, Jan Cederquist, Shiping Chen, Lukasz Chmielewski, Daniel J.T. Chong, Morshed Chowdhury, Siu-Leung Chung, Jolyon Clulow, Céline Coma, Luca Compagna, Ricardo Corin, Veronique Cortier, Nora Cuppens-Boulahia, Marcin Czenko, Mads Dam, Marnix Dekker, Markus Dürmuth, Ulrich Flegel, Jun Furukawa, David Galindo, Han Gao, Flavio D. Garcia, Joaquin Garcia, Meng Ge, Pablo Giambiagi, Hidehito Gomi, Maria Isabel González Vasco, Thomas Gross, Toshiyuki Isshiki, Ana Jancic, Thomas Jensen, Florian Kerschbaum, Naoki Kobayashi, Steve Kremer, Jan Krhovjak, Marek Kumpost, Sven Lachmund, Julien Laganier, Yassine Lakhnech, Peeter Laud, Corrado Leita, Anyi Liu, Vaclav Lorenc, Henning Makholm, Matteo Maffei, Michael Meier, Dale Miller, Kengo Mori, Antonio Muñoz Gallego, Steven Murdoch, Thanh Son Nguyen, Christoffer Rosenkilde Nielsen, Satoshi Obana, Yutaka Oiwa, Joseph Pamula, Maura Paterson, Jean-Christophe Pazzaglia, Thea Peacock, Van Hau Pham, François Pottier, Christian W. Probst, Tony Ramard, Sankardas Roy, Pierangela Samarati, Thierry Sans, Andreas Schaad, Ludwig Seitz, Fred Spiessens, Henning Sudbrock, Hongwei Sun, Petr Svenda, Isamu Teranishi, Tachio Terauchi, Olivier Thonnard, Terkel K. Tolstrup, Laurent Vigneron, Jan Vitek, Lingyu Wang, Stephen D. Wolthusen, Konrad Wrona, Hirosuke Yamamoto, Yanjiang Yang, Chao Yao, Stefano Zanero, Ye Zhang, Xibin Zhao, Hongbin Zhou, Anna Zych

Local Organization

Wiebke Frauen, Andreas Günter, Martin Johns (workshop chair), Klaus-Peter Kossakowski (sponsorship chair), Jan Meier, Joachim Stehmann (Web design), Margit Wichmann

Table of Contents

Finding Peer-to-Peer File-Sharing Using Coarse Network Behaviors 1
M.P. Collins, M.K. Reiter

Timing Analysis in Low-Latency Mix Networks:
Attacks and Defenses 18
V. Shmatikov, M.-H. Wang

TrustedPals: Secure Multiparty Computation Implemented
with Smart Cards 34
M. Fort, F. Freiling, L. Draque Penso, Z. Benenson, D. Kesdogan

Private Information Retrieval Using Trusted Hardware 49
S.H. Wang, X.H. Ding, R.H. Deng, F. Bao

Bridging the Gap Between Inter-communication Boundary and Internal
Trusted Components 65
Y. Watanabe, S. Yoshihama, T. Mishina, M. Kudo, H. Maruyama

License Transfer in OMA-DRM 81
C.N. Chong, S. Iacob, P. Koster, J. Montaner, R. van Buuren

Enhanced Security Architecture for Music Distribution on Mobile 97
A. Benjelloun-Touimi, J.-B. Fischer, C. Fontaine, C. Giraud,
M. Milhau

A Formal Model of Access Control for Mobile Interactive Devices 110
F. Besson, G. Dufay, T. Jensen

Discretionary Capability Confinement 127
P.W.L. Fong

Minimal Threshold Closure 145
X.-B. Zhao, K.-Y. Lam, G. Luo, S.-L. Chung, M. Gu

Reducing the Dependence of SPKI/SDSI on PKI 156
H. Wang, S. Jha, T. Reps, S. Schwoon, S. Stubblebine

Delegation in Role-Based Access Control 174
J. Crampton, H. Khambhammettu

Applying a Security Requirements Engineering Process 192
D. Mellado, E. Fernández-Medina, M. Piattini

Modeling and Evaluating the Survivability of an Intrusion Tolerant Database System 207
H. Wang, P. Liu

A Formal Framework for Confidentiality-Preserving Refinement 225
T. Santen

Timing-Sensitive Information Flow Analysis for Synchronous Systems 243
B. Köpf, D. Basin

HBAC: A Model for History-Based Access Control and Its Model Checking 263
J. Wang, Y. Takata, H. Seki

From Coupling Relations to Mated Invariants for Checking Information Flow 279
D.A. Naumann

A Linear Logic of Authorization and Knowledge 297
D. Garg, L. Bauer, K.D. Bowers, F. Pfenning, M.K. Reiter

Prêt à Voter with Re-encryption Mixes 313
P.Y.A. Ryan, S.A. Schneider

Secure Key-Updating for Lazy Revocation 327
M. Backes, C. Cachin, A. Oprea

Key Derivation Algorithms for Monotone Access Structures in Cryptographic File Systems 347
M. Srivatsa, L. Liu

Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos 362
M. Backes, I. Cervesato, A.D. Jaggard, A. Scedrov, J.-K. Tsay

Deriving Secrecy in Key Establishment Protocols 384
D. Pavlovic, C. Meadows

Limits of the BRSIM/UC Soundness of Dolev-Yao Models with Hashes 404
M. Backes, B. Pfitzmann, M. Waidner

Conditional Reactive Simulatability 424
M. Backes, M. Dürmuth, D. Hofheinz, R. Küsters

SessionSafe: Implementing XSS Immune Session Handling 444
M. Johns

Policy-Driven Memory Protection for Reconfigurable Hardware 461
T. Huffmire, S. Prasad, T. Sherwood, R. Kastner

Privacy-Preserving Queries on Encrypted Data 479
Z. Yang, S. Zhong, R.N. Wright

Analysis of Policy Anomalies on Distributed Network Security Setups 496
J.G. Alfaro, F. Cuppens, N. Cuppens-Boulahia

Assessment of a Vulnerability in Iterative Servers Enabling Low-Rate DoS Attacks 512
G. Maciá-Fernández, J.E. Díaz-Verdejo, P. García-Teodoro

Towards an Information-Theoretic Framework for Analyzing Intrusion Detection Systems 527
G. Gu, P. Fogla, D. Dagon, W. Lee, B. Skoric

Author Index 547